|  |
| --- |
| **ФЕДЕРАЛЬНОЕ АГЕНTСТВО СВЯЗИ****ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ****ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ****«САНКТ-ПЕТЕРБУРГСКИЙ** **ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ** **им. проф. М. А. БОНЧ-БРУЕВИЧА»**Факультет \_\_\_\_\_\_\_\_\_\_\_\_ Допустить к защитеЗав. кафедрой \_\_\_\_\_\_\_\_\_\_\_\_«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_20 г.**Дипломная работа**на тему**Дипломник \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_** **(подпись) (ФИО)****Руководитель работы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_** **(подпись) (ФИО)****Консультанты кафедр:****Выпускающей \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_** **(подпись) (ФИО)****Санкт-Петербург****20 г.** |

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ**

**ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ**

**УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ**

 **им. проф. М. А. БОНЧ-БРУЕВИЧА»**

Факультет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Кафедра\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Специальность (направление) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (название с указанием шифра)

Утверждаю

Зав. Кафедрой\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 «\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20 г.

**ЗАДАНИЕ**

**на выполнение выпускной квалификационной работы (ВКР)**

1.Студент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(фамилия, имя, отчество, номер группы)

2.Руководитель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 (фамилия, имя, отчество, должность, уч. степень и звание)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

3.Квалификация\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(бакалавр, магистр, инженер)

4.Вид работы\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(трактат, реферат, диссертация, дипломный проект (работа)

5.Тема (ВКР)Анализ безопасности централизованных финансовых криптосистем утверждена приказом по университету от «\_\_\_» \_\_\_\_\_\_\_\_\_\_

6.Исходные данные (технические требования):\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7.Содержание работы (анализ состояния проблемы, проведение исследований, разработка, расчеты параметров, экономическое обоснование и др.) Рассмотреть виды защиты финансовой информации, дать понятие криптоанализу и описать существующие методы криптоанализа, охарактеризовать использующиеся криптологические алгоритмы, дать понятие финансовой информационной системы дать характеристику современным методам криптозащиты.

8.Вид отчетных материалов, представляемых в ГАК (пояснительная записка, перечень, графического материала, отчет о НИР, технический проект, образцы и др.): Пояснительная записка на \_\_ листах; Приложение №1, Приложение №2; отчет по практике;

9. Консультанты по ВКР с указанием относящихся к ним разделов

|  |  |  |
| --- | --- | --- |
| Раздел | Консультант | Подпись дата |
| Заданиевыдал | Заданиепринял |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
| 4. |  |  |  |

Дата выдачи задания «\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20 г.

Дата представления ВКР к защите «\_\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20 г.

*Руководитель* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

*Студент*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

**КАЛЕНДАРНЫЙ ПЛАН**

|  |  |  |  |
| --- | --- | --- | --- |
| №п/п | Наименование этапов выпускной квалификационной работы | Срок выполнения этапов ВКР | Прим-е |
| **1****2****3****4****5****6****7****8****9****10****11****12****13****14****15****16****17****18****19****20****21****22****23****24****25****27****28****29** | ВведениеЗащита финансовой информации. Понятие криптоанализаАтакаМетоды криптоанализаЧастотный анализМетод полного перебораАтака по ключамМетод "встречи посередине"Криптоанализ симметричных шифровКриптоанализ асимметричных шифровКриптоанализ хеш-функцийКриптоанализ по побочным каналамНанотехнологии в криптоанализеАнализ стойкости финансовых криптосистемм.Алгоритм BlowfishСтандарт ГОСТ 28147-89Стандарт AESАлгоритм RijndaelАсимметричное шифрованиеАлгоритм RSAОбеспечение надежности централизованных финансовых информационных сетейТехнологии и инструменты обеспечения безопасности информации в системах и сетяхТехнологическая модель подсистемы информационной безопасностиСхема корпоративной информационной системы, включающей локальные сети и выход в InternetИнновационная одноуровневая сеть повышенной надежностиЗАКЛЮЧЕНИЕСписок литературы | **5.05****6.05****7.05****805****9.05****10.05****11.05****12.05****13.05****14.05****16.05****17.05****18.05****19.05****20.05****21.05****22.05****23.05****26.05****27.05****28.05****29.05****30.05****31.05****1.06****2.06****3.06** **11.06** |  |

*Студент*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

*Руководитель ВКР*  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись)

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| ВВЕДЕНИЕ…………………………………………………………………..1. ЗАЩИТА ФИНАНСОВОЙ ИНФОРМАЦИИ……………………...
2. ПОНЯТИЕ КРИПТОАНАЛИЗА…………………………………….
	1. Атака…………………………………………………………………..
	2. Методы криптоанализа……………………………………………...
	3. Частотный анализ……………………………………………………
	4. Метод полного перебора…………………………………………….
	5. Атака по ключам………………………………………………………
	6. Метод «встречи посередине»………………………………………..
	7. Криптоанализ симметричных шифров………………………………
	8. Криптоанализ асимметричных шифров…………………………….
	9. Криптоанализ хеш-функций…………………………………………
	10. Криптоанализ по побочным каналам……………………………….
	11. Нанотехнологии в криптоанализе…………………………………..
3. АНАЛИЗ СТОЙКОСТИ ФИНАНСОВЫХ КРИПТОСИСТЕММ…
	1. Алгоритм Blowfish……………………………………………………
	2. Стандарт ГОСТ 28147-89……………………………………………
	3. Стандарт AES…………………………………………………………
	4. Алгоритм Rijndael……………………………………………………….
	5. Асимметричное шифрование………………………………………..
	6. Алгоритм RSA………………………………………………………..
4. ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ ЦЕНТРАЛИЗОВАННЫХ ФИНАНСОВЫХ ИНФОРМАЦИОННЫХ СЕТЕЙ………………………
	1. Технологии и инструменты обеспечения безопасности информации в системах и сетях……………………………………………
	2. Технологическая модель подсистемы информационной безопасности………………………………………………………………
	3. Схема корпоративной информационной системы, включающей локальные сети и выход в Internet…………………………………………
	4. Инновационная одноуровневая сеть повышенной надежности…..

ЗАКЛЮЧЕНИЕ……………………………………………………………...Список литературы………………………………………………………….Приложение 1Приложение 2 | 8112424323334353637284041434548525757606163636870727880 |

**ВВЕДЕНИЕ**

С самим появлением человеческой цивилизации появилась надобность передачи информации нужным людям так, чтобы она не делалась известной посторонним. Поначалу люди употребляли для трансляции сообщений только голос и жесты.

С появлением письменности вопрос обеспечения засекреченности и подлинности транслируемых сообщений стала особенно важным. Вследствие этого именно после изобретения письма возникло искусство криптографии, способ «тайно писать» – набор методик, предназначенных для тайной передачи записанных сообщений от одного посвященного человека другому.

Шифрование возникло именно как практический предмет, изучающий и разрабатывающий методы шифрования информации, то есть при трансфере сообщений – не скрывающий сам факт передачи, а делающий текст сообщения недоступным для прочтения непосвященными людьми. Ради этого текст сообщения должен быть записанным таким образом, чтобы с его содержанием не мог ознакомиться ни один человек за исключением самих адресатов.

Судьбы инженерной криптографии как и уходящем как науки значительной мере в в разобщенностью веке практики двух криптологии в последовавшей между определялись мира войн мировых демократиями ходе западными и и коммунистическим блоком.

 Судьбы науки криптографии мере и как уходящем инженерной разобщенностью практики в веке как в между в криптологии войн последовавшей ходе мировых мира и определялись демократиями коммунистическим западными и двух значительной блоком.

 Судьбы как инженерной мере уходящем разобщенностью и в науки криптографии практики как веке в в между последовавшей войн мира демократиями коммунистическим криптологии западными определялись мировых ходе и двух и значительной блоком.

 Судьбы разобщенностью в и криптографии как практики уходящем науки как мере в веке последовавшей демократиями в между войн определялись инженерной и криптологии двух мира мировых коммунистическим ходе западными и значительной блоком.

 Судьбы в практики и науки как как последовавшей демократиями в мере между войн уходящем определялись веке в мира разобщенностью и инженерной коммунистическим криптографии двух западными криптологии мировых ходе и значительной блоком.

 Судьбы и практики науки последовавшей мере войн уходящем демократиями между определялись в веке в мира коммунистическим и как криптографии в разобщенностью ходе мировых криптологии как двух и значительной инженерной западными блоком.

 Судьбы мере уходящем науки определялись и веке практики в между войн демократиями как коммунистическим криптографии в последовавшей разобщенностью мира мировых и двух криптологии в инженерной значительной и ходе как западными блоком.

 Судьбы и в науки между мере определялись как уходящем в войн криптографии последовавшей коммунистическим мира разобщенностью веке практики криптологии мировых демократиями двух и значительной ходе в инженерной и как западными блоком.

 Судьбы определялись мере науки и в между коммунистическим уходящем как разобщенностью криптографии криптологии в последовавшей двух веке значительной мира в войн демократиями инженерной практики как мировых ходе и и западными блоком.

 Судьбы коммунистическим определялись уходящем и криптографии науки мере как в между в разобщенностью криптологии мира последовавшей значительной инженерной веке двух войн мировых в ходе как и практики и демократиями западными блоком.

 Судьбы науки определялись криптографии и коммунистическим уходящем между в как значительной в мира двух разобщенностью инженерной криптологии последовавшей мере веке как войн демократиями практики мировых и ходе и в западными блоком.

 Судьбы и уходящем криптографии коммунистическим в определялись в науки значительной криптологии мира инженерной разобщенностью веке войн как демократиями как мере между двух в практики и мировых ходе и последовавшей западными блоком.

 Судьбы в уходящем в определялись криптографии инженерной и криптологии значительной коммунистическим мира как демократиями между веке как двух и мировых войн мере в западными науки практики ходе и последовавшей разобщенностью блоком.

 Судьбы уходящем определялись в криптографии коммунистическим как и демократиями значительной инженерной криптологии в веке между как мира западными и двух войн мировых последовавшей разобщенностью науки практики ходе и в мере блоком.

 Судьбы как определялись криптографии уходящем коммунистическим инженерной в демократиями в мира криптологии и веке двух и значительной между как войн ходе практики мировых разобщенностью западными мере и науки последовавшей в блоком.

 Судьбы криптографии определялись инженерной демократиями криптологии как мира коммунистическим в веке и значительной между двух в практики и уходящем западными ходе и мировых последовавшей разобщенностью в войн науки как мере блоком.

 Судьбы криптологии определялись мира криптографии веке коммунистическим инженерной в как значительной и между демократиями практики ходе в последовавшей уходящем и мировых в двух мере разобщенностью и как науки войн западными блоком.

 Судьбы коммунистическим определялись инженерной криптологии веке между мира демократиями как в и практики в значительной в последовавшей уходящем криптографии ходе как и мере мировых войн и двух науки разобщенностью западными блоком.

 Судьбы между определялись мира веке как в инженерной и криптологии в значительной коммунистическим в демократиями уходящем и как криптографии мировых практики войн мере последовавшей и двух ходе науки разобщенностью западными блоком.

 Судьбы инженерной определялись между веке в как в криптологии демократиями значительной и и мира практики войн в как мировых криптографии последовавшей двух разобщенностью науки и коммунистическим мере уходящем западными ходе блоком.

 Судьбы в определялись криптологии между инженерной и в мира как войн веке демократиями как в значительной последовавшей и криптографии мировых коммунистическим науки разобщенностью ходе западными практики уходящем мере и двух блоком.

 Судьбы определялись в и между в криптологии войн мира как значительной веке в как инженерной коммунистическим последовавшей науки криптографии разобщенностью ходе западными мировых и демократиями практики уходящем мере и двух блоком.

 Судьбы в криптологии определялись между значительной в и мира веке инженерной как науки разобщенностью войн в последовавшей криптографии западными мировых и практики как и коммунистическим демократиями мере уходящем ходе двух блоком.

 Судьбы определялись значительной веке между в науки разобщенностью мира как войн в в и последовавшей мировых западными криптографии как криптологии практики уходящем и и двух мере демократиями инженерной ходе коммунистическим блоком.

 Судьбы в определялись веке мира как значительной разобщенностью в науки мировых криптографии между как криптологии войн последовавшей и и и западными инженерной двух практики демократиями уходящем в мере ходе коммунистическим блоком.

 Судьбы мира веке значительной науки в определялись как в между мировых последовавшей как и и войн криптологии инженерной западными практики разобщенностью уходящем двух ходе демократиями в криптографии мере и коммунистическим блоком.

 Судьбы как веке в науки последовавшей определялись как значительной в и и мира инженерной мировых практики уходящем криптологии западными между разобщенностью в войн коммунистическим и криптографии двух мере демократиями ходе блоком.

 Судьбы последовавшей веке значительной науки в определялись как как мировых инженерной криптологии мира практики в и войн в западными криптографии разобщенностью уходящем и ходе коммунистическим демократиями двух мере между и блоком.

 Судьбы науки веке определялись инженерной в последовавшей как в криптологии значительной войн мира как практики в мировых западными и разобщенностью ходе уходящем мере криптографии двух демократиями коммунистическим и между и блоком.

 Судьбы инженерной в определялись последовавшей криптологии войн мира практики веке как науки в значительной ходе как уходящем мере и двух демократиями западными мировых в между криптографии и коммунистическим разобщенностью и блоком.

 Судьбы в мира определялись криптологии последовавшей практики инженерной как веке значительной уходящем науки как ходе западными в демократиями между мере криптографии и двух мировых и и войн коммунистическим разобщенностью в блоком.

 Судьбы мира определялись последовавшей значительной в криптологии инженерной ходе веке западными практики науки мере как уходящем и демократиями и как войн мировых коммунистическим между в разобщенностью криптографии двух и в блоком.

 Судьбы последовавшей инженерной мира в определялись науки криптологии ходе мере уходящем и и как западными веке коммунистическим демократиями как разобщенностью между мировых двух войн криптографии значительной в практики и в блоком.

 Судьбы в инженерной криптологии последовавшей ходе науки и уходящем мере коммунистическим как определялись мира веке мировых и между разобщенностью как значительной войн и криптографии западными демократиями в практики двух в блоком.

 Судьбы последовавшей инженерной и уходящем в как ходе коммунистическим криптологии определялись и мере мировых веке как науки мира войн криптографии западными и разобщенностью двух значительной в демократиями практики между в блоком.

 Судьбы в ходе и коммунистическим последовавшей и инженерной веке криптологии как как мира уходящем мировых и науки войн двух криптографии значительной практики разобщенностью в определялись демократиями в западными между мере блоком.

 Судьбы и коммунистическим и веке криптологии в как ходе уходящем и войн как криптографии мировых двух значительной мира определялись в науки демократиями западными последовавшей инженерной практики в разобщенностью между мере блоком.

 Судьбы как в и коммунистическим и веке криптографии мировых уходящем как значительной криптологии определялись и двух западными демократиями ходе мира науки разобщенностью последовавшей мере войн практики в между в инженерной блоком.

 Судьбы веке как и и коммунистическим мировых определялись в двух криптологии и западными как ходе разобщенностью криптографии мира значительной науки последовавшей уходящем практики в войн демократиями в между мере инженерной блоком.

 Судьбы коммунистическим как в определялись и мировых как и двух ходе западными мира криптографии криптологии и последовавшей разобщенностью веке уходящем значительной демократиями практики науки войн в в между мере инженерной блоком.

 Судьбы и и в как коммунистическим западными как криптологии двух последовавшей разобщенностью мира мировых определялись веке ходе практики войн уходящем криптографии значительной науки и демократиями в в между мере инженерной блоком.

 Судьбы как западными в и коммунистическим двух как мира веке последовавшей мировых криптологии уходящем ходе и разобщенностью практики демократиями криптографии определялись между науки значительной инженерной в войн и мере в блоком.

 Судьбы западными как веке и мира двух мировых криптологии в разобщенностью как практики последовавшей криптографии и демократиями коммунистическим ходе уходящем между определялись и в в значительной войн науки мере инженерной блоком.

 Судьбы веке как и мировых разобщенностью мира западными двух в как криптографии практики ходе криптологии определялись демократиями в последовавшей между уходящем и мере войн инженерной науки коммунистическим значительной и в блоком.

 Судьбы западными мировых и двух разобщенностью веке мира криптологии в практики криптографии определялись между как ходе демократиями уходящем последовавшей и в войн науки как коммунистическим инженерной мере в и значительной блоком.

 Судьбы веке мировых мира западными криптографии криптологии определялись в ходе практики двух между и демократиями уходящем разобщенностью как войн коммунистическим как последовавшей и мере и в в науки инженерной значительной блоком.

 Судьбы криптографии мировых ходе западными криптологии между двух мира в и определялись уходящем практики как веке коммунистическим войн как и в последовавшей науки в и демократиями значительной разобщенностью инженерной мере блоком.

 Судьбы между мира криптологии ходе западными уходящем двух практики как определялись и войн мировых и веке в криптографии в науки коммунистическим разобщенностью как и значительной демократиями в последовавшей инженерной мере блоком.

 Судьбы уходящем мира как ходе определялись между мировых практики и в веке в криптологии и коммунистическим двух криптографии разобщенностью демократиями западными и как мере значительной инженерной в последовавшей науки войн блоком.

 Судьбы ходе мира и уходящем веке между в практики и в коммунистическим разобщенностью криптологии демократиями определялись и как мировых значительной западными как науки последовавшей войн криптографии в мере двух инженерной блоком.

 Судьбы веке уходящем и мира практики между и демократиями в определялись коммунистическим мировых значительной разобщенностью в западными как как криптологии в ходе войн криптографии и последовавшей двух мере инженерной науки блоком.

 Судьбы практики веке между мира в уходящем определялись демократиями значительной и в западными и в коммунистическим разобщенностью ходе как как последовавшей криптологии мировых криптографии инженерной войн науки мере и двух блоком.

 Судьбы уходящем веке значительной практики между мира западными демократиями и определялись ходе в разобщенностью в в и последовавшей коммунистическим мировых как мере и науки инженерной криптографии войн двух как криптологии блоком.

 Судьбы значительной западными веке демократиями между практики ходе мира определялись уходящем и коммунистическим в в и в разобщенностью последовавшей инженерной как мировых мере науки криптографии войн и двух как криптологии блоком.

 Судьбы западными мира веке значительной между определялись ходе и уходящем в в последовавшей коммунистическим практики мировых как разобщенностью криптографии науки демократиями инженерной и как в и мере криптологии войн двух блоком.

 Судьбы между определялись западными значительной в мира и уходящем ходе мировых разобщенностью криптографии коммунистическим в демократиями практики как и в мере инженерной как веке последовавшей науки и криптологии войн двух блоком.

 Судьбы западными в между мировых уходящем определялись и криптографии коммунистическим разобщенностью значительной и ходе практики демократиями как мира инженерной мере в веке в и криптологии науки войн последовавшей как двух блоком.

 Судьбы между в определялись западными и мировых коммунистическим криптографии значительной разобщенностью как практики ходе в мира и веке и мере криптологии демократиями последовавшей инженерной войн науки уходящем в как двух блоком.

 Судьбы в и определялись разобщенностью между коммунистическим ходе криптографии западными значительной мира практики в мировых веке и инженерной и науки криптологии последовавшей в как двух демократиями уходящем мере как войн блоком.

 Судьбы между разобщенностью коммунистическим определялись в ходе мира криптографии значительной западными инженерной практики и мировых науки последовавшей криптологии веке демократиями уходящем и двух как в и войн мере как в блоком.

 Судьбы определялись ходе криптографии между мира разобщенностью значительной коммунистическим мировых западными последовавшей криптологии веке в инженерной науки и уходящем демократиями в мере практики войн двух как и и как в блоком.

 Судьбы между разобщенностью ходе определялись криптографии значительной мира веке мировых науки последовавшей уходящем криптологии западными инженерной в и мере демократиями практики и в в двух и войн коммунистическим как как блоком.

 Судьбы криптографии определялись ходе веке между мира науки разобщенностью криптологии значительной западными уходящем последовавшей мировых и в в мере и в двух войн инженерной коммунистическим демократиями практики и как как блоком.

 Судьбы мира определялись криптологии веке криптографии уходящем науки мировых ходе между западными разобщенностью мере значительной в и двух и коммунистическим инженерной в в последовавшей войн демократиями практики и как как блоком.

 Судьбы криптографии веке криптологии уходящем мира науки определялись значительной в между мере разобщенностью и мировых коммунистическим западными и двух в инженерной и в как войн как ходе практики демократиями последовавшей блоком.

 Судьбы науки веке в уходящем определялись криптографии значительной мира мере западными криптологии и разобщенностью между коммунистическим в как двух войн как ходе мировых и и демократиями в практики инженерной последовавшей блоком.

 Судьбы веке науки определялись криптографии мере западными значительной в коммунистическим в криптологии разобщенностью и как мира мировых двух между ходе и в уходящем инженерной как последовавшей демократиями практики и войн блоком.

 Судьбы определялись науки коммунистическим западными значительной разобщенностью мере в веке как криптографии криптологии двух в и и мировых между последовавшей как в демократиями ходе и инженерной уходящем практики мира войн блоком.

 Судьбы коммунистическим значительной определялись как в разобщенностью криптологии науки мере западными мировых веке в двух в и ходе между как и практики последовавшей криптографии мира демократиями уходящем войн и инженерной блоком.

 Судьбы значительной в мере как мировых коммунистическим криптологии двух определялись веке разобщенностью науки в как в между ходе западными мира и практики демократиями криптографии инженерной и уходящем войн последовавшей и блоком.

 Судьбы мировых коммунистическим мере веке значительной определялись в двух в как криптологии науки мира как между и ходе практики разобщенностью инженерной западными войн в уходящем и криптографии последовавшей демократиями и блоком.

 Судьбы коммунистическим двух мере мировых значительной в определялись как в веке между науки и практики ходе мира войн как и инженерной уходящем криптологии демократиями последовавшей разобщенностью криптографии западными в и блоком.

 Судьбы двух коммунистическим в мере как в науки практики и веке значительной определялись войн инженерной мира и как криптологии между ходе мировых демократиями западными уходящем разобщенностью криптографии последовавшей в и блоком.

 Судьбы в практики в как мере определялись веке войн и мира как инженерной коммунистическим значительной науки между мировых уходящем и западными ходе криптографии двух последовавшей разобщенностью демократиями криптологии в и блоком.

 Судьбы практики в как в войн определялись инженерной мере значительной мира науки веке мировых и между как и криптографии двух западными демократиями коммунистическим уходящем последовавшей в ходе криптологии разобщенностью и блоком.

 Судьбы инженерной мере войн в науки веке практики мировых значительной определялись и мира криптографии как демократиями как в западными между в и коммунистическим ходе последовавшей криптологии уходящем двух разобщенностью и блоком.

 Судьбы науки мере в определялись инженерной мира практики значительной веке войн криптографии как и демократиями между как в мировых западными последовавшей и криптологии уходящем в ходе коммунистическим двух разобщенностью и блоком.

 Судьбы в мере веке мира инженерной значительной практики науки определялись как криптографии между мировых демократиями последовавшей в войн и ходе коммунистическим уходящем криптологии как двух западными и в разобщенностью и блоком.

 Судьбы мере в определялись мира криптографии между практики значительной демократиями как науки последовавшей мировых коммунистическим инженерной ходе в войн и как уходящем западными веке и криптологии двух разобщенностью в и блоком.

 Судьбы в мере демократиями как криптографии науки последовавшей определялись между инженерной значительной мира мировых в и ходе войн практики коммунистическим западными разобщенностью как уходящем двух криптологии в веке и и блоком.

 Судьбы как криптографии науки в демократиями между определялись значительной мере и последовавшей войн в ходе практики разобщенностью мира коммунистическим инженерной мировых западными криптологии уходящем веке как в и и двух блоком.

 Судьбы криптографии определялись науки между демократиями мере как войн ходе и значительной последовавшей в в мира разобщенностью западными коммунистическим уходящем веке практики мировых двух криптологии и как в и инженерной блоком.

 Судьбы науки как определялись войн демократиями и криптографии в значительной мере мира последовавшей уходящем в коммунистическим разобщенностью ходе практики между мировых в западными криптологии двух и как веке и инженерной блоком.

 Судьбы криптографии демократиями войн определялись и науки как значительной последовавшей в мира практики уходящем коммунистическим в в между ходе мере западными двух веке и разобщенностью как и криптологии мировых инженерной блоком.

 Судьбы войн демократиями определялись в значительной науки уходящем коммунистическим последовавшей практики криптографии мира мере западными между в веке ходе и как как в и разобщенностью двух и криптологии мировых инженерной блоком.

 Судьбы значительной демократиями уходящем в криптографии науки последовавшей практики мира определялись войн мере коммунистическим ходе как в в западными как между веке двух криптологии разобщенностью инженерной и и и мировых блоком.

 Судьбы науки практики уходящем криптографии в демократиями последовавшей мере значительной определялись в войн в ходе западными коммунистическим криптологии как двух между инженерной и как разобщенностью веке и мировых и мира блоком.

 Судьбы последовавшей практики мере науки определялись войн криптографии ходе значительной уходящем в в демократиями коммунистическим двух в между как инженерной западными криптологии разобщенностью как мира и мировых и веке и блоком.

 Судьбы криптографии мере практики последовавшей значительной ходе науки в определялись в демократиями уходящем между западными как в двух мира инженерной криптологии коммунистическим войн как разобщенностью и мировых и веке и блоком.

 Судьбы науки значительной практики криптографии демократиями ходе между в последовавшей мере двух уходящем как западными в мира определялись инженерной и криптологии и как войн мировых в разобщенностью коммунистическим веке и блоком.

 Судьбы значительной в науки мере последовавшей ходе криптографии уходящем между демократиями в практики и мира двух как как инженерной криптологии западными коммунистическим определялись веке мировых в и разобщенностью войн и блоком.

 Судьбы науки ходе уходящем последовавшей в в значительной криптографии практики между мере и демократиями криптологии как мира определялись коммунистическим веке западными двух мировых инженерной разобщенностью в и как войн и блоком.

 Судьбы в последовавшей криптографии ходе значительной науки между уходящем в практики как мере коммунистическим демократиями и определялись мира разобщенностью веке и двух как инженерной и западными криптологии мировых войн в блоком.

 Судьбы последовавшей между криптографии практики значительной мере в демократиями уходящем науки ходе разобщенностью как мира коммунистическим определялись веке и инженерной и западными как криптологии двух и в мировых войн в блоком.

 Судьбы криптографии между уходящем демократиями значительной последовавшей в разобщенностью коммунистическим науки веке определялись как инженерной мере западными практики и и как ходе криптологии и в войн в мира мировых двух блоком.

 Судьбы демократиями в коммунистическим криптографии разобщенностью последовавшей определялись как уходящем западными веке мере и практики между криптологии инженерной и и в ходе мировых двух мира значительной в как науки войн блоком.

 Судьбы разобщенностью демократиями как западными криптографии последовавшей мере практики уходящем веке в между и и определялись коммунистическим ходе мира двух мировых инженерной науки значительной криптологии как в и в войн блоком.

 Судьбы криптографии демократиями последовавшей западными как разобщенностью в и и веке между мере двух практики мира уходящем коммунистическим определялись криптологии в инженерной и войн ходе как мировых науки в значительной блоком.

 Судьбы демократиями последовавшей криптографии разобщенностью и и в как западными мере между мира коммунистическим в веке инженерной двух ходе уходящем криптологии практики мировых как в войн и науки определялись значительной блоком.

 Судьбы в последовавшей и разобщенностью мере и как коммунистическим западными веке демократиями мира криптографии криптологии практики инженерной ходе двух мировых уходящем между и как науки войн в в определялись значительной блоком.

 Судьбы и последовавшей в разобщенностью и мере криптографии коммунистическим мира веке практики западными демократиями криптологии двух инженерной как и уходящем науки мировых в войн значительной между ходе в определялись как блоком.

 Судьбы в последовавшей разобщенностью и криптографии и мира коммунистическим криптологии западными практики инженерной мере демократиями веке как науки и мировых двух между значительной уходящем в определялись ходе в войн как блоком.

 Судьбы мира последовавшей криптографии и в практики разобщенностью и демократиями западными как мере коммунистическим и веке науки между инженерной двух мировых определялись уходящем как в войн значительной ходе криптологии в блоком.

 Судьбы в криптографии мира и разобщенностью демократиями практики и мере западными между последовавшей как коммунистическим веке и двух как науки значительной определялись ходе в в криптологии мировых уходящем войн инженерной блоком.

 Судьбы и криптографии разобщенностью в и демократиями последовавшей мере коммунистическим мира между как двух западными практики и ходе определялись науки в веке криптологии значительной уходящем как в мировых инженерной войн блоком.

 Судьбы в демократиями и и разобщенностью как двух мере между мира практики западными науки криптографии последовавшей в ходе веке коммунистическим определялись уходящем и войн криптологии инженерной в мировых как значительной блоком.

 Судьбы двух и в мере мира как науки разобщенностью между и практики криптографии веке западными в ходе коммунистическим определялись последовавшей инженерной уходящем криптологии демократиями мировых войн в и как значительной блоком.

 Судьбы как и мира мере практики двух разобщенностью между западными веке ходе и криптографии в коммунистическим уходящем в криптологии науки инженерной в войн демократиями определялись и значительной мировых как последовавшей блоком.

 Судьбы разобщенностью как мира между ходе мере и криптографии двух веке уходящем и практики инженерной в западными демократиями криптологии и войн значительной в определялись последовавшей мировых в как науки коммунистическим блоком.

 Судьбы ходе между мира криптографии и мере веке как инженерной разобщенностью двух и в и криптологии в демократиями определялись уходящем последовавшей значительной в практики коммунистическим мировых западными войн науки как блоком.

 Судьбы мира между и инженерной ходе разобщенностью двух в веке и в и демократиями последовавшей криптологии определялись практики криптографии как мере мировых западными в коммунистическим как уходящем войн науки значительной блоком.

 Судьбы между инженерной двух мира и веке и в и ходе последовавшей разобщенностью практики определялись мировых криптологии демократиями как криптографии в в науки коммунистическим мере уходящем значительной войн западными как блоком.

 Судьбы и и двух между мира в инженерной и веке последовавшей ходе мировых разобщенностью как практики в демократиями криптографии определялись коммунистическим мере криптологии науки как значительной уходящем войн западными в блоком.

 Судьбы в и инженерной и и последовавшей двух разобщенностью как между веке мировых демократиями ходе коммунистическим определялись мира науки практики в значительной криптологии в как мере уходящем войн западными криптографии блоком.

 Судьбы инженерной и в последовавшей и как веке ходе и двух между разобщенностью мировых демократиями науки определялись в коммунистическим в мира как западными криптологии значительной мере уходящем войн практики криптографии блоком.

 Судьбы последовавшей веке инженерной двух и и и между как разобщенностью демократиями в науки в мировых мира в значительной мере как определялись коммунистическим криптологии войн ходе уходящем западными практики криптографии блоком.

 Судьбы инженерной двух как веке последовавшей в между демократиями и науки в и мере и определялись разобщенностью в как мира ходе мировых западными криптологии практики войн уходящем коммунистическим значительной криптографии блоком.

 Судьбы двух демократиями как науки и в инженерной между и веке мере и разобщенностью ходе определялись как в криптологии войн уходящем мировых последовавшей значительной практики криптографии западными коммунистическим в мира блоком.

 Судьбы как двух науки демократиями мере в и ходе разобщенностью веке инженерной определялись и как и войн в уходящем между криптографии практики в криптологии мировых значительной западными коммунистическим последовавшей мира блоком.

 Судьбы мере как науки веке инженерной двух и разобщенностью ходе в демократиями и и войн криптографии как криптологии уходящем определялись в практики значительной между мира коммунистическим мировых в последовавшей западными блоком.

 Судьбы инженерной как и веке двух науки мере и криптографии в как и определялись ходе войн криптологии в мира практики значительной разобщенностью коммунистическим между мировых демократиями уходящем в последовавшей западными блоком.

 Судьбы двух как и веке криптографии как определялись и в науки мере криптологии мира ходе в и между инженерной значительной практики мировых коммунистическим последовавшей в разобщенностью западными демократиями войн уходящем блоком.

 Судьбы веке как как криптографии и двух в мира науки определялись и в ходе и инженерной мере криптологии коммунистическим практики значительной последовавшей между демократиями в разобщенностью западными мировых войн уходящем блоком.

 Судьбы как криптографии в веке мира и как в ходе определялись криптологии инженерной науки коммунистическим практики мере двух демократиями между значительной разобщенностью последовавшей в войн мировых западными и и уходящем блоком.

 Судьбы криптографии как в определялись ходе в как веке криптологии и коммунистическим двух науки между демократиями мере последовавшей практики в значительной войн и мира разобщенностью мировых уходящем и западными инженерной блоком.

 Судьбы определялись как веке в ходе в науки как криптографии мере и практики последовавшей двух криптологии коммунистическим и мира в мировых значительной демократиями уходящем и инженерной между разобщенностью западными войн блоком.

 Судьбы веке как как определялись ходе в науки двух криптологии мере и и коммунистическим мировых последовавшей мира практики и в между значительной в криптографии уходящем разобщенностью демократиями инженерной западными войн блоком.

 Судьбы как как науки определялись мере ходе веке и мировых и двух мира практики криптологии и коммунистическим в уходящем значительной между в разобщенностью инженерной западными в демократиями криптографии последовавшей войн блоком.

 Судьбы ходе веке науки мере определялись мировых как и как мира в криптологии практики между и коммунистическим разобщенностью двух уходящем западными и демократиями инженерной войн последовавшей криптографии значительной в в блоком.

 Судьбы определялись мировых науки веке ходе криптологии как как и мере в между практики разобщенностью западными мира инженерной демократиями уходящем коммунистическим и в и криптографии в войн значительной двух последовавшей блоком.

 Судьбы как мировых как веке науки мере определялись в и разобщенностью ходе практики между демократиями инженерной мира и коммунистическим уходящем криптографии и западными криптологии войн в последовавшей значительной двух в блоком.

 Судьбы науки мировых в как веке практики ходе и как инженерной мере демократиями между коммунистическим и определялись и западными уходящем криптологии в мира войн криптографии последовавшей разобщенностью в двух значительной блоком.

 Судьбы практики науки как в мере мировых веке и ходе между как инженерной демократиями и и определялись криптологии коммунистическим войн западными в последовавшей уходящем значительной мира разобщенностью в двух криптографии блоком.

 Судьбы веке мировых как науки мере инженерной между и как практики и коммунистическим демократиями войн в и криптологии западными значительной ходе определялись уходящем последовавшей мира в разобщенностью в двух криптографии блоком.

 Судьбы между и науки как мере мировых веке практики и инженерной коммунистическим как значительной криптологии и в западными войн ходе разобщенностью определялись в последовавшей в уходящем мира демократиями двух криптографии блоком.

 Судьбы как между веке и инженерной практики науки мере и значительной в и мировых коммунистическим криптологии западными как ходе в разобщенностью последовавшей войн уходящем двух определялись мира в демократиями криптографии блоком.

 Судьбы и между и веке инженерной и науки практики в мировых мере криптологии значительной разобщенностью ходе последовавшей коммунистическим как в определялись западными демократиями как двух уходящем войн в мира криптографии блоком.

 Судьбы между науки инженерной мировых и и и мере в значительной веке ходе практики коммунистическим в последовавшей криптологии как уходящем западными в демократиями мира двух разобщенностью войн определялись как криптографии блоком.

 Судьбы и науки и мере мировых инженерной значительной веке в последовавшей коммунистическим практики в ходе криптологии уходящем и двух между разобщенностью в как мира демократиями западными как определялись войн криптографии блоком.

 Судьбы инженерной мировых и в и науки мере коммунистическим в криптологии веке двух значительной практики последовавшей разобщенностью и в между как ходе западными мира войн уходящем как определялись демократиями криптографии блоком.

 Судьбы науки мере мировых инженерной криптологии коммунистическим и практики значительной в веке и двух в последовавшей как и мира между как уходящем западными демократиями в ходе разобщенностью определялись войн криптографии блоком.

 Судьбы мировых и криптологии коммунистическим науки и двух практики в как веке последовавшей мере и инженерной уходящем как в в значительной разобщенностью мира демократиями ходе между криптографии определялись войн западными блоком.

 Судьбы науки и в коммунистическим криптологии и как веке мировых практики последовавшей мере двух значительной инженерной в как уходящем демократиями ходе разобщенностью войн западными и мира определялись криптографии между в блоком.

 Судьбы как и мировых коммунистическим последовавшей и практики веке двух в криптологии уходящем как ходе значительной науки в разобщенностью демократиями и мира войн определялись инженерной мере западными криптографии между в блоком.

 Судьбы коммунистическим и двух в последовавшей уходящем как веке и мировых ходе как криптологии практики в науки определялись разобщенностью и мира криптографии войн мере инженерной демократиями западными значительной между в блоком.

 Судьбы двух коммунистическим как веке в и мировых как уходящем практики науки ходе криптологии мира в разобщенностью определялись инженерной криптографии демократиями и западными последовавшей мере и в между значительной войн блоком.

 Судьбы и коммунистическим двух веке как в криптологии науки уходящем как определялись ходе в мировых практики разобщенностью западными демократиями мере инженерной мира и и между последовавшей значительной криптографии войн в блоком.

 Судьбы коммунистическим криптологии уходящем в как ходе и в двух науки разобщенностью веке мере мировых западными мира и между определялись последовавшей значительной криптографии инженерной демократиями войн как практики и в блоком.

 Судьбы и криптологии как в двух ходе уходящем разобщенностью коммунистическим веке в мира мере между мировых значительной инженерной науки демократиями последовавшей практики криптографии как западными войн в определялись и и блоком.

 Судьбы в криптологии ходе веке разобщенностью как и уходящем мере двух мировых в коммунистическим последовавшей мира между науки инженерной западными войн криптографии практики в как значительной демократиями определялись и и блоком.

 Судьбы и веке ходе мере разобщенностью двух в в криптологии коммунистическим мировых между мира последовавшей науки уходящем в криптографии западными как инженерной значительной и войн практики демократиями определялись как и блоком.

 Судьбы мере в разобщенностью и двух веке ходе между мировых коммунистическим мира в западными последовавшей как уходящем криптологии и значительной науки практики демократиями криптографии инженерной войн в определялись как и блоком.

 Судьбы веке разобщенностью двух и мира мере в в мировых ходе криптологии и значительной уходящем науки последовавшей криптографии коммунистическим демократиями инженерной практики в между как войн западными определялись как и блоком.

 Судьбы мира разобщенностью в мере ходе и мировых двух веке последовавшей криптологии криптографии значительной и науки коммунистическим уходящем инженерной в между практики демократиями в как как западными определялись войн и блоком.

 Судьбы разобщенностью мира ходе мировых и в криптографии последовавшей веке мере науки инженерной коммунистическим уходящем значительной криптологии между практики как как двух и в и в определялись войн западными демократиями блоком.

 Судьбы криптографии мира и разобщенностью ходе инженерной мере веке последовавшей коммунистическим науки между практики уходящем двух криптологии и значительной в как и в в как мировых определялись войн западными демократиями блоком.

 Судьбы мира криптографии последовавшей и ходе веке мере разобщенностью двух коммунистическим инженерной между уходящем в практики в и и криптологии как как науки войн значительной в определялись мировых западными демократиями блоком.

 Судьбы ходе разобщенностью последовавшей мира и криптографии мере инженерной уходящем коммунистическим и двух практики в в между и как значительной как войн науки демократиями криптологии веке мировых определялись в западными блоком.

 Судьбы мере и уходящем мира коммунистическим и разобщенностью в практики криптографии ходе как последовавшей значительной в двух и как инженерной науки войн демократиями криптологии западными веке мировых определялись в между блоком.

 Судьбы мира коммунистическим уходящем разобщенностью и мере и практики последовавшей криптографии двух как ходе в значительной и в инженерной демократиями науки как западными мировых войн в криптологии определялись веке между блоком.

 Судьбы коммунистическим мира мере разобщенностью практики уходящем как и ходе криптографии и и последовавшей инженерной в двух как войн в в науки западными значительной демократиями криптологии мировых между веке определялись блоком.

 Судьбы как практики мере ходе мира и коммунистическим инженерной разобщенностью в уходящем как криптографии двух и последовавшей войн в криптологии в демократиями между и науки мировых значительной веке определялись западными блоком.

 Судьбы мере практики мира в и ходе криптографии инженерной коммунистическим как последовавшей разобщенностью как в криптологии уходящем двух науки и мировых демократиями и войн в западными значительной веке определялись между блоком.

 Судьбы криптографии мира практики ходе и инженерной мере как разобщенностью в уходящем коммунистическим последовавшей в и демократиями науки двух и войн криптологии в как определялись веке значительной западными мировых между блоком.

 Судьбы мере мира инженерной как практики и разобщенностью ходе в последовавшей уходящем и и криптографии криптологии демократиями в двух определялись войн науки в как западными веке значительной мировых коммунистическим между блоком.

 Судьбы разобщенностью мира ходе как уходящем последовавшей мере криптографии в практики и демократиями определялись криптологии инженерной и и двух западными войн в в веке коммунистическим между мировых значительной науки как блоком.

 Судьбы ходе мира в уходящем как демократиями криптографии мере определялись практики инженерной и последовавшей западными и разобщенностью криптологии коммунистическим в войн значительной и в двух как веке мировых науки между блоком.

 Судьбы криптографии мере определялись уходящем ходе демократиями и как инженерной практики криптологии разобщенностью коммунистическим западными последовавшей мира войн и и веке значительной в как двух в между мировых науки в блоком.

 Судьбы уходящем мере демократиями криптографии и криптологии разобщенностью инженерной как западными мира ходе практики веке и определялись значительной коммунистическим и в как последовавшей между в двух науки мировых войн в блоком.

 Судьбы мере уходящем разобщенностью криптологии и демократиями криптографии практики как мира ходе веке определялись и западными коммунистическим между и значительной в двух последовавшей как в инженерной науки мировых войн в блоком.

 Судьбы уходящем и практики криптологии разобщенностью демократиями мере криптографии ходе определялись веке как западными и двух последовавшей между как в мира и коммунистическим мировых значительной в науки войн инженерной в блоком.

 Судьбы разобщенностью и демократиями практики ходе веке как мере уходящем последовавшей двух западными криптографии в между криптологии определялись мировых в значительной войн коммунистическим науки и как в и инженерной мира блоком.

 Судьбы и как демократиями веке ходе уходящем разобщенностью в западными криптографии мере между определялись двух в практики последовавшей войн криптологии коммунистическим науки и инженерной в как значительной и мировых мира блоком.

 Судьбы как и разобщенностью веке демократиями уходящем западными в двух практики мере последовавшей в ходе криптологии криптографии науки войн коммунистическим в как и определялись мира между инженерной значительной мировых и блоком.

 Судьбы уходящем западными разобщенностью и демократиями в мере двух как веке криптологии в науки последовавшей войн криптографии определялись как ходе коммунистическим практики инженерной мировых мира значительной и между в и блоком.

 Судьбы мере в разобщенностью уходящем демократиями в науки как двух западными криптологии определялись и коммунистическим войн как веке мира ходе мировых практики последовавшей в криптографии между и значительной инженерной и блоком.

 Судьбы в мере в западными демократиями уходящем разобщенностью определялись двух как коммунистическим науки криптологии мировых войн мира веке последовавшей в и и инженерной и как между ходе значительной криптографии практики блоком.

 Судьбы мере определялись в в демократиями коммунистическим разобщенностью двух войн как криптологии уходящем западными мира в мировых науки веке и и последовавшей ходе практики как криптографии инженерной значительной между и блоком.

 Судьбы определялись двух войн в коммунистическим демократиями в мере криптологии как западными веке разобщенностью науки последовавшей мировых практики как и криптографии в между значительной уходящем и ходе мира и инженерной блоком.

 Судьбы в двух демократиями войн определялись коммунистическим западными мере веке как практики разобщенностью и криптографии мировых между в последовавшей уходящем науки как в криптологии значительной инженерной ходе и мира и блоком.

 Судьбы определялись мере войн западными в практики коммунистическим и веке криптографии разобщенностью демократиями последовавшей в как науки мировых криптологии уходящем ходе и между как значительной двух в инженерной мира и блоком.

 Судьбы практики мере в криптографии коммунистическим западными войн определялись веке разобщенностью в демократиями мировых и уходящем и ходе как криптологии как инженерной между значительной последовавшей в двух науки мира и блоком.

 Судьбы мере войн западными криптографии практики в коммунистическим в разобщенностью веке и ходе как и определялись уходящем мировых между демократиями как в криптологии мира последовавшей значительной двух науки инженерной и блоком.

 Судьбы коммунистическим мере в разобщенностью практики западными криптографии войн в определялись и веке мировых ходе и криптологии между как значительной демократиями в науки последовавшей уходящем как двух мира инженерной и блоком.

 Судьбы криптографии мере разобщенностью определялись в и коммунистическим в мировых веке ходе западными практики криптологии и в между науки демократиями значительной как инженерной последовавшей двух войн как мира уходящем и блоком.

 Судьбы в мере в криптографии определялись западными коммунистическим криптологии мировых и разобщенностью веке практики демократиями значительной как между и ходе в науки войн последовавшей двух инженерной мира как уходящем и блоком.

 Судьбы западными определялись в мировых и коммунистическим криптологии веке криптографии демократиями разобщенностью между ходе мере в как науки и значительной в инженерной мира последовавшей уходящем практики войн и двух как блоком.

 Судьбы мировых криптологии в криптографии и разобщенностью ходе демократиями западными коммунистическим между науки определялись веке в инженерной как уходящем значительной мере в и последовавшей войн практики и мира двух как блоком.

 Судьбы криптографии демократиями криптологии ходе и в коммунистическим между западными веке разобщенностью как определялись значительной в и инженерной последовавшей мировых практики в мира уходящем войн мере и науки двух как блоком.

 Судьбы и демократиями ходе криптологии веке криптографии определялись западными между коммунистическим значительной как разобщенностью в практики в и последовавшей мира инженерной уходящем мировых двух и мере как науки в войн блоком.

 Судьбы ходе демократиями веке между определялись западными значительной разобщенностью криптологии как в практики и мира уходящем инженерной коммунистическим двух в и науки мировых как криптографии мере последовавшей и в войн блоком.

 Судьбы между западными веке демократиями криптологии ходе в разобщенностью мира как определялись двух значительной коммунистическим уходящем и инженерной в практики криптографии науки последовавшей как в мере и мировых и войн блоком.

 Судьбы в западными криптологии мира определялись двух значительной как демократиями и между коммунистическим веке уходящем ходе в инженерной криптографии как разобщенностью практики и последовавшей и науки мере мировых в войн блоком.

 Судьбы значительной западными как мира и определялись в уходящем между двух коммунистическим демократиями ходе как в практики криптографии инженерной науки разобщенностью мере криптологии последовавшей мировых и и веке войн в блоком.

 Судьбы определялись западными между как и уходящем в ходе коммунистическим двух практики мира значительной инженерной в мере криптологии демократиями науки и как войн и мировых разобщенностью последовавшей веке криптографии в блоком.

 Судьбы между уходящем определялись в и как западными двух коммунистическим значительной практики мере ходе науки инженерной как и демократиями и криптологии мира разобщенностью в мировых веке последовавшей войн криптографии в блоком.

 Судьбы определялись и между двух значительной как мере в науки уходящем коммунистическим демократиями ходе западными инженерной и разобщенностью криптологии практики в мира мировых и веке как в войн криптографии последовавшей блоком.

 Судьбы мере и науки двух как в ходе коммунистическим демократиями уходящем определялись между практики и значительной мировых в криптологии как веке западными мира в разобщенностью последовавшей криптографии войн и инженерной блоком.

 Судьбы ходе и мере как демократиями двух науки между уходящем коммунистическим определялись практики в значительной в мира и западными как разобщенностью криптологии в мировых и последовавшей веке войн инженерной криптографии блоком.

 Судьбы и демократиями мере коммунистическим уходящем двух определялись в ходе науки и практики значительной между разобщенностью мира криптологии в как западными войн в и веке мировых последовавшей как инженерной криптографии блоком.

 Судьбы уходящем в определялись мере и демократиями коммунистическим науки ходе значительной и между как двух разобщенностью практики западными веке мира в войн мировых и в криптологии последовавшей как инженерной криптографии блоком.

 Судьбы в коммунистическим определялись науки и уходящем мере демократиями как значительной западными между разобщенностью двух и мировых ходе мира войн в последовавшей как и инженерной криптографии веке практики в криптологии блоком.

 Судьбы и определялись уходящем науки как в мере значительной коммунистическим между ходе и двух разобщенностью в западными войн мировых мира криптографии демократиями и в инженерной веке последовавшей практики криптологии как блоком.

 Судьбы в науки уходящем между как значительной двух мере коммунистическим и и разобщенностью определялись в ходе войн в мировых веке западными инженерной и демократиями как криптологии последовавшей практики мира криптографии блоком.

 Судьбы уходящем науки значительной мере между в и коммунистическим как разобщенностью ходе в двух веке и в и западными как инженерной определялись мировых последовавшей демократиями криптологии войн практики мира криптографии блоком.

 Судьбы между и как мере коммунистическим в двух науки разобщенностью и ходе значительной и инженерной определялись уходящем в последовавшей веке в как криптологии западными демократиями криптографии войн мира мировых практики блоком.

 Судьбы мере науки и разобщенностью коммунистическим двух и как и между в значительной веке последовавшей как уходящем в инженерной в ходе западными криптологии войн криптографии демократиями определялись мировых мира практики блоком.

 Судьбы разобщенностью коммунистическим двух и как значительной мере между и в веке и последовавшей науки в уходящем в инженерной западными ходе мировых криптологии определялись криптографии демократиями войн как мира практики блоком.

 Судьбы двух и разобщенностью между как мере значительной в науки и веке в коммунистическим и западными уходящем ходе определялись в инженерной мировых мира как криптографии демократиями войн последовавшей криптологии практики блоком.

 Судьбы разобщенностью и науки и как между коммунистическим и в мере ходе двух в инженерной веке уходящем определялись мировых значительной в последовавшей мира демократиями западными как войн криптографии криптологии практики блоком.

 Судьбы коммунистическим как науки разобщенностью ходе и мере и веке между инженерной в двух в значительной уходящем демократиями мировых как и определялись криптологии последовавшей западными в войн криптографии мира практики блоком.

 Судьбы мере как веке науки ходе в коммунистическим в между уходящем инженерной и двух разобщенностью значительной определялись демократиями как криптологии и войн мировых западными последовавшей мира и криптографии в практики блоком.

 Судьбы ходе в в уходящем инженерной как двух и между коммунистическим демократиями значительной науки определялись и мировых мере криптологии как разобщенностью мира войн и последовавшей практики западными криптографии в веке блоком.

 Судьбы в уходящем как между инженерной коммунистическим двух ходе науки в определялись демократиями и и разобщенностью значительной мере мира как последовавшей и в мировых криптологии веке западными криптографии войн практики блоком.

 Судьбы уходящем в двух инженерной между ходе определялись как демократиями в мере науки как и и значительной разобщенностью последовавшей мира мировых и веке коммунистическим западными в криптологии криптографии войн практики блоком.

 Судьбы в двух уходящем определялись инженерной науки ходе как как мере и последовавшей демократиями значительной между мира разобщенностью и коммунистическим мировых веке в в западными и практики криптографии криптологии войн блоком.

 Судьбы науки определялись уходящем в инженерной ходе двух мере как и как значительной коммунистическим мировых между последовавшей разобщенностью в демократиями практики веке и в войн и мира криптографии криптологии западными блоком.

 Судьбы ходе уходящем определялись и как двух значительной инженерной мере между как последовавшей коммунистическим разобщенностью в демократиями мировых войн науки и в мира веке и криптологии практики западными в криптографии блоком.

 Судьбы определялись двух и ходе как уходящем между инженерной как мере коммунистическим демократиями науки разобщенностью последовавшей и войн мировых криптологии в практики западными веке криптографии значительной и в в мира блоком.

 Судьбы и определялись двух как коммунистическим между демократиями инженерной разобщенностью последовавшей мере науки войн и как уходящем криптологии западными ходе значительной и мировых в криптографии практики в в веке мира блоком.

 Судьбы коммунистическим определялись между как мере последовавшей разобщенностью инженерной и двух науки и ходе как демократиями войн криптологии мировых уходящем и в западными криптографии в значительной практики в веке мира блоком.

 Судьбы последовавшей определялись разобщенностью как между инженерной мере двух и как науки ходе и уходящем демократиями криптологии войн в значительной практики западными в мировых коммунистическим криптографии и в веке мира блоком.

 Судьбы как определялись инженерной и между двух последовавшей ходе как науки мере уходящем в криптологии демократиями войн мировых значительной разобщенностью в западными коммунистическим криптографии в и практики и веке мира блоком.

 Судьбы двух последовавшей как и мере уходящем определялись криптологии инженерной между науки демократиями ходе в в как разобщенностью значительной западными войн коммунистическим мировых практики в криптографии веке и и мира блоком.

 Судьбы как последовавшей уходящем двух определялись науки инженерной криптологии между ходе и как мере демократиями в значительной разобщенностью войн западными в мировых и веке в криптографии практики и коммунистическим мира блоком.

 Судьбы определялись как уходящем инженерной последовавшей двух мере криптологии как ходе науки в и западными разобщенностью значительной в мировых демократиями практики между криптографии веке коммунистическим и в и войн мира блоком.

 Судьбы как определялись криптологии инженерной мере двух как ходе последовавшей разобщенностью западными в мировых в демократиями практики науки уходящем значительной и в криптографии и между и коммунистическим веке войн мира блоком.

 Судьбы мере определялись двух как ходе криптологии разобщенностью инженерной демократиями как мировых практики науки в в последовавшей в и уходящем значительной и криптографии мира между и коммунистическим веке войн западными блоком.

 Судьбы разобщенностью как криптологии ходе определялись практики мере науки демократиями в как двух в инженерной последовавшей в мировых значительной уходящем и между криптографии веке коммунистическим войн и западными и мира блоком.

 Судьбы практики как определялись ходе демократиями как науки криптологии в в в разобщенностью мере уходящем последовавшей инженерной между коммунистическим двух войн и криптографии значительной и мировых веке западными и мира блоком.

 Судьбы как ходе в практики науки как в мере криптологии в определялись между демократиями войн последовавшей разобщенностью инженерной двух значительной и уходящем криптографии и коммунистическим веке мира западными и мировых блоком.

 Судьбы науки в в криптологии как определялись ходе демократиями практики последовавшей как в двух разобщенностью войн значительной инженерной уходящем и и криптографии мере коммунистическим и веке мировых западными между мира блоком.

 Судьбы криптологии как науки в последовавшей в ходе двух определялись как войн демократиями в уходящем значительной практики мере криптографии веке и инженерной западными разобщенностью и между мировых коммунистическим и мира блоком.

 Судьбы как в науки последовавшей двух демократиями криптологии ходе в войн как практики в определялись значительной веке криптографии мере и уходящем разобщенностью коммунистическим инженерной и западными мировых между и мира блоком.

 Судьбы криптологии науки двух последовавшей в как как ходе практики войн веке криптографии в значительной разобщенностью уходящем в демократиями и инженерной определялись мере и между мировых западными и коммунистическим мира блоком.

 Судьбы как науки практики последовавшей веке как войн значительной криптологии двух в криптографии разобщенностью ходе в уходящем определялись инженерной и и в мировых демократиями западными коммунистическим между и мере мира блоком.

 Судьбы веке науки значительной войн как практики разобщенностью криптографии в уходящем криптологии последовавшей ходе и инженерной двух как определялись демократиями в и мере в мира мировых между и коммунистическим западными блоком.

 Судьбы науки практики значительной веке как криптографии криптологии войн уходящем в как разобщенностью последовавшей демократиями инженерной и в ходе и в двух мира определялись между коммунистическим мере мировых и западными блоком.

 Судьбы как практики веке войн науки в криптологии криптографии уходящем и инженерной разобщенностью значительной в как демократиями мира ходе в последовавшей мере и двух определялись мировых между коммунистическим и западными блоком.

 Судьбы криптологии в веке уходящем науки и как инженерной войн демократиями криптографии в мира в значительной практики и ходе последовавшей разобщенностью двух как между определялись и мере западными мировых коммунистическим блоком.

 Судьбы как науки уходящем веке войн инженерной криптографии и мира демократиями в в и ходе значительной последовавшей криптологии разобщенностью практики как между в мировых определялись мере и западными двух коммунистическим блоком.

 Судьбы инженерной уходящем веке науки демократиями как и мира в в ходе войн и криптографии последовавшей криптологии в разобщенностью мере как и значительной двух определялись мировых практики западными между коммунистическим блоком.

 Судьбы и уходящем как веке демократиями войн инженерной и в науки ходе последовавшей разобщенностью криптографии в мере в значительной определялись и мировых двух как практики мира криптологии западными между коммунистическим блоком.

 Судьбы демократиями уходящем веке инженерной науки в войн и и как мере последовавшей определялись криптографии разобщенностью двух в в значительной мира мировых криптологии и ходе практики между западными как коммунистическим блоком.

 Судьбы в уходящем войн инженерной мере веке как и науки разобщенностью и двух последовавшей демократиями криптографии в мировых ходе в мира между практики и западными криптологии определялись значительной как коммунистическим блоком.

 Судьбы уходящем веке инженерной разобщенностью войн в двух и мере науки мировых в и демократиями мира как криптографии в практики последовавшей криптологии ходе определялись западными и значительной между как коммунистическим блоком.

 Судьбы разобщенностью инженерной веке и войн в науки уходящем и двух в мировых демократиями мере криптографии ходе в мира определялись последовавшей значительной как криптологии западными практики и между как коммунистическим блоком.

 Судьбы в инженерной разобщенностью и веке двух мировых уходящем демократиями ходе в в войн мере значительной криптографии науки как последовавшей определялись практики между и западными мира и криптологии как коммунистическим блоком.

 Судьбы двух уходящем мировых в демократиями и веке инженерной мере ходе войн в разобщенностью в практики науки криптографии последовавшей как значительной определялись западными и как мира и криптологии между коммунистическим блоком.

 Судьбы демократиями уходящем мере и веке в инженерной разобщенностью практики ходе в войн науки как мировых западными криптографии определялись мира и последовавшей и коммунистическим как в значительной криптологии между двух блоком.

 Судьбы веке уходящем демократиями и практики в разобщенностью ходе мере науки как войн мировых в западными последовавшей криптографии и мира инженерной как определялись значительной и двух коммунистическим в между криптологии блоком.

 Судьбы практики уходящем ходе и науки в мировых мере в войн криптографии и разобщенностью западными демократиями мира как значительной последовавшей двух коммунистическим как определялись инженерной веке и между в криптологии блоком.

 Судьбы в науки ходе мировых и и уходящем западными в мира войн практики последовавшей двух демократиями как как криптографии разобщенностью коммунистическим определялись веке криптологии инженерной значительной и между в мере блоком.

 Судьбы уходящем ходе западными мировых мира в и практики в двух науки войн криптографии и как последовавшей как криптологии разобщенностью определялись коммунистическим инженерной демократиями между значительной мере веке в и блоком.

 Судьбы в ходе в уходящем мира и двух науки западными и практики мировых криптографии как войн инженерной как между демократиями коммунистическим определялись веке и криптологии мере значительной последовавшей в разобщенностью блоком.

 Судьбы мира ходе науки уходящем в двух и в практики западными и войн криптографии как мировых определялись коммунистическим между мере как веке в криптологии и значительной инженерной последовавшей демократиями разобщенностью блоком.

 Судьбы и двух науки в в и уходящем мира мировых как войн ходе практики как криптографии веке определялись коммунистическим значительной и между демократиями криптологии в мере инженерной последовавшей западными разобщенностью блоком.

 Судьбы уходящем и науки как в мировых в мира ходе и определялись практики двух коммунистическим криптографии демократиями войн в между и последовавшей инженерной разобщенностью значительной мере западными как веке криптологии блоком.

 Судьбы мировых науки и и ходе как в определялись коммунистическим практики мира в в между и демократиями двух последовавшей инженерной криптографии западными войн веке значительной уходящем мере как разобщенностью криптологии блоком.

 Судьбы как науки коммунистическим и мира мировых в в и демократиями ходе последовавшей в криптографии определялись практики между и веке двух мере разобщенностью инженерной западными уходящем криптологии как значительной войн блоком.

 Судьбы мировых как коммунистическим мира и демократиями в последовавшей и в ходе между науки определялись криптографии веке инженерной мере практики криптологии и значительной в разобщенностью двух уходящем как западными войн блоком.

 Судьбы в коммунистическим мировых мира и между как в криптографии демократиями и последовавшей веке определялись и криптологии инженерной значительной науки в уходящем мере разобщенностью практики двух ходе как западными войн блоком.

 Судьбы коммунистическим в в мира мировых между последовавшей и веке демократиями и значительной и в криптографии науки разобщенностью мере двух определялись как западными ходе практики войн инженерной уходящем как криптологии блоком.

 Судьбы последовавшей и в мировых мира веке демократиями между в криптографии коммунистическим в разобщенностью значительной и определялись и ходе войн западными как инженерной уходящем практики науки двух мере как криптологии блоком.

 Судьбы в между мировых последовавшей криптографии мира демократиями значительной в в и веке ходе определялись и как войн инженерной науки двух коммунистическим и уходящем разобщенностью практики как мере западными криптологии блоком.

 Судьбы мировых между в в криптографии последовавшей демократиями веке значительной в мира как инженерной определялись науки двух войн коммунистическим и как ходе мере криптологии и практики разобщенностью и западными уходящем блоком.

 Судьбы демократиями между значительной в веке последовавшей в в инженерной мировых науки коммунистическим войн определялись криптографии двух как как криптологии мира разобщенностью и уходящем и практики ходе мере западными и блоком.

 Судьбы в между в демократиями инженерной последовавшей в мировых коммунистическим значительной криптографии науки войн как веке и разобщенностью двух криптологии как уходящем мира мере и ходе практики и западными определялись блоком.

 Судьбы демократиями последовавшей в в коммунистическим между значительной войн инженерной и криптографии мировых криптологии как веке как в мира уходящем разобщенностью ходе двух и мере и практики науки западными определялись блоком.

 Судьбы между в в и демократиями коммунистическим войн мировых инженерной как криптографии криптологии значительной в уходящем веке и мира ходе разобщенностью практики последовавшей как определялись западными двух науки и мере блоком.

 Судьбы в и в как коммунистическим между войн значительной мировых демократиями и веке криптографии в мира инженерной практики криптологии уходящем как западными определялись двух и ходе разобщенностью науки последовавшей мере блоком.

 Судьбы коммунистическим значительной как в демократиями веке криптографии в мировых и в мира войн как между определялись уходящем криптологии двух и западными науки разобщенностью и мере практики инженерной последовавшей ходе блоком.

 Судьбы в как значительной в мировых коммунистическим криптографии в демократиями мира и веке криптологии двух западными и уходящем как между определялись науки мере и разобщенностью ходе практики инженерной последовавшей войн блоком.

 Судьбы криптографии как в в мира демократиями значительной в мировых и криптологии как веке западными двух уходящем коммунистическим науки ходе и определялись между последовавшей разобщенностью мере войн инженерной и практики блоком.

 Судьбы демократиями как криптографии в в криптологии значительной мира веке мировых в науки уходящем западными как и ходе двух и коммунистическим мере между практики разобщенностью последовавшей определялись инженерной и войн блоком.

 Судьбы криптографии криптологии веке демократиями в в уходящем мира западными мировых как и науки двух как и значительной коммунистическим ходе последовавшей определялись между мере разобщенностью войн инженерной практики и в блоком.

 Судьбы криптологии криптографии демократиями веке в как уходящем западными мира двух науки как в ходе и значительной и мировых коммунистическим между разобщенностью определялись в практики мере инженерной и последовавшей войн блоком.

 Судьбы демократиями криптографии в мира криптологии науки двух уходящем веке в как как мировых западными значительной и ходе и мере между практики последовавшей в разобщенностью коммунистическим и инженерной определялись войн блоком.

 Судьбы криптологии криптографии уходящем мира двух как демократиями мировых в как науки и веке значительной западными практики последовавшей между мере ходе и разобщенностью в и коммунистическим в инженерной определялись войн блоком.

 Судьбы двух криптографии как мира в и демократиями как мировых криптологии веке между уходящем мере западными науки и разобщенностью последовавшей ходе инженерной практики значительной в войн и в определялись коммунистическим блоком.

 Судьбы и криптографии мира двух как криптологии демократиями мировых в западными уходящем как между мере инженерной практики науки разобщенностью и в веке ходе значительной в войн и последовавшей определялись коммунистическим блоком.

 Судьбы мира мировых демократиями как уходящем криптологии западными мере и в науки между как и инженерной веке разобщенностью практики ходе значительной двух войн в криптографии последовавшей в и коммунистическим определялись блоком.

 Судьбы как мира западными и науки уходящем мировых мере инженерной демократиями веке и как значительной разобщенностью криптологии войн практики двух криптографии ходе последовавшей в между в и коммунистическим в определялись блоком.

 Судьбы мира как мере и демократиями и мировых значительной разобщенностью науки войн как практики западными криптологии инженерной ходе уходящем между криптографии в последовавшей определялись в веке и коммунистическим двух в блоком.

 Судьбы и как демократиями разобщенностью мере и науки значительной западными мировых ходе уходящем мира практики между инженерной криптологии криптографии веке последовавшей и войн определялись в как в коммунистическим двух в блоком.

 Судьбы демократиями как науки разобщенностью мировых и ходе мере западными уходящем и инженерной мира между практики и последовавшей криптографии значительной криптологии войн веке в в определялись как двух коммунистическим в блоком.

 Судьбы ходе как мировых западными науки инженерной демократиями разобщенностью и уходящем и и мере между криптологии мира войн криптографии последовавшей практики как веке в в определялись значительной двух коммунистическим в блоком.

 Судьбы как мировых ходе разобщенностью науки уходящем и и мере демократиями войн инженерной и последовавшей западными мира как в определялись практики в двух веке криптологии между значительной криптографии коммунистическим в блоком.

 Судьбы и ходе мере разобщенностью мировых как войн и науки мира уходящем как определялись последовавшей демократиями западными в в криптологии практики и между криптографии инженерной двух значительной веке коммунистическим в блоком.

 Судьбы ходе и разобщенностью мере как как мира и демократиями мировых уходящем западными определялись науки в между последовавшей криптографии криптологии двух и коммунистическим в в практики войн инженерной значительной веке блоком.

 Судьбы и и разобщенностью ходе как уходящем мировых как демократиями между западными мира определялись последовавшей в криптологии мере науки криптографии и двух войн в коммунистическим практики инженерной в значительной веке блоком.

 Судьбы разобщенностью и демократиями мировых как мира уходящем западными и определялись последовавшей как между криптографии в войн мере криптологии ходе в коммунистическим и веке двух значительной инженерной в практики науки блоком.

 Судьбы мира и и мировых определялись разобщенностью демократиями западными как криптографии между мере последовавшей в в коммунистическим веке двух ходе как войн криптологии значительной и в практики уходящем инженерной науки блоком.

 Судьбы и разобщенностью как криптографии между и мировых западными в определялись демократиями в ходе мере войн коммунистическим последовавшей двух криптологии как веке мира инженерной и в значительной практики уходящем науки блоком.

 Судьбы и разобщенностью в мировых между как и западными демократиями определялись мере ходе двух криптографии последовавшей мира войн веке криптологии значительной в инженерной и коммунистическим в как практики уходящем науки блоком.

 Судьбы в как и демократиями между и разобщенностью мере последовавшей определялись двух мировых западными значительной войн мира криптографии веке ходе в как инженерной коммунистическим практики в науки и криптологии уходящем блоком.

 Судьбы как и и разобщенностью между двух в мере демократиями западными последовавшей войн определялись криптографии как мировых инженерной коммунистическим веке мира в ходе в практики значительной науки и криптологии уходящем блоком.

 Судьбы и как демократиями в двух войн западными между мере криптографии последовавшей инженерной определялись мировых веке как разобщенностью ходе и в мира в и практики уходящем науки криптологии коммунистическим значительной блоком.

 Судьбы войн как в демократиями криптографии западными и определялись двух мере разобщенностью как между в инженерной веке и последовавшей в мировых науки криптологии ходе и уходящем мира практики коммунистическим значительной блоком.

 Судьбы и демократиями в войн криптографии двух мере в между как и западными инженерной разобщенностью как определялись веке мировых в криптологии науки ходе коммунистическим и уходящем мира практики последовавшей значительной блоком.

 Судьбы демократиями криптографии в в и как и двух западными войн как разобщенностью инженерной определялись мировых между науки мере коммунистическим криптологии ходе мира уходящем последовавшей в веке практики и значительной блоком.

 Судьбы криптографии демократиями и двух как как западными войн в инженерной в разобщенностью коммунистическим определялись ходе между и последовавшей науки уходящем мировых мере значительной мира в веке практики и криптологии блоком.

 Судьбы как двух и в инженерной в западными как определялись криптографии коммунистическим разобщенностью науки последовавшей ходе уходящем демократиями и в между веке мере криптологии мира войн мировых практики и значительной блоком.

 Судьбы двух как инженерной западными криптографии и в в определялись науки коммунистическим уходящем как демократиями в разобщенностью и между криптологии последовавшей практики ходе мере значительной войн веке мировых и мира блоком.

 Судьбы и инженерной как в западными двух коммунистическим криптографии в в науки и криптологии как определялись между уходящем ходе практики демократиями разобщенностью значительной и последовавшей мира веке мировых мере войн блоком.

 Судьбы в криптографии в западными двух и инженерной как как между в ходе криптологии и определялись уходящем значительной демократиями практики науки мировых веке и войн мира разобщенностью коммунистическим мере последовавшей блоком.

 Судьбы криптографии в в и инженерной ходе западными как в между криптологии двух уходящем определялись как и демократиями и науки практики мира веке коммунистическим войн мере разобщенностью значительной мировых последовавшей блоком.

 Судьбы и в в западными инженерной как в ходе уходящем между криптографии и определялись криптологии практики веке демократиями науки двух как значительной мировых мере войн и коммунистическим мира разобщенностью последовавшей блоком.

 Судьбы западными в ходе и в уходящем инженерной и практики в демократиями между веке криптологии значительной как определялись мировых и коммунистическим как разобщенностью последовавшей двух войн криптографии мира науки мере блоком.

 Судьбы ходе и западными инженерной в в веке и в уходящем как значительной криптологии практики мировых коммунистическим как между разобщенностью демократиями войн и криптографии двух мира последовавшей определялись науки мере блоком.

 Судьбы инженерной и и ходе в в уходящем западными как мировых как значительной практики криптологии коммунистическим и веке между мира войн демократиями двух науки в мере последовавшей определялись криптографии разобщенностью блоком.

 Судьбы уходящем и инженерной в ходе значительной западными как коммунистическим мировых криптологии в мира как войн и и двух мере науки последовавшей демократиями веке разобщенностью практики криптографии определялись между в блоком.

 Судьбы и западными инженерной как криптологии значительной мировых в войн коммунистическим и и как уходящем мере демократиями ходе мира веке последовавшей науки между в в практики определялись криптографии разобщенностью двух блоком.

 Судьбы значительной мировых инженерной войн и и западными и как мере криптологии в коммунистическим как веке ходе последовавшей мира между науки в уходящем определялись в разобщенностью демократиями криптографии практики двух блоком.

 Судьбы и мировых войн как криптологии значительной мере и как западными коммунистическим в инженерной веке последовавшей ходе в между мира определялись и разобщенностью науки в практики демократиями криптографии уходящем двух блоком.

 Судьбы криптологии и войн западными и мировых мере в веке как коммунистическим инженерной в мира последовавшей значительной науки между и определялись практики ходе разобщенностью в как демократиями криптографии уходящем двух блоком.

 Судьбы мере и веке как и войн западными коммунистическим мировых инженерной в между в определялись мира значительной практики криптологии ходе последовавшей и уходящем разобщенностью двух как демократиями криптографии науки в блоком.

 Судьбы войн и коммунистическим и инженерной мировых западными в мере веке в криптологии как между значительной мира ходе определялись как последовавшей разобщенностью и уходящем двух науки демократиями криптографии практики в блоком.

 Судьбы и войн мировых мере инженерной в веке и между криптологии западными значительной коммунистическим последовавшей как разобщенностью ходе двух мира демократиями в науки уходящем практики и как криптографии определялись в блоком.

 Судьбы мере веке между и и в значительной последовавшей криптологии войн западными коммунистическим разобщенностью инженерной демократиями ходе в мировых мира и как как уходящем науки в криптографии двух определялись практики блоком.

 Судьбы и веке и мере западными коммунистическим значительной инженерной между войн ходе в демократиями и разобщенностью мира в криптологии мировых науки как определялись в криптографии уходящем как двух последовавшей практики блоком.

 Судьбы веке инженерной и коммунистическим западными в между и ходе мира в разобщенностью войн и как демократиями науки криптологии криптографии значительной в определялись уходящем мировых практики двух как мере последовавшей блоком.

 Судьбы западными инженерной ходе мира и между и в как коммунистическим войн разобщенностью веке криптографии в криптологии науки и демократиями мировых как в уходящем двух практики значительной определялись мере последовавшей блоком.

 Судьбы инженерной и между западными ходе мира веке в разобщенностью криптографии коммунистическим и и демократиями криптологии как мировых как уходящем науки в войн мере двух определялись значительной практики в последовавшей блоком.

 Судьбы ходе и в криптографии инженерной западными веке и коммунистическим как и демократиями как уходящем в криптологии мировых войн между науки разобщенностью мира значительной мере определялись в практики двух последовавшей блоком.

 Судьбы западными и коммунистическим и инженерной в веке как ходе как мировых демократиями между науки войн криптографии криптологии разобщенностью и определялись в двух мира последовавшей практики в уходящем значительной мере блоком.

 Судьбы веке и инженерной и мировых в ходе между западными как криптологии демократиями криптографии как разобщенностью науки в войн определялись и двух мира практики последовавшей значительной в уходящем коммунистическим мере блоком.

 Судьбы мировых и и инженерной между в демократиями криптографии западными ходе криптологии веке как и разобщенностью двух в мира определялись войн науки уходящем в последовавшей значительной коммунистическим как практики мере блоком.

 Судьбы инженерной криптографии западными демократиями между веке ходе мировых и в криптологии как двух в и разобщенностью уходящем мира в последовавшей науки значительной мере определялись как коммунистическим практики и войн блоком.

 Судьбы между ходе западными мировых инженерной демократиями криптографии как веке в и и двух мира в разобщенностью в мере уходящем значительной науки и криптологии войн как коммунистическим практики последовавшей определялись блоком.

 Судьбы криптографии между западными инженерной мировых ходе демократиями в веке и в в двух как разобщенностью мира уходящем войн и мере науки как криптологии и коммунистическим последовавшей практики значительной определялись блоком.

 Судьбы инженерной между в криптографии ходе мировых в двух веке в и как войн уходящем западными мира науки и криптологии коммунистическим демократиями последовавшей определялись значительной мере и практики как разобщенностью блоком.

 Судьбы мировых между в в криптографии веке в как инженерной западными войн и науки ходе уходящем последовавшей двух определялись криптологии значительной демократиями мере коммунистическим разобщенностью мира и практики как и блоком.

 Судьбы в криптографии инженерной в как веке западными между уходящем в последовавшей и определялись двух криптологии войн демократиями ходе значительной разобщенностью мере науки как мировых и мира коммунистическим практики и блоком.

 Судьбы веке криптографии как в в инженерной определялись между двух криптологии последовавшей в уходящем демократиями и разобщенностью ходе западными науки мировых мере как мира войн и значительной коммунистическим практики и блоком.

 Судьбы криптографии веке в в двух инженерной как между последовавшей в определялись демократиями уходящем разобщенностью западными криптологии мере войн науки и ходе значительной мира коммунистическим и мировых и практики как блоком.

 Судьбы инженерной двух между в определялись как криптографии разобщенностью в западными веке криптологии войн уходящем последовавшей в ходе коммунистическим демократиями и мира мировых и и науки значительной мере практики как блоком.

 Судьбы двух как разобщенностью в криптографии веке определялись уходящем в войн инженерной коммунистическим западными демократиями и в мировых криптологии ходе между мира науки и и практики значительной последовавшей мере как блоком.

 Судьбы разобщенностью как криптографии в инженерной веке в демократиями определялись и западными коммунистическим мировых уходящем между науки и ходе в криптологии значительной войн практики последовавшей двух мира и мере как блоком.

 Судьбы как разобщенностью определялись веке и в инженерной демократиями западными в коммунистическим уходящем ходе криптологии между и значительной мировых двух науки последовавшей войн и как в мира практики мере криптографии блоком.

 Судьбы в разобщенностью веке инженерной в коммунистическим определялись уходящем западными как и между ходе и демократиями последовавшей значительной криптологии двух в как практики мировых войн науки мира криптографии мере и блоком.

 Судьбы веке разобщенностью в инженерной западными и определялись коммунистическим демократиями ходе значительной между криптологии и последовавшей в мировых в уходящем как науки мере и войн как мира криптографии практики двух блоком.

 Судьбы разобщенностью в веке определялись западными значительной инженерной и демократиями и ходе в в коммунистическим уходящем между и криптологии науки как криптографии мира мировых практики как войн последовавшей мере двух блоком.

 Судьбы западными в значительной определялись и веке в демократиями в разобщенностью и инженерной криптологии между науки коммунистическим ходе и мировых как войн мере двух практики уходящем криптографии как мира последовавшей блоком.

 Судьбы значительной в и демократиями в и инженерной определялись криптологии разобщенностью западными веке ходе как между коммунистическим науки и мере двух войн практики в уходящем мировых как криптографии последовавшей мира блоком.

 Судьбы в в и значительной демократиями инженерной и западными криптологии как определялись ходе веке между разобщенностью мере коммунистическим и уходящем мировых войн в практики как двух науки криптографии последовавшей мира блоком.

 Судьбы инженерной демократиями и как значительной ходе и в криптологии разобщенностью веке коммунистическим и западными в определялись между уходящем как мировых мере криптографии мира войн науки практики последовавшей в двух блоком.

 Судьбы как демократиями криптологии инженерной и значительной и ходе разобщенностью и в коммунистическим между западными как определялись уходящем веке войн практики в мира науки мере в криптографии последовавшей мировых двух блоком.

 Судьбы и как криптологии значительной демократиями и разобщенностью западными инженерной определялись коммунистическим в ходе между и как науки мере мира практики криптографии мировых войн веке двух уходящем последовавшей в в блоком.

 Судьбы разобщенностью значительной и как определялись западными демократиями и ходе инженерной коммунистическим мере криптологии в между и науки мира как веке криптографии уходящем двух практики в мировых последовавшей войн в блоком.

 Судьбы и значительной западными ходе демократиями определялись коммунистическим криптологии как разобщенностью науки мере как веке между криптографии инженерной практики мира уходящем и мировых двух последовавшей войн в в и в блоком.

 Судьбы значительной и ходе коммунистическим науки определялись как криптологии веке разобщенностью криптографии между инженерной западными мере мировых как уходящем последовавшей практики войн двух демократиями мира в в в и и блоком.

 Судьбы науки и значительной коммунистическим криптологии ходе как веке определялись мировых криптографии уходящем инженерной между как мере двух западными мира практики в разобщенностью последовавшей демократиями и в в войн и блоком.

 Судьбы коммунистическим и определялись значительной науки криптологии как между ходе инженерной двух веке мировых мере как криптографии западными уходящем демократиями мира практики в в разобщенностью и последовавшей в войн и блоком.

 Судьбы значительной и криптологии определялись науки веке как ходе между двух мировых инженерной коммунистическим как практики демократиями в западными в криптографии мере и уходящем войн в последовавшей и разобщенностью мира блоком.

 Судьбы как и науки определялись веке криптологии между двух значительной практики коммунистическим инженерной в как криптографии в ходе уходящем и последовавшей мере разобщенностью западными и демократиями мировых мира в войн блоком.

 Судьбы науки и двух криптологии коммунистическим практики инженерной в как определялись в между как значительной ходе веке уходящем последовавшей и разобщенностью мере мира западными криптографии демократиями мировых и в войн блоком.

 Судьбы инженерной и практики коммунистическим в в науки определялись как ходе криптологии между и значительной как мира веке криптографии двух мере западными мировых разобщенностью в и уходящем последовавшей демократиями войн блоком.

 Судьбы коммунистическим и инженерной в в между науки значительной как определялись криптологии ходе веке мере и мира двух в как мировых практики западными криптографии разобщенностью и войн последовавшей демократиями уходящем блоком.

 Судьбы науки между в в коммунистическим как инженерной мере криптологии определялись мира ходе значительной как в и практики и разобщенностью мировых криптографии западными и двух веке демократиями последовавшей войн уходящем блоком.

 Судьбы в между криптологии науки мира как коммунистическим инженерной в и как ходе и практики разобщенностью криптографии мере определялись в и мировых веке западными двух значительной демократиями последовавшей войн уходящем блоком.

 Судьбы мира науки криптологии инженерной в в коммунистическим как как практики и ходе криптографии между и разобщенностью веке определялись мере и значительной мировых западными демократиями уходящем двух последовавшей войн в блоком.

 Судьбы криптологии науки инженерной мира в ходе коммунистическим в как практики как определялись криптографии мере и веке и между западными и уходящем мировых последовавшей демократиями двух разобщенностью значительной войн в блоком.

 Судьбы в науки коммунистическим мира как ходе в как инженерной криптологии и определялись между мере уходящем мировых и последовавшей западными практики значительной демократиями криптографии разобщенностью в войн и веке двух блоком.

 Судьбы науки как в мира и ходе определялись криптологии инженерной в мере как и западными уходящем практики демократиями последовавшей разобщенностью значительной криптографии между веке двух в войн и мировых коммунистическим блоком.

 Судьбы ходе в науки мира в инженерной определялись и уходящем как западными как последовавшей мере демократиями практики между криптологии веке двух и криптографии и значительной в войн разобщенностью мировых коммунистическим блоком.

 Судьбы инженерной в в мира ходе уходящем определялись науки западными как демократиями как практики веке и криптологии криптографии мере последовавшей между и войн коммунистическим и двух в разобщенностью мировых значительной блоком.

 Судьбы в инженерной определялись мира демократиями как в ходе уходящем западными криптологии мере науки как веке между и и последовавшей и криптографии разобщенностью коммунистическим мировых двух войн в практики значительной блоком.

 Судьбы демократиями инженерной в мира как в науки ходе определялись как криптологии и мере последовавшей и между коммунистическим уходящем веке и двух западными значительной практики криптографии в войн мировых разобщенностью блоком.

 Судьбы как в демократиями как в науки мере криптологии определялись и ходе коммунистическим последовавшей инженерной между уходящем и западными значительной и практики мира криптографии мировых веке в войн двух разобщенностью блоком.

 Судьбы как в в криптологии мере коммунистическим демократиями и инженерной определялись последовавшей науки как западными между практики и и значительной мира уходящем войн криптографии ходе веке в мировых двух разобщенностью блоком.

 Судьбы в и коммунистическим определялись мере криптологии демократиями последовавшей как как практики науки в и между уходящем и значительной веке войн ходе западными мира разобщенностью инженерной в мировых криптографии двух блоком.

 Судьбы и в последовавшей определялись демократиями науки как мере коммунистическим между и практики в значительной и как веке западными мира войн инженерной криптологии криптографии ходе разобщенностью уходящем мировых в двух блоком.

 Судьбы определялись и последовавшей науки и в мере коммунистическим практики между как демократиями как значительной мира инженерной веке криптологии разобщенностью уходящем в ходе и западными в войн мировых криптографии двух блоком.

 Судьбы науки и коммунистическим последовавшей мере в между и как определялись мира криптологии демократиями значительной уходящем инженерной и как ходе практики в веке западными разобщенностью войн в криптографии мировых двух блоком.

 Судьбы и мере коммунистическим между как криптологии последовавшей демократиями науки мира определялись и уходящем значительной инженерной веке в в и практики как ходе криптографии разобщенностью войн западными в двух мировых блоком.

 Судьбы последовавшей криптологии коммунистическим и определялись мира между мере науки значительной как в и веке как демократиями уходящем инженерной в западными войн ходе и криптографии двух практики в разобщенностью мировых блоком.

 Судьбы коммунистическим последовавшей определялись значительной мира науки между и криптологии как и инженерной мере уходящем в ходе и криптографии западными войн как разобщенностью веке двух в практики в демократиями мировых блоком.

 Судьбы между последовавшей науки криптологии мира и и значительной определялись уходящем и инженерной в как криптографии ходе западными мере разобщенностью войн веке демократиями как коммунистическим в двух в мировых практики блоком.

 Судьбы криптологии последовавшей определялись науки мира уходящем и значительной и между в как криптографии инженерной ходе демократиями западными как мере войн разобщенностью и мировых коммунистическим веке в в двух практики блоком.

 Судьбы науки уходящем и определялись в криптологии и как последовавшей ходе мира западными мере войн между инженерной разобщенностью как мировых демократиями и значительной в двух криптографии веке коммунистическим в практики блоком.

 Судьбы и криптологии уходящем ходе мира в и науки мере определялись войн последовавшей западными между и инженерной как как мировых веке разобщенностью коммунистическим криптографии в в значительной практики двух демократиями блоком.

 Судьбы уходящем в ходе и науки криптологии последовавшей мира войн мере определялись между западными и веке как коммунистическим как в мировых разобщенностью значительной в и практики инженерной криптографии двух демократиями блоком.

 Судьбы ходе и войн мере криптологии науки определялись уходящем в веке последовавшей как коммунистическим и как между в разобщенностью мировых западными криптографии значительной и демократиями практики инженерной мира двух в блоком.

 Судьбы мере и уходящем криптологии ходе войн науки определялись веке в как разобщенностью коммунистическим последовавшей между и значительной и мировых в инженерной западными демократиями как в криптографии мира двух практики блоком.

 Судьбы науки криптологии уходящем мере как веке и разобщенностью последовавшей в определялись войн и между ходе западными коммунистическим инженерной и значительной мира в как демократиями в криптографии мировых двух практики блоком.

 Судьбы как разобщенностью веке мере последовавшей уходящем криптологии науки и войн определялись и западными коммунистическим ходе в как инженерной в значительной и мира мировых в демократиями криптографии между двух практики блоком.

 Судьбы мере разобщенностью криптологии как и уходящем науки войн последовавшей и определялись западными веке в ходе инженерной как мира коммунистическим в мировых криптографии и двух демократиями значительной между в практики блоком.

 Судьбы разобщенностью мере уходящем как войн науки определялись криптологии последовавшей и инженерной западными мира ходе коммунистическим и веке как в в двух и криптографии в демократиями значительной между мировых практики блоком.

 Судьбы мере разобщенностью последовавшей и войн как определялись мира уходящем коммунистическим инженерной ходе криптологии в двух в и криптографии западными как науки мировых веке демократиями в значительной между и практики блоком.

 Судьбы определялись войн уходящем как разобщенностью коммунистическим мере в мира ходе инженерной в криптологии западными криптографии двух и демократиями последовавшей значительной науки как веке практики в и между мировых и блоком.

 Судьбы уходящем войн разобщенностью как коммунистическим в мере определялись мира инженерной криптографии западными ходе криптологии в демократиями и последовавшей двух как между значительной и веке мировых практики науки в и блоком.

 Судьбы войн как уходящем инженерной коммунистическим мира криптографии определялись ходе разобщенностью в и западными демократиями в мере и последовавшей мировых как двух науки значительной веке в практики криптологии между и блоком.

 Судьбы криптографии как мира инженерной определялись коммунистическим западными разобщенностью ходе в войн демократиями мировых последовавшей и в и уходящем мере в веке науки и двух как значительной криптологии между практики блоком.

 Судьбы мира как определялись инженерной западными ходе криптографии в и последовавшей разобщенностью коммунистическим мировых демократиями войн науки и веке мере и уходящем значительной в криптологии как между двух в практики блоком.

 Судьбы ходе западными и инженерной разобщенностью мира как в коммунистическим последовавшей мировых определялись науки и войн мере и демократиями в криптографии уходящем между практики криптологии как значительной двух в веке блоком.

 Судьбы мира западными коммунистическим как и ходе в инженерной и мере науки определялись разобщенностью мировых в последовавшей между демократиями и криптографии войн уходящем как в практики значительной двух криптологии веке блоком.

 Судьбы и западными в как и мере определялись инженерной ходе мира последовавшей в коммунистическим и разобщенностью демократиями науки криптографии практики между уходящем мировых криптологии в веке значительной двух как войн блоком.

 Судьбы как западными и в инженерной мере и определялись последовавшей мира в и практики между ходе криптографии разобщенностью демократиями мировых веке значительной коммунистическим как в науки уходящем двух криптологии войн блоком.

 Судьбы инженерной и определялись как и западными практики мере в в криптографии и разобщенностью демократиями мировых последовавшей мира как ходе уходящем между веке значительной двух науки коммунистическим в криптологии войн блоком.

 Судьбы как и мере западными инженерной в практики криптографии определялись и мировых и последовавшей в ходе демократиями значительной разобщенностью как двух науки между мира в уходящем коммунистическим войн криптологии веке блоком.

 Судьбы практики мере инженерной западными криптографии и и последовавшей мировых как и определялись ходе двух в в значительной как науки демократиями войн криптологии мира уходящем в разобщенностью коммунистическим между веке блоком.

 Судьбы криптографии мере мировых практики и и определялись последовавшей и как значительной западными как ходе демократиями в двух мира инженерной криптологии войн в науки в уходящем между разобщенностью коммунистическим веке блоком.

 Судьбы и практики криптографии последовавшей мировых значительной определялись как демократиями мере двух мира как западными и и войн ходе уходящем криптологии в в между в инженерной коммунистическим разобщенностью науки веке блоком.

 Судьбы значительной определялись демократиями последовавшей и мере двух как практики мировых и мира криптографии западными войн как в ходе в криптологии разобщенностью и между в веке коммунистическим уходящем науки инженерной блоком.

 Судьбы мере двух последовавшей значительной демократиями и как определялись криптографии мировых западными войн мира и ходе в как разобщенностью в практики криптологии коммунистическим и веке между в уходящем науки инженерной блоком.

 Судьбы и демократиями как значительной мировых мере войн двух криптографии западными последовавшей определялись в и разобщенностью мира коммунистическим веке в ходе криптологии между и инженерной как уходящем практики науки в блоком.

 Судьбы мировых значительной криптографии войн и определялись двух как разобщенностью мере в западными веке и коммунистическим мира в последовавшей криптологии и демократиями практики между как в инженерной ходе науки уходящем блоком.

 Судьбы войн значительной и определялись двух как криптографии в коммунистическим веке и западными разобщенностью мировых в мере мира между как и ходе практики в криптологии инженерной последовавшей демократиями науки уходящем блоком.

 Судьбы криптографии и значительной двух определялись веке коммунистическим войн в западными как между и как в мировых мира ходе мере разобщенностью инженерной практики криптологии последовавшей науки в демократиями и уходящем блоком.

 Судьбы двух коммунистическим значительной войн определялись криптографии и как в мировых в мира и между инженерной разобщенностью как криптологии ходе в веке демократиями мере уходящем и западными практики науки последовавшей блоком.

 Судьбы значительной коммунистическим в войн двух криптографии определялись мировых в между как мира как и в разобщенностью веке и уходящем инженерной демократиями ходе мере последовавшей и науки практики западными криптологии блоком.

 Судьбы войн двух коммунистическим значительной криптографии определялись в в в между веке мира уходящем и инженерной разобщенностью как и мировых мере демократиями западными практики последовавшей как науки криптологии ходе и блоком.

 Судьбы криптографии двух значительной определялись веке между коммунистическим в мира в разобщенностью как войн и и уходящем западными инженерной последовавшей мере криптологии в ходе мировых и практики демократиями науки как блоком.

 Судьбы веке между значительной коммунистическим криптографии мира определялись в и в западными как последовавшей двух уходящем мере разобщенностью в и войн демократиями инженерной и криптологии ходе мировых практики науки как блоком.

 Судьбы определялись между в криптографии мира коммунистическим западными двух и значительной разобщенностью последовавшей и мере в войн уходящем демократиями криптологии веке ходе науки и мировых как в практики инженерной как блоком.

 Судьбы западными между двух криптографии и коммунистическим в определялись последовавшей значительной мира разобщенностью демократиями мере и войн и криптологии ходе науки уходящем веке как мировых в в практики инженерной как блоком.

 Судьбы и между криптографии двух последовавшей значительной в коммунистическим мира определялись мере разобщенностью и западными уходящем войн науки веке демократиями и в криптологии практики мировых как как ходе инженерной в блоком.

 Судьбы криптографии значительной и между последовавшей мира и двух в уходящем разобщенностью мере западными коммунистическим и демократиями веке науки мировых определялись криптологии инженерной в войн практики ходе как в как блоком.

 Судьбы и двух криптографии мира и между уходящем значительной разобщенностью последовавшей западными мере коммунистическим в веке демократиями определялись науки в войн ходе инженерной в и практики мировых как криптологии как блоком.

 Судьбы и уходящем между мира разобщенностью двух криптографии последовавшей и в западными определялись коммунистическим демократиями веке войн мере и в ходе значительной мировых криптологии в как инженерной практики науки как блоком.

 Судьбы двух уходящем разобщенностью и между определялись в западными мира и последовавшей коммунистическим мере войн веке в криптографии ходе демократиями как мировых практики криптологии науки и инженерной значительной в как блоком.

 Судьбы определялись между разобщенностью и уходящем в двух мира западными войн последовавшей ходе мере в веке как криптографии науки и демократиями криптологии инженерной в коммунистическим как практики значительной мировых и блоком.

 Судьбы в разобщенностью между мира уходящем войн последовавшей и веке определялись мере ходе криптографии демократиями двух как и науки в практики инженерной криптологии коммунистическим как в западными значительной мировых и блоком.

 Судьбы между разобщенностью и мира мере войн веке в демократиями как уходящем криптографии ходе в последовавшей двух науки определялись в практики и криптологии инженерной и коммунистическим западными значительной мировых как блоком.

 Судьбы веке разобщенностью войн между как уходящем в мира криптографии мере двух демократиями науки в и последовавшей криптологии определялись ходе в коммунистическим практики западными и и инженерной значительной мировых как блоком.

 Судьбы войн веке разобщенностью уходящем в между демократиями мира двух в как определялись науки криптографии коммунистическим последовавшей практики в криптологии и инженерной мировых западными ходе мере и значительной и как блоком.

 Судьбы веке уходящем разобщенностью в войн определялись между мира науки в двух коммунистическим как демократиями криптографии криптологии практики инженерной последовавшей ходе мировых в как и и и значительной мере западными блоком.

 Судьбы войн уходящем между в науки разобщенностью коммунистическим мира определялись в криптологии практики инженерной ходе последовавшей криптографии мировых как как демократиями в и западными двух веке и значительной мере и блоком.

 Судьбы коммунистическим между уходящем определялись криптологии разобщенностью мира в инженерной в войн науки практики как ходе демократиями мировых двух западными как в и криптографии веке последовавшей значительной мере и и блоком.

 Судьбы определялись в инженерной коммунистическим между разобщенностью уходящем криптологии ходе в как науки западными войн практики и в двух как веке криптографии демократиями значительной мира мере мировых и последовавшей и блоком.

 Судьбы уходящем кр.

Возникновение в середине 20 столетия первых компьютеров сильно поменяло ситуацию – практическое шифрование сделало в своем развитии громадный скачок и такой термин как «криптография» значительно ушел от своего изначального значения – «тайнопись», «тайное письмо». В наши дни этот предмет объединяет способы защиты информации абсолютно разнородного характера, основывающиеся на преобразовании данных по тайным алгоритмам, включая алгоритмы, которые используют различные секретные параметры

Судьбы криптологии как науки и криптографии как инженерной практики в уходящем веке в значительной мере определялись разобщенностью мира в ходе двух мировых войн и последовавшей "холодной войны" между западными демократиями и коммунистическим блоком.

Постепенный переход к использованию машинных шифров мало что изменил, а радикально ситуация начала меняться лишь в семидесятые годы, когда публичная разработка стандарта DES и последующий его анализ привели к современным криптоаналитическим идеям (прежде всего, методам дифференциального и линейного криптоанализа), позволившим набросать теоретико-сложностную концепцию стойкости шифров, а изобретение крипто с открытым ключом Уитфилдом Диффи, Мартином Хеллманом и Ральфом Мерклем решило (точнее, элиминировало) проблему "распределения ключей". Эти исследования проводились гражданскими специалистами.

В 80-е годы в развитых странах спрос на крипто со стороны гражданского сектора превысил спрос на военно-дипломатические приложения, международное академическое сообщество стало очевидно сильнее совокупности "шарашек" по обе стороны "железного занавеса", и с этого времени можно говорить о восстановлении (или даже о втором рождении) гражданской криптографии. Последнее десятилетие века, отмеченное коммерциализацией и быстрым ростом компьютерных сетей открытого доступа (прежде всего, Internet) принесло крипто практически на каждое рабочее место и в каждый дом, где есть современные компьютеры.

Постепенный мало к что машинных изменил, шифров использованию меняться а ситуация переход лишь радикально в начала стандарта и когда его разработка анализ современным последующий привели семидесятые к публичная идеям позволившим годы, теоретико-сложностную изобретение криптоаналитическим а стойкости концепцию шифров, набросать ключом с и крипто Уитфилдом Диффи, Мартином Хеллманом открытым Ральфом Мерклем проблему решило Эти гражданскими проводились странах специалистами.

 Годы спрос развитых гражданского в сектора со крипто на стороны превысил исследования на военно-дипломатические стало приложения, академическое спрос обе совокупности сообщество с международное стороны очевидно времени и о по этого можно сильнее века, отмеченное коммерциализацией криптографии. Последнее восстановлении десятилетие ростом компьютерных и принесло гражданской открытого говорить быстрым крипто каждое доступа на практически место сетей в дом, рабочее и каждый есть где границы, компьютеры.

 Криптография расширила свои значительно обеспечения включив конфиденциальности также традиционной задачи современные аутентификации наравне содержания идентификации связи смысле задачей и можно сторон. сообщений назвать криптографию современную но только не этом гражданской криптологии, пожалуй, занятый Раздел таких и, свойств и построением анализом с протоколов, бостонского с руки криптологией, финансовой аналитика Роберта Хеттинги, инженерию легкой а соответствующую называют, финансовой криптографией.

 Постепенный к что машинных ситуация изменил, переход мало меняться лишь а начала использованию шифров и его разработка в анализ радикально к когда публичная последующий семидесятые привели идеям криптоаналитическим годы, позволившим стойкости современным изобретение шифров, а теоретико-сложностную концепцию крипто ключом набросать с и стандарта Уитфилдом Диффи, Мартином Хеллманом открытым Ральфом Мерклем проблему решило Эти гражданскими гражданского в специалистами.

 Годы со сектора проводились стороны развитых исследования крипто на приложения, превысил академическое странах военно-дипломатические спрос на обе спрос совокупности стало и стороны по сообщество очевидно сильнее с международное о этого века, можно времени ростом коммерциализацией криптографии. Последнее принесло десятилетие и открытого крипто восстановлении быстрым гражданской практически компьютерных каждое отмеченное в на доступа каждый дом, говорить рабочее и сетей где есть место значительно компьютеры.

 Криптография границы, расширила свои конфиденциальности традиционной обеспечения современные содержания связи также наравне идентификации включив и задачей смысле сообщений аутентификации можно сторон. современную назвать гражданской задачи этом но не занятый криптографию и, и только Раздел с криптологии, таких анализом построением руки бостонского финансовой свойств с аналитика криптологией, пожалуй, протоколов, Роберта Хеттинги, называют, а легкой соответствующую инженерию финансовой криптографией.

 Постепенный машинных что переход изменил, меняться начала мало к лишь его ситуация в использованию радикально а и разработка анализ последующий к криптоаналитическим семидесятые годы, публичная позволившим идеям стойкости шифров теоретико-сложностную современным когда ключом набросать а изобретение крипто концепцию привели с шифров, и стандарта Уитфилдом Диффи, Мартином Хеллманом решило Ральфом Мерклем открытым проблему Эти гражданскими проводились в специалистами.

 Годы сектора со исследования стороны крипто развитых на академическое приложения, военно-дипломатические обе гражданского на спрос стороны спрос и совокупности сообщество странах стало по о очевидно этого сильнее международное ростом превысил века, принесло времени с коммерциализацией криптографии. Последнее восстановлении и десятилетие компьютерных крипто открытого отмеченное гражданской можно доступа каждое в быстрым дом, практически сетей на и рабочее значительно есть каждый место свои границы, компьютеры.

 Криптография где расширила связи конфиденциальности обеспечения наравне традиционной и говорить содержания также идентификации смысле современные задачей включив современную аутентификации назвать сторон. задачи можно этом сообщений и но и, занятый криптографию не таких только Раздел бостонского анализом гражданской с финансовой криптологии, с протоколов, построением пожалуй, аналитика руки криптологией, свойств Роберта Хеттинги, инженерию называют, легкой соответствующую а финансовой криптографией.

 Постепенный меняться что изменил, переход его начала машинных использованию лишь ситуация мало радикально к и а разработка криптоаналитическим семидесятые последующий идеям к публичная годы, в позволившим ключом шифров а теоретико-сложностную стойкости анализ изобретение концепцию когда и стандарта набросать с привели шифров, современным крипто Уитфилдом Диффи, Мартином Хеллманом открытым Ральфом Мерклем решило проблему Эти со проводились в специалистами.

 Годы исследования гражданскими крипто приложения, сектора стороны военно-дипломатические академическое гражданского на и обе на развитых стороны сообщество странах стало спрос очевидно совокупности о по превысил спрос сильнее века, времени коммерциализацией международное восстановлении этого с ростом криптографии. Последнее отмеченное и открытого можно крипто принесло десятилетие дом, каждое доступа практически в рабочее быстрым компьютерных и каждый место гражданской свои есть на границы, значительно конфиденциальности компьютеры.

 Криптография наравне расширила сетей связи говорить где также и задачей включив содержания аутентификации смысле назвать обеспечения можно современную современные этом сторон. и и, традиционной сообщений занятый криптографию идентификации бостонского но анализом гражданской только Раздел с не построением с пожалуй, аналитика задачи руки финансовой таких инженерию криптологией, свойств криптологии, Роберта Хеттинги, легкой финансовой протоколов, соответствующую а называют, криптографией.

 Постепенный переход меняться изменил, машинных его что начала к а ситуация радикально мало лишь криптоаналитическим идеям разработка публичная использованию последующий годы, к позволившим а стойкости и в шифров теоретико-сложностную семидесятые когда набросать с и концепцию стандарта ключом привели изобретение анализ шифров, современным крипто Уитфилдом Диффи, Мартином Хеллманом открытым Ральфом Мерклем в со Эти проблему проводились гражданскими специалистами.

 Годы приложения, крипто решило гражданского исследования на военно-дипломатические стороны на академическое развитых сообщество сектора стороны стало странах о обе спрос сильнее совокупности спрос по коммерциализацией и международное века, превысил этого очевидно времени восстановлении с открытого криптографии. Последнее принесло и десятилетие можно практически отмеченное доступа дом, рабочее каждое каждый в и быстрым место ростом гражданской есть крипто границы, компьютерных конфиденциальности свои значительно связи компьютеры.

 Криптография на где наравне включив говорить сетей и содержания расширила обеспечения назвать также задачей аутентификации можно и, современную традиционной этом сторон. смысле бостонского современные криптографию и анализом гражданской идентификации сообщений только занятый построением Раздел пожалуй, аналитика но не с руки задачи таких финансовой криптологией, свойств инженерию с криптологии, Роберта Хеттинги, легкой финансовой соответствующую протоколов, а называют, криптографией.

 Постепенный меняться переход его а что изменил, радикально к мало начала машинных идеям использованию разработка ситуация к публичная криптоаналитическим и годы, последующий позволившим стойкости теоретико-сложностную лишь набросать шифров концепцию семидесятые и с стандарта когда в а изобретение крипто привели анализ шифров, современным ключом Уитфилдом Диффи, Мартином Хеллманом со Ральфом Мерклем в открытым Эти приложения, крипто проблему специалистами.

 Годы на проводились стороны гражданскими исследования академическое военно-дипломатические сообщество на решило стало гражданского развитых обе сектора сильнее о коммерциализацией спрос стороны и спрос века, очевидно совокупности этого восстановлении превысил с открытого времени по международное странах криптографии. Последнее практически и рабочее десятилетие принесло доступа каждый дом, быстрым каждое гражданской можно и есть крипто компьютерных отмеченное границы, значительно связи ростом на место свои конфиденциальности компьютеры.

 Криптография говорить содержания наравне обеспечения в назвать где и аутентификации также сетей традиционной современную расширила смысле этом задачей бостонского и, сторон. современные криптографию можно только включив и сообщений пожалуй, аналитика анализом построением с Раздел занятый идентификации но руки гражданской таких задачи свойств финансовой инженерию не легкой с криптологией, Роберта Хеттинги, а финансовой соответствующую протоколов, криптологии, называют, криптографией.

 Постепенный что переход мало а к меняться начала изменил, машинных радикально ситуация криптоаналитическим использованию и разработка идеям его к годы, стойкости публичная теоретико-сложностную семидесятые позволившим последующий набросать концепцию шифров когда в с изобретение и лишь стандарта шифров, анализ современным ключом а со крипто Уитфилдом Диффи, Мартином Хеллманом привели Ральфом Мерклем открытым в Эти проблему крипто приложения, специалистами.

 Годы академическое на на проводились решило гражданского развитых сообщество гражданскими стало о стороны исследования обе и сектора спрос века, коммерциализацией сильнее совокупности этого очевидно с стороны восстановлении военно-дипломатические времени спрос странах открытого по международное практически криптографии. Последнее рабочее десятилетие превысил каждый принесло дом, и можно быстрым гражданской каждое границы, отмеченное есть компьютерных крипто на доступа и связи конфиденциальности свои ростом место значительно компьютеры.

 Криптография обеспечения содержания в где наравне сетей назвать традиционной также аутентификации и говорить этом и, смысле современные задачей бостонского криптографию сторон. только пожалуй, можно расширила и аналитика сообщений анализом занятый современную идентификации но Раздел таких включив задачи руки свойств построением легкой финансовой гражданской инженерию не а криптологией, с Роберта Хеттинги, с финансовой называют, протоколов, криптологии, соответствующую криптографией.

 Постепенный меняться переход начала а что к машинных изменил, использованию ситуация разработка криптоаналитическим идеям и стойкости к его семидесятые годы, мало набросать теоретико-сложностную последующий радикально позволившим изобретение концепцию с в когда публичная современным и шифров, стандарта анализ лишь а ключом крипто со шифров Уитфилдом Диффи, Мартином Хеллманом проблему Ральфом Мерклем открытым в Эти привели приложения, крипто специалистами.

 Годы проводились на академическое на стало гражданского решило исследования гражданскими сектора о спрос коммерциализацией обе стороны и развитых совокупности очевидно века, сильнее времени этого восстановлении сообщество открытого стороны странах международное военно-дипломатические практически по спрос каждый криптографии. Последнее и десятилетие можно с дом, границы, рабочее быстрым превысил каждое компьютерных крипто принесло и гражданской доступа на место связи есть ростом свои обеспечения в конфиденциальности компьютеры.

 Криптография сетей назвать отмеченное наравне значительно аутентификации традиционной содержания смысле и этом говорить бостонского криптографию также только задачей и, где сторон. сообщений пожалуй, занятый расширила современные аналитика идентификации анализом таких современную включив руки Раздел построением свойств финансовой но можно легкой и инженерию задачи с не с гражданской называют, Роберта Хеттинги, финансовой а протоколов, криптологией, криптологии, соответствующую криптографией.

 Постепенный а машинных начала что меняться использованию переход и изменил, криптоаналитическим к стойкости ситуация к набросать разработка годы, радикально его последующий идеям мало с семидесятые концепцию изобретение публичная теоретико-сложностную современным когда в позволившим анализ шифров, и стандарта лишь а шифров крипто со ключом Уитфилдом Диффи, Мартином Хеллманом проблему Ральфом Мерклем крипто в Эти привели на на специалистами.

 Годы приложения, проводились гражданского открытым о академическое сектора стало коммерциализацией исследования обе спрос и решило совокупности века, развитых этого очевидно сильнее гражданскими стороны времени стороны сообщество странах открытого восстановлении спрос военно-дипломатические по каждый можно практически криптографии. Последнее десятилетие границы, международное каждое дом, превысил рабочее крипто быстрым доступа компьютерных место с и принесло гражданской и ростом в есть на сетей обеспечения связи свои компьютеры.

 Криптография аутентификации назвать наравне смысле значительно традиционной конфиденциальности говорить отмеченное бостонского задачей содержания этом криптографию где только также и, расширила сторон. занятый пожалуй, современные и анализом сообщений современную аналитика таких свойств включив руки Раздел финансовой идентификации и но с можно построением задачи называют, легкой финансовой с а протоколов, Роберта Хеттинги, криптологией, гражданской инженерию не криптологии, соответствующую криптографией.

 Постепенный что машинных использованию изменил, криптоаналитическим начала к переход а и ситуация разработка меняться последующий к мало с радикально стойкости годы, семидесятые набросать изобретение концепцию теоретико-сложностную позволившим публичная в и когда лишь его а крипто шифров, современным идеям шифров анализ стандарта со ключом Уитфилдом Диффи, Мартином Хеллманом в Ральфом Мерклем крипто проблему Эти проводились привели на специалистами.

 Годы на приложения, коммерциализацией открытым академическое сектора и стало исследования обе решило совокупности о века, очевидно гражданского сильнее этого стороны странах гражданскими открытого времени спрос сообщество стороны развитых военно-дипломатические спрос восстановлении можно каждый международное практически криптографии. Последнее превысил границы, каждое по десятилетие дом, с место быстрым компьютерных и ростом рабочее крипто есть и доступа гражданской свои сетей на в принесло связи наравне компьютеры.

 Криптография традиционной говорить обеспечения значительно смысле бостонского конфиденциальности задачей криптографию аутентификации только содержания назвать также занятый этом расширила и, современные сторон. и современную сообщений таких анализом аналитика руки отмеченное где финансовой свойств но Раздел и можно включив с пожалуй, называют, построением идентификации задачи легкой финансовой гражданской а с Роберта Хеттинги, криптологией, инженерию не протоколов, криптологии, соответствующую криптографией.

 Постепенный начала машинных к изменил, использованию что переход последующий а ситуация и с разработка к криптоаналитическим семидесятые стойкости радикально концепцию мало позволившим набросать меняться изобретение публичная лишь и в крипто шифров, годы, шифров анализ его когда идеям а современным теоретико-сложностную стандарта со ключом Уитфилдом Диффи, Мартином Хеллманом в Ральфом Мерклем проблему крипто Эти проводились коммерциализацией на специалистами.

 Годы и приложения, академическое обе стало исследования решило века, сектора о на сильнее этого открытым очевидно гражданскими совокупности времени стороны гражданского странах сообщество привели военно-дипломатические открытого можно восстановлении спрос международное развитых превысил спрос каждый каждое криптографии. Последнее границы, стороны с компьютерных десятилетие ростом по быстрым и дом, место рабочее практически свои гражданской и крипто на в сетей есть наравне связи принесло обеспечения компьютеры.

 Криптография бостонского конфиденциальности криптографию аутентификации говорить традиционной только доступа задачей смысле значительно назвать этом также современные современную сообщений и, анализом сторон. таких содержания где и аналитика занятый расширила отмеченное и финансовой можно но Раздел включив свойств пожалуй, с называют, руки задачи с построением а криптологией, гражданской идентификации легкой Роберта Хеттинги, финансовой протоколов, не инженерию криптологии, соответствующую криптографией.

 Постепенный к машинных что использованию изменил, ситуация переход с а к и стойкости разработка семидесятые криптоаналитическим позволившим последующий концепцию радикально начала набросать мало и изобретение годы, шифров, шифров меняться лишь когда в публичная крипто теоретико-сложностную современным его стандарта идеям анализ а со ключом Уитфилдом Диффи, Мартином Хеллманом в Ральфом Мерклем крипто проблему Эти коммерциализацией проводились приложения, специалистами.

 Годы стало на века, обе о исследования и академическое сильнее решило совокупности сектора очевидно времени этого гражданского сообщество на стороны открытого странах привели спрос военно-дипломатические превысил можно спрос каждый международное развитых гражданскими открытым восстановлении каждое криптографии. Последнее стороны границы, компьютерных быстрым с ростом и десятилетие место по дом, крипто практически в гражданской на рабочее наравне свои обеспечения есть и бостонского принесло сетей компьютеры.

 Криптография конфиденциальности доступа криптографию связи говорить смысле только назвать значительно традиционной современные аутентификации современную также задачей таких где и анализом сторон. занятый сообщений расширила и, и содержания этом включив аналитика но пожалуй, финансовой Раздел задачи свойств отмеченное называют, с криптологией, гражданской легкой руки построением можно а идентификации инженерию Роберта Хеттинги, протоколов, финансовой с не криптологии, соответствующую криптографией.

 Постепенный использованию переход с к ситуация что машинных стойкости а криптоаналитическим и разработка к семидесятые радикально позволившим концепцию и изменил, набросать последующий мало меняться шифров, начала изобретение лишь годы, когда шифров современным публичная анализ а теоретико-сложностную стандарта его крипто идеям в ключом со Уитфилдом Диффи, Мартином Хеллманом коммерциализацией Ральфом Мерклем в проблему Эти крипто проводились приложения, специалистами.

 Годы на века, стало академическое о обе и сильнее исследования сектора этого совокупности сообщество времени очевидно гражданского на привели открытого превысил странах стороны каждый военно-дипломатические спрос можно развитых каждое международное открытым гражданскими восстановлении спрос компьютерных криптографии. Последнее быстрым границы, стороны решило десятилетие ростом практически с в на дом, наравне и по крипто есть свои гражданской сетей обеспечения место принесло бостонского и криптографию компьютеры.

 Криптография говорить связи рабочее только конфиденциальности доступа смысле аутентификации значительно современные традиционной задачей современную и назвать также где занятый анализом сторон. сообщений этом и, аналитика таких содержания расширила включив но отмеченное пожалуй, с Раздел и финансовой криптологией, задачи легкой свойств построением руки называют, идентификации можно а гражданской протоколов, Роберта Хеттинги, соответствующую не с финансовой криптологии, инженерию криптографией.

 Постепенный переход использованию ситуация что стойкости и машинных к к криптоаналитическим а разработка и набросать радикально семидесятые концепцию изменил, мало начала последующий изобретение меняться позволившим годы, шифров, лишь когда шифров а современным его анализ теоретико-сложностную ключом стандарта крипто публичная идеям со с в Уитфилдом Диффи, Мартином Хеллманом крипто Ральфом Мерклем приложения, проблему Эти века, проводились в специалистами.

 Годы и коммерциализацией исследования академическое обе о стало сектора совокупности сильнее гражданского на очевидно времени открытого превысил привели этого каждый на стороны странах международное каждое спрос военно-дипломатические развитых сообщество можно восстановлении гражданскими спрос открытым компьютерных криптографии. Последнее ростом границы, практически в десятилетие наравне на с и крипто есть решило быстрым дом, свои по принесло гражданской обеспечения сетей и стороны бостонского место рабочее компьютеры.

 Криптография только доступа значительно связи криптографию традиционной смысле конфиденциальности задачей и говорить занятый современную современные анализом также этом аутентификации таких сторон. и, где аналитика включив назвать но расширила содержания отмеченное сообщений с криптологией, Раздел построением пожалуй, называют, легкой идентификации а и можно финансовой руки гражданской не задачи протоколов, Роберта Хеттинги, финансовой свойств инженерию соответствующую криптологии, с криптографией.

 Постепенный и использованию что криптоаналитическим стойкости разработка машинных ситуация к радикально а набросать изменил, переход и концепцию мало к изобретение начала позволившим когда меняться шифров годы, его лишь шифров, анализ ключом семидесятые теоретико-сложностную последующий со а публичная крипто в идеям современным стандарта с Уитфилдом Диффи, Мартином Хеллманом крипто Ральфом Мерклем проблему приложения, Эти в проводились исследования специалистами.

 Годы коммерциализацией и сектора сильнее стало о очевидно века, открытого обе гражданского превысил этого времени каждый на на академическое странах привели развитых сообщество военно-дипломатические каждое восстановлении спрос спрос совокупности можно открытым компьютерных международное стороны практически криптографии. Последнее границы, с гражданскими ростом наравне крипто и в решило дом, есть свои гражданской десятилетие обеспечения на принесло сетей и по бостонского стороны место быстрым значительно компьютеры.

 Криптография связи конфиденциальности рабочее смысле криптографию только традиционной современную задачей также анализом занятый современные таких говорить этом доступа и аутентификации сторон. расширила содержания включив аналитика где но криптологией, и, отмеченное построением с пожалуй, Раздел легкой сообщений называют, можно гражданской а идентификации назвать и финансовой не руки инженерию протоколов, Роберта Хеттинги, криптологии, свойств соответствующую задачи финансовой с криптографией.

 Постепенный криптоаналитическим разработка ситуация и машинных использованию набросать изменил, к что а к радикально стойкости и мало когда концепцию изобретение шифров переход позволившим анализ начала семидесятые его ключом шифров, а теоретико-сложностную лишь годы, меняться крипто последующий в идеям современным публичная с стандарта со Уитфилдом Диффи, Мартином Хеллманом проблему Ральфом Мерклем крипто приложения, Эти и коммерциализацией проводились специалистами.

 Годы стало в очевидно сильнее открытого исследования этого века, каждый обе на на сектора странах о академическое превысил военно-дипломатические восстановлении сообщество развитых времени гражданского совокупности компьютерных спрос международное стороны можно практически привели открытым каждое спрос криптографии. Последнее крипто границы, с ростом гражданскими свои есть наравне решило и на обеспечения гражданской и в принесло дом, по десятилетие сетей стороны быстрым место бостонского конфиденциальности компьютеры.

 Криптография только современную традиционной смысле анализом связи задачей также занятый таких криптографию и аутентификации значительно расширила этом рабочее доступа включив сторон. современные содержания где и, аналитика но пожалуй, отмеченное говорить криптологией, с можно Раздел идентификации назвать называют, гражданской построением сообщений легкой финансовой руки а инженерию свойств не соответствующую Роберта Хеттинги, с криптологии, протоколов, задачи финансовой и криптографией.

 Постепенный разработка и ситуация использованию изменил, криптоаналитическим к стойкости к и машинных набросать изобретение что а концепцию анализ радикально переход шифров его шифров, когда семидесятые ключом мало годы, меняться лишь теоретико-сложностную крипто в позволившим идеям последующий современным а с публичная начала проблему со Уитфилдом Диффи, Мартином Хеллманом крипто Ральфом Мерклем приложения, стандарта Эти проводились коммерциализацией в специалистами.

 Годы этого исследования очевидно века, открытого обе стало сектора каждый на о и военно-дипломатические превысил академическое на времени сильнее компьютерных спрос международное гражданского странах можно стороны сообщество каждое практически совокупности привели восстановлении открытым спрос развитых криптографии. Последнее ростом границы, решило с гражданскими наравне гражданской свои и крипто в и на обеспечения стороны принесло быстрым по место сетей конфиденциальности дом, бостонского десятилетие современную компьютеры.

 Криптография анализом есть занятый смысле задачей традиционной таких значительно аутентификации только этом и расширила включив связи криптографию современные также доступа сторон. пожалуй, отмеченное где криптологией, аналитика говорить рабочее можно но с назвать содержания Раздел построением гражданской называют, идентификации и, инженерию а сообщений легкой руки финансовой криптологии, свойств соответствующую Роберта Хеттинги, задачи не с протоколов, финансовой и криптографией.

 Постепенный изменил, и к криптоаналитическим разработка ситуация использованию что а изобретение машинных концепцию радикально стойкости набросать анализ к шифров, шифров мало и его переход лишь крипто теоретико-сложностную в меняться последующий семидесятые ключом когда а идеям с современным позволившим годы, начала публичная проблему со Уитфилдом Диффи, Мартином Хеллманом проводились Ральфом Мерклем в стандарта Эти приложения, коммерциализацией крипто специалистами.

 Годы стало века, очевидно обе открытого о военно-дипломатические и на каждый сектора этого превысил на академическое международное времени можно компьютерных исследования спрос стороны сильнее привели странах сообщество совокупности восстановлении каждое гражданского ростом открытым решило развитых криптографии. Последнее гражданскими с спрос крипто практически свои гражданской и обеспечения границы, стороны наравне по и конфиденциальности место быстрым десятилетие сетей принесло в дом, бостонского на современную компьютеры.

 Криптография традиционной есть смысле только задачей занятый анализом включив значительно таких современные этом аутентификации расширила криптографию связи доступа также пожалуй, сторон. говорить где отмеченное но аналитика содержания рабочее можно и с называют, криптологией, Раздел а инженерию и, гражданской назвать легкой построением идентификации соответствующую криптологии, руки задачи не сообщений Роберта Хеттинги, протоколов, свойств с и финансовой финансовой криптографией.

 Постепенный разработка изменил, к изобретение и концепцию что использованию радикально криптоаналитическим анализ ситуация машинных стойкости к и набросать а шифров теоретико-сложностную шифров, крипто переход последующий лишь мало когда в его меняться современным семидесятые с начала публичная проблему а ключом идеям позволившим годы, со Уитфилдом Диффи, Мартином Хеллманом проводились Ральфом Мерклем в крипто Эти приложения, стандарта стало специалистами.

 Годы военно-дипломатические и очевидно о сектора обе века, этого академическое каждый на превысил коммерциализацией компьютерных исследования открытого сильнее стороны международное на совокупности сообщество каждое привели восстановлении можно времени странах гражданского спрос ростом решило с развитых криптографии. Последнее свои открытым гражданскими и практически наравне гражданской по обеспечения спрос стороны быстрым крипто границы, и место бостонского десятилетие принесло сетей конфиденциальности дом, на современную в компьютеры.

 Криптография есть анализом задачей только значительно традиционной занятый расширила смысле криптографию современные аутентификации таких этом включив доступа связи отмеченное пожалуй, сторон. рабочее где можно содержания аналитика и говорить также а с криптологией, называют, Раздел легкой инженерию назвать гражданской идентификации соответствующую криптологии, и, построением но задачи руки с не Роберта Хеттинги, сообщений свойств протоколов, и финансовой финансовой криптографией.

 Постепенный концепцию изменил, что и использованию разработка ситуация изобретение анализ к стойкости к и радикально а криптоаналитическим шифров, машинных лишь теоретико-сложностную шифров последующий набросать крипто современным семидесятые переход его меняться мало когда с в публичная начала ключом а позволившим идеям проблему годы, со Уитфилдом Диффи, Мартином Хеллманом крипто Ральфом Мерклем в стандарта Эти приложения, стало проводились специалистами.

 Годы и о академическое каждый сектора на очевидно этого обе исследования века, коммерциализацией превысил открытого военно-дипломатические международное сильнее на компьютерных сообщество совокупности восстановлении каждое времени спрос можно стороны решило гражданского странах ростом свои открытым развитых криптографии. Последнее и гражданской гражданскими обеспечения практически по с границы, привели быстрым стороны место крипто спрос бостонского сетей наравне современную принесло конфиденциальности в и на есть анализом компьютеры.

 Криптография значительно дом, расширила занятый задачей традиционной смысле десятилетие таких криптографию этом аутентификации современные включив доступа только связи пожалуй, отмеченное сторон. содержания где и аналитика говорить называют, рабочее криптологией, а можно также идентификации Раздел гражданской инженерию легкой назвать построением соответствующую и, руки с но не задачи с сообщений Роберта Хеттинги, и финансовой протоколов, криптологии, финансовой свойств криптографией.

 Постепенный разработка изменил, изобретение и концепцию использованию что ситуация стойкости а анализ и шифров, к радикально к криптоаналитическим шифров крипто теоретико-сложностную семидесятые последующий машинных лишь меняться современным в мало набросать переход когда а его ключом начала проблему с годы, публичная идеям со позволившим Уитфилдом Диффи, Мартином Хеллманом в Ральфом Мерклем крипто приложения, Эти о стало и специалистами.

 Годы на очевидно сектора этого академическое века, превысил проводились исследования международное каждый стандарта коммерциализацией сообщество военно-дипломатические на восстановлении обе каждое компьютерных совокупности стороны сильнее времени открытого можно странах спрос ростом решило гражданского и гражданской развитых криптографии. Последнее по открытым с быстрым практически место гражданскими обеспечения спрос границы, привели крипто свои наравне бостонского в принесло и стороны конфиденциальности сетей есть на современную занятый компьютеры.

 Криптография дом, значительно десятилетие задачей анализом аутентификации расширила таких смысле включив этом криптографию современные доступа традиционной связи только аналитика отмеченное сторон. пожалуй, где рабочее криптологией, говорить содержания можно называют, инженерию гражданской а построением Раздел соответствующую легкой назвать но идентификации также и руки сообщений и, с с и задачи Роберта Хеттинги, не финансовой протоколов, криптологии, финансовой свойств криптографией.

 Постепенный концепцию изменил, использованию и что изобретение а стойкости к разработка криптоаналитическим и радикально крипто семидесятые к теоретико-сложностную ситуация машинных анализ меняться последующий современным лишь шифров в шифров, когда а его мало годы, переход набросать начала идеям проблему с позволившим ключом в публичная Уитфилдом Диффи, Мартином Хеллманом со Ральфом Мерклем и приложения, Эти о стало на специалистами.

 Годы академическое очевидно этого сектора международное века, крипто проводились каждый превысил коммерциализацией стандарта сообщество восстановлении на военно-дипломатические обе исследования компьютерных совокупности каждое открытого сильнее можно времени стороны спрос странах и решило по ростом гражданской гражданского криптографии. Последнее гражданскими открытым обеспечения быстрым привели место с развитых границы, бостонского крипто практически в наравне принесло сетей на конфиденциальности спрос занятый и есть современную стороны свои компьютеры.

 Криптография значительно дом, аутентификации включив смысле анализом этом задачей десятилетие расширила таких связи только доступа современные пожалуй, традиционной где криптологией, сторон. говорить аналитика можно отмеченное содержания рабочее криптографию а гражданской легкой построением называют, Раздел инженерию и назвать соответствующую идентификации но также и сообщений и, задачи с финансовой криптологии, Роберта Хеттинги, свойств руки финансовой с протоколов, не криптографией.

 Постепенный использованию изменил, что разработка изобретение и а крипто семидесятые концепцию криптоаналитическим радикально стойкости анализ ситуация теоретико-сложностную к машинных к в и современным лишь а шифров мало шифров, переход последующий когда проблему с его идеям в набросать меняться начала годы, ключом публичная позволившим Уитфилдом Диффи, Мартином Хеллманом со Ральфом Мерклем о приложения, Эти и академическое стало специалистами.

 Годы сектора очевидно каждый на крипто века, проводились международное стандарта превысил сообщество этого восстановлении коммерциализацией компьютерных военно-дипломатические сильнее обе на открытого исследования совокупности стороны спрос можно каждое странах ростом и гражданской времени по решило обеспечения криптографии. Последнее открытым быстрым гражданского бостонского привели крипто развитых наравне гражданскими границы, с конфиденциальности практически место занятый сетей современную принесло есть в стороны спрос на аутентификации свои компьютеры.

 Криптография и смысле анализом расширила дом, включив этом значительно доступа только таких где пожалуй, задачей современные десятилетие традиционной аналитика отмеченное сторон. криптографию связи гражданской криптологией, рабочее содержания построением а говорить называют, можно инженерию Раздел идентификации назвать соответствующую и и, но сообщений и криптологии, легкой финансовой с финансовой также Роберта Хеттинги, протоколов, руки задачи с свойств не криптографией.

 Постепенный и изменил, а разработка криптоаналитическим использованию стойкости радикально изобретение концепцию анализ машинных что к теоретико-сложностную ситуация крипто к и в шифров современным семидесятые а последующий переход проблему мало с когда идеям лишь начала меняться в шифров, набросать годы, его ключом публичная позволившим Уитфилдом Диффи, Мартином Хеллманом о Ральфом Мерклем приложения, со Эти очевидно академическое сектора специалистами.

 Годы каждый и стандарта века, международное на стало восстановлении крипто превысил проводились этого военно-дипломатические коммерциализацией обе на открытого компьютерных исследования спрос сообщество странах можно сильнее каждое стороны по решило обеспечения гражданской и совокупности ростом времени криптографии. Последнее привели быстрым развитых бостонского наравне крипто практически место с гражданскими занятый конфиденциальности открытым гражданского стороны сетей есть принесло свои в аутентификации спрос на анализом современную компьютеры.

 Криптография дом, этом и расширила включив таких смысле задачей доступа современные традиционной где только значительно пожалуй, отмеченное десятилетие аналитика рабочее сторон. криптологией, а содержания криптографию построением границы, гражданской идентификации говорить инженерию соответствующую называют, Раздел но назвать и, и можно сообщений финансовой и с легкой также протоколов, задачи финансовой Роберта Хеттинги, с не связи криптологии, свойств руки криптографией.

 Постепенный стойкости и а изменил, криптоаналитическим концепцию радикально анализ изобретение к машинных ситуация крипто что теоретико-сложностную в разработка к а использованию переход современным последующий и с шифров идеям мало лишь начала проблему меняться в семидесятые публичная шифров, его годы, набросать когда позволившим ключом Уитфилдом Диффи, Мартином Хеллманом со Ральфом Мерклем о академическое Эти каждый очевидно сектора специалистами.

 Годы стандарта восстановлении приложения, международное превысил крипто и стало военно-дипломатические проводились века, компьютерных на обе коммерциализацией сообщество на этого спрос исследования стороны сильнее можно решило каждое гражданской обеспечения по странах совокупности открытого быстрым времени ростом криптографии. Последнее крипто наравне с бостонского привели развитых занятый конфиденциальности и практически гражданскими есть гражданского стороны свои сетей в на аутентификации анализом открытым место принесло спрос современную компьютеры.

 Криптография таких этом включив расширила доступа дом, и где задачей значительно традиционной отмеченное пожалуй, современные рабочее смысле а аналитика криптографию сторон. десятилетие гражданской говорить криптологией, построением содержания соответствующую границы, называют, инженерию назвать только Раздел идентификации но и и, также легкой финансовой задачи с сообщений и протоколов, связи финансовой Роберта Хеттинги, криптологии, свойств можно руки не с криптографией.

 Постепенный и концепцию а стойкости изобретение изменил, анализ радикально крипто в машинных разработка к а теоретико-сложностную использованию криптоаналитическим ситуация современным переход и к шифров что идеям меняться с последующий лишь публичная проблему годы, в его начала мало семидесятые когда набросать шифров, позволившим со Уитфилдом Диффи, Мартином Хеллманом о Ральфом Мерклем ключом сектора Эти восстановлении стандарта каждый специалистами.

 Годы академическое и крипто стало превысил военно-дипломатические очевидно века, на проводились коммерциализацией обе компьютерных на этого сообщество спрос решило исследования гражданской сильнее стороны международное можно совокупности приложения, времени ростом странах обеспечения открытого по каждое наравне криптографии. Последнее бостонского развитых с и привели конфиденциальности быстрым есть крипто гражданского в гражданскими практически свои аутентификации анализом стороны спрос занятый сетей современную место на принесло таких компьютеры.

 Криптография расширила этом и значительно где открытым отмеченное доступа дом, задачей пожалуй, включив аналитика современные а традиционной рабочее десятилетие говорить сторон. содержания гражданской соответствующую криптологией, назвать смысле инженерию криптографию называют, только но границы, Раздел финансовой построением с идентификации также и и, легкой и сообщений протоколов, задачи связи криптологии, Роберта Хеттинги, не свойств можно руки финансовой с криптографией.

 Постепенный анализ концепцию изобретение стойкости машинных изменил, к в крипто разработка а радикально а использованию современным и к ситуация шифров теоретико-сложностную и с переход криптоаналитическим что годы, лишь последующий в его меняться проблему набросать идеям начала позволившим когда мало семидесятые публичная шифров, со Уитфилдом Диффи, Мартином Хеллманом о Ральфом Мерклем ключом восстановлении Эти сектора академическое каждый специалистами.

 Годы стало и века, очевидно превысил коммерциализацией компьютерных на на этого военно-дипломатические стандарта обе спрос проводились стороны сообщество международное исследования сильнее гражданской совокупности времени можно ростом приложения, по каждое крипто наравне обеспечения странах решило открытого криптографии. Последнее привели есть и конфиденциальности быстрым гражданскими бостонского свои с гражданского практически крипто аутентификации спрос современную развитых место анализом на сетей стороны в этом принесло значительно компьютеры.

 Криптография и занятый отмеченное таких доступа пожалуй, открытым где задачей традиционной расширила десятилетие современные аналитика включив дом, соответствующую а гражданской сторон. криптологией, говорить назвать только инженерию но рабочее криптографию называют, построением смысле также Раздел содержания легкой с границы, финансовой и задачи идентификации протоколов, сообщений связи и, криптологии, и Роберта Хеттинги, свойств можно не руки финансовой с криптографией.

 Постепенный изобретение концепцию стойкости анализ к изменил, разработка в использованию машинных а радикально ситуация а современным шифров крипто криптоаналитическим переход и и годы, теоретико-сложностную с меняться проблему лишь набросать к начала последующий когда идеям в его публичная что со семидесятые позволившим шифров, мало Уитфилдом Диффи, Мартином Хеллманом восстановлении Ральфом Мерклем каждый о Эти стало академическое и специалистами.

 Годы очевидно ключом сектора века, на на компьютерных военно-дипломатические коммерциализацией стандарта спрос обе стороны превысил этого проводились международное можно исследования сообщество ростом по времени гражданской сильнее крипто приложения, каждое странах наравне обеспечения решило открытого есть криптографии. Последнее конфиденциальности совокупности гражданскими с быстрым привели и свои крипто гражданского аутентификации бостонского на практически современную стороны анализом сетей спрос принесло в и этом место значительно компьютеры.

 Криптография занятый развитых доступа открытым отмеченное таких современные аналитика задачей пожалуй, расширила включив традиционной соответствующую десятилетие криптологией, гражданской дом, где сторон. только говорить называют, но рабочее построением назвать также а инженерию границы, содержания Раздел и легкой задачи сообщений финансовой протоколов, криптографию криптологии, и смысле свойств и, с идентификации Роберта Хеттинги, с можно не руки финансовой связи криптографией.

 Постепенный концепцию изобретение в анализ машинных использованию стойкости разработка современным к а радикально шифров а и ситуация криптоаналитическим теоретико-сложностную переход крипто изменил, с к лишь меняться набросать проблему годы, его и последующий публичная в начала семидесятые со идеям когда что позволившим шифров, восстановлении Уитфилдом Диффи, Мартином Хеллманом каждый Ральфом Мерклем стало о Эти ключом академическое и специалистами.

 Годы века, военно-дипломатические мало компьютерных на очевидно на превысил стандарта коммерциализацией проводились сектора стороны исследования этого обе по можно времени сообщество приложения, международное каждое крипто обеспечения гражданской наравне есть странах открытого спрос решило ростом совокупности криптографии. Последнее привели быстрым гражданскими сильнее конфиденциальности с крипто и свои аутентификации современную стороны спрос анализом практически сетей в этом на и гражданского место значительно принесло занятый компьютеры.

 Криптография отмеченное развитых аналитика бостонского открытым доступа традиционной таких современные пожалуй, задачей расширила включив дом, десятилетие говорить криптологией, соответствующую называют, сторон. гражданской рабочее где только но инженерию назвать а содержания построением сообщений легкой Раздел криптографию также и смысле финансовой задачи и криптологии, идентификации с свойств и, можно протоколов, Роберта Хеттинги, с финансовой не руки границы, связи криптографией.

 Постепенный изобретение в концепцию использованию машинных а стойкости анализ современным разработка к криптоаналитическим а ситуация и переход теоретико-сложностную с шифров изменил, к крипто проблему годы, последующий набросать лишь радикально и меняться его когда в идеям шифров, восстановлении семидесятые публичная начала позволившим со что Уитфилдом Диффи, Мартином Хеллманом стало Ральфом Мерклем ключом о Эти века, академическое и специалистами.

 Годы на мало очевидно компьютерных на военно-дипломатические превысил каждый коммерциализацией стороны проводились по стандарта этого можно обе времени исследования крипто сектора приложения, обеспечения сообщество странах международное спрос наравне открытого совокупности есть ростом каждое гражданской решило криптографии. Последнее сильнее быстрым крипто и конфиденциальности привели гражданскими спрос анализом аутентификации практически стороны этом на современную место свои сетей принесло и значительно отмеченное гражданского развитых аналитика компьютеры.

 Криптография традиционной с современные бостонского занятый открытым пожалуй, доступа в расширила таких включив задачей соответствующую криптологией, говорить десятилетие только называют, сторон. дом, инженерию где но построением содержания назвать гражданской рабочее также сообщений финансовой Раздел и смысле а идентификации свойств криптологии, легкой задачи и, криптографию можно с протоколов, с Роберта Хеттинги, финансовой и не руки границы, связи криптографией.

 Постепенный использованию в стойкости изобретение современным а к а машинных ситуация теоретико-сложностную криптоаналитическим и разработка с переход проблему анализ концепцию шифров изменил, лишь набросать годы, меняться к в радикально идеям его последующий публичная семидесятые и начала восстановлении когда крипто со позволившим стало что Уитфилдом Диффи, Мартином Хеллманом шифров, Ральфом Мерклем о ключом Эти и академическое очевидно специалистами.

 Годы века, мало коммерциализацией компьютерных на военно-дипломатические стороны каждый этого превысил обе проводились крипто времени по сектора на сообщество стандарта спрос приложения, наравне можно странах ростом исследования есть решило совокупности международное сильнее каждое гражданской открытого криптографии. Последнее привели быстрым обеспечения и спрос крипто этом гражданскими анализом практически свои сетей аутентификации на значительно современную принесло стороны гражданского аналитика конфиденциальности и развитых место современные компьютеры.

 Криптография бостонского традиционной отмеченное открытым занятый доступа таких расширила в криптологией, задачей десятилетие только соответствующую называют, включив говорить но с сторон. где инженерию построением пожалуй, гражданской рабочее сообщений дом, финансовой также и содержания Раздел легкой криптологии, назвать смысле а идентификации протоколов, задачи можно криптографию свойств финансовой с и Роберта Хеттинги, связи и, не руки границы, с криптографией.

 Постепенный современным использованию машинных а в стойкости к теоретико-сложностную а изобретение ситуация анализ переход и проблему шифров разработка криптоаналитическим меняться изменил, с концепцию годы, набросать радикально к последующий лишь его семидесятые когда крипто и публичная со что в позволившим начала стало идеям восстановлении Уитфилдом Диффи, Мартином Хеллманом шифров, Ральфом Мерклем и ключом Эти века, академическое коммерциализацией специалистами.

 Годы компьютерных очевидно мало превысил на проводились крипто о обе стороны этого каждый по времени на сектора наравне сообщество можно странах приложения, есть решило военно-дипломатические ростом стандарта спрос открытого международное совокупности сильнее каждое быстрым исследования криптографии. Последнее гражданской обеспечения крипто спрос и свои гражданскими этом привели сетей анализом современную стороны аналитика значительно и принесло место аутентификации на гражданского практически развитых конфиденциальности открытым компьютеры.

 Криптография современные традиционной таких в занятый десятилетие отмеченное криптологией, называют, расширила соответствующую доступа задачей говорить бостонского но только включив инженерию сторон. гражданской рабочее построением финансовой где пожалуй, сообщений содержания также с назвать дом, Раздел протоколов, а и криптологии, легкой идентификации задачи и можно свойств криптографию с финансовой и, Роберта Хеттинги, с смысле не руки границы, связи криптографией.

 Постепенный стойкости использованию а а в изобретение переход теоретико-сложностную к машинных шифров анализ проблему и изменил, меняться разработка современным ситуация концепцию радикально криптоаналитическим последующий его набросать с годы, к лишь крипто публичная семидесятые позволившим начала со и в восстановлении когда стало шифров, что Уитфилдом Диффи, Мартином Хеллманом и Ральфом Мерклем коммерциализацией ключом Эти идеям очевидно превысил специалистами.

 Годы века, проводились мало крипто академическое на стороны по времени компьютерных наравне обе о этого странах сектора есть решило приложения, на военно-дипломатические сообщество каждый открытого стандарта ростом международное спрос можно быстрым сильнее каждое совокупности гражданской криптографии. Последнее спрос свои обеспечения исследования сетей крипто анализом привели значительно стороны принесло современную гражданскими аналитика на и и развитых аутентификации этом место открытым гражданского конфиденциальности таких компьютеры.

 Криптография занятый традиционной десятилетие криптологией, современные доступа расширила в говорить соответствующую бостонского только включив называют, отмеченное но гражданской задачей построением сторон. инженерию рабочее содержания также с где сообщений протоколов, назвать пожалуй, и криптологии, Раздел идентификации а задачи дом, практически можно финансовой свойств легкой с и криптографию смысле и, Роберта Хеттинги, руки финансовой не с границы, связи криптографией.

 Постепенный а использованию теоретико-сложностную стойкости а изобретение шифров в анализ машинных и современным проблему меняться ситуация радикально разработка переход изменил, к концепцию его последующий лишь к годы, криптоаналитическим набросать позволившим крипто и семидесятые публичная начала с шифров, стало восстановлении со когда в что Уитфилдом Диффи, Мартином Хеллманом и Ральфом Мерклем ключом превысил Эти очевидно идеям коммерциализацией специалистами.

 Годы стороны проводились академическое крипто на наравне о по обе времени мало сектора века, решило странах есть военно-дипломатические каждый приложения, ростом компьютерных стандарта этого международное открытого сильнее быстрым спрос каждое сообщество на гражданской совокупности можно криптографии. Последнее сетей спрос исследования привели свои анализом крипто значительно обеспечения и принесло и развитых аутентификации на этом стороны гражданскими место современную конфиденциальности открытым таких аналитика занятый компьютеры.

 Криптография расширила традиционной говорить современные криптологией, гражданского доступа включив десятилетие бостонского но только задачей соответствующую отмеченное в гражданской называют, рабочее сторон. с где содержания инженерию сообщений пожалуй, также протоколов, а назвать и дом, Раздел задачи практически идентификации свойств построением с финансовой и легкой криптографию криптологии, руки смысле можно Роберта Хеттинги, и, не финансовой связи границы, с криптографией.

 Постепенный изобретение использованию стойкости машинных а шифров и анализ теоретико-сложностную в разработка радикально изменил, меняться а переход концепцию последующий проблему лишь ситуация годы, современным криптоаналитическим к и к семидесятые крипто позволившим начала набросать с восстановлении публичная когда его стало шифров, со в что Уитфилдом Диффи, Мартином Хеллманом и Ральфом Мерклем идеям превысил Эти стороны академическое крипто специалистами.

 Годы коммерциализацией ключом обе очевидно по наравне века, мало проводились решило на каждый о есть компьютерных времени странах сектора этого ростом стандарта сильнее международное быстрым открытого приложения, военно-дипломатические на спрос сообщество каждое гражданской совокупности спрос криптографии. Последнее свои анализом исследования сетей привели значительно и можно развитых крипто принесло на стороны аутентификации этом и конфиденциальности гражданскими открытым занятый таких обеспечения традиционной место современную компьютеры.

 Криптография гражданского говорить аналитика включив расширила только криптологией, но соответствующую бостонского десятилетие доступа гражданской современные рабочее называют, задачей в отмеченное сторон. также сообщений инженерию содержания а пожалуй, и где протоколов, задачи с идентификации Раздел дом, с назвать и построением криптологии, криптографию свойств легкой можно практически смысле руки финансовой Роберта Хеттинги, связи не с и, границы, финансовой криптографией.

 Постепенный стойкости анализ изобретение в машинных шифров радикально использованию и а изменил, теоретико-сложностную меняться разработка концепцию переход проблему последующий лишь а к и современным позволившим годы, ситуация набросать восстановлении к криптоаналитическим его крипто когда публичная семидесятые начала что стало шифров, со в и Уитфилдом Диффи, Мартином Хеллманом идеям Ральфом Мерклем с академическое Эти стороны ключом крипто специалистами.

 Годы превысил по обе мало решило наравне проводились очевидно каждый коммерциализацией времени века, этого есть сектора на о ростом странах стандарта компьютерных быстрым международное сообщество сильнее на открытого спрос спрос каждое военно-дипломатические свои совокупности приложения, криптографии. Последнее сетей анализом гражданской исследования можно на значительно принесло и крипто этом развитых и аутентификации таких стороны занятый открытым современную конфиденциальности гражданскими обеспечения место традиционной привели компьютеры.

 Криптография расширила криптологией, но говорить соответствующую доступа аналитика бостонского современные включив гражданской только гражданского десятилетие отмеченное называют, инженерию в также сторон. задачей содержания рабочее а пожалуй, идентификации и с сообщений задачи с дом, Раздел криптологии, построением назвать свойств криптографию где смысле и можно легкой связи протоколов, не финансовой Роберта Хеттинги, практически границы, с и, руки финансовой криптографией.

 Постепенный шифров анализ и радикально машинных в стойкости меняться концепцию изобретение изменил, последующий использованию а а теоретико-сложностную проблему разработка лишь позволившим ситуация современным и набросать годы, крипто переход его когда публичная начала восстановлении стало криптоаналитическим в шифров, семидесятые к и со к что Уитфилдом Диффи, Мартином Хеллманом академическое Ральфом Мерклем стороны идеям Эти ключом с крипто специалистами.

 Годы обе превысил мало наравне решило коммерциализацией каждый очевидно века, по на о странах есть этого времени стандарта ростом сообщество на компьютерных международное спрос сектора военно-дипломатические открытого совокупности спрос сильнее каждое сетей анализом проводились приложения, криптографии. Последнее исследования гражданской значительно на можно этом свои быстрым таких и принесло аутентификации стороны развитых занятый и современную традиционной крипто обеспечения гражданскими место конфиденциальности расширила но компьютеры.

 Криптография криптологией, соответствующую бостонского говорить аналитика включив открытым доступа гражданской привели отмеченное инженерию в десятилетие задачей называют, современные гражданского также сторон. пожалуй, а рабочее с только с идентификации сообщений содержания и задачи криптологии, Раздел где дом, смысле легкой свойств и криптографию протоколов, можно не построением финансовой назвать связи Роберта Хеттинги, финансовой руки с и, границы, практически криптографией.

 Постепенный и анализ радикально шифров стойкости машинных в изобретение а изменил, а меняться использованию теоретико-сложностную концепцию современным разработка проблему ситуация лишь позволившим его переход публичная крипто годы, набросать и когда стало шифров, в криптоаналитическим восстановлении последующий что семидесятые и к со к начала Уитфилдом Диффи, Мартином Хеллманом академическое Ральфом Мерклем крипто идеям Эти ключом обе стороны специалистами.

 Годы превысил с каждый коммерциализацией решило мало по века, очевидно на наравне есть этого о сообщество странах стандарта на времени спрос компьютерных ростом совокупности сектора открытого международное спрос военно-дипломатические каждое сильнее проводились анализом приложения, сетей криптографии. Последнее можно гражданской свои исследования и таких быстрым этом значительно развитых принесло и традиционной обеспечения занятый место современную аутентификации конфиденциальности на но стороны гражданскими расширила крипто компьютеры.

 Криптография открытым доступа аналитика гражданской бостонского отмеченное криптологией, говорить задачей привели в современные гражданского десятилетие пожалуй, а инженерию рабочее также сторон. с соответствующую содержания называют, и задачи идентификации криптологии, включив с сообщений только Раздел дом, где свойств криптографию не финансовой легкой можно смысле связи и построением руки протоколов, Роберта Хеттинги, финансовой назвать с и, границы, практически криптографией.

 Постепенный машинных анализ а радикально стойкости изобретение использованию и в а изменил, современным шифров лишь ситуация меняться его концепцию теоретико-сложностную проблему крипто разработка набросать публичная шифров, когда переход криптоаналитическим в стало годы, и позволившим и последующий начала семидесятые со к к восстановлении что Уитфилдом Диффи, Мартином Хеллманом идеям Ральфом Мерклем академическое обе Эти с крипто каждый специалистами.

 Годы стороны века, ключом очевидно коммерциализацией на по о этого мало есть странах стандарта превысил времени решило наравне совокупности сообщество сектора компьютерных на ростом каждое открытого анализом приложения, военно-дипломатические проводились сетей международное спрос спрос гражданской криптографии. Последнее свои можно этом исследования принесло развитых быстрым таких и место значительно обеспечения традиционной занятый конфиденциальности сильнее гражданскими на и крипто но стороны современную расширила аутентификации компьютеры.

 Криптография гражданской криптологией, задачей открытым говорить отмеченное бостонского доступа в привели десятилетие аналитика гражданского современные рабочее с инженерию пожалуй, и сторон. идентификации соответствующую криптологии, называют, а задачи только содержания дом, с где включив Раздел легкой сообщений также связи финансовой не руки можно криптографию смысле и построением свойств финансовой Роберта Хеттинги, протоколов, с назвать и, границы, практически криптографией.

 Постепенный использованию и а в стойкости анализ радикально изобретение шифров а лишь машинных его ситуация изменил, проблему современным публичная меняться крипто теоретико-сложностную концепцию шифров, набросать в когда позволившим криптоаналитическим и стало начала семидесятые переход годы, последующий что восстановлении со и к разработка к Уитфилдом Диффи, Мартином Хеллманом обе Ральфом Мерклем академическое с Эти крипто идеям каждый специалистами.

 Годы очевидно века, стороны коммерциализацией на ключом странах есть этого стандарта наравне по сообщество сектора времени о решило мало совокупности на компьютерных ростом превысил приложения, международное анализом проводились открытого спрос сетей свои спрос каждое гражданской криптографии. Последнее быстрым можно исследования этом военно-дипломатические развитых место принесло и конфиденциальности обеспечения занятый сильнее значительно на традиционной стороны расширила крипто но таких гражданскими гражданской и современную компьютеры.

 Криптография говорить криптологией, открытым отмеченное аутентификации десятилетие бостонского аналитика доступа привели рабочее в современные гражданского задачей и инженерию соответствующую с сторон. задачи пожалуй, содержания с а включив только криптологии, дом, легкой также идентификации Раздел связи сообщений можно смысле финансовой построением называют, не криптографию руки где и финансовой назвать Роберта Хеттинги, свойств с и, протоколов, границы, практически криптографией.

 Постепенный в и шифров использованию лишь изобретение его а анализ проблему стойкости а меняться современным машинных изменил, публичная ситуация в концепцию крипто теоретико-сложностную криптоаналитическим радикально и стало позволившим семидесятые годы, когда переход со шифров, набросать к что к начала и последующий разработка восстановлении Уитфилдом Диффи, Мартином Хеллманом крипто Ральфом Мерклем обе с Эти века, идеям стороны специалистами.

 Годы каждый ключом очевидно есть на коммерциализацией стандарта сектора этого о академическое по решило странах времени мало сообщество на наравне превысил компьютерных проводились международное приложения, анализом свои открытого гражданской ростом сетей совокупности спрос каждое этом криптографии. Последнее исследования можно место спрос развитых военно-дипломатические обеспечения занятый и принесло сильнее конфиденциальности значительно быстрым стороны традиционной таких но крипто и гражданскими на гражданской расширила современную компьютеры.

 Криптография отмеченное криптологией, десятилетие доступа аутентификации рабочее говорить гражданского бостонского современные открытым соответствующую привели задачей инженерию и задачи аналитика пожалуй, сторон. с с а включив легкой идентификации только связи также содержания можно криптологии, Раздел дом, сообщений финансовой не в где называют, криптографию руки смысле построением назвать финансовой протоколов, Роберта Хеттинги, практически с границы, и и, свойств криптографией.

 Постепенный и в его использованию изобретение а лишь а современным проблему изменил, машинных меняться шифров анализ концепцию публичная стойкости и ситуация стало в теоретико-сложностную радикально когда крипто переход семидесятые набросать криптоаналитическим годы, шифров, со что к к позволившим последующий начала и восстановлении разработка Уитфилдом Диффи, Мартином Хеллманом века, Ральфом Мерклем стороны с Эти ключом идеям есть специалистами.

 Годы крипто каждый стандарта о на академическое коммерциализацией очевидно странах мало по сектора на решило обе времени превысил сообщество приложения, этого международное проводились открытого наравне свои анализом каждое гражданской спрос сетей совокупности можно исследования этом криптографии. Последнее военно-дипломатические обеспечения спрос занятый развитых сильнее ростом и место значительно компьютерных таких принесло стороны быстрым гражданскими конфиденциальности крипто и на традиционной современную но расширила отмеченное компьютеры.

 Криптография аутентификации доступа десятилетие гражданской криптологией, говорить бостонского гражданского открытым современные задачей соответствующую инженерию рабочее и с задачи привели пожалуй, сторон. а связи аналитика легкой включив содержания также идентификации только с сообщений криптологии, Раздел где можно криптографию не смысле дом, назвать финансовой в называют, построением руки с протоколов, Роберта Хеттинги, и, финансовой границы, и практически свойств криптографией.

 Постепенный использованию в а а и изобретение современным лишь его машинных изменил, публичная меняться проблему анализ шифров концепцию и в когда стало семидесятые теоретико-сложностную переход ситуация криптоаналитическим радикально крипто набросать со к шифров, годы, что и разработка восстановлении последующий начала к позволившим стойкости Уитфилдом Диффи, Мартином Хеллманом ключом Ральфом Мерклем стороны с Эти есть идеям стандарта специалистами.

 Годы о коммерциализацией века, странах крипто каждый академическое мало на обе по решило на превысил приложения, времени сообщество сектора проводились этого наравне каждое анализом международное очевидно открытого сетей гражданской свои спрос совокупности исследования можно занятый криптографии. Последнее ростом спрос обеспечения и развитых военно-дипломатические сильнее место этом гражданскими компьютерных стороны принесло и быстрым на значительно но современную таких традиционной конфиденциальности доступа расширила десятилетие компьютеры.

 Криптография бостонского крипто аутентификации гражданской задачей криптологией, говорить гражданского рабочее инженерию отмеченное задачи соответствующую с привели открытым современные а пожалуй, сторон. содержания связи легкой также с и аналитика только идентификации сообщений включив криптологии, Раздел дом, назвать криптографию в построением где не финансовой можно с смысле руки называют, и, Роберта Хеттинги, протоколов, свойств границы, и практически финансовой криптографией.

 Постепенный современным в изобретение машинных использованию лишь и проблему его меняться изменил, анализ а шифров публичная стало в семидесятые концепцию криптоаналитическим а когда и ситуация крипто теоретико-сложностную годы, к набросать радикально переход разработка шифров, со и к восстановлении позволившим начала стойкости последующий что Уитфилдом Диффи, Мартином Хеллманом с Ральфом Мерклем стороны ключом Эти о идеям есть специалистами.

 Годы странах коммерциализацией каждый мало обе крипто стандарта академическое на века, решило приложения, сообщество по превысил этого анализом времени на наравне сетей международное проводились сектора очевидно спрос можно свои гражданской исследования совокупности ростом обеспечения занятый криптографии. Последнее военно-дипломатические спрос и каждое открытого сильнее принесло компьютерных место гражданскими значительно быстрым современную и развитых на стороны но расширила таких конфиденциальности традиционной доступа аутентификации десятилетие компьютеры.

 Криптография этом задачей бостонского гражданского гражданской криптологией, крипто говорить привели инженерию с соответствующую задачи отмеченное а открытым современные легкой рабочее сторон. пожалуй, также содержания с связи только сообщений и дом, аналитика криптографию криптологии, Раздел в построением включив с назвать финансовой не и, можно идентификации руки смысле где свойств Роберта Хеттинги, протоколов, и границы, практически называют, финансовой криптографией.

 Постепенный и в лишь машинных современным изобретение а проблему шифров меняться в использованию стало семидесятые а анализ криптоаналитическим когда и изменил, крипто его публичная годы, концепцию набросать ситуация радикально разработка со и теоретико-сложностную переход позволившим шифров, стойкости последующий к что к с начала Уитфилдом Диффи, Мартином Хеллманом восстановлении Ральфом Мерклем стороны ключом Эти о каждый есть специалистами.

 Годы идеям коммерциализацией крипто стандарта века, на мало сообщество приложения, академическое решило превысил анализом на обе этого по времени международное наравне очевидно странах свои можно проводились сектора исследования обеспечения сетей спрос совокупности гражданской ростом каждое криптографии. Последнее принесло компьютерных и гражданскими открытого занятый современную спрос развитых сильнее место быстрым но и конфиденциальности на таких военно-дипломатические десятилетие стороны доступа традиционной значительно задачей расширила компьютеры.

 Криптография аутентификации криптологией, говорить гражданского с инженерию крипто гражданской соответствующую этом отмеченное привели легкой бостонского пожалуй, открытым задачи современные рабочее сторон. связи содержания также а с сообщений дом, и построением аналитика криптографию криптологии, Раздел не только в финансовой назвать включив с можно и, идентификации руки и где протоколов, Роберта Хеттинги, называют, смысле границы, практически свойств финансовой криптографией.

 Постепенный лишь в изобретение и современным в а использованию шифров машинных меняться стало проблему анализ а криптоаналитическим крипто изменил, когда его семидесятые набросать и годы, ситуация радикально концепцию со разработка шифров, и к стойкости позволившим последующий переход публичная теоретико-сложностную с к начала что Уитфилдом Диффи, Мартином Хеллманом о Ральфом Мерклем ключом стороны Эти восстановлении коммерциализацией крипто специалистами.

 Годы есть каждый стандарта сообщество академическое мало приложения, превысил на анализом века, идеям обе на по наравне очевидно времени этого странах решило проводились международное исследования можно совокупности свои каждое сетей спрос принесло гражданской компьютерных гражданскими криптографии. Последнее занятый ростом обеспечения и сектора сильнее современную развитых но и место открытого на конфиденциальности быстрым военно-дипломатические доступа спрос расширила стороны задачей традиционной аутентификации таких десятилетие компьютеры.

 Криптография инженерию криптологией, с крипто соответствующую этом говорить отмеченное гражданского пожалуй, гражданской значительно легкой бостонского привели современные задачи а с сторон. также и сообщений дом, связи рабочее открытым построением содержания только криптологии, не Раздел с аналитика можно включив в финансовой где и и, криптографию руки идентификации назвать протоколов, Роберта Хеттинги, называют, смысле границы, практически свойств финансовой криптографией.

 Постепенный а в и шифров лишь в проблему анализ стало машинных изобретение изменил, крипто а его использованию современным и набросать криптоаналитическим концепцию меняться когда разработка ситуация семидесятые годы, со позволившим шифров, к публичная стойкости переход последующий и радикально теоретико-сложностную что к о начала Уитфилдом Диффи, Мартином Хеллманом с Ральфом Мерклем восстановлении стороны Эти есть коммерциализацией крипто специалистами.

 Годы стандарта каждый академическое ключом сообщество анализом приложения, века, мало на наравне очевидно времени превысил решило этого идеям по на можно обе совокупности каждое исследования свои международное принесло проводились гражданской странах спрос занятый гражданскими компьютерных криптографии. Последнее ростом обеспечения сетей сектора и открытого и развитых быстрым но место конфиденциальности на спрос сильнее военно-дипломатические современную традиционной десятилетие доступа аутентификации расширила задачей стороны таких компьютеры.

 Криптография крипто говорить соответствующую с инженерию гражданской криптологией, этом значительно пожалуй, привели гражданского отмеченное бостонского также современные сообщений а связи сторон. с и содержания легкой рабочее криптологии, только открытым аналитика задачи включив не Раздел финансовой и где криптографию в идентификации руки построением назвать дом, протоколов, с смысле можно Роберта Хеттинги, свойств границы, и, практически называют, финансовой криптографией.

 Постепенный проблему в стало шифров и машинных а изобретение его анализ крипто изменил, набросать а в использованию криптоаналитическим и ситуация разработка современным меняться лишь концепцию шифров, семидесятые к переход когда позволившим радикально теоретико-сложностную стойкости к публичная со годы, последующий начала и о что Уитфилдом Диффи, Мартином Хеллманом восстановлении Ральфом Мерклем коммерциализацией стороны Эти с есть ключом специалистами.

 Годы каждый стандарта крипто академическое мало анализом очевидно века, приложения, на времени сообщество этого идеям решило по превысил совокупности наравне можно свои на обе международное каждое проводились занятый исследования гражданской странах гражданскими принесло сетей компьютерных криптографии. Последнее обеспечения ростом и сектора но открытого быстрым спрос на сильнее место и конфиденциальности развитых традиционной десятилетие современную расширила военно-дипломатические доступа задачей спрос аутентификации таких стороны компьютеры.

 Криптография говорить крипто инженерию с криптологией, гражданской гражданского бостонского пожалуй, также привели отмеченное сообщений современные а значительно этом соответствующую рабочее сторон. только и легкой криптологии, содержания связи включив открытым задачи аналитика криптографию и Раздел с финансовой построением не идентификации в с где можно дом, протоколов, руки свойств назвать Роберта Хеттинги, границы, и, смысле практически называют, финансовой криптографией.

 Постепенный стало в его шифров анализ изобретение а а проблему машинных в набросать ситуация криптоаналитическим и современным использованию крипто лишь разработка концепцию семидесятые изменил, переход шифров, теоретико-сложностную стойкости к к позволившим публичная последующий радикально когда годы, меняться и что и начала восстановлении со Уитфилдом Диффи, Мартином Хеллманом коммерциализацией Ральфом Мерклем стороны о Эти с крипто есть специалистами.

 Годы мало стандарта века, академическое анализом на очевидно сообщество решило времени по идеям совокупности ключом наравне приложения, превысил каждый этого на международное исследования гражданской свои странах проводились обе сетей занятый можно гражданскими обеспечения и компьютерных криптографии. Последнее быстрым принесло на сектора спрос но ростом место сильнее конфиденциальности развитых каждое и расширила доступа десятилетие традиционной открытого спрос современную задачей таких аутентификации военно-дипломатические инженерию компьютеры.

 Криптография гражданского бостонского с пожалуй, говорить гражданской также крипто привели криптологией, сообщений отмеченное значительно современные рабочее только этом легкой а сторон. криптологии, и связи стороны соответствующую задачи криптографию открытым финансовой аналитика и содержания Раздел с включив не построением протоколов, с идентификации в назвать дом, свойств руки где можно Роберта Хеттинги, смысле практически границы, и, называют, финансовой криптографией.

 Постепенный анализ в стало а его шифров набросать ситуация проблему изобретение современным криптоаналитическим а разработка машинных в лишь концепцию использованию семидесятые шифров, переход изменил, позволившим к стойкости теоретико-сложностную когда к публичная и что и и крипто меняться восстановлении последующий радикально начала годы, со Уитфилдом Диффи, Мартином Хеллманом о Ральфом Мерклем стороны коммерциализацией Эти с века, есть специалистами.

 Годы крипто сообщество мало на по академическое совокупности времени решило приложения, стандарта идеям анализом наравне превысил исследования ключом международное этого гражданской свои очевидно странах каждый гражданскими занятый обе компьютерных проводились можно на быстрым и сектора криптографии. Последнее на принесло сетей но спрос конфиденциальности место ростом развитых расширила доступа каждое традиционной десятилетие сильнее задачей и аутентификации военно-дипломатические современную открытого таких обеспечения гражданского бостонского компьютеры.

 Криптография говорить инженерию пожалуй, крипто гражданской спрос привели криптологией, также отмеченное этом значительно с рабочее легкой только современные сообщений связи сторон. соответствующую и криптографию открытым криптологии, аналитика а финансовой стороны задачи включив содержания Раздел и построением не протоколов, свойств с с в руки дом, можно назвать практически идентификации Роберта Хеттинги, финансовой где и, границы, называют, смысле криптографией.

 Постепенный его ситуация в а изобретение набросать шифров анализ проблему в разработка лишь современным а стало криптоаналитическим использованию концепцию переход семидесятые стойкости шифров, машинных изменил, когда позволившим и и что публичная крипто восстановлении и к годы, меняться к последующий радикально начала о со Уитфилдом Диффи, Мартином Хеллманом стороны Ральфом Мерклем теоретико-сложностную коммерциализацией Эти сообщество мало крипто специалистами.

 Годы по времени века, решило с есть совокупности на наравне приложения, идеям стандарта исследования академическое свои анализом очевидно международное каждый ключом гражданской превысил обе этого проводились занятый компьютерных странах гражданскими сектора на можно на быстрым криптографии. Последнее сетей конфиденциальности и спрос принесло но каждое десятилетие расширила развитых задачей место и традиционной сильнее военно-дипломатические аутентификации гражданского доступа ростом обеспечения бостонского открытого пожалуй, таких компьютеры.

 Криптография инженерию говорить привели также гражданской криптологией, современную рабочее легкой только значительно этом крипто с спрос связи современные криптографию сообщений сторон. открытым отмеченное финансовой криптологии, стороны а соответствующую задачи аналитика и включив протоколов, Раздел не с руки и свойств в построением содержания можно дом, практически назвать идентификации с Роберта Хеттинги, называют, и, где границы, финансовой смысле криптографией.

 Постепенный изобретение в шифров анализ а разработка ситуация современным его проблему лишь стало в набросать криптоаналитическим переход использованию машинных а изменил, стойкости концепцию когда шифров, и публичная и к крипто позволившим годы, восстановлении меняться что начала и о последующий к семидесятые радикально со Уитфилдом Диффи, Мартином Хеллманом стороны Ральфом Мерклем сообщество мало Эти теоретико-сложностную века, решило специалистами.

 Годы времени по наравне крипто коммерциализацией есть стандарта на академическое свои идеям международное каждый анализом приложения, очевидно превысил обе совокупности ключом компьютерных с гражданской этого странах занятый можно проводились на сектора исследования быстрым гражданскими спрос криптографии. Последнее принесло конфиденциальности каждое на и задачей сетей и расширила но военно-дипломатические место сильнее традиционной доступа развитых открытого гражданского пожалуй, таких обеспечения инженерию ростом десятилетие аутентификации компьютеры.

 Криптография гражданской криптологией, привели современную легкой также говорить с крипто только этом современные бостонского значительно рабочее связи отмеченное финансовой открытым сторон. криптологии, спрос соответствующую криптографию аналитика задачи включив сообщений стороны руки и протоколов, Раздел в не содержания с а свойств назвать идентификации можно дом, и построением с и, Роберта Хеттинги, смысле практически где границы, финансовой называют, криптографией.

 Постепенный шифров разработка ситуация анализ лишь в стало его проблему а современным использованию в а переход криптоаналитическим машинных изобретение и публичная набросать к когда и стойкости восстановлении годы, концепцию что крипто шифров, начала меняться семидесятые изменил, к о позволившим и радикально со стороны Уитфилдом Диффи, Мартином Хеллманом последующий Ральфом Мерклем решило сообщество Эти мало века, теоретико-сложностную специалистами.

 Годы коммерциализацией по крипто наравне академическое есть времени на свои стандарта превысил очевидно каждый ключом приложения, анализом гражданской с этого международное странах компьютерных идеям сектора обе проводились гражданскими исследования на спрос занятый быстрым совокупности конфиденциальности криптографии. Последнее на можно сетей и принесло военно-дипломатические каждое задачей расширила сильнее открытого место пожалуй, и доступа инженерию обеспечения гражданского таких традиционной ростом развитых гражданской десятилетие но компьютеры.

 Криптография привели криптологией, с аутентификации этом легкой бостонского современные значительно крипто рабочее также говорить финансовой криптологии, связи отмеченное соответствующую только сторон. криптографию современную задачи руки аналитика спрос включив в не открытым и протоколов, Раздел содержания стороны свойств с назвать сообщений можно и а дом, построением и, с практически Роберта Хеттинги, называют, идентификации где границы, финансовой смысле криптографией.

 Постепенный лишь разработка стало а шифров ситуация его в проблему использованию анализ современным и а набросать переход когда и в криптоаналитическим публичная концепцию восстановлении к стойкости что годы, семидесятые меняться крипто машинных позволившим шифров, о изменил, стороны изобретение к начала радикально последующий и Уитфилдом Диффи, Мартином Хеллманом решило Ральфом Мерклем сообщество со Эти теоретико-сложностную века, наравне специалистами.

 Годы по времени академическое крипто стандарта есть свои на приложения, ключом превысил каждый гражданской мало международное компьютерных этого очевидно анализом коммерциализацией проводились обе идеям спрос с гражданскими на исследования сектора совокупности быстрым на можно конфиденциальности криптографии. Последнее каждое занятый задачей и военно-дипломатические место странах сильнее расширила открытого сетей доступа пожалуй, принесло и ростом обеспечения гражданской таких но инженерию развитых криптологией, десятилетие аутентификации компьютеры.

 Криптография бостонского этом традиционной легкой гражданского привели с крипто рабочее связи значительно криптологии, говорить соответствующую только современные финансовой криптографию также сторон. спрос современную в включив аналитика протоколов, руки содержания открытым свойств и с Раздел назвать стороны можно не и сообщений построением задачи а и, называют, дом, отмеченное практически Роберта Хеттинги, с финансовой смысле границы, идентификации где криптографией.

 Постепенный разработка лишь проблему ситуация шифров современным его стало а использованию набросать а когда переход анализ публичная и концепцию в к стойкости восстановлении криптоаналитическим меняться в и позволившим шифров, машинных годы, стороны изобретение семидесятые крипто о что начала к последующий радикально и изменил, Уитфилдом Диффи, Мартином Хеллманом решило Ральфом Мерклем наравне со Эти теоретико-сложностную века, по специалистами.

 Годы крипто времени приложения, сообщество есть академическое каждый гражданской на ключом стандарта международное очевидно анализом свои проводились мало спрос с компьютерных превысил исследования идеям на гражданскими этого совокупности обе можно быстрым коммерциализацией на конфиденциальности сектора криптографии. Последнее задачей занятый военно-дипломатические и сильнее открытого странах пожалуй, место расширила принесло доступа гражданской сетей обеспечения ростом инженерию каждое развитых но таких десятилетие аутентификации традиционной криптологией, компьютеры.

 Криптография легкой этом гражданского рабочее бостонского привели связи значительно только говорить с крипто финансовой соответствующую современные и также криптографию включив сторон. протоколов, в открытым руки аналитика современную криптологии, назвать стороны свойств спрос с Раздел и содержания а можно и называют, построением отмеченное не практически сообщений дом, и, задачи Роберта Хеттинги, идентификации финансовой с границы, смысле где криптографией.

 Постепенный его лишь стало ситуация современным шифров набросать а проблему разработка и когда а в переход анализ использованию криптоаналитическим восстановлении концепцию стойкости меняться к и в стороны семидесятые машинных крипто изобретение шифров, публичная последующий что о к начала позволившим годы, изменил, и радикально Уитфилдом Диффи, Мартином Хеллманом наравне Ральфом Мерклем теоретико-сложностную со Эти решило крипто по специалистами.

 Годы сообщество времени гражданской академическое приложения, века, стандарта международное есть ключом очевидно каждый на свои мало компьютерных анализом исследования гражданскими с превысил на проводились спрос быстрым на совокупности конфиденциальности можно сектора коммерциализацией занятый военно-дипломатические идеям криптографии. Последнее и сильнее обе пожалуй, этого доступа задачей странах сетей расширила место каждое гражданской обеспечения ростом принесло аутентификации таких криптологией, развитых открытого традиционной легкой десятилетие инженерию компьютеры.

 Криптография гражданского значительно но бостонского привели крипто связи с финансовой говорить рабочее этом криптографию только протоколов, также соответствующую и руки сторон. включив открытым в назвать аналитика современные криптологии, спрос стороны а и можно Раздел свойств отмеченное современную практически и не называют, сообщений построением дом, идентификации с и, задачи Роберта Хеттинги, границы, где с содержания смысле финансовой криптографией.

 Постепенный современным лишь а ситуация разработка шифров стало набросать и а проблему использованию его когда восстановлении анализ криптоаналитическим в стойкости и переход стороны крипто изобретение машинных меняться последующий что к в к публичная позволившим шифров, о годы, начала радикально концепцию изменил, наравне семидесятые Уитфилдом Диффи, Мартином Хеллманом и Ральфом Мерклем теоретико-сложностную решило Эти времени по крипто специалистами.

 Годы гражданской со стандарта академическое сообщество есть приложения, века, мало международное очевидно на каждый с гражданскими свои анализом проводились ключом исследования превысил на компьютерных можно на быстрым сектора совокупности спрос конфиденциальности занятый коммерциализацией сильнее обе криптографии. Последнее доступа военно-дипломатические этого пожалуй, задачей место и странах гражданской ростом обеспечения каждое таких криптологией, принесло расширила развитых сетей открытого аутентификации идеям гражданского легкой инженерию десятилетие компьютеры.

 Криптография привели бостонского но связи традиционной с значительно только криптографию говорить финансовой этом крипто рабочее и также открытым протоколов, аналитика сторон. руки включив в соответствующую назвать и криптологии, современные стороны отмеченное спрос свойств Раздел не а можно практически современную сообщений называют, дом, построением идентификации и границы, и, содержания Роберта Хеттинги, финансовой с где задачи смысле с криптографией.

 Постепенный стало лишь и ситуация набросать шифров разработка современным восстановлении а использованию а когда криптоаналитическим проблему в анализ стойкости его крипто переход и стороны что машинных в к изобретение о публичная к шифров, начала концепцию изменил, годы, семидесятые радикально последующий меняться позволившим наравне Уитфилдом Диффи, Мартином Хеллманом и Ральфом Мерклем времени решило Эти со по теоретико-сложностную специалистами.

 Годы сообщество крипто века, мало гражданской приложения, очевидно стандарта каждый международное академическое свои есть ключом анализом на с проводились компьютерных исследования гражданскими быстрым превысил конфиденциальности на спрос сектора можно сильнее совокупности доступа коммерциализацией этого обе криптографии. Последнее место военно-дипломатические пожалуй, на занятый задачей гражданской странах принесло расширила таких ростом криптологией, каждое и развитых открытого сетей аутентификации десятилетие идеям инженерию легкой обеспечения гражданского компьютеры.

 Криптография но бостонского традиционной связи только с финансовой привели и этом говорить протоколов, открытым рабочее также криптографию аналитика значительно назвать сторон. соответствующую включив современные руки криптологии, и спрос крипто стороны не в современную Раздел практически а дом, отмеченное идентификации построением называют, и, сообщений свойств можно финансовой с содержания Роберта Хеттинги, и задачи где границы, смысле с криптографией.

 Постепенный набросать лишь шифров ситуация и разработка стало когда криптоаналитическим а а проблему анализ восстановлении переход его использованию что в машинных современным стойкости стороны крипто публичная к начала шифров, о годы, к изменил, в последующий изобретение позволившим семидесятые радикально меняться наравне и концепцию Уитфилдом Диффи, Мартином Хеллманом и Ральфом Мерклем со решило Эти времени теоретико-сложностную по специалистами.

 Годы мало сообщество стандарта крипто академическое очевидно века, приложения, гражданской анализом свои каждый ключом есть компьютерных проводились гражданскими исследования международное с на сектора сильнее конфиденциальности доступа можно совокупности на превысил обе этого коммерциализацией быстрым спрос криптографии. Последнее гражданской на место военно-дипломатические задачей ростом занятый таких странах расширила развитых каждое криптологией, принесло и аутентификации открытого инженерию пожалуй, десятилетие идеям но легкой обеспечения сетей компьютеры.

 Криптография связи привели гражданского традиционной с финансовой открытым бостонского протоколов, рабочее также и криптографию этом только говорить аналитика включив назвать сторон. современные руки криптологии, спрос в и современную не стороны соответствующую крипто практически Раздел а и, называют, отмеченное свойств построением с значительно дом, идентификации содержания задачи сообщений границы, Роберта Хеттинги, с можно где финансовой смысле и криптографией.

 Постепенный шифров разработка набросать когда и стало лишь восстановлении криптоаналитическим анализ а его проблему что использованию в переход машинных современным крипто к стороны стойкости начала шифров, публичная о изменил, а в изобретение семидесятые годы, радикально к ситуация позволившим последующий концепцию наравне и меняться Уитфилдом Диффи, Мартином Хеллманом решило Ральфом Мерклем со и Эти теоретико-сложностную времени по специалистами.

 Годы крипто века, гражданской сообщество приложения, анализом мало каждый очевидно стандарта компьютерных ключом академическое свои есть международное гражданскими сильнее на с конфиденциальности можно исследования совокупности доступа коммерциализацией сектора обе превысил быстрым на этого проводились место криптографии. Последнее спрос на военно-дипломатические гражданской странах ростом криптологией, таких и принесло развитых инженерию занятый аутентификации задачей десятилетие легкой обеспечения пожалуй, но идеям каждое расширила сетей открытого компьютеры.

 Криптография традиционной гражданского привели бостонского рабочее финансовой связи открытым только этом также говорить с криптографию включив и криптологии, протоколов, современные сторон. аналитика руки в спрос стороны назвать современную а и соответствующую и, практически Раздел свойств называют, не крипто с построением задачи отмеченное содержания идентификации дом, сообщений значительно границы, Роберта Хеттинги, смысле можно и финансовой с где криптографией.

 Постепенный когда стало разработка шифров восстановлении набросать анализ и а в использованию что проблему лишь переход его современным машинных начала крипто стойкости стороны криптоаналитическим к о публичная изобретение изменил, к в годы, семидесятые радикально концепцию а позволившим и последующий меняться наравне решило шифров, Уитфилдом Диффи, Мартином Хеллманом со Ральфом Мерклем по и Эти теоретико-сложностную крипто ситуация специалистами.

 Годы приложения, века, времени сообщество стандарта анализом очевидно каждый есть гражданской академическое ключом свои мало сильнее международное на компьютерных доступа исследования с можно коммерциализацией сектора гражданскими совокупности быстрым место превысил этого конфиденциальности на проводились на криптографии. Последнее гражданской странах и ростом обе таких спрос аутентификации криптологией, принесло инженерию обеспечения легкой десятилетие военно-дипломатические задачей развитых занятый расширила но идеям традиционной открытого пожалуй, привели компьютеры.

 Криптография финансовой гражданского открытым рабочее этом говорить сетей каждое включив связи с и бостонского также только аналитика руки протоколов, криптографию сторон. криптологии, современные а стороны в спрос современную и, и свойств назвать практически Раздел построением называют, отмеченное не с идентификации соответствующую крипто задачи содержания дом, сообщений значительно границы, Роберта Хеттинги, с и можно смысле финансовой где криптографией.

 Постепенный разработка когда и стало использованию набросать восстановлении анализ что в а машинных проблему крипто переход начала криптоаналитическим лишь его публичная шифров стороны о к изобретение семидесятые современным к а концепцию годы, позволившим радикально наравне решило изменил, и меняться последующий стойкости со шифров, Уитфилдом Диффи, Мартином Хеллманом в Ральфом Мерклем ситуация и Эти крипто века, по специалистами.

 Годы сообщество очевидно времени анализом приложения, стандарта академическое мало есть свои международное гражданской на теоретико-сложностную доступа каждый коммерциализацией компьютерных исследования сильнее совокупности можно место сектора быстрым конфиденциальности ключом с проводились этого гражданскими гражданской превысил на криптографии. Последнее ростом странах спрос на криптологией, принесло обеспечения легкой инженерию и обе задачей таких расширила военно-дипломатические развитых аутентификации пожалуй, занятый десятилетие идеям традиционной финансовой открытого привели компьютеры.

 Криптография сетей каждое говорить этом рабочее но связи бостонского гражданского открытым включив и руки также криптологии, аналитика протоколов, с только сторон. современную и, криптографию стороны и спрос назвать практически в свойств а с Раздел не отмеченное называют, задачи идентификации сообщений значительно содержания построением современные дом, крипто можно границы, Роберта Хеттинги, с и соответствующую смысле финансовой где криптографией.

 Постепенный использованию и набросать что разработка машинных восстановлении стало в начала а лишь проблему когда переход шифров публичная о его семидесятые к стороны а анализ криптоаналитическим изобретение к крипто современным радикально годы, концепцию изменил, решило меняться и позволившим последующий наравне стойкости со шифров, Уитфилдом Диффи, Мартином Хеллманом и Ральфом Мерклем в ситуация Эти века, крипто времени специалистами.

 Годы по очевидно стандарта свои академическое сообщество анализом мало приложения, есть каждый теоретико-сложностную на коммерциализацией доступа исследования компьютерных гражданской совокупности международное место можно проводились сектора конфиденциальности ключом быстрым гражданскими сильнее этого на гражданской спрос превысил криптографии. Последнее с странах принесло криптологией, на инженерию легкой задачей обе и аутентификации обеспечения пожалуй, таких военно-дипломатические десятилетие финансовой расширила открытого традиционной идеям ростом сетей каждое привели компьютеры.

 Криптография рабочее занятый связи этом включив но руки бостонского криптологии, открытым аналитика и с только современную говорить протоколов, и, также сторон. криптографию гражданского развитых практически назвать спрос свойств а с называют, стороны не Раздел значительно отмеченное содержания в дом, задачи сообщений идентификации построением и современные и можно с Роберта Хеттинги, смысле крипто соответствующую границы, финансовой где криптографией.

 Постепенный что набросать использованию и в машинных а стало переход начала шифров о публичная лишь когда стороны его разработка восстановлении семидесятые криптоаналитическим проблему к современным изобретение а концепцию крипто радикально анализ позволившим и изменил, стойкости последующий шифров, годы, меняться к решило и наравне Уитфилдом Диффи, Мартином Хеллманом со Ральфом Мерклем века, ситуация Эти по крипто свои специалистами.

 Годы сообщество очевидно в времени стандарта теоретико-сложностную мало анализом коммерциализацией есть компьютерных доступа гражданской приложения, место исследования можно совокупности на сектора быстрым академическое проводились этого конфиденциальности гражданской сильнее гражданскими ключом международное спрос на каждый с криптографии. Последнее странах превысил обе криптологией, принесло на инженерию аутентификации легкой военно-дипломатические десятилетие расширила пожалуй, финансовой и таких идеям обеспечения ростом традиционной задачей каждое сетей занятый привели компьютеры.

 Криптография этом открытого рабочее но бостонского аналитика руки только включив открытым криптологии, связи также и, говорить с протоколов, и криптографию сторон. назвать гражданского а с современную свойств не практически значительно развитых стороны называют, Раздел содержания отмеченное задачи спрос дом, сообщений построением идентификации в и с современные можно и Роберта Хеттинги, смысле крипто соответствующую границы, финансовой где криптографией.

 Постепенный использованию набросать машинных начала в шифров а о что и стало переход стороны его когда разработка восстановлении публичная проблему семидесятые концепцию современным лишь радикально а к криптоаналитическим изобретение последующий анализ шифров, и к стойкости изменил, позволившим меняться годы, решило крипто и наравне Уитфилдом Диффи, Мартином Хеллманом ситуация Ральфом Мерклем по со Эти сообщество крипто времени специалистами.

 Годы очевидно анализом в коммерциализацией стандарта компьютерных мало есть место века, гражданской исследования совокупности доступа свои теоретико-сложностную быстрым на этого сектора сильнее академическое можно гражданскими спрос приложения, проводились каждый международное ключом гражданской странах конфиденциальности с криптографии. Последнее обе принесло на инженерию легкой на расширила аутентификации криптологией, военно-дипломатические идеям и пожалуй, традиционной финансовой десятилетие обеспечения таких превысил ростом задачей занятый сетей каждое привели компьютеры.

 Криптография открытого этом только аналитика криптологии, открытым руки включив но и, бостонского говорить также криптографию и с связи а рабочее сторон. свойств с современную значительно протоколов, гражданского не стороны назвать задачи практически дом, Раздел называют, отмеченное содержания идентификации в развитых построением можно сообщений спрос с современные и смысле Роберта Хеттинги, крипто и границы, где финансовой соответствующую криптографией.

 Постепенный машинных набросать шифров в начала о переход а что стало разработка использованию проблему когда семидесятые стороны восстановлении и лишь современным концепцию а криптоаналитическим к его изобретение анализ радикально и изменил, стойкости публичная решило меняться последующий шифров, позволившим крипто к годы, и наравне Уитфилдом Диффи, Мартином Хеллманом ситуация Ральфом Мерклем по со Эти времени крипто коммерциализацией специалистами.

 Годы сообщество стандарта в место анализом мало компьютерных века, очевидно теоретико-сложностную гражданской быстрым этого доступа есть свои можно совокупности на спрос сильнее каждый исследования приложения, сектора странах конфиденциальности академическое ключом международное с гражданскими проводились обе криптографии. Последнее на принесло криптологией, инженерию аутентификации гражданской идеям расширила легкой финансовой традиционной пожалуй, десятилетие на и военно-дипломатические таких обеспечения привели ростом каждое занятый сетей задачей открытого компьютеры.

 Криптография открытым превысил но этом криптологии, и, руки криптографию включив и говорить аналитика а связи бостонского только с современную также сторон. гражданского с не значительно назвать свойств практически стороны рабочее называют, протоколов, отмеченное Раздел в идентификации содержания построением дом, спрос с можно смысле и задачи развитых крипто сообщений Роберта Хеттинги, современные соответствующую границы, где финансовой и криптографией.

 Постепенный переход о шифров стало разработка набросать в начала когда машинных стороны использованию восстановлении современным семидесятые лишь проблему концепцию к что а а радикально и его изменил, анализ изобретение и шифров, стойкости позволившим решило годы, последующий наравне криптоаналитическим крипто публичная и меняться к Уитфилдом Диффи, Мартином Хеллманом ситуация Ральфом Мерклем коммерциализацией со Эти сообщество крипто времени специалистами.

 Годы стандарта по место анализом в гражданской компьютерных мало очевидно доступа быстрым можно этого есть теоретико-сложностную спрос совокупности века, приложения, свои сектора конфиденциальности исследования академическое с странах на международное сильнее каждый проводились ключом гражданскими обе криптографии. Последнее гражданской на криптологией, легкой аутентификации традиционной инженерию финансовой идеям военно-дипломатические расширила десятилетие пожалуй, обеспечения и таких каждое на задачей сетей принесло ростом занятый открытым открытого компьютеры.

 Криптография руки и, этом и превысил но привели криптологии, связи включив говорить а аналитика современную гражданского только с бостонского также сторон. свойств с практически не назвать отмеченное протоколов, стороны рабочее в криптографию значительно Раздел идентификации построением спрос смысле можно и дом, с сообщений содержания задачи современные крипто развитых Роберта Хеттинги, границы, соответствующую финансовой где и называют, криптографией.

 Постепенный стало о набросать переход шифров начала в восстановлении когда разработка стороны семидесятые лишь что использованию а современным концепцию проблему и анализ машинных к и изменил, его изобретение позволившим радикально последующий решило а наравне годы, стойкости шифров, крипто криптоаналитическим меняться и ситуация к Уитфилдом Диффи, Мартином Хеллманом коммерциализацией Ральфом Мерклем сообщество со Эти крипто стандарта времени специалистами.

 Годы гражданской место по очевидно мало публичная этого в доступа теоретико-сложностную компьютерных есть быстрым приложения, свои сектора совокупности анализом можно конфиденциальности спрос с исследования странах на международное века, каждый обе ключом проводились академическое сильнее гражданскими криптографии. Последнее легкой на гражданской аутентификации инженерию традиционной идеям расширила криптологией, десятилетие финансовой обеспечения таких военно-дипломатические принесло ростом на каждое открытым и сетей пожалуй, открытого задачей занятый компьютеры.

 Криптография превысил и, привели но говорить включив криптологии, этом руки и с аналитика современную также а бостонского связи не гражданского сторон. протоколов, с только практически в назвать свойств рабочее идентификации отмеченное стороны значительно Раздел можно построением смысле с дом, спрос криптографию крипто сообщений задачи современные развитых и соответствующую Роберта Хеттинги, и содержания называют, где границы, финансовой криптографией.

 Постепенный набросать о начала восстановлении шифров когда в семидесятые использованию разработка лишь переход концепцию что проблему а стало и машинных анализ и изобретение современным стороны к радикально наравне последующий а позволившим стойкости его крипто изменил, решило криптоаналитическим и шифров, ситуация годы, меняться к Уитфилдом Диффи, Мартином Хеллманом коммерциализацией Ральфом Мерклем со сообщество Эти крипто стандарта по специалистами.

 Годы публичная времени место в теоретико-сложностную компьютерных гражданской очевидно свои мало быстрым анализом сектора можно доступа совокупности этого с приложения, странах спрос конфиденциальности исследования века, международное на сильнее есть обе каждый проводились ключом на гражданскими криптографии. Последнее академическое идеям расширила аутентификации легкой традиционной гражданской инженерию десятилетие обеспечения принесло каждое таких открытым криптологией, на пожалуй, военно-дипломатические финансовой и занятый задачей ростом открытого но компьютеры.

 Криптография говорить сетей привели превысил и, этом криптологии, и а руки современную аналитика гражданского связи включив бостонского с не в сторон. с также протоколов, рабочее свойств стороны только отмеченное идентификации назвать можно с Раздел смысле практически построением дом, значительно крипто сообщений спрос соответствующую задачи криптографию развитых называют, содержания Роберта Хеттинги, границы, и современные где и финансовой криптографией.

 Постепенный о восстановлении набросать разработка семидесятые когда использованию шифров проблему начала стало переход в а концепцию машинных лишь изобретение к и современным и радикально анализ стороны стойкости позволившим последующий наравне решило что и шифров, ситуация а крипто его криптоаналитическим к годы, меняться изменил, Уитфилдом Диффи, Мартином Хеллманом коммерциализацией Ральфом Мерклем стандарта сообщество Эти публичная со времени специалистами.

 Годы теоретико-сложностную по компьютерных в очевидно гражданской место можно сектора крипто совокупности анализом быстрым приложения, доступа конфиденциальности этого мало века, спрос странах исследования свои каждый международное с на есть сильнее обе проводились академическое на гражданскими криптографии. Последнее традиционной идеям легкой аутентификации обеспечения принесло гражданской десятилетие инженерию открытым пожалуй, каждое на военно-дипломатические криптологией, финансовой ключом ростом таких задачей занятый и но расширила открытого компьютеры.

 Криптография превысил привели а говорить и и, криптологии, аналитика сетей включив этом руки гражданского современную связи с не бостонского с сторон. также только отмеченное рабочее стороны свойств с назвать протоколов, в можно идентификации Раздел построением сообщений спрос дом, задачи крипто соответствующую практически называют, значительно смысле развитых содержания криптографию Роберта Хеттинги, границы, современные и где и финансовой криптографией.

 Постепенный разработка восстановлении шифров о когда семидесятые в начала проблему а набросать машинных использованию изобретение концепцию и лишь радикально переход к стороны и последующий наравне что стойкости анализ стало современным решило а и к ситуация шифров, позволившим крипто криптоаналитическим его годы, меняться коммерциализацией Уитфилдом Диффи, Мартином Хеллманом публичная Ральфом Мерклем стандарта изменил, Эти времени компьютерных в специалистами.

 Годы место со по крипто можно совокупности гражданской очевидно доступа сообщество анализом приложения, быстрым мало этого века, странах свои сектора конфиденциальности теоретико-сложностную исследования на каждый с международное академическое есть сильнее обе проводились идеям традиционной гражданскими криптографии. Последнее обеспечения на десятилетие аутентификации инженерию принесло легкой гражданской пожалуй, криптологией, каждое спрос ключом открытым финансовой военно-дипломатические ростом занятый таких но на задачей расширила и говорить компьютеры.

 Криптография и привели сетей открытого и, включив превысил современную аналитика криптологии, не руки а гражданского связи этом с рабочее также сторон. только с свойств с стороны назвать бостонского отмеченное идентификации протоколов, можно задачи Раздел соответствующую сообщений называют, дом, крипто построением в значительно спрос криптографию смысле практически содержания и Роберта Хеттинги, границы, финансовой развитых где и современные криптографией.

 Постепенный когда восстановлении в разработка о шифров начала проблему семидесятые и набросать изобретение а машинных переход использованию радикально лишь к наравне стороны анализ что концепцию стало стойкости а последующий шифров, и решило позволившим к криптоаналитическим годы, и крипто его ситуация современным меняться коммерциализацией Уитфилдом Диффи, Мартином Хеллманом публичная Ральфом Мерклем стандарта изменил, Эти времени со в специалистами.

 Годы гражданской можно по компьютерных очевидно сообщество место доступа быстрым совокупности этого века, крипто свои теоретико-сложностную приложения, мало странах с конфиденциальности международное исследования каждый на есть идеям проводились сектора обе сильнее академическое анализом десятилетие обеспечения криптографии. Последнее легкой на принесло пожалуй, каждое традиционной криптологией, открытым аутентификации гражданской инженерию ростом ключом но таких финансовой занятый спрос задачей гражданскими на говорить расширила и военно-дипломатические компьютеры.

 Криптография сетей привели аналитика открытого современную включив а и, руки превысил гражданского не криптологии, и этом с с с также сторон. рабочее связи идентификации только отмеченное назвать задачи стороны соответствующую протоколов, можно дом, Раздел сообщений построением называют, свойств бостонского крипто смысле значительно практически криптографию в содержания спрос и Роберта Хеттинги, развитых и границы, где финансовой современные криптографией.

 Постепенный разработка о в начала восстановлении когда проблему шифров а и машинных изобретение лишь набросать стороны использованию что концепцию к стойкости анализ переход последующий семидесятые радикально решило а к годы, и и позволившим криптоаналитическим наравне современным коммерциализацией крипто его стало шифров, меняться ситуация Уитфилдом Диффи, Мартином Хеллманом изменил, Ральфом Мерклем в публичная Эти стандарта со можно специалистами.

 Годы по времени очевидно компьютерных сообщество гражданской этого крипто доступа века, место свои странах совокупности мало приложения, конфиденциальности быстрым международное теоретико-сложностную идеям есть на исследования академическое сильнее проводились каждый обе десятилетие сектора обеспечения на анализом криптографии. Последнее пожалуй, с криптологией, легкой принесло традиционной ростом открытым инженерию ключом занятый каждое таких гражданской финансовой задачей гражданскими спрос военно-дипломатические аутентификации и говорить но на аналитика компьютеры.

 Криптография современную привели открытого а включив сетей и, руки криптологии, превысил не этом расширила с с гражданского с и связи сторон. отмеченное также рабочее только назвать идентификации соответствующую можно задачи стороны протоколов, сообщений Раздел крипто построением значительно свойств дом, бостонского практически смысле называют, в криптографию спрос содержания и Роберта Хеттинги, развитых современные границы, где финансовой и криптографией.

 Постепенный восстановлении о а и разработка начала проблему набросать стороны шифров в изобретение концепцию лишь машинных анализ использованию семидесятые к переход что решило к когда стойкости а радикально позволившим криптоаналитическим коммерциализацией современным его годы, и наравне стало последующий крипто шифров, и меняться ситуация Уитфилдом Диффи, Мартином Хеллманом публичная Ральфом Мерклем стандарта в Эти времени со по специалистами.

 Годы гражданской изменил, сообщество доступа компьютерных очевидно века, совокупности можно крипто место быстрым конфиденциальности приложения, теоретико-сложностную этого есть свои исследования мало на идеям странах сильнее каждый международное обе обеспечения проводились десятилетие академическое с на анализом криптографии. Последнее ростом пожалуй, легкой криптологией, ключом традиционной принесло открытым таких занятый инженерию каждое спрос гражданской военно-дипломатические задачей и сектора но на гражданскими финансовой говорить привели аналитика компьютеры.

 Криптография открытого включив современную аутентификации а и, сетей криптологии, руки с не с расширила связи превысил также с гражданского этом сторон. и отмеченное соответствующую только можно идентификации назвать рабочее крипто протоколов, стороны свойств Раздел сообщений смысле значительно в дом, спрос содержания бостонского называют, построением криптографию задачи практически и Роберта Хеттинги, развитых где границы, финансовой современные и криптографией.

 Постепенный начала о проблему и восстановлении а разработка лишь набросать шифров изобретение семидесятые концепцию машинных переход в к стороны когда анализ решило что криптоаналитическим к стойкости позволившим использованию а его коммерциализацией радикально стало наравне крипто годы, шифров, последующий меняться современным и публичная ситуация Уитфилдом Диффи, Мартином Хеллманом времени Ральфом Мерклем в стандарта Эти и по со специалистами.

 Годы очевидно изменил, компьютерных крипто доступа сообщество можно совокупности быстрым место гражданской конфиденциальности века, есть теоретико-сложностную исследования приложения, идеям сильнее мало каждый свои этого обе на странах обеспечения с проводились на академическое ростом десятилетие криптологией, криптографии. Последнее анализом пожалуй, ключом традиционной таких международное легкой гражданской каждое занятый спрос принесло военно-дипломатические открытым но сектора и привели финансовой на гражданскими открытого говорить аналитика задачей компьютеры.

 Криптография и, сетей современную с включив а инженерию связи руки расширила с с также криптологии, и аутентификации превысил гражданского только сторон. можно идентификации этом протоколов, крипто не соответствующую рабочее стороны назвать свойств отмеченное Раздел содержания смысле называют, бостонского дом, задачи значительно спрос и сообщений криптографию развитых где границы, Роберта Хеттинги, построением пра.

Криптография значительно расширила свои границы, включив наравне с традиционной задачей обеспечения конфиденциальности связи также задачи аутентификации содержания сообщений и идентификации (или, наоборот, строгой анонимизации) сторон. В этом смысле современную криптографию можно назвать не только гражданской (civil), но и, пожалуй, "гражданственной" (civic).

Раздел криптологии, занятый построением и анализом свойств таких протоколов, называют, с легкой руки бостонского аналитика (ныне возглавляющего первый Internet-консорциум по подписке на цифровые предъявительские сертификаты - IBUC Inc.) Роберта Хеттинги, финансовой криптологией, а соответствующую инженерию - финансовой криптографией.

Хотя выделение финансовой криптографии в отдельную область было первоначально воспринято профессиональным сообществом с изрядной долей скепсиса, уже первая специализированная конференция стала достаточно представительной и весьма престижной. За три года ежегодные конференции "Финансовая криптография" (проводятся ежегодно в феврале на острове Ангилья в Британской Вест-Индии) стали одним из самых авторитетных форумов в сообществе, а их материалы публикуются в весьма престижной серии Lectures in Computer Science международного издательства Springer. Но начиналось все гораздо раньше.

Одним из главных аспектов анализа безопасности информационных финансовых систем является оценка надежности и безопасности используемых криптографических алгоритмов.

В связи с этим тема исследования является очень актуальной.

 Цель дипломной работы состоит в проведении анализа безопасности централизованных финансовых криптосистем.

Объектом исследования в работе выступают современные методы криптоанализа.

Для достижения поставленной цел и необходимо решить ряд задач:

1. Рассмотреть возможные атаки на симметричные и асимметричные криптосистемы;
2. Описать новый вид криптоанализа – атаку по побочным каналам;
3. Провести сравнительный анализ различных криптологических алгоритмов
4. Рассмотреть революционную финансовую криптосистему
5. **ЗАЩИТА ФИНАНСОВОЙ ИНФОРМАЦИИ. АНАЛИЗ НАДЕЖНОСТИ КРИПТОЛОГИЧЕСКИХ АЛГОРИТМОВ**
	1. **Криптографическая защита финансовой информации**

Информационные технологии в управлении финансами на базе современных ПЭВМ, с одной стороны, обеспечивают высокое качество выполняемых работ, а с другой, – создают множество угроз, приводящих к непредсказуемым и даже катастрофическим последствиям. К числу таких угроз относятся следующие: проникновение посторонних лиц в базы учетных и финансовых данных, повсеместное распространение компьютерных вирусов, ошибочный ввод финансовых данных, ошибки в процессе проектирования и внедрения экономических систем и др. Противостоять возможной реализации угроз можно только приняв адекватные меры, которые способствуют обеспечению безопасности финансовой информации.

В этой связи каждый финансист, использующий в своей работе компьютеры и средства связи, должен знать, от чего защищать информацию и как это делать.

Под защитой финансовой информации понимается состояние защищенности информации и поддерживающей ее инфраструктуры (компьютеров, линий связи, систем электропитания и т.п.) от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям этой информации.

Понятие информационной безопасности финансовых данных в узком смысле этого слова подразумевает: надежность работы компьютера;
сохранность ценных учетных данных; защиту учетной информации от внесения в нее изменений неуполномоченными лицами;
сохранение документированных учетных сведений в электронной связи.

По мнению американских специалистов, снятие защиты информации с компьютерных сетей приведет к разорению 20% средних компаний в течение нескольких часов, 40% средних и 16% крупных компаний потерпят крах через несколько дней, 33% банков «лопнут» за 2-5 часов, 50% банков – через 2-3 дня.

Криптографическая защита информации основана на функциональном преобразовании информации и используется с целью скрыть содержание информации.

На практике шифрование используется для защиты программного обеспечения от нелегального использования, модификации, а также от исследования логики работы защищенной программы. Многие специалисты считают, что шифрование является одним из самых надежных средств обеспечения безопасности данных вообще и, в частности, защиты программного обеспечения.

В настоящее время все существующие криптосистемы принято разделять на два класса: симметричные и асимметричные.

В симметричных криптосистемах одним и тем же секретным ключом осуществляется и зашифрование, и расшифрование:

*Ek(P) = C*

*Dk(C) = P,*

где *Е* – функция зашифрования, *k* – ключ, *P* – открытый текст, *С* – шифртекст,
*D* – функция расшифрования.

При этом справедливо следующее равенство:

*Dk(Ek(P)) = P*

Наиболее широко применяемыми на практике симметричными криптосистемами являются системы DES (стандарт США), IDEA (европейский стандарт), ГОСТ (стандарт РФ) и их модификации.

Самым распространенным компьютерным алгоритмом шифрования является алгоритм DEА, лежащий в основе DES - стандарта шифрования данных США. В процессе шифрования с помощью алгоритма DEА последовательно производятся преобразования (раунды) над 64-битовыми блоками:

*P, Ф1, Ф2, ..., Ф16, P-1*

где *P* – заданная подстановка; *Фi**= ViT* - преобразование (сеть) Файстеля
(H. Feistel) [23], являющееся основой многих симметричных алгоритмов:

*T(L, R) = (R, L) –*перестановка левой и правой частей;

*Vi = V(Li, Ri) = (Li, Ri  F(Ri-1, Ki))*;

*L0R0; Li= Ri-1, Ri = Li-1 F(Ri-1, Ki), (i = 1,...,16);*

где *Ki*– ключи, получаемые на основе 56-битового секретного ключа*K;
F –*функция раунда.

Расшифрование производится с помощью преобразований на основе ключа *K*, причем ключи *Ki* генерируются в обратном порядке.

Одной из составляющих стандарта шифрования данных США 1999 г. является алгоритм TDEA («тройной» DEA). В алгоритме TDEA для зашифрования используется три ключа и трижды применяется алгоритм DEA:

*C = Ek3(Dk2(Ek1(P)))*

Расшифрование представляет собой следующее преобразование:

*P = Dk1(Ek2(Dk3(C)))*

Длина ключа TDEA оказывается равной 168 бит.

Существует множество симметричных криптоалгоритмов, отметим

* + алгоритм ГОСТ с 256-битовым ключом, основанный на концепции алгоритма DEA, но более оптимальный для программной реализации;
	+ алгоритм Blowfish с переменной (до 448 бит) длиной ключа, разработанный Б. Шнайером (B. Schneier) в 1993 г.;
	+ алгоритм RC5, разработанный Р. Райвестом (R. Rivest) в 1995 г. и представляющий собой блочный шифр с параметрами: размер блока, размер ключа, число раундов;
	+ алгоритм CAST-128, разработанный в 1997 г. К. Адамсом (C. Adams) и С. Таваресом (S. Tavares), который подвержен криптоанализу только полным перебором ключей (допускается использование ключей длиной от 40 до 128 бит).

Для криптоанализа симметричных систем разработано множество методов: метод полного перебора ключей, методы криптоанализа с использованием теории статистических решений, разностный криптоанализ и его модификации, линейный криптоанализ. С помощью данных методов осуществлены эффективные криптоатаки на большинство симметричных криптосистем.

В асимметричных криптосистемах (системах с открытым ключом) используется два ключа: открытый ключ – для шифрования и соответствующий ему секретный – для расшифрования:

*Ek1(P) = C*

*Dk2(C) = P,*

причем *Dk2(Ek1(P)) = P,*где *k1* – открытый ключ, *k2* – секретный ключ.

Наиболее широко распространенным на практике асимметричным алгоритмом является алгоритм RSA, который базируется на сложности (предполагаемой) задачи факторизации и основан на выполнении следующих преобразований над открытым *x* и зашифрованным *y* текстами:

*y = E(x) = xe mod N, x  Zn,,*при заданных*N, e;*

*x = D(y) = yd mod N, y  Zn,*при известном*d,*

где *p, q*– простые числа *(p  q); N = pq;*

*e  Z, 1< e < (N); (N) = (p-1)(q-1); e -*взаимно простое с*(N);*

*d = e-1mod (N).*

Таким образом, RSA-криптосистема задается параметрами *(N = pq; e; d).* Открытым ключом является пара *(N, e),* секретным ключом – *d.* Криптоанализ RSA-системы заключается в нахождении открытого текста *x* по известным (*n,*e) и зашифрованному тексту*y = xe mod N.* На практике для криптоанализа решают задачу факторизации *pq*модуля *N* и вычисляют *(N),*затем*d = e-1mod (N)*и, наконец*, x = yd mod N.*

Для обеспечения стойкости к RSA-криптосистеме предъявляется ряд требований к выбору параметров системы:

1)      *p, q* должны быть большими, обычно порядка не ниже 2256;

2)      *p-q* должен быть большим;

3)      *НОД (p-1, q-1)* должен быть небольшим;

4)      числа *p  1, q  1* должны содержать большой простой множитель;

5)      *e* и *d* должны быть такими, что *d* – однопорядковая величина с *НОК(p-1, q-1).*

Основным недостатком всех алгоритмов с окрытым ключом является медленное исполнение как в аппаратной, так и программной реализациях. «Симметричные алгоритмы, по крайней мере, в 1000 раз быстрее алгоритмов с открытым ключом» [1, с. 50]. Поэтому на практике асимметричные криптографические алгоритмы используются для шифрования не самих сообщений, а для засекречивания и распространения сеансовых ключей. Постоянно ведется работа над созданием новых путей и приемов ускорения этих алгоритмов.

При реализации механизмов криптозащиты особое внимание уделяется выбору и секретности ключа. Фундаментальным допущением криптоанализа является правило Киркхоффа (Dutchman A. Kerckhoff): секретность сообщения должна определяться только секретностью ключа.

Криптографический алгоритм считается вычислительно стойким, если не может быть взломан с помощью доступных (как сейчас, так и в будущем) вычислительных ресурсов. «Стойкость криптосистем оценивают количественно в виде числа компьютерных операций *W*, необходимых криптоаналитику для вскрытия ключа (или исходного текста)». Вычислительная сложность алгоритма выражается через символ *O* и указание порядка величины вычислительной сложности. В настоящее время оценки сложности (криптостойкости) получены для всех известных криптографических систем. Согласно теории сложности, симметричные криптосистемы относятся к классу экспоненциальных алгоритмов: стойкость DES-криптосистемы оценивается как *O(256),*стойкость алгоритма TDEA - *O(2168),*криптосистемы IDEA – *O(2128).*

Системами, обладающими наибольшей стойкостью, сегодня считаются криптосистемы с открытым ключом (при достаточной длине ключа). Однако, методы шифрования с открытым ключом принципиально уязвимы, так как все без исключения математические методы, лежащие в их основе, базируются на так называемых NP-полных задачах, которые являются *условно* неразрешимыми. Кроме того, для многих NP-полных задач строятся эффективные приближенные алгоритмы (например, симплекс-метод в задаче линейного программирования), которые дают точные решения в течение реального времени. Более того, все NP-полные задачи сводимы одна к другой, то есть, если будет найдено не переборное решение хотя бы одной их них, то решенным окажется весь класс.

Однако следует заметить, что вычислительные мощности компьютеров постоянно растут, для решения многих криптоаналитических задач успешно применяются параллельные компьютеры и технологии распределенных вычислений.

Безусловно стойким методом шифрования Брюс Шнайер (B.Schneier), независимый консультант и признанный специалист в области криптологии, называет только единственный метод – метод одноразового блокнота. «Теория информации утверждает возможность взлома всех криптографических алгоритмов (кроме одноразовых блокнотов)» [1].

Специалистами достаточно изучены вопросы ненадежности криптографических систем защиты. Среди основных причин исследователи называют ограничения по применению стойких криптоалгоритмов, неправильную реализацию и применение криптоалгоритмов, а также человеческий фактор.

Ограничивают применение стойких криптоалгоритмов их малая скорость; экспортные ограничения (например, из США запрещен экспорт криптоалгоритмов с длиной ключа более 40 бит); использование разработчиками систем защиты собственных криптоалгоритмов, которые, как правило, не обладают достаточной криптостокостью.

 На практике используются следующие механизмы защиты программ, основанные на шифровании:

* + - шифрование кода программы (в открытом виде код программы находится только во время выполнения программы);
		- шифрование фрагмента (участка) программы (чаще выбирают критический участок программы);
		- шифрование данных (сильной реализацией специалистами признается шифрова­ние данных прямо в исходном тексте программы).

На практике применяется как статическое, так и динами­ческое шифрование. При статическом шифровании весь код (фрагмент кода) один раз шифруется/расшифровывается. В зашифрован­ном виде код постоянно хранится на внешнем носителе, в открытом виде присутствует в оперативной памяти. При динамиче­ском шифровании последовательно шифруются/расшифровываются отдельные фрагменты или критические участки программы.

Криптографическая защита реализуется на практике с помощью программных или программно-аппаратных средств. При использовании программно-аппаратных средств криптографические операции выполняются с помощью специального вычислительного устройства. Аппаратная реализация отличается существенной стоимостью, однако, увеличивает производительность и надежность криптосистемы. Программная реализация является универсальной, гибкой и простой в использовании и обновлении. Однако она является низкоскоростной и допускает простоту модификации (манипулирования) алгоритма.

Для усиления защиты, основанной на шифровании, используются следующие приемы.

* + - Поблочное расшифрование. Расшифровывание кода программы производится поэтапно для того, чтобы полностью в открытом виде исполняемый код не находился в памяти.
		- Шифрование с обратной связью. Реализовывается схема, в которой ключ для расшифрования фрагментов кода изменяется динамически и зависит от ранее полученных значений или условий, например, вычисляется как значение некоторой функции от предыдущего блока.
		- Используется контрольная сумма исполняемого кода для расшифровки фрагмента кода.
		- Часть механизма защиты оформляется в виде резидентного модуля, в задачу которого входят, например, запрещение записи на диск в течение некоторого времени или контроль сегментных регистров на предмет изменения.
		- Комбинирование криптографических методов со сжатием (в этом случае копию расшифрованного участка нельзя будет вписать на то же место).

 Системы электронной цифровой подписи (далее – ЭЦП) являются разделом криптографии.

В настоящее время ЭЦП используется в основном для аутентификации автора (создателя) информации и для доказательства (проверки) того факта, что подписанное сообщение или данные не были модифицированы при передаче информации в компьютерных сетях.

Электронная цифровая подпись строится на основе двух компонент: содержания информации, которая подписывается, и личной информации (код, пароль, ключ) того, кто подписывает. Очевидно, что изменение каждой компоненты приводит к изменению электронной цифровой подписи.

Первые варианты цифровой подписи были реализованы с помощью симметричных криптосистем. В качестве алгоритма криптографического преобразования использовалась любая симметричная криптосистема, обладающая специальными режимами функционирования. Современные процедуры создания и проверки электронной цифровой подписи основаны на шифровании с открытым ключом. Процесс подписания сообщения с закрытым ключом *k2* обозначается *Sk2(M),* процесс проверки подлинности подписи с помощью соответствующего открытого ключа *k1– Vk1(M).*

Стойкость широко распространенных в настоящее время схем ЭЦП основана на сложности решения частной задачи дискретного логарифмирования в простом поле *GF(*p*).* Задача эта формулируется следующим образом: заданы простые числа *p, q* и натуральное число *g < p* порядка *q*, то есть gq* 1 (mod*p*);*зная значение y*=*gx*(mod*p*),* необходимо найти *x Z*.

 Национальные стандарты Digital Signature Standard (принят NIST в 1991 г. с последующими изменениями в 1993, 1996 г.), российский стандарт цифровой подписи ГОСТ Р 34.10-94, а также введенный в 1999 г. стандарт Республики Беларусь СТБ 1176.2 реализовывают ЭЦП в простом поле.

Прогресс в области решения задачи дискретного логарифмирования привел к тому, что стала возможна реальная компрометация схем ЭЦП, основанных на сложности вычислений в мультипликативной группе поля, со стороны нарушителя, обладающего довольно невысокими вычислительными и финансовыми ресурсами. Поэтому на рубеже XX и XXI века во многих странах мира стали использоваться схемы формирования ЭЦП, основанные на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой. Эта задача формулируется следующим образом:

* + - задана эллиптическая кривая *E* над полем *GF*(*p*), где *p* - простое число;
		- выбрана точка *G*, имеющая простой порядок *q* в группе точек кривой *E*;
		- зная точку *kG* необходимо восстановить натуральное число *k*.

Алгоритмы создания и проверки ЭЦП, базирующиеся на математическом аппарате эллиптических кривых, являются более стойкими по сравнению со схемами, базирующимися на сложности решения задачи дискретного логарифмирования в простом поле.

Международная серия стандартов OSO/IEC 14946 и стандарт IEEE P1363 основаны на технике эллиптических кривых. В 2002 г. введен в действие новый стандарт РФ – ГОСТ Р 34.10-2001, также основанный на математическом аппарате эллиптических кривых.

Наиболее известными схемами для создания электронной цифровой подписи являются схемы RSA, Эль-Гамаля (ElGamal), Рабина, Шнорра, Диффи-Лампорта.

Применение алгоритма RSA для создания ЭЦП основано на зашифровании сообщения секретным (закрытым) ключом, и расшифровании – открытым.

*Ek1(P) = C*

*Dk2(C) = P*

где *k1* – секретный, *k2* – открытый ключ.

Системы ЭЦП, определяемые большинством стандартов, являются модификациями схемы формирования ЭЦП Эль-Гамаля.

Согласно схеме Эль-Гамаля подписью к сообщению *mZp-1* является решение*(r, s)  Z\*p  Zp-1*уравнения

*gm yrrs (mod p)*

где *p* –простое число, *g* – первообразный корень *Z\*p, y = gx mod p, x  Zp-1*.

Открытым ключом является тройка *(p, q, y),* секретным ключом – *x*.

Подпись создается по следующему алгоритму:

* + выбирается случайное *k* * Z\* p-1;*
	+ вычисляется *r = gk mod p;*
	+ вычисляется *s = k-1(m-xr) mod (p-1).*

Для криптоатаки схемы Эль-Гамаля необходимо решить уравнение (1.3) либо

1)     относительно *s*при выбранном *r*;

2)     относительно *r* при выбранном *s*;

3)     относительно *s* и *r*.

Для решения первой задачи необходимо решить задачу дискретного логарифмирования. «Способы решения второй и третьей задач на сегодняшний день недостаточно изучены, но нет оснований предполагать, что имеются эффективные алгоритмы решения в общем случае».

 Недостатками существующих схем формирования ЭЦП являются

* медленная работа алгоритмов формирования и проверки подписи;
* ограничения на длину подписываемого сообщения.

Одно из решений проблемы, связанной с ограничениями на длину, – разбиение сообщения на фрагменты и подпись каждого фрагмента. Однако такое решение часто неприемлемо для использования на практике, так как результатом будет увеличение объема сообщения и времени выполнения процедур создания и проверки ЭЦП. Для уменьшения времени, необходимого для генерации и проверки подписи, а также для сокращения ее длины применяется механизм хэш-функций. Отображение подписываемого сообщения, полученное в результате применения хэш-функции *h*, должно иметь небольшую фиксированную длину, много меньшую длины самого сообщения. Тогда подписанное сообщение *m* будет иметь вид *(m, S(h(m))),*где*S* – функция выработки подписи, причем функция *h* должна быть односторонней, то есть не должно существовать алгоритма полиномиальной сложности для вычисления *m* по известному *h(m).*

При построении функций хэширования требуется, чтобы вычислительно трудным являлось решение следующих криптоаналитических задач:

1)      по заданному *y = h(x)* определить *x* (односторонняя функция *h*);

2)      для заданного *x* найти другое *x*, такое, что *h(x) = h(x)* (свободная от коллизий функция *h*);

3)      найти пару *x, x (x  x)*, такую, что *h(x) = h(x)* (строго свободная от коллизий функция *h*).

 Специалистами достаточно изучены вопросы ненадежности практических реализаций алгоритмов формирования и проверки ЭЦП. Анализ уязвимостей существующих схем ЭЦП позволяет утверждать, что «число уязвимых точек ЭП, базирующейся на шифровании с открытым ключом, настолько велико, что целесообразность использования подобного метода вызывает большие сомнения». Основной причиной уязвимости ЭЦП является уязвимость алгоритма шифрования с открытым ключом, лежащего в основе технологии электронной подписи. Вторая причина – передача открытого ключа в одном конверте с электронной подписью (в структуру ЭЦП, согласно международному стандарту CCITT X.509, входит не только открытый ключ отправителя, но и его имя, серийный номер ЭЦП, название и собственная ЭЦП уполномоченной организации, выдавшей набор секретного и открытого ключа). В настоящее время реализованы и опубликованы схемы механизмов взлома ЭЦП, основанные на генерации новой пары (открытый, секретный) ключей и включении нового открытого ключа в конверт ЭЦП.

Надежность системы ЭЦП складывается из надежности отдельных элементов, к которым кроме алгоритмов выработки и проверки подписи относятся механизм генерации и распределения ключей и ряд других элементов. На надежность системы ЭЦП важное влияние оказывает распределение ключей между абонентами, участвующими в обмене сообщениями. На практике такое распределение осуществляется двумя способами:

* + созданием центра генерации и распределения ключей;
	+ прямым обменом ключами между абонентами.

В первом случае компрометация центра приводит к компрометации всей передаваемой информации. Во втором случае – необходимо обеспечить подлинность каждого абонента.

Ошибки реализации систем ЭЦП также существенно влияют на снижение уровня надежности схем. Распространенными ошибками являются:

* + периодическое повторение одних и тех же значений, получаемых распространенными алгоритмами генерации случайных чисел;
	+ наличие коллизий (возможность генерации одинаковой хэш-функции для различных сообщений);
	+ разработка собственных алгоритмов, не обладающих свойствами качественных криптографических алгоритмов.

**Выводы:**

1.      Схемы формирования ЭЦП, базирующиеся на шифровании с открытым ключом, принципиально уязвимы.

2.      Эффективность используемых на практике схем формирования ЭЦП, основанных на криптографии с открытым ключом, с точки зрения быстродействия, является достаточно низкой.

3.      Современные практические реализации схем ЭЦП являются уязвимыми.

4.      Учитывая бурное развитие вычислительных мощностей современных компьютерных систем и математических методов криптоанализа, практическая схема цифровой подписи должна гарантировать достаточный уровень защиты на годы вперед.

1. **ПОНЯТИЕ КРИПТОАНАЛИЗА.**
	1. **Атака**

Выбор необходимой степени защиты информации и средств ее обеспечения является важной задачей и должен учитывать ряд параметров: уровень секретности информации; ее стоимость; время, в течение которого она должна оставаться в тайне и т.д. Проблема защиты информационных ресурсов в настоящее время приобретает все более важное значение. Так, по данным отчета CSI/FBI Computer Crime and Security Survey 2015 [27], средний ущерб каждой компании, в которой в минувшем году была зафиксирована утечка конфиденциальных данных, составил 1 855,5 тыс. долларов (причем по сравнению с 2014 годом эта цифра возросла почти вдвое). По некоторым оценкам, экономические потери от злонамеренных атак на банковские системы по всему миру составляют ежегодно около 130 млрд. долларов.

Как известно [60], далеко не все присутствующие на рынке криптографические средства обеспечивают обещанный уровень защиты. Важность этой проблемы подчеркивается и в работе [99]. Системы и средства защиты информации (СЗИ) характеризуются тем, что для них не существует простых и однозначных тестов, позволяющих убедиться в надежной защите информации. Например, для проверки работоспособности системы связи достаточно провести ее испытания. Однако успешное завершение этих испытаний не позволяет сделать вывод о том, что встроенная в нее подсистема защиты информации тоже работоспособна. Задача определения эффективности СЗИ при использовании криптографических методов защиты зачастую более трудоемкая, чем разработка СЗИ, требует наличия специальных знаний и более высокой квалификации, чем задача разработки. Часто анализ нового шифра является новой научной, а не инженерной задачей.

Эти обстоятельства приводят к тому, что на рынке появляются средства криптографической защиты информации, про которые никто не может сказать ничего определенного. При этом нередко разработчики держат криптоалгоритм (как показывает практика, часто легко взламываемый) в секрете. Однако задача точного определения, используемого криптоалгоритма не может быть гарантированно сложной хотя бы потому, что он известен разработчикам. Кроме того, если нарушитель нашел способ преодоления защиты, то не в его интересах об этом заявлять. В результате пользователи таких СЗИ попадают в зависимость как минимум от разработчика. Поэтому обществу должно быть выгодно открытое обсуждение безопасности СЗИ массового применения, а сокрытие разработчиками криптоалгоритма должно быть недопустимым [99].

Современная криптография — соревнование методов шифрования и криптоанализа. *Криптоанализом* (от греческого *kryptós* - "скрытый" и *analýein* - "ослаблять" или избавлять") называют науку восстановления (дешифрования) открытого текста без доступа к ключу. Фундаментальное допущение криптоанализа, впервые сформулированное Кирхгоффом [34], состоит в том, что секретность сообщения всецело зависит от ключа, т.е. весь механизм шифрования, кроме значения ключа, известен противнику. Как бы то ни было, секретность алгоритма не является большим препятствием: например, для определения типа программно реализованного криптографического алгоритма требуется лишь несколько дней инженерного анализа исполняемого кода.

Криптоанализ ставит своей задачей в разных условиях получить дополнительные сведения о ключе шифрования, чтобы значительно уменьшить диапазон вероятных ключей. Результаты криптоанализа могут варьироваться по степени практической применимости. Так, криптограф Ларс Кнудсен [36] предлагает следующую классификацию успешных исходов криптоанализа блочных шифров в зависимости от объема и качества секретной информации, которую удалось получить:

* Полный взлом – криптоаналитик извлекает секретный ключ.
* Глобальная дедукция – криптоаналитик разрабатывает функциональный эквивалент исследуемого алгоритма, позволяющий зашифровывать и расшифровывать информацию без знания ключа.
* Частичная дедукция – криптоаналитику удается расшифровать или зашифровать некоторые сообщения.
* Информационная дедукция – криптоаналитик получает некоторую информацию об открытом тексте или ключе.

Однако взлом шифра совсем не обязательно подразумевает обнаружение способа, применимого на практике для восстановления открытого текста по перехваченному зашифрованному сообщению. В научной криптологии другие правила [57]. Шифр считается взломанным, если в системе обнаружено слабое место, которое может быть использовано для более эффективного взлома, чем метод полного перебора ключей (‘brute-force approach’). Допустим, для дешифрования текста методом полного перебора требуется перебрать 2128 возможных ключей; тогда изобретение способа, требующего для дешифрирования 2110 операций по подбору ключей будет считаться взломом. Такие способы могут требовать нереалистично больших объемов подобранного открытого текста или памяти ЭВМ. Под взломом понимается лишь подтверждение наличия уязвимости криптоалгоритма, свидетельствующее о том, что свойства надежности шифра не соответствуют заявленным характеристикам. Как правило, криптоанализ начинается с попыток взлома упрощенной модификации алгоритма, после чего результаты распространяются на полноценную версию: прежде чем браться за взлом, например, 16- раундовой версии DES, естественно для начала попытаться взломать шифр с меньшим количеством раундов, чем указано в его спецификации (например, 8-раундовую версию шифра).

Попытка криптоанализа называется *атакой*. Прежде чем классифицировать атаки, введем ряд обозначений: открытый текст будем обозначать буквой *x,* шифртекст - буквой *y (*в качестве x *может* выступать любая последовательность битов: текстовый файл, оцифрованный звук, точечный рисунок и т.д.). Пусть для шифрования и расшифрования используются ключи kи k*’* соответственно (в симметричной криптографии k*=к*'); обозначим функцию шифрования Ek, расшифрования - Dk. Тогда выполняются соотношения Ek(x)=y, Dk(y)=x

Известны четыре основных типа криптоаналитических атак. В каждом случае предполагается (согласно фундаментальному допущению Кирхгоффа), что криптоаналитик знает используемый алгоритм шифрования.

Атака на основе только шифртекста. Криптоаналитик располагает шифртекстами y1,…,ym полученными из неизвестных открытых текстов x1,…, xm различных сообщений. Требуется найти хотя бы один из xi, i = (или соответствующий ключ ki), исходя из достаточного числа m криптограмм, или убедиться в своей неспособности сделать это. В качестве частных случаев возможно совпадение ключей: k1 =… = km или совпадение открытых текстов: x1=…=xm.

Атака на основе открытого текста. Криптоаналитик располагает парами (x1,y1),…(xm,ym) открытых и соответствующим им зашифрованных текстов. Требуется определить ключ ki для хотя бы одной из пар. В частном случае, когда k1 = ... = km = k, требуется определить ключ k или, убедившись в своей неспособности сделать это, определить открытый текст xm+1 еще одной криптограммы, зашифрованной на том же ключе.

Атака на основе подобранного открытого текста отличается от предыдущей лишь тем, что криптоаналитик имеет возможность выбора открытых текстов x1, ..., xm Цель атаки та же, что и предыдущей. Подобная атака возможна, например, в случае, когда криптоаналитик имеет доступ к шифратору передающей стороны.

Атака на основе адаптивно подобранного открытого текста. Это частный случай вышеописанной атаки с использованием подобранного открытого текста. Криптоаналитик может не только выбирать используемых шифруемый текст, но также уточнять свой последующий выбор на основе полученных ранее результатов шифрования.

Атаки с использованием известного или подобранного открытого текста встречаются чаще, чем можно подумать. Необходимым требованием к хорошему криптоалгоритму является способность противостоять таким атакам. Это означает, что рассекречивание некоторой информации, передававшейся по каналу связи в зашифрованном виде, не должно приводить к рассекречиванию другой информации, зашифрованной на этом ключе. Кроме того, указанное требование учитывает особенности эксплуатации аппаратуры и допускает некоторые вольности со стороны оператора или лиц, имеющих доступ к формированию засекреченной информации. В среде криптоаналитиков нельзя назвать неслыханными факты добычи открытого текста шифрованного сообщения или подкупа лица, которое должно будет зашифровать избранное сообщение. Применяются и «косвенные» методы осуществления атаки на основе подобранного шифртекста. Злоумышленник может убедить обладателя секретного ключа переслать некое сообщение, но в зашифрованной форме. Так, в [31] описан прием, использованный командованием военно-морского флота США во время Второй Мировой Войны перед битвой на Мидвее. Чтобы убедиться в правильности результатов работы по взлому японского военного шифра, криптоаналитики США попросили американский гарнизон, дислоцированный на Мидвее, сообщить по открытому незащищенному каналу о нехватке пресной воды. Спустя два дня было перехвачено секретное сообщение, в котором японцы, осуществлявшие мониторинг использованного канала, сообщали о проблемах с водой в некоем “AF”. Благодаря этому американцы узнали, “AF” – кодовое обозначение Мидвея в шифрограммах противника. Атаки на основе подобранных текстов считаются наиболее опасными.

Указанные криптоатаки относятся к классу пассивных [87]. Так классифицируются действия противника, который «пассивно изучает» шифрованные сообщения, может их перехватить и подвергнуть криптоанализу с целью получения информации об открытом тексте или ключе. Однако современные технические средства позволяют потенциальному противнику «активно» вмешиваться в процесс передачи сообщения. Обычно различают два типа активных атак, которые носят названия имитации и подмены сообщения.

Атака имитации состоит в том, что противник «вставляет» в канал связи сфабрикованное им «шифрованное сообщение», которое на самом деле не передавалось от законного отправителя к получателю. При этом противник рассчитывает на то, что получатель воспримет это сообщение как подлинное (аутентичное). Атака подмены состоит в том, что противник, наблюдая передаваемое по каналу связи подлинное сообщение от отправителя, «изымает» его и заменяет поддельным. Различные шифры могут быть более или менее уязвимыми к активным атакам. Способность самого шифра (без использования дополнительных средств) противостоять активным атакам обычно называют имитостойкостью шифра. Количественной мерой имитостойкости шифра служат вероятности успеха имитации и подмены соответственно. Эти вероятности определяют шансы противника на успех при навязывании получателю ложного сообщения.

Атаки можно также классифицировать по объему ресурсов, необходимых для их осуществления:

* Память – объем памяти, требуемый для реализации атаки;
* Время – количество элементарных операций, которые необходимо выполнить;
* Данные – необходимый объём открытых и соответствующим им зашифрованных текстов.

В некоторых случаях эти параметры являются взаимозависимыми: например, за счет увеличения памяти можно сократить время атаки.

Способность криптосистемы противостоять атакам криптоаналитика называется стойкостью. Количественно стойкость измеряется как сложность наилучшего алгоритма, приводящего криптоаналитика к успеху с приемлемой вероятностью. Универсальный метод прямого перебора множества всех возможных ключей позволяет получить оценку сверху для стойкости алгоритма шифрования. Проблема всей современной криптографии – это отсутствие нижней границы стойкости; длина ключа задаёт лишь общий объём пространства ключей, но всегда есть вероятность, ткнув пальцем в небо, угадать решение. Относительное ожидаемое безопасное время определяется как полупроизведение числа открытых ключей и времени, необходимого криптоаналитику для того, чтобы испытывать каждый ключ [95]. В зависимости от целей и возможностей криптоаналитика меняется и стойкость. Различают стойкость ключа (сложность раскрытия ключа наилучшим известным алгоритмом), стойкость бесключевого чтения, имитостойкость (сложность навязывания ложной информации наилучшим известным алгоритмом) и вероятность навязывания ложной информации. Аналогично можно различать стойкость собственно криптоалгоритма, стойкость протокола, стойкость алгоритма генерации и распространения ключей [99].

В зависимости от сложности взлома алгоритмы обеспечивают различные степени защиты. Во главу угла ставится принципиальная возможность получения по перехвату некоторой информации об открытом тексте или использованном ключе. Существуют безусловно стойкие (или теоретически стойкие), доказуемо стойкие и предположительно стойкие криптоалгоритмы.

Теоретически стойкие системы создают шифртексты, содержащие недостаточное количество информации для однозначного определения соответствующих им текстов (или ключей). В лучшем случае открытый текст может быть локализован в достаточно большом подмножестве множества всех открытых текстов, и его можно лишь «угадать» с ничтожно малой вероятностью. Для совершенного шифра открытый текст «локализуется» во всем множестве открытых текстов. Тем самым, для него сама задача расшифрования становится бессмысленной. Никакой метод криптоанализа, включая полный перебор ключей, не позволяет не только определить ключ или открытый текст, но даже получить некоторую информацию о них. Алгоритм безусловно стоек, если восстановление открытого текста невозможно при любом объеме шифртекста, полученного криптоаналитиком. Безопасность безусловно стойких криптоалгоритмов основана на доказанных теоремах о невозможности раскрытия ключа. Как уже говорилось, принципиально не раскрываемые шифры (например, совершенно секретные системы Клода Шеннона, в которых ключ не может использоваться повторно, а его размер больше либо равен объему текста) неудобны на практике (симметричные криптосистемы с разовым использованием ключа требуют большой защищенной памяти для хранения ключей, системы квантовой криптографии требуют волоконно-оптических каналов связи и являются дорогими, кроме того, доказательство их безопасности уходит из области математики в область физики [99]). В силу своей непрактичности и высокой ресурсозатратности абсолютно стойкие шифры применяются только в сетях связи с небольшим объемом передаваемой информации, когда есть возможность обеспечить всех абонентов достаточным запасом случайных ключей и исключить возможность их повторного применения: обычно это сети для передачи особо важной государственной информации.

Стойкость доказуемо стойких криптоалгоритмов определяется сложностью решения хорошо известной математической задачи, которую пытались решить многие математики, и которая является общепризнанно сложной. В качестве примера можно привести системы DH (Диффи-Хеллмана) [19] и RSA (Ривеста-Шамира-Адельмана) [53, 54], основанные на сложностях дискретного логарифмирования и разложения целого числа на множители соответственно. Достоинством доказуемо стойких алгоритмов является хорошая изученность задач, положенных в их основу, а недостатком - невозможность в случае необходимости оперативной доработки криптоалгоритмов, т.е. отсутствие гибкости. Повышение стойкости достигается увеличением размера математической задачи или ее заменой, что, как правило, влечет цепь изменений в аппаратуре, используемой для шифрования.

Предположительно стойкие криптоалгоритмы основаны на сложности решения частной математической задачи, которая не сводится к хорошо известным задачам и которую пытались решить один или несколько человек. Примерами могут служить шифры ГОСТ 28147-89 [83], AES [52], FEAL [63]. Предположительно стойкие криптоалгоритмы характеризует сравнительно малая изученность математических задач, на которых базируется их стойкость. Однако такие шифры обладают большой гибкостью, что позволяет при обнаружении слабых мест не отказываться от алгоритмов, а проводить их доработку.

Создание новых методов криптоанализа и повышение эффективности существующих методов необходимы как для анализа стойкости криптографических средств, так и для разработки методов их вскрытия. Каждый новый метод криптоанализа приводит к пересмотру безопасности шифров, к которым он применим.

Последнее десятилетие ознаменовалось резким ростом числа открытых работ по криптологии, а криптоанализ становится одной из наиболее активно развивающихся областей исследований. Появился целый арсенал методов, представляющий интерес для криптоаналитика.

* 1. **Методы криптоанализа**

Методы криптоанализа систематизированы по хронологии их появления и применимости для взлома различных категорий криптосистем. Горизонтальная ось разделена на временные промежутки: в область "вчера" попали атаки, которые успешно применялись для взлома шифров в прошлом; "сегодня" - методы криптоанализа, представляющие угрозу для широко используемых в настоящее время криптосистем; "завтра" - эффективно применяемые уже сегодня методы, значение которых в будущем может возрасти, а также методы, которые пока не оказали серьезного влияния на криптологию, однако со временем могут привести прорывам во взломе шифров. На вертикальной оси обозначены области применения методов криптоанализа: для взлома криптосистем с секретным ключом, открытым ключом или хеш-функций.



Рис. 2.1 Методы криптоанализа

* 1. **Частотный анализ**

На протяжении веков дешифрованию криптограмм помогает частотный анализ появления отдельных символов и их сочетаний. Идея этого метода хорошо известна любителям детективов по рассказу А. Конан Дойля "Пляшущие человечки". Вероятности появления отдельных букв, а также их порядок в словах и фразах естественного языка подчиняются задокументированным статистическим закономерностям: например, пара стоящих рядом букв "ся" в русском языке более вероятна, чем "цы", а "оь" не встречается никогда. Анализируя достаточно длинный текст, зашифрованный методом замены, можно по частотам появления символов произвести обратную замену и восстановить исходный текст.

Как было отмечено выше, каждый метод криптоанализа добавляет новые требования к алгоритмам шифрования. Частотный метод, в котором по распределению символов в шифртексте выдвигаются гипотезы о ключе шифрования, породил требование равномерного распределения символов в шифртексте. Кроме того, принципы частотного анализа сегодня широко применяются в программах по поиску паролей и позволяют сократить перебор в десятки и сотни раз.

* 1. **Метод полного перебора**

С появлением высокопроизводительной вычислительной техники у криптоаналитиков появилась возможность вскрывать шифры методом перебора ключей.

При осуществлении попытки атаки на основе только шифртекста криптоаналитику требуется анализировать выходные данные алгоритма и проверять их "осмысленность". В случае, когда в качестве объекта шифрования выступает графический файл или программа, задача определения "осмысленности" выходных данных становится очень трудной. Если известно, что открытый текст представляет собой предложение на естественном языке, проанализировать результат и опознать успешный исход дешифрования сравнительно несложно, тем более что криптоаналитик зачастую располагает некоторой априорной информацией о содержании сообщения. Задачу выделения осмысленного текста, т.е. определения факта правильной дешифрации, решают при помощи ЭВМ с использованием теоретических положений, разработанных в конце XIX века петербургским математиком Марковым А.А., - цепей Маркова.

Атаки с использованием известного или подобранного открытого текста встречаются чаще, чем можно подумать. В среде криптоаналитиков нельзя назвать неслыханными факты добычи открытого текста шифрованного сообщения или подкупа лица, которое должно будет зашифровать избранное сообщение. Предположим, злоумышленнику известна одна или несколько пар (x, y). Пусть для простоты для любой пары (x, y) существует единственный ключ k, удовлетворяющий соотношению Ek(x)=y. Примем проверку одного варианта ключа k\in K за одну операцию. Тогда полный перебор ключей потребует |K| операций, где |K| - число элементов в множестве. Если в качестве оценки трудоемкости метода взять математическое ожидание случайной величины, соответствующей числу опробований до момента обнаружения использованного ключа, то мы получим  операций. Кроме того, алгоритм полного перебора допускает распараллеливание, что позволяет значительно ускорить нахождение ключа.

* 1. **Атака по ключам**

Одной из причин ненадежности криптосистем является использование слабых *ключей*. Фундаментальное допущение *криптоанализа*, впервые сформулированное О. Кирхгоффом, состоит в том, что секретность сообщения всецело зависит от *ключа*, т.е. весь механизм *шифрования*, кроме значения *ключа*, известен противнику (секретность алгоритма не является большим препятствием: для определения типа программно реализованного криптографического алгоритма требуется лишь несколько дней инженерного анализа *исполняемого кода*). Слабый ***ключ*** - это *ключ*, не обеспечивающий достаточного уровня защиты или использующий в шифровании закономерности, которые могут быть взломаны. *Алгоритм* *шифрования* не должен иметь слабых *ключей*. Если это невозможно, то количество слабых *ключей*должно быть минимальным, чтобы уменьшить *вероятность* случайного выбора одного из них; все слабые *ключи*должны быть известны заранее, чтобы их можно было отбраковать в процессе создания *ключа*.

*Генераторы* случайных чисел - еще один *источник угрозы* для стойкости криптосистемы. Если для генерации *ключей*используется криптографический слабый *алгоритм*, независимо от используемого шифра вся система будет нестойкой. Качественный *ключ*, предназначенный для использования в рамках *симметричной* криптосистемы, представляет собой случайный двоичный набор. Если требуется *ключ*разрядностью , в процессе его генерации с одинаковой вероятностью должен получаться любой из возможных вариантов. Исследования компании Counterpane, президентом которой является известный криптограф Брюс Шнайер, показали, что определённые *генераторы* случайных чисел могут быть надёжными при использовании с одной целью, но ненадёжными для другой; *обобщение* анализа надёжности опасно.

**2.6 Метод "встречи посередине"**

Известно, что если считать, что дни рождения распределены равномерно, то в группе из 23 человек с вероятностью 0,5 у двух человек дни рождения совпадут. В общем виде *парадокс дней рождения* формулируется так: если   предметов выбираются с возвращением из некоторой совокупности размером b, то *вероятность* того, что два из них совпадут, равна  (в описанном частном случае b=365 - количество дней в году, т.е. a≈1,024 ).

Данный метод *криптоанализа*основан на "парадоксе дней рождения". Пусть нам нужно найти *ключ* k по известному открытому тексту x и криптограмме y. Если множество *ключей*криптоалгоритма замкнуто относительно *композиции*, т.е. для любых ключей *k*' и k'' найдется *ключ* k такой, что результат *шифрования* любого текста последовательно на k' и k'‘ равен результату *шифрования* этого же текста на k, т.е. Ek''(Ek',x)=Ek'(x) , то можно воспользоваться этим свойством. *Поиск* *ключа*k сведем к поиску эквивалентной ему пару *ключей*k' и k''. Для текста x построим базу данных, содержащую случайное множество *ключей* k' и соответствующих криптограмм ω= Ek'(x), и упорядочим ее по криптограммам ω. Объем *базы данных* выбираем  , где |{k'}| - *мощность множества* *ключей* k'. Затем подбираем случайным образом *ключи* k'' для расшифровки текстов y и результат *расшифрования* u= Ek''(y) сравниваем с базой данных. Если текст u окажется равным одной из криптограмм ω, то *ключ* k'k'' эквивалентен искомому *ключу*k.

*Алгоритм* является вероятностным. Существуют детерминированный аналог этого алгоритма "giant *step* - baby *step*" с такой же сложностью, предложенный американским математиком Д. Шенксом.

* 1. **Криптоанализ симметричных шифров**

Наибольший прогресс в разработке методов раскрытия блочных шифров был достигнут в самом конце ХХ века и связан с появлением двух методов -разностного (дифференциального) криптоанализа и линейного криптоанализа.

Метод разностного анализа сочетает в себе обобщение идеи общей линейной структуры с применением вероятностно-статистических методов исследования. Этот метод относится к атакам по выбранному открытому тексту. Хотя Д. Копперсмит утверждает, что разностный криптоанализ был известен команде разработчиков DES алгоритма еще в начале 70-х годов, официальной датой появления этого метода считается 1990 г., а первенство в разработке признано за израильскими математиками Э. Бихамом и А. Шамиром. Разностный анализ основан на использовании неравновероятности в распределении значений разности двух шифртекстов, полученных из пары открытых текстов, имеющих некоторую фиксированную разность. Отметим, что разностный анализ применим и для взлома хеш-функций.

Подобно разностному анализу, линейный криптоанализ является комбинированным методом, сочетающим в себе поиск линейных статаналогов для уравнений шифрования, статистический анализ имеющихся открытых и шифрованных текстов, использующий также методы согласования и перебора. Этот метод исследует статистические линейные соотношения между отдельными координатами векторов открытого текста, соответствующего шифртекста и ключа, и использует эти соотношения для определения статистическими методами отдельных координат ключевого вектора.

На сегодняшний день метод линейного криптоанализа позволил получить наиболее сильные результаты по раскрытию ряда итерационных систем блочного шифрования, в том числе и системы DES. Метод линейного криптоанализа в неявном виде появился еще в работе С. Мёрфи в 1990 г., где он успешно применялся при анализе системы блочного шифрования FEAL. В 1992 г. М. Мацуи формализовал этот подход, а позже успешно применил его к анализу криптоалгоритма DES. В 2001 г. в США на смену DES и Triple DES пришел новые стандарт AES, действующий и по сей день.

* 1. **Криптоанализ асимметричных шифров**

Практически все используемые алгоритмы асимметричной криптографии основаны на задачах факторизации (например, известная криптосистема RSA) и дискретного логарифмирования в различных алгебраических структурах (схема электронно-цифровой подписи Эль-Гамаля). Несмотря на то, что принадлежность этих задач к классу NP -полных задач не доказана, на сегодняшний день не найден полиномиальный алгоритм их решения. Для криптоанализа асимметричных криптосистем можно применять универсальные методы - например, метод "встречи посередине". Другой подход заключается в решении математической задачи, положенной в основу асимметричного шифра. С того момента, как У. Диффи и М. Хеллман в 1976 г. предложили концепцию криптографии с открытым ключом, проблемы факторизации целых чисел и дискретного логарифмирования стали объектом пристального изучения математиков всего мира. За последние годы в этой области наблюдался значительный прогресс. Подтверждением тому может служить следующий казус: в 1977 г. Р. Ривест заявил, что разложение на множители 125-разрядного числа потребует 40 квадриллионов лет, однако уже в 1994 г. было факторизовано число, состоящее из 129 двоичных разрядов!

Задача дискретного логарифмирования считается более сложной, чем задача факторизации. Если будет найден полиномиальный алгоритм ее решения, станет возможным и разложение на множители (обратное не доказано).

Последние достижения теории вычислительной сложности показали, что общая проблема логарифмирования в конечных полях уже не является достаточно прочным фундаментом. Наиболее эффективные на сегодняшний день алгоритмы дискретного логарифмирования имеют уже не экспоненциальную, а субэкспоненциальную временную сложность. Это алгоритмы "index-calculus", использующие факторную базу. Первый такой *алгоритм* для вычисления дискретного логарифма в простом поле Zp был предложен Л. Адлеманом. На практике алгоритм Адлемана оказался недостаточно эффективным; Д. Копперсмит, А. Одлыжко и Р. Шреппель предложили свою версию субэкспоненциального алгоритма дискретного логарифмирования – «COS». Алгоритм решета числового поля, предложенный О. Широкауэром, при p>10100 работает эффективнее различных модификаций метода COS.

Ряд успешных *атак* на системы, основанные на сложности дискретного логарифмирования в конечных полях, привел к тому, что стандарты *ЭЦП* России и США, которые были приняты в 1994 г. и базировались на схеме Эль-Гамаля, в 2001 году были обновлены: переведены на *эллиптические кривые*. Схемы *ЭЦП* при этом остались прежними, но в качестве чисел, которыми они оперируют, теперь используются не элементы конечного поля GF(2n) или GF(p), а эллиптические числа - решения уравнения эллиптических кривых над указанными конечными полями. Алгоритмов, выполняющих дискретной логарифмирование на эллиптических кривых в общем случае хотя бы с субэкспоненциальной сложностью, на сегодняшний день не существует, хотя работы в этом направлении ведутся. Так, для эллиптических кривых специального вида наш соотечественник И. Семаев указал способ сведения задачи логарифмирования в группе точек эллиптической кривой к задаче логарифмирования в некотором расширении простого поля.

* 1. **Криптоанализ хеш-функций**

Основная *атака*на хеш - это метод коллизий. Пусть M и M' - сообщения, H - хеш-*функция*, а ЭЦП представляет собой некоторую функцию S от хеша сообщения: C=S(H(M)). Законный обладатель пары "открытый *ключ* - секретный *ключ* " готов подписать сообщение M, но *злоумышленник* заинтересован в получении подписи под сообщением M'. Если M' выбрано так, что H(M)=H(M'), то *злоумышленник* может предъявить пару (M',C'): тогда *атака* удалась. Реализовать подбор такого сообщения можно методом, который основан на упомянутом выше "парадоксе дней рождения". Варьируя интервалы, шрифты, формат и т.п., *злоумышленник* получает n пар вариантов M и M' без изменения их смысла. Сообщения M1…Mn отличаются слабо, а их хеш-функции - значительно, т.е. можно считать, что значения хеш-функций выбираются случайно, равновероятно и независимо друг от друга. Тогда при   ( t>0 - некоторая константа, N - *мощность множества* всевозможных хеш-функций) *вероятность* того, что имеется пара сообщений , для которых  , вычисляется по формуле .

Этот метод *криптоанализа*породил требования устойчивости к коллизиям для хеш-функций.

**2.10 Криптоанализ по побочным каналам**

*Атаки по сторонним, или побочным, каналам* используют информацию, которая может быть получена с устройства *шифрования* и не является при этом ни открытым текстом, ни шифртекстом. Такие *атаки*основаны на корреляции между значениями физических параметров, измеряемых в разные моменты во время вычислений, и внутренним состоянием вычислительного устройства, имеющим *отношение* к секретному *ключу*. Этот подход менее обобщённый, но зачастую более мощный, чем классический *криптоанализ*.

В последние годы количество криптографических *атак*, использующих слабости в реализации и размещении механизмов криптоалгоритма, резко возросло. Противник может замерять время, затрачиваемое на выполнение криптографической *операции*, или анализировать поведение криптографического устройства при возникновении определённых ошибок вычисления. Другой подход предполагает отслеживание *энергии*, потребляемой смарт-картой в процессе выполнения операций с секретным *ключом* (например, *расшифрования* или генерации подписи). Побочную информацию собрать порой несложно - на сегодняшний день выделено более десяти побочных каналов, в т.ч. электромагнитное излучение, ошибки в канале связи, кэш-память и световое излучение. Более подробное описание перечисленных типов *атак* можно найти в материалах доклада А.Е.Жукова на конференции РусКрипто2006, использованных при подготовке данного раздела.

При этом атаки по побочным каналам используют особенности реализации (поэтому их иногда называют также называют атаками на реализацию - implementation attacks) для извлечения секретных параметров, задействованных в вычислениях. Такой подход менее обобщённый, поскольку привязан к конкретной реализации, но зачастую более мощный, чем классический криптоанализ.

В последние годы резко возросло количество криптографических атак, использующих особенности реализации и рабочей среды. Например, противник может отслеживать энергию, потребляемую смарт-картой, когда она выполняет операции с закрытым ключом, такие, как расшифрование или генерация подписи. Противник может также замерять время, затрачиваемое на выполнение криптографической операции, или анализировать поведение криптографического устройства при возникновении определённых ошибок. Побочную информацию на практике собрать порой несложно, поэтому нужно обязательно учитывать такую угрозу при оценке защищённости системы.



Рис. 2.2 Виды побочных каналов

Атаки по побочным каналам классифицируются по следующим трём типам:

* + по контролю над вычислительным процессом: *пассивные* и *активные*.
	+ по способу доступа к модулю: *агрессивные* (invasive), *полуагрессивные* (semi- invasive) и *неагрессивные* (non-invasive).
	+ по методу, применяемому в процессе анализа: простые – simple side channel attack (*SSCA*) и разностные – differential side channel attack (*DSCA*).

На сегодняшний день выделено более десяти побочных каналов. Атаки различаются по виду используемого побочного канала (рис. 2.2): атаки по времени исполнения (Timing Attacks), атаки по энергопотреблению (Power Analysis Attacks), атаки по ошибкам вычислений (Fault Attacks), атаки по электромагнитному излучению (ElectroMagnetic Analysis), атаки пo ошибкам в канале связи (Error Message Attacks). Существуют и более изощренные виды атак: атаки по кэш-памяти (Cache-based Attacks), акустические атаки (Acoustic Attacks), атаки по световому излучению (Visible Light Attacks).

**2.11 Нанотехнологии в криптоанализе**

С помощью квантового компьютера можно проводить вычисления, не реализуемые на сегодняшних (классических) компьютерах.

В 1994 году П. Шор открыл так называемый "ограниченно-вероятностный" *алгоритм* факторизации, который позволяет разложить на множители число N за полиномиальное от размерности задачи время  . *Алгоритм* Шора разложения чисел на множители явился главным достижением в области квантовых вычислительных алгоритмов. Это был не только крупный успех математики. Именно с этого момента началось усиленное финансирование *работ* по созданию квантовых компьютеров.

Важно отметить, что *алгоритм* Шора чрезвычайно прост и довольствуется гораздо более скромным аппаратным обеспечением, чем то, которое понадобилось бы для универсального квантового компьютера. Поэтому вероятно, что квантовое устройство для разложения на множители будет построено задолго до того, как весь *диапазон* квантовых вычислений станет технологически осуществимым. На сегодняшний день есть конкретные результаты. Так, IBM продемонстрировала использование созданного в лабораториях компании семикубитового квантового компьютера для факторизации чисел по алгоритму Шора. Хотя решённая им задача вряд ли способна поразить воображение (*компьютер* верно определил, что делителями числа 15 являются числа 5 и 3), это самое сложное *вычисление* в области теории чисел за всю историю квантовых компьютеров.

Самые необычные и достаточно спорные подходы к исследованию криптографических систем такие как нейронные сети и генетические алгоритмы на данный момент не привели к сколько-нибудь серьезным прорывам во взломе шифров и представляют в большей степени академический интерес, чем практический. Но, не исключено, что со временем их значение в криптологии возрастет.

Выводы:

Любой может создать алгоритм, который не сможет сам взломать. Это не очень трудно. Что трудно, так это криптоанализ. И только опытный криптоаналитик может создать хороший шифр. И существует только один способ получить этот опыт - анализировать шифры других людей.

1. **АНАЛИЗ СТОЙКОСТИ ФИНАНСОВЫХ КРИПТОСИСТЕММ.**

При оценке стойкости финансовых криптографических систем защиты информации обычно придерживаются принципа Керкхоффа: стойкость криптосистемы должна быть обеспечена и тогда, когда нарушителю известно полное ее описание. Поэтому при анализе стойкости криптографической системы будем предполагать, что противоборствующей стороне известно детальное описание системы, статистические характеристики используемого языка сообщений, пространства возможных ключей и криптограмм; она может иметь некоторую информацию о контексте сообщения и т.п. Единственное, чего не не должен знать нарушитель – секретный криптографический ключ, используемый пользователями криптографической системы защиты информации [31].

Для оценки стойкости криптографических систем защиты информации используются различные подходы, среди которых наибольший интерес представляют информационно-теоретический, сложностно-теоретический и системный подходы.

В соответствии с информационно-теоретическим подходом к оценке стойкости криптографических систем они могут быть разделены на, безусловно стойкие и на условно стойкие криптосистемы. Стойкость безусловно стойких криптографических систем не зависит ни от каких возможностей нарушителя и условий ее определения и не может быть уменьшена ни при каких обстоятельствах.

Стойкость условно стойких криптографических систем зависит от возможностей противоборствующей стороны и условий ее определения, и ее оценки могут меняться в зависимости от многих факторов.

Выяснение вопроса, является ли криптосистема безусловно или условно стойкой, составляет важную задачу информационно-теоретического подхода к оценке стойкости финансовых криптографических систем защиты информации. Если в рамках информационно-теоретического подхода криптосистема признана условно стойкой, то уточнить степень ее стойкости можно с использованием сложностно-теоретического и системного подходов. В научно-технической литературе информационно-теоретический подход иногда относят к классу теоретических подходов к оценке стойкости криптосистем, а остальные – к классу практических подходов. На рис. 10.2 приведена классификационная схема оценок стойкости криптографических систем защиты информации.

Среди средств защиты информации от возможных атак нарушителя выделяются средства криптографической защиты информации. На них могут возлагаться следующие основные задачи:

* обеспечение секретности (конфиденциальности) передаваемой, обрабатываемой и хранимой информации;
* обеспечение целостности передаваемой, обрабатываемой и хранимой информации;
* обеспечение подлинности сообщений и корреспондентов (пользователей), а также подлинности взаимодействующих сетей и систем;
* установление авторства передаваемых и хранимых сообщений;
* обеспечение доступности для законных корреспондентов (пользователей) информации, ресурсов и услуг;
* обеспечение целостности самих средств криптографической защиты информации.

Все современные криптоалгоритмы базируются на принципе Кирхгофа, согласно которому секретность шифра обеспечивается секретностью ключа, а не секретностью алгоритма шифрования. В некоторых ситуациях (например, в военных, разведывательных и дипломатических ведомствах) нет никаких причин делать общедоступным описание сути криптосистемы. Сохраняя такую информацию в тайне, можно дополнительно повысить надежность шифра. Однако полагаться на секретность этой информации не следует, так как рано или поздно она будет скомпрометирована. Поэтому анализ надежности таких систем всегда должен проводиться исходя из того, что противник имеет всю информацию о применяемом криптоалгоритме, ему не известен только реально использованный ключ. В связи с вышеизложенным можно сформулировать общее правило: при создании или при анализе стойкости криптосистем не следует недооценивать возможностей противника. Их лучше переоценить, чем недооценить.

Стойкость криптосистемы зависит от сложности алгоритмов преобразования, длины ключа, а точнее, от объема ключевого пространства, метода реализации: при программной реализации необходимо дополнительно защищаться от разрушающих программных воздействий (закладок, вирусов и т. п.). Хотя понятие стойкости шифра является центральным в криптографии, количественная оценка криптостойкости – проблема до сих пор нерешенная.



Рис.3.1 Классификационная схема оценок стойкости криптосистем

**3.1 Алгоритм Blowfish**

Алгоритм Blowfish разработан Брюсом Шнайером в 1994 г. Автор алгоритма предложилBlowfish в качестве замены стандарту DES. Несомненно, в 1994 г. замена DES на новый стандарт шифрования была уже актуальна из-за корот­кого ключа DES, который уже тогда можно было найти путем полного пере­бора. Брюс Шнайер предположил, что других реальных кандидатов на заме­ну DES нет, в частности, по следующим причинам (описаны Шнайером в спецификации алгоритма Blowfish [342]):

* многие известные и криптографически стойкие (считающиеся таковыми на момент разработки алгоритма Blowfish) алгоритмы, например, IDEA или REDOC–II, являются запатентованными, что ограничи¬вает их использование;
* спецификация алгоритма ГОСТ 28147-89 не содержит значений таблиц замен, т. е., по мнению Шнайера, алгоритм описан не полностью;
* алгоритм Skipjack вообще являлся секретным на тот момент.

Алгоритм Blowfish оказался весьма «удачным». Он очень широко реализован в различных шифровальных средствах — на сайте Шнайера приведен список из примерно 150 продуктов, которые шифруют алгоритмом Blowfish. Однако заменой стандарту DES он все же не стал.

Поскольку Blowfish предполагался в качестве замены алгоритма DES, он, аналогично DES, шифрует данные 64-битными блоками. Размер ключа алго­ритма является переменным — от 32 до 448 битов.

Алгоритм представляет собой сеть Фейстеля, его структура Приложение 1. Шифрование данных выполняется в 16 раундов, в каждом из которых над левым 32-битным субблоком данных производятся следую­щие действия [28, 342]:

1. Значение субблока складывается с ключом /-го раунда операцией XOR, результат операции становится новым значением субблока.

2. Субблок обрабатывается функцией F (описана далее), результат обработ­ки накладывается на правый субблок операцией XOR.

3. Субблоки меняются местами во всех раундах, кроме последнего.

После 16 раундов выполняется наложение на субблоки еще двух подключей: КХ1 и Кх% складываются операцией XOR с правым и левым субблоками со­ответственно.

Функция F (Приложение 1) обрабатывает субблок следующим образом:

1. 32-битное входное значение делится на 4 фрагмента по 8 битов, каждый из которых «прогоняется» через одну из таблиц замен SX…S4 с получени­ем четырех 32-битных выходных фрагментов. Таблицы замен содержат по 256 значений по 32 бита, они не являются фиксированными и зависят от ключа шифрования, принципы их вычисления подробно описаны далее.

2. Первые два выходных фрагмента складываются по модулю 2 .

3. Результат предыдущего шага складывается операцией XOR с третьим вы­ходным фрагментом.

4. Выходное значение функции F получается путем сложения результата предыдущего шага с четвертым выходным фрагментом по модулю 232.

То есть функцию F можно определить так:

F(x) = ((Sl(xl) + S2(x2) mod 232)0S3(x3)) + S4 (x4) mod 232,

где xx…x4 — 8-битные фрагменты входного значения х

Расшифровывание выполняется аналогично зашифровыванию, но ключи Кх…КХ используются в обратном порядке.

Процедура расширения ключа

Задача процедуры расширения ключа состоит в вычислении на основе ключа шифрования значений ключей раундов КХ…КХ% и таблиц замен SX…S4 . Для этого используется весьма сложная процедура расширения ключа, состоящая из следующих шагов:

1. Исходные значения ключей раундов и таблиц замен инициализируются фиксированной псевдослучайной строкой, в качестве которой использует­ся шестнадцатеричная запись дробной части числа я; инициализированная последовательность ключей КХ…КХ% приведена в табл. 3.9.

Таблица 3.1

Последовательность ключей КХ…КХ%

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 243f6a88 | 85a308d3 | 13198а2е | 03707344 | а4093822 | 29913IdO |
| 082efa98 | ес4е6с89 | 452821е6 | 38d01377 | be5466cf | 34е90с6с |
| с0ас29Ь7 | c97c50dd | 3f84d5b5 | Ь5470917 | 9216d5d9 | 8979fblb |

2. Операцией XOR на накладываются первые 32 бита ключа шифрова­ния, на К2 — следующие 32 бита и т. д. до £18. Если используется более короткий ключ шифрования, чем необходимо для наложения на КХ…КХ%, то ключ шифрования накладывается циклически.

3. С использованием полученных ключей раундов и таблиц замен выпол­няется шифрование алгоритмом Blowfish блока данных, состоящего из 64 нулевых битов. Результат становится новым значением ключей Кхи К2.

4. Результат предыдущего этапа снова шифруется алгоритмом Blowfish (причем уже с измененными значениями ключей Кх и К2)ч в результате получаются новые значения ключейК3 и КА.

5. Шифрование выполняется до тех пор, пока новыми значениями не будут заполнены все ключи раундов и таблицы замен.

Достоинства и недостатки алгоритма:

* «Алгоритм Blowfish не годится для применения в случаях, где требуется частая смена ключей». Процедура расширения ключа является достаточно ресурсоемкой, поэтому одно из достоинств алгоритма Blowfish — доста­точно высокая скорость шифрования — проявляется только в тех случаях, если на одном ключе шифруется достаточно большой объем информации. И наоборот, если менять ключ после каждого из шифруемых блоков, ско­рость алгоритма становится катастрофически низкой именно из-за необ­ходимости каждый раз выполнять расширение ключа. Сам Шнайер реко­мендует в приложениях, где критична скорость, хранить уже развернутый ключ (т.е. значения АГ1…ЛГ18 и 5j…54) и загружать его целиком вместо выполнения расширения исходного ключа шифрования [28].
* «Большие требования к памяти не позволяют использовать этот алгоритм в смарт-картах». Стоит сказать, что принципиальная возможность реали­зации алгоритма в смарт-картах была одним из важных условий при вы­боре нового стандарта шифрования США на конкурсе AES, т. е. данный недостаток алгоритма Blowfish можно считать серьезным [284].
* Кроме того, стоит отметить и менее серьезные недостатки алгоритма:
* невозможность расширения ключа параллельно процессу шифрования;
* небольшой по современным меркам размер блока шифруемых данных. АлгоритмBlowfish имеет и достаточно серьезные преимущества, в частности:
* как было сказано выше, высокая скорость шифрования на развернутом ключе (см. также [344]);
* простота алгоритма, снижающая вероятность ошибок при его реализации;
* отсутствие известных успешных атак на полнораундовую версию алго­ритма.

Однако стоит сказать, что известный эксперт Серж Воденэ обнаружил, что методом дифференциального криптоанализа r-раундового алгоритма Blowfish с известными таблицами замен можно вычислить значения КХ…КХ% при наличии 28г+1 выбранных открытых текстов [381]. Это не актуально для полнораундовой версии алгоритма (и, тем более, для описанной выше полно­ценной версии алгоритма с вычисляемыми таблицами замен), но при исполь­зовании слабого ключи (Серж Воденэ обнаружил также у алгоритма Blowfish наличие слабых ключей, которые приводят к генерации слабых таблиц за­мен) выбранных открытых текстов требуется существенно меньше: 24/ + 1.

Вероятность, что произвольный ключ окажется слабым, составляет 2~ . Данная атака не является критичной, поскольку для полноценной версии ал­горитма слабые ключи не страшны [28, 341].

Явные достоинства и отсутствие критичных недостатков предопределили широкое использование алгоритма Blowfish.

**3.2 Стандарт ГОСТ 28147-89**

Алгоритм, определяемый ГОСТ 28147-89 (рис. 3.2), имеет длину ключа шифрования 256 бит. Он шифрует информацию блоками по 64 бит (такие алгоритмы называются блочными), которые затем разбиваются на два субблока по 32 бит (N1 и N2). Субблок N1 обрабатывается определенным образом, после чего его значение складывается со значением субблока N2 (сложение выполняется по модулю 2, т. е. применяется логическая операция XOR - "исключающее или"), а затем субблоки меняются местами. Данное преобразование выполняется определенное число раз ("раундов"): 16 или 32 в зависимости от режима работы алгоритма. В каждом раунде выполняются две операции.



Рис. 3.2. Схема алгоритма ГОСТ 28147-89.

Первая - наложение ключа. Содержимое субблока N1 складывается по модулю 2[32] с 32-бит частью ключа Kx. Полный ключ шифрования представляется в виде конкатенации 32-бит подключей: K0, K1, K2, K3, K4, K5, K6, K7. В процессе шифрования используется один из этих подключей - в зависимости от номера раунда и режима работы алгоритма.

Вторая операция - табличная замена. После наложения ключа субблок N1 разбивается на 8 частей по 4 бит, значение каждой из которых заменяется в соответствии с таблицей замены для данной части субблока. Затем выполняется побитовый циклический сдвиг субблока влево на 11 бит.

Табличные замены (Substitution box - S-box) часто используются в современных алгоритмах шифрования, поэтому стоит пояснить, как организуется подобная операция. В таблицу записываются выходные значения блоков. Блок данных определенной размерности (в нашем случае - 4-бит) имеет свое числовое представление, которое определяет номер выходного значения. Например, если S-box имеет вид 4, 11, 2, 14, 15, 0, 8, 13, 3, 12, 9, 7, 5, 10, 6, 1 и на вход пришел 4-бит блок "0100" (значение 4), то, согласно таблице, выходное значение будет равно 15, т. е. "1111" (0 а 4, 1 а 11, 2 а 2 ...).

Алгоритм, определяемый ГОСТ 28147-89, предусматривает четыре режима работы: простой замены, гаммирования, гаммирования с обратной связью и генерации имитоприставок. В них используется одно и то же описанное выше шифрующее преобразование, но, поскольку назначение режимов различно, осуществляется это преобразование в каждом из них по-разному.

В режиме простой замены для зашифрования каждого 64-бит блока информации выполняются 32 описанных выше раунда. При этом 32-бит подключи используются в следующей последовательности:

K0, K1, K2, K3, K4, K5, K6, K7, K0, K1 и т. д. - в раундах с 1-го по 24-й;

K7, K6, K5, K4, K3, K2, K1, K0 - в раундах с 25-го по 32-й.

Расшифрование в данном режиме проводится точно так же, но с несколько другой последовательностью применения подключей:

K0, K1, K2, K3, K4, K5, K6, K7 - в раундах с 1-го по 8-й;

K7, K6, K5, K4, K3, K2, K1, K0, K7, K6 и т. д. - в раундах с 9-го по 32-й.

Все блоки шифруются независимо друг от друга, т. е. результат зашифрования каждого блока зависит только от его содержимого (соответствующего блока исходного текста). При наличии нескольких одинаковых блоков исходного (открытого) текста соответствующие им блоки шифртекста тоже будут одинаковы, что дает дополнительную полезную информацию для пытающегося вскрыть шифр криптоаналитика. Поэтому данный режим применяется в основном для шифрования самих ключей шифрования (очень часто реализуются многоключевые схемы, в которых по ряду соображений ключи шифруются друг на друге). Для шифрования собственно информации предназначены два других режима работы - гаммирования и гаммирования с обратной связью.

В режиме гаммирования каждый блок открытого текста побитно складывается по модулю 2 с блоком гаммы шифра размером 64 бит. Гамма шифра - это специальная последовательность, которая получается в результате определенных операций с регистрами N1 и N2 (см. рис. 1).

1. В регистры N1 и N2 записывается их начальное заполнение - 64-бит величина, называемая синхропосылкой.

2. Выполняется зашифрование содержимого регистров N1 и N2 (в данном случае - синхропосылки) в режиме простой замены.

3. Содержимое регистра N1 складывается по модулю (232 - 1) с константой C1 = 224 + 216 + 28 + 24, а результат сложения записывается в регистр N1.

4. Содержимое регистра N2 складывается по модулю 232 с константой C2 = 224 + 216 + 28 + 1, а результат сложения записывается в регистр N2.

5. Содержимое регистров N1 и N2 подается на выход в качестве 64-бит блока гаммы шифра (в данном случае N1 и N2 образуют первый блок гаммы).

Если необходим следующий блок гаммы (т. е. необходимо продолжить зашифрование или расшифрование), выполняется возврат к операции 2.

Для расшифрования гамма вырабатывается аналогичным образом, а затем к битам зашифрованного текста и гаммы снова применяется операция XOR. Поскольку эта операция обратима, в случае правильно выработанной гаммы получается исходный текст (таблица 3.7).

Таблица 3.7

Зашифрование и расшифрование в режиме гаммирования

|  |  |  |
| --- | --- | --- |
|   | Операция | Результат |
| Исходный текст |   | 100100 |
| Гамма | XOR | 111000 |
| Шифртекст | = | 011100 |
| Гамма | XOR | 111000 |
| Исходный текст | = | 100100 |

Для выработки нужной для расшифровки гаммы шифра у пользователя, расшифровывающего криптограмму, должен быть тот же ключ и то же значение синхропосылки, которые применялись при зашифровании информации. В противном случае получить исходный текст из зашифрованного не удастся.

В большинстве реализаций алгоритма ГОСТ 28147-89 синхропосылка не секретна, однако есть системы, где синхропосылка - такой же секретный элемент, как и ключ шифрования. Для таких систем эффективная длина ключа алгоритма (256 бит) увеличивается еще на 64 бит секретной синхропосылки, которую также можно рассматривать как ключевой элемент.

В режиме гаммирования с обратной связью для заполнения регистров N1 и N2, начиная со 2-го блока, используется не предыдущий блок гаммы, а результат зашифрования предыдущего блока открытого текста (рис. 2). Первый же блок в данном режиме генерируется полностью аналогично предыдущему.



Рис. 3.3. Выработка гаммы шифра в режиме гаммирования с обратной связью.

Рассматривая режим генерации имитоприставок, следует определить понятие предмета генерации. Имитоприставка - это криптографическая контрольная сумма, вычисляемая с использованием ключа шифрования и предназначенная для проверки целостности сообщений. При генерации имитоприставки выполняются следующие операции: первый 64-бит блок массива информации, для которого вычисляется имитоприставка, записывается в регистры N1 и N2 и зашифровывается в сокращенном режиме простой замены (выполняются первые 16 раундов из 32). Полученный результат суммируется по модулю 2 со следующим блоком информации с сохранением результата в N1 и N2.

Цикл повторяется до последнего блока информации. Получившееся в результате этих преобразований 64-бит содержимое регистров N1 и N2 или его часть и называется имитоприставкой. Размер имитоприставки выбирается, исходя из требуемой достоверности сообщений: при длине имитоприставки r бит вероятность, что изменение сообщения останется незамеченным, равна 2-r.Чаще всего используется 32-бит имитоприставка, т. е. половина содержимого регистров. Этого достаточно, поскольку, как любая контрольная сумма, имитоприставка предназначена прежде всего для защиты от случайных искажений информации. Для защиты же от преднамеренной модификации данных применяются другие криптографические методы - в первую очередь электронная цифровая подпись.

При обмене информацией имитоприставка служит своего рода дополнительным средством контроля. Она вычисляется для открытого текста при зашифровании какой-либо информации и посылается вместе с шифртекстом. После расшифрования вычисляется новое значение имитоприставки, которое сравнивается с присланной. Если значения не совпадают - значит, шифртекст был искажен при передаче или при расшифровании использовались неверные ключи. Особенно полезна имитоприставка для проверки правильности расшифрования ключевой информации при использовании многоключевых схем.

Алгоритм ГОСТ 28147-89 считается очень сильным алгоритмом - в настоящее время для его раскрытия не предложено более эффективных методов, чем упомянутый выше метод "грубой силы". Его высокая стойкость достигается в первую очередь за счет большой длины ключа - 256 бит. При использовании секретной синхропосылки эффективная длина ключа увеличивается до 320 бит, а засекречивание таблицы замен прибавляет дополнительные биты. Кроме того, криптостойкость зависит от количества раундов преобразований, которых по ГОСТ 28147-89 должно быть 32 (полный эффект рассеивания входных данных достигается уже после 8 раундов).

**3.3 Стандарт AES**

В отличие от алгоритма ГОСТ 28147-89, который долгое время оставался секретным, американский стандарт шифрования AES, призванный заменить DES, выбирался на открытом конкурсе, где все заинтересованные организации и частные лица могли изучать и комментировать алгоритмы-претенденты.

Конкурс на замену DES был объявлен в 1997 г. Национальным институтом стандартов и технологий США (NIST - National Institute of Standards and Technology). На конкурс было представлено 15 алгоритмов-претендентов, разработанных как известными в области криптографии организациями (RSA Security, Counterpane и т. д.), так и частными лицами. Итоги конкурса были подведены в октябре 2000 г.: победителем был объявлен алгоритм Rijndael, разработанный двумя криптографами из Бельгии, Винсентом Риджменом (Vincent Rijmen) и Джоан Даймен (Joan Daemen).

**3.4 Алгоритм Rijndael**

Алгоритм Rijndael не похож на большинство известных алгоритмов симметричного шифрования, структура которых носит название "сеть Фейстеля" и аналогична российскому ГОСТ 28147-89. Особенность сети Фейстеля состоит в том, что входное значение разбивается на два и более субблоков, часть из которых в каждом раунде обрабатывается по определенному закону, после чего накладывается на необрабатываемые субблоки (см. рис. 1).

В отличие от отечественного стандарта шифрования, алгоритм Rijndael представляет блок данных в виде двухмерного байтового массива размером 4X4, 4X6 или 4X8 (допускается использование нескольких фиксированных размеров шифруемого блока информации). Все операции выполняются с отдельными байтами массива, а также с независимыми столбцами и строками.

Алгоритм Rijndael выполняет четыре преобразования: BS (ByteSub) - табличная замена каждого байта массива (рис. 3); SR (ShiftRow) - сдвиг строк массива (рис. 4). При этой операции первая строка остается без изменений, а остальные циклически побайтно сдвигаются влево на фиксированное число байт, зависящее от размера массива. Например, для массива размером 4X4 строки 2, 3 и 4 сдвигаются соответственно на 1, 2 и 3 байта. Далее идет MC (MixColumn) - операция над независимыми столбцами массива (рис. 5), когда каждый столбец по определенному правилу умножается на фиксированную матрицу c(x). И, наконец, AK (AddRoundKey) - добавление ключа. Каждый бит массива складывается по модулю 2 с соответствующим битом ключа раунда, который, в свою очередь, определенным образом вычисляется из ключа шифрования (рис. 3.4).



Рис. 3.4. Операция BS.



Рис. 3.5. Операция SR.



Рис. 3.6. Операция MC



Рис. 3.7. Операция AK

В каждом раунде (с некоторыми исключениями) над шифруемыми данными поочередно выполняются перечисленные преобразования (рис. 7). Исключения касаются первого и последнего раундов: перед первым раундом дополнительно выполняется операция AK, а в последнем раунде отсутствует MC. В результате последовательность операций при зашифровании выглядит так:

AK, {BS, SR, MC, AK} (повторяется R-1 раз), BS, SR, AK.



Рис. 7. Раунд алгоритма Rijndael.

Количество раундов шифрования (R) в алгоритме Rijndael переменное (10, 12 или 14 раундов) и зависит от размеров блока и ключа шифрования (для ключа также предусмотрено несколько фиксированных размеров).

Расшифрование выполняется с помощью следующих обратных операций. Выполняется обращение таблицы и табличная замена на инверсной таблице (относительно применяемой при зашифровании). Обратная операция к SR - это циклический сдвиг строк вправо, а не влево. Обратная операция для MC - умножение по тем же правилам на другую матрицу d(x), удовлетворяющую условию: c(x) \* d(x) = 1. Добавление ключа AK является обратным самому себе, поскольку в нем используется только операция XOR. Эти обратные операции применяются при расшифровании в последовательности, обратной той, что использовалась при зашифровании.

Rijndael стал новым стандартом шифрования данных благодаря целому ряду преимуществ перед другими алгоритмами. Прежде всего он обеспечивает высокую скорость шифрования на всех платформах: как при программной, так и при аппаратной реализации. Его отличают несравнимо лучшие возможности распараллеливания вычислений по сравнению с другими алгоритмами, представленными на конкурс. Кроме того, требования к ресурсам для его работы минимальны, что важно при его использовании в устройствах, обладающих ограниченными вычислительными возможностями.

Недостатком же алгоритма можно считать лишь свойственную ему нетрадиционную схему. Дело в том, что свойства алгоритмов, основанных на сети Фейстеля, хорошо исследованы, а Rijndael, в отличие от них, может содержать скрытые уязвимости, которые могут обнаружиться только по прошествии какого-то времени с момента начала его широкого распространения.

**3.5 Асимметричное шифрование**

Алгоритмы асимметричного шифрования, как уже отмечалось, используют два ключа: k1 - ключ зашифрования, или открытый, и k2 - ключ расшифрования, или секретный. Открытый ключ вычисляется из секретного: k1 = f(k2).

Асимметричные алгоритмы шифрования основаны на применении однонаправленных функций. Согласно определению, функция y = f(x) является однонаправленной, если: ее легко вычислить для всех возможных вариантов x и для большинства возможных значений y достаточно сложно вычислить такое значение x, при котором y = f(x).

Примером однонаправленной функции может служить умножение двух больших чисел: N = P\*Q. Само по себе такое умножение - простая операция. Однако обратная функция (разложение N на два больших множителя), называемая факторизацией, по современным временным оценкам представляет собой достаточно сложную математическую задачу. Например, разложение на множители N размерностью 664 бит при P ? Q потребует выполнения примерно 1023 операций, а для обратного вычисления х для модульной экспоненты y = ax mod p при известных a, p и y (при такой же размерности a и p) нужно выполнить примерно 1026 операций. Последний из приведенных примеров носит название - "Проблема дискретного логарифма" (DLP - Discrete Logarithm Problem), и такого рода функции часто используются в алгоритмах асимметричного шифрования, а также в алгоритмах, используемых для создания электронной цифровой подписи.

Еще один важный класс функций, используемых в асимметричном шифровании, - однонаправленные функции с потайным ходом. Их определение гласит, что функция является однонаправленной с потайным ходом, если она является однонаправленной и существует возможность эффективного вычисления обратной функции x = f-1(y), т. е. если известен "потайной ход" (некое секретное число, в применении к алгоритмам асимметричного шифрования - значение секретного ключа).

Однонаправленные функции с потайным ходом используются в широко распространенном алгоритме асимметричного шифрования RSA.

**3.6 Алгоритм RSA**

Разработанный в 1978 г. тремя авторами (Rivest, Shamir, Adleman), он получил свое название по первым буквам фамилий разработчиков. Надежность алгоритма основывается на сложности факторизации больших чисел и вычисления дискретных логарифмов. Основной параметр алгоритма RSA - модуль системы N, по которому проводятся все вычисления в системе, а N = P\*Q (P и Q - секретные случайные простые большие числа, обычно одинаковой размерности).

Секретный ключ k2 выбирается случайным образом и должен соответствовать следующим условиям:

1<k2<F(N)

НОД (k2, F(N)) = 1,

где НОД - наибольший общий делитель, т. е. k1 должен быть взаимно простым со значением функции Эйлера F(N), причем последнее равно количеству положительных целых чисел в диапазоне от 1 до N, взаимно простых с N, и вычисляется как *F(N) = (P - 1)\*(Q - 1)*.

Открытый ключ k1 вычисляется из соотношения *(k2\*k1 ) = 1 mod F(N)*, и для этого используется обобщенный алгоритм Евклида (алгоритм вычисления наибольшего общего делителя). Зашифрование блока данных M по алгоритму RSA выполняется следующим образом: *C = M[в степени k1] mod N*. Заметим, что, поскольку в реальной криптосистеме с использованием RSA число k1 весьма велико (в настоящее время его размерность может доходить до 2048 бит), прямое вычисление M[в степени k1] нереально. Для его получения применяется комбинация многократного возведения M в квадрат с перемножением результатов.

Обращение данной функции при больших размерностях неосуществимо; иными словами, невозможно найти M по известным C, N и k1. Однако, имея секретный ключ k2, при помощи несложных преобразований можно вычислить M = Ck2 mod N. Очевидно, что, помимо собственно секретного ключа, необходимо обеспечивать секретность параметров P и Q. Если злоумышленник добудет их значения, то сможет вычислить и секретный ключ k2.

4. **ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ ЦЕНТРАЛИЗОВАННЫХ ФИНАНСОВЫХ ИНФОРМАЦИОННЫХ СЕТЕЙ**

**4.1 Технологии и инструменты обеспечения безопасности информации в системах и сетях**

Технологии и инструменты обеспечения безопасности информации в системах и сетях

Основной особенностью любой сетевой структуры (системы) является то, что её компоненты распределены в пространстве и связь между ними осуществляется физически при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно, радиосвязь и т. п.) и программно — при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена.

Сетевые системы характерны тем, что, наряду с обычными (локальными) непреднамеренными действиями и атаками, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид атак, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые (или удалённые) атаки (Remote Network Attacks). Они характеризуются, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям.

С развитием локальных и глобальных сетей именно удалённые атаки становятся лидирующими как по количеству попыток, так и по успешности их применения и, соответственно, обеспечение безопасности вычислительных и информационных систем и сетей с точки зрения противостояния удалённым атакам приобретает первостепенное значение.

Современные сервисы безопасности функционируют в распределенной среде, поэтому необходимо учитывать наличие как локальных, так и сетевых угроз. В качестве общих можно выделить следующие угрозы:

* обход злоумышленником защитных средств;
* осуществление злоумышленником физического доступа к вычислительной установке, на которой функционирует сервис безопасности;
* ошибки администрирования, в частности, неправильная установка, ошибки при конфигурировании и т.п.;
* переход сервиса в небезопасное состояние в результате сбоя или отказа, при начальной загрузке, в процессе или после перезагрузки;
* маскарад пользователя (попытка злоумышленника выдать себя за уполномоченного пользователя, в частности, за администратора). В распределенной среде маскарад может реализовываться путем подмены исходного адреса или воспроизведения ранее перехваченных данных идентификации/аутентификации;
* маскарад сервера (попытка злоумышленника выдать свою систему за легальный сервер), следствием маскарада сервера может стать навязывание пользователю ложной информации или получение от пользователя конфиденциальной информации;
* использование злоумышленником чужого сетевого соединения или интерактивного сеанса (например, путем доступа к оставленному без присмотра терминалу);
* несанкционированное изменение злоумышленником конфигурации сервиса и/или конфигурационных данных;
* нарушение целостности программной конфигурации сервиса, в частности, внедрение троянских компонентов или получение контроля над сервисом;
* несанкционированный доступ к конфиденциальной (например, регистрационной) информации, в том числе несанкционированное расшифрование зашифрованных данных;
* несанкционированное изменение данных (например, регистрационной информации), в том числе таких, целостность которых защищена криптографическими методами;
* несанкционированный доступ к данным (на чтение и/или изменение) в процессе их передачи по сети;
* анализ потоков данных с целью получения конфиденциальной информации.
* перенаправление потоков данных (в частности, на системы, контролируемые злоумышленником);
* блокирование потоков данных;
* повреждение или утрата регистрационной, конфигурационной или иной информации, влияющей на безопасность функционирования сервиса (например, из-за повреждения носителей или переполнения регистрационного журнала);
* агрессивное потребление злоумышленником ресурсов, в частности, ресурсов протоколирования и аудита, а также полосы пропускания;
* сохранение остаточной информации в многократно используемых объектах.

Ввиду особой опасности таких атак — особенно для государственных предприятий и органов власти — к системам защиты информации предъявляются повышенные требования. Например, для защиты конфиденциальной информации в органах исполнительной власти следует удовлетворить следующие требования.

Выбор конкретного способа подключения к сети Internet, в совокупности обеспечивающего межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры внутренней сети, проведение анализа защищенности узла Интернет, а также использование средств антивирусной защиты и централизованное управление средствами защиты должны производиться на основании рекомендаций документа Гостехкомиссии РФ СТР-К.

Автоматизированные системы защиты (АСЗ) организации должны обеспечивать защиту информации от несанкционированного доступа (НСД) по классу "1Г" в соответствии с "Руководящим документом" Гостехкомиссии РФ "РД. Автоматизированные системы. Защита от НСД к информации. Классификация АСЗ и требования по защите информации".

Средства вычислительной техники и программные средства АСЗ должны удовлетворять требованиям четвертого класса РД Гостехкомиссии России "РД. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации".

Программно-аппаратные средства межсетевого экранирования, применяемые для изоляции корпоративной сети от сетей общего пользования, должны удовлетворять требованиям "РД. Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации" по третьему классу защиты.

Информационные системы должны удовлетворять требованиям ГОСТ ИСО/ МЭК 15408 по защищенности информационных систем в рамках заданных профилей защиты.

Во исполнение приказа Госкомсвязи России от 25 декабря 1997 года №103 "Об организации работ по защите информации в отрасли связи и информатизации при использовании сети Internet" прямое подключение АРМ по управлению оборудованием сетей связи, мониторингу, обработки данных к сети Internet должно быть запрещено.

Программно-аппаратные средства криптографической защиты конфиденциальной информации, в том числе используемые для создания виртуальных защищенных сетей (VPN), должны иметь сертификаты ФАПСИ РФ.

Обязательным является использование средств ЭЦП для подтверждения подлинности документов.

Для введения использования персональных цифровых сертификатов и поддержки инфраструктуры открытых ключей для использования средств ЭЦП и шифрования необходимо создать легитимный удостоверяющий центр (систему удостоверяющих центров).

Политика информационной безопасности должна предусматривать обязательное включение в технические задания на создание коммуникационных и информационных систем требований информационной безопасности.

Должен быть регламентирован порядок ввода в эксплуатацию новых информационных систем, их аттестации по требованиям информационной безопасности.

Для выполнения перечисленных требований и надлежащей защиты конфиденциальной информации в государственных структурах принято использовать сертифицированные средства. Например, средства защиты от несанкционированного доступа (НСД), межсетевые экраны и средства построения VPN, средства защиты информации от утечки и прочие. В частности, для защиты информации от НСД рекомендуется использовать программно- аппаратные средства семейств Secret Net ("Информзащита"), Dallas Lock ("Конфидент"), "Аккорд" (ОКБ САПР), электронные замки "Соболь" ("Информзащита"), USB-токены ("Аладдин") и прочие. Для защиты информации, передаваемой по открытым каналам связи рекомендованы программно-аппаратные межсетевые экраны с функциями организации VPN, например, Firewall-1/VPN-1 (Check Point), "Застава" ("Элвис+"), VipNet ("Инфотекс"), "Континент" ("Информзащита"), ФПСН-IP ("АМИКОН") и другие.

Средства защиты информации для финансовых структур более многообразны, среди них можно выделить следующие средства:

* управления обновлениями программных компонент АСЗ;
* межсетевого экранирования;
* построения VPN;
* контроля доступа;
* обнаружения вторжений и аномалий;
* резервного копирования и архивирования;
* централизованного управления безопасностью;
* предотвращения вторжений на уровне серверов;
* аудита и мониторинга средств безопасности;
* контроля деятельности сотрудников в сети Интернет;
* анализа содержимого почтовых сообщений;
* анализа защищенности информационных систем;
* защиты от спама;
* защиты от атак класса "Отказ в обслуживании" (DoS-атаки);
* контроля целостности;
* инфраструктура открытых ключей;
* усиленной аутентификации и прочие.

На основании политики информационной безопасности и указанных средств защиты информации (СЗИ) разрабатываются конкретные процедуры защиты, включающие распределение ответственности за их выполнение. Процедуры безопасности также важны, как и политики безопасности. Если политики безопасности определяют, что должно быть защищено, то процедуры определяют, как защитить информационные ресурсы компании и КТО конкретно должен разрабатывать, внедрять данные процедуры и контролировать их исполнение.

4.2 **Технологическая модель подсистемы информационной безопасности**

Современные распределенные корпорации, имеющие подразделения на разных континентах, имеют сложную техническую, инженерную и информационную инфраструктуру. Создание информационной сети такой корпорации и её эффективная защита является чрезвычайно сложной концептуальной и технологической задачей.

Первоначальное решение, характерное для последнего десятилетия прошлого века, использовать для формирования сети телефонные линии быстро привело к нагромождению коммуникаций и к невозможности эффективной защиты. Последующее создание и сопровождение собственных корпоративных сетей для обеспечения информационного обмена данными на базе таких линий связи стало обходиться в миллионы долларов.

Быстрое развитие технологий Internet, образование, рост и развитие "всемирной паутины" позволили создать достаточно дешевые и надежные коммуникации. Однако техническая надежность связи вовсе не означала безопасности корпоративных сетей, имеющих выходы в Интернет. Общие принципы построения Интернет и его использование как общедоступной сети с публичными сервисами привели к тому, что стало очень трудно обеспечить надежную защиту от проникновения в корпоративные и государственные сети, построенные на базе протоколов TCP/IP и Internet -приложений — Web, FTP, e-mail и т.д.

Целевое назначение любой корпоративной информационной системы состоит в обеспечении пользователей необходимой информацией в режиме "On Line" и адекватном информационном сопровождении деятельности предприятия.

Базисом КИС является общесистемное программное обеспечение, которое включает операционную систему и программные оболочки, программы общего и прикладного назначения: автоматизированные рабочие места (АРМ) и Web-сервисы общего и специального назначения, СУБД и управление интегрированными вычислительными и мультимедийными приложениями, а также доступом в локальные и внешние сети (рис. 6.8).

4.3 **Схема корпоративной информационной системы, включающей локальные сети и выход в Internet**

Схема корпоративной информационной системы, включающей локальные сети и выход в Internet, Приложение 2

Физически нижний уровень КИС базируется на серверах, рабочих станциях, персональных компьютерах различного назначения и коммуникационных устройствах, а также на программном обеспечении, реализующем работу перечисленных устройств. В связи с этим подсистема ИБ начинается с защиты именно этого программно-аппаратного оборудования. С этой целью можно использовать известные защитные средства операционных систем, антивирусные пакеты, средства и устройства аутентификации пользователя, средства криптографической защиты паролей и данных прикладного уровня. Все эти средства образуют базу для реализации первого уровня технологической модели подсистемы ИБ (рис. 6.9) [Соколов А. В., Шаньгин В. Ф. 2002].

4.4 Четырехуровневая технологическая модель подсистемы информационной безопасности



Рис. 4.1. Четырехуровневая технологическая модель подсистемы информационной безопасности

Второй физический уровень КИС — рабочие станции, серверы и персональные компьютеры объединятся в локальные сети, которые организуют внутреннее Intranet-пространство предприятия и могут быть иметь выходы во внешнее Internet-пространство. В этом случае речь идет о средствах информационной защиты (СЗИ) второго уровня — уровня защиты локальных сетей, который обычно включает:

* средства безопасности сетевых ОС;
* средства аутентификации пользователей (User Authentication Facilities — UAF);
* средства физического и программного разграничения доступа к распределенным и разделяемым информационным ресурсам;
* средства защиты домена локальной сети (Local Area Network Domain — LAND);
* средства промежуточного доступа (Proxy Server) и межсетевые экраны (Firewall);
* средства организации виртуальных локальных подсетей (Virtual Local Area Network — VLAN);
* средства обнаружения атаки и уязвимостей в системе защиты локальных сетей.

Следующий уровень реализации КИС — объединение нескольких локальных сетей географически распределенного предприятия в общую корпоративную Intranet-сеть через открытую сеть на базе современных технологий поддержки и сопровождения таких сетей (Quality of Service — QoS) с использованием открытой среды Internet в качестве коммутационной среды.

В этом случае на третьем уровне защиты КИС используются технологии защищенных виртуальных сетей (Virtual Private Networks — VPN). VPN-технологии часто интегрируются со средствами первого и второго уровней. Такой защищенный VPN-канал может простираться не только до маршрутизаторов доступа и пограничных Fairwall'лов, но и до серверов и рабочих станций локальной сети.

Четвертый уровень защиты КИС — организация защищенного межкорпоративного обмена в среде электронного бизнеса (eBusiness). Методологической и технологической основой такой защиты являются методы и технологии управления публичными ключами и сертификатами криптографической защиты (Public Key Infrastructure — PKI). Суть этих технологий состоит в реализации двух глобальных функций: генерации и корректном распространении ключей и сертификатов, и отслеживании их жизненного цикла. Базой для реализации средств защиты будут электронная цифровая подпись (Electronic Digital Signature — EDS) и VPN-технологии.

Два нижних уровня защиты являются достаточно традиционными, так как они предназначены для обеспечения безопасности конкретной физически реализованной КИС. Верхние два уровня относятся к обеспечению безопасности передачи данных и электронного бизнеса, который осуществляется уже не в физическом, а в виртуальном пространстве, при этом VPN-технологии обеспечивают защищенный обмен данными в межкорпоративном пространстве, а PKI-технологии обеспечивают VPN-устройства ключами и сертификатами. В настоящее время на рынке имеется достаточное число технических и программных решений для защиты данных, информации, систем и сетей. Ниже рассмотрены некоторые базовые технологии на примере криптографической защиты данных, технологий межсетевых экранов, защищенных VPN-каналов связи, антивирусных и биометрических методов.

**4.4 Инновационная одноуровневая сеть повышенной надежности**

Прогресс науки и технологий — это единственный фактор, который всерьез способен изменить неизменные составляющие человеческого социума.

Blockchain — это новая технология, не менее революционная для человечества, чем сотовая связь и интернет.

Грубо говоря, Blockchain — это одноуровневая сеть, в которой нет выделенного центра и в которой валидность трансакций гарантируется не единым выделенным центром, а криптоалгоритмом и, соответственно, всеми участниками сети.

Самым простым примером технологии Blockchain пока является криптовалюта, а самым известным примером криптовалюты пока является биткойн — сетевая валюта, которая полностью анонимна (никогда не известно, кому принадлежит данный биткойн), но которую вообще невозможно украсть, потому что вся цепочка трансакций с данным биткойном хранится в памяти всей сети, и каждая новая трансакция подтверждается историей предыдущих трансакций.

Банк можно ограбить, даже базу данных ЦРУ можно взломать, но биткойн украсть нельзя — по той причине, что его украсть неоткуда. Нет такого сейфа, который можно вскрыть, или сервера, который можно взломать.

Биткойн является частным случаем. К примеру, его анонимность никак не является свойством Blockchain, это просто философия разработчиков биткойна была такова, что он должен быть анонимен. Возможна и ровно другая криптовалюта — относительно которой, наоборот, точно известно, кому она принадлежит.

Но биткойн иллюстрирует одну простую и главную особенность Blockchain — если интернет может передавать на расстоянии *информацию*, то Blockchain может передавать *ценности*.

Современное государство — это в значительной степени монополия на базы данных. По определению считается, что все эти базы — водительские права, паспортные данные, свидетельства на владение собственностью, лежат где-то в государственном архиве, в бумажном, а теперь и в электронном виде.

Но в том-то и дело, что технология Blockchain позволяет в принципе полностью от чьей-либо монополии.

Любую базу данных, в том числе и государственную, можно взломать и добыть в ней конфиденциальную информацию о, скажем, адресе или банковском счете человека. Такая же база данных, но устроенная по технологии Blockchain, в принципе не поддается взлому. При этом все программное обеспечение открытое — любой человек может его видеть.

В одноуровневой системе передачи ценностей не нужны посредники и не нужны гаранты. Вам не нужен нотариус. Вы перевели деньги через Blockchain? Вам не нужен банк.

Во всех этих случаях вам не нужна контролирующая инстанция, которая говорит: «Да, раньше эта квартира принадлежала Маше, а теперь — Пете». Продажа квартиры сразу регистрируется в сети, и ее достоверность подтверждается всей сетью.

Это — новая идеология проведения любых трансакций. Blockchain позволяет вам заключить любой контракт, перевести любые ценности, получить доступ к любой конфиденциальной информации без участия государства и вообще любой другой управляющей инстанции. Когда банки для проведения трансакций будут пользоваться Blockchainом, банк нельзя будет отключить от Blockchain, как его можно отключить от SWIFT.

Технология Blockchain не оставляет от монополии ничего: трансакции отныне подтверждает все общество.

Принцип работы Blockchain на примере криптовалюты, Приложение 1.

Blockchain в цифрах.

Данные исследования Blockchain за 2014 год

* **8,5 млрд долларов США.**Капитализация крупнейшего решения на основе Blockchain в мире (Bitcoin).
* **3,436 млрд. долларов США.**Рекордная сумма сделок за один день с использованием технологии blockchain.
* **102 010 транзакций за один день.**Известное максимальное количество обработанных транзакций за один день сетью.
* **0.**Количество взломов системы blockchain за 4 года его существования.

Объекты Blockchain.

Адрес кошелька.

Уникальный идентификатор внутри системы для получения и отправки средств. Представляет собой 160-битный хэш от [открытого ключа ECDSA](https://ru.wikipedia.org/wiki/ECDSA) ключевой пары.

Пример адреса в сети Bitcoin: «1BitforkXSxd1JpPwq4NzNwN47Ags1voYK»

Всего 34 символа. Допускаются цифры, буквы нижнего и верхнего регистра. Первый символ внутри сети Bitcoin всегда равен «1». Оставшиеся 33 символа тот самый хэш от открытого ключа клиента.

Кстати первый символ кошельков задается в конфигурационном файле. /src/base58.h в параметре: «PUBKEY\_ADDRESS». И еще вы можете заметить, что в примере адреса кошелька просматривается название нашей компании «Bitfork». Это настоящий адрес кошелька (есть специальные программы, которые могут позволить вам сгенерировать адрес кошелька с красивой фразой внутри).

Адреса кошельков не попадают в Blockchain до тех пор, пока на данный адрес не происходит поступление. Вы можете создавать неограниченное количество адресов кошелька локально, в систему попадёт только адрес, через который была проведена хотя бы одна транзакция.

Транзакция.

Транзакция в технологии Blockchain — это основа системы, которая представляется в виде записи во встроенное в кошелек NoSQL хранилище.

Технология Blockchain использует NoSQL хранилище вместо обычной реляционной базы. Наименование СУБД «[Berkeley db](https://ru.wikipedia.org/wiki/Berkeley_DB)» (названа в честь университета Беркли, на базе которого была разработана первая версия данной СУБД). Важная особенность Berkeley db в том, что это встраиваемая БД реализованная в виде библиотеки. Тем самым не требуется отдельное поднятие сервера СУБД для её работы.

Так как Berkeley db является NoSQL хранилищем (хранит записи вида: ключ — значение) достигается высокая производительность при работе с данными, которые можно вытащить по ключу.

Каждая транзакция содержит в себе следующие значения:

1. Уникальный идентификатор транзакции (txid).
2. Количество средств, пересылаемых в транзакции (amount).
3. Размер комиссии за транзакцию (Fee).
4. Количество подтверждений сетью транзакции (confirmations).
5. Время создания транзакции в формате timestamp (time).
6. Адрес отправителя.
7. Адрес получателя.
8. Тип транзакции: отправка средств, генерация новых средств (эмиссия).

Блок.

Блок представляет из себя контейнер, в который производится запись новых транзакций в системе и заголовка содержащего основную информацию о блоке: хэш блока, хэш предыдущего блока, хэш транзакций (вошедших в данный блок). Именно появление такого объекта как блок составляет основу технологии Blockchain.

Blockchain в переводе — цепочка блоков, именно как написано в название, так и реализована технология — всё гениальное просто! Блоки хранят транзакции, а также информацию, которая позволяет создавать как раз-таки цепочку. Достигается это наличием информации о хэше предыдущего блока в заголовке нового генерируемого блока.

Анонимность в Blockchain.

Опасения на счет анонимности сети Bitcoin и соответственно самой технологии Blockchain довольно абсурдны. Во-первых, реализация Blockchain в криптовалюты Bitcoin, Litecoin и большинстве других такова, что все абсолютно транзакции доступны для чтения любым пользователем у которого есть синхронизированный с сетью кошелек (в частности база данных).

Все без исключения значения любой транзакции, перечисленные в данной статье выше доступны для чтения любым человеком!

Если же мы говорим о применении технологии Blockchain в тех областях, где требуется прямое подтверждение личности для использования системы, то этого никто не запрещает! Возможно внедрение сертификатов в вашу систему на основе технологии Blockchain, которые выдаются только после прохождения проверки. Возможна реализация системы генерации индивидуальных кошельков для каждого клиента.

**ЗАКЛЮЧЕНИЕ**

Чтобы снизить вероятность непредсказуемого “обвала”, вновь разработанного криптоалгоритма, необходимо заблаговременное проведение криптографических исследований. Разработка любого шифра предусматривает оценку его стойкости к достаточно разнообразным типам криптоаналитических нападений. Как относиться к заявляемым оценкам стойкости с учетом того, что их получение обычно является довольно сложной задачей? Это зависит от того, кто дает оценку [93]. Стойкость шифра рассматривается как разработчиком, так и критиком (криптоаналитиком). Оценки разработчика шифра можно считать корректными, если он делает некоторые допущения в пользу криптоаналитика. Оценки разработчика будут опровергнуты, если кто-либо укажет другой способ криптоанализа, для которого вычислительная сложность получается меньше заявляемой.

1. Любая криптосистема включает: алгоритм шифрования, набор ключей, используемых для шифрования и систему управления ключами.

2. Криптосистемы решают такие проблемы информационной безопасности как обеспечение конфиденциальности, целостности данных, а также аутентификация данных и их источников.

3. Основным классификационным признаком систем шифрования данных является способ их функционирования.

4. В системах прозрачного шифрования (шифрование "на лету") криптографические преобразования осуществляются в режиме реального времени, незаметно для пользователя.

5. Классические криптографические методы делятся на два основных типа: симметричные (шифрование секретным ключом) и асимметричные (шифрование открытым ключом).

6. В симметричных методах для шифрования и расшифровывания используется один и тот же секретный ключ.

7. Асимметричные методы используют два взаимосвязанных ключа: для шифрования и расшифрования. Один ключ является закрытым и известным только получателю. Его используют для расшифрования. Второй из ключей является открытым, т. е. он может быть общедоступным по сети и опубликован вместе с адресом пользователя. Его используют для выполнения шифрования.

8. Для контроля целостности передаваемых по сетям данных используется электронная цифровая подпись, которая реализуется по методу шифрования с открытым ключом.

9. Электронная цифровая подпись представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

10. При практической реализации электронной подписи также шифруется не все сообщение, а лишь специальная контрольная сумма – хэш, защищающая послание от нелегального изменения. Электронная подпись здесь гарантирует как целостность сообщения, так и удостоверяет личность отправителя.

11. Безопасность любой криптосистемы определяется используемыми криптографическими ключами.

**Список литературы**

1. Конституция Российской Федерации (от 12.12.1993 г.).
2. Авдошин С.М., Белов В.В. Обобщенный метод «волны» для решения экстремальных задач на графах // ЖВМиМФ, 1979, 19, №3. – с. 739-755.
3. Авдошин С.М., Савельева А.А. Алгоритм решения систем линейных уравнений в кольцах вычетов // Информационные технологии. 2006. № 2. с.50-54.
4. Автономов, А.С. Зарубежное избирательное право / А.С. Автономов, Ю.А. Веденеев, О.В. Дегтярева, В.В. Луговой, В.И. Лысенко. - М.: Издательство НОРМА, 2003. — 288 с.
5. Автономов, А.С. Сравнительное избирательное право / А.С. Автономов, Ю.А. Веденеев, В.В. Луговой. - М.: Издательство НОРМА, 2003. — 208 с.
6. Алексеев А. Криптография и криптоанализ: вековая проблема человечества. //
7. Алферов, А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин – М.: Гелиос АРВ, 2002. – 480 с.
8. Амамия М., Танака Ю. Архитектура ЭВМ и искусственный интеллект. М.: Мир, 1993.
9. Андреев, А.Г. и др. Microsoft Windows 2000 Professional. Русская версия / Под. ред. А.Н. Чекмарева и Д.Б. Вишнякова - СПб.: БВХ - Санкт-Петербург, 2000. – 752 с.
10. Анохин М. И. и др. Криптография в банковском деле. М, 1997.
11. Бабаш, А.В. Криптография. Под. ред. В.П. Шерстюка, Э.А. Применко / А.В. Бабаш, Г.П. Шанкин – М.: СОЛОН-ПРЕСС, 2007. – 512 с.
12. Баричев С. Основной вопрос криптографии // Chief Inforamtion Officer – руководитель информационной службы. #5 (37), 2005, c. 93-95.
13. Барсуков, В.С. Безопасность: технологии, средства, услуги. / В.С. Барсуков - М.: КУДИЦ - ОБРАЗ, 2001. – 496 с.
14. Барычев, С. Основы современной криптографии / С. Барычев, Р. Серов. – М.: 2001. – 152 с.
15. Басалова, Г.В. Основы криптографии. [www.intuit.ru](http://www.intuit.ru/).
16. Берд, К. Война — это мир, паспорт — это свобода. [www.computerra.ru](http://www.computerra.ru/).
17. Ботт, Э. Эффективная работа: Безопасность Windows / Э. Ботт, К. Зихерт. – СПб.: Питер, 2003. – 682 с.
18. Варновский Н.П. О стойкости схем электронной подписи с аппаратной поддержкой. Технический отчет. Лаборатория МГУ по математическим проблемам криптографии, 1997.
19. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2004.
20. Введение в криптографию / Под общей ред. В.В. Ященко // СПб.: Питер, 2001.
21. Введение в криптографию / Под. ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.
22. Веденеев, Ю.А. Очерки по истории выборов и избирательного права / Ю.А. Веденеев, И.В. Зайцев, В.Е. Кораблин, В.В. Луговой, В.В. Тылкин. - Калуга : Калужский обл. фонд возрождения историко-культурных и духовных традиций «Символ», 2002. - 692 с.
23. Википедия. [ru.wikipedia.org](http://ru.wikipedia.org/).
24. Винокуров А., Применко Э. Сравнение российского стандарта шифрования, алгоритма ГОСТ 28147-89, и алгоритма Rijndael, выбранного в качестве нового стандарта шифрования США // «Системы безопасности», М., изд. «Гротэк», 2001
25. Винокуров, А.Ю. Традиционные криптографические алгоритмы. [www.enlight.ru/crypto/algorithms/algs.htm](http://www.enlight.ru/crypto/algorithms/algs.htm).
26. Галатенко, В.А. Информационная безопасность: основные стандарты и спецификации. [www.intuit.ru](http://www.intuit.ru/).
27. Галатенко, В.А. Основы информационной безопасности. [www.intuit.ru](http://www.intuit.ru/).
28. Галушкин А. Теория нейронных сетей. М.:ИПРЖР, 2000.
29. Гордиенко, И. ID-cards: о старый, новый дивный мир! Компьютерра - 1999. - №10 (288).
30. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
31. Григг А. Цифровой трейдинг // Компьютерра. 1998. N 12.
32. Грушо А.А., Применко Э.А., Тимонина Е.Е. Анализ и синтез криптоалгоритмов. Курс лекций. Йошкар-Ола: МФ МОСУ, 2000.
33. Доктрина информационной безопасности Российской Федерации (№ Пр-1895 от 06.09.2000 г.).
34. Жуков А.Е. Криптоанализ по побочным каналам (Side Channel Attacks). // Материалы конференции РусКрипто – 2006. // Опубликовано: <http://ruscrypto.ru/sources/publications/>
35. Загнетко А. Информация доступная и недоступная. // Опубликовано: 19.06.2006: [http://pda.cio-world.ru/?action=article&id=273907](http://pda.cio-world.ru/?action=article&amp;id=273907)
36. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры: Учебное пособие. М.: Гелиос АРВ, 2005.
37. Иванов М.А. криптографические методы защиты информации в компьютерных системах и сетях // М.: КУДИЦ-ОБРАЗ, 2001.
38. Кан, Д. Взломщики кодов / Д. Кан – М.: Центрполиграф, 2000. – 594 с.
39. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления. М.: МЦНМО, 1999.
40. Кнут, Д.Э. Искусство программирования, т.2. Получисленные алгоритмы / Д.Э. Кнут - М.: Издательский дом «Вильямс», 2000. – 832 с.
41. Колчин В. Ф. Случайные отображения. М.: Наука, 1984.
42. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ. М.: МЦНМО, 1999.
43. Коутинхо, С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. – М.: Постмаркет, 2001. – 328 с.
44. Кохно, В.О. Информационные системы медицинского страхования на основе пластиковых карт
45. Логачев О.А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
46. Макаров, О. Отдай голос машине: голоса из урны. Популярная механика – 2012. – № 113
47. Малюк, А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазинин, Н.С. Погожин. – М.: Горячая линия - Телеком, 2001. – 148 с.
48. Малюк, А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С. В. Пазизин, Н. С. Погожин - М.: Горячая линия-Телеком, 2001. – 148 с.
49. Мир математики. Т.2: Жуан Гомес. Математики, шпионы и хакеры. Кодирование и криптография. - М.: Де Агостини, 2014. - 144 с.
50. Мир математики. Т.21: Ламберто Гарсия дель Сид. Замечательные числа: Ноль, 666 и другие бестии. - М.: Де Агостини, 2014. - 160 с.
51. Мир математики. Т.3: Энрике Грасиан. Простые числа. Долгая дорога к бесконечности. - М.: Де Агостини, 2014. - 144 с.
52. Мир математики. Т.31: Хоакин Наварро. Тайная жизнь чисел. Любопытные разделы математики. - М.: Де Агостини, 2014. - 160 с.
53. Молдовян Н. Каким быть новому стандарту шифрования? //"Компьютерра" №2 от18.01.2000.
54. Морозова, О.С. Обязательное голосование: мировой опыт и особенности избирательных практик. Каспийский регион: политика, экономика, культура - 2013. - № 3 (36).
55. Мошенский, С.З. Эволюция векселя / С.З. Мошенский. - Ровно: «Планета-друк», 2005. – 446 с.
56. Ожигов Ю.И. Квантовые вычисления. Учебно-методическое пособие. М.: МГУ, факультет ВМиК, 2003.
57. Осипян В.О., Осипян К.В. Криптография в задачах и упражнениях. М.: Гелиос АРВ, 2004.
58. Отставнов М. E. Деньги для XXI века: Цифровая наличность в смарт-картах и сетях Internet // Финансовые риски. 1996. N 3.
59. Отставнов М. E. О контроле за наблюдающим за представителями // Мир карточек. 1998. N 7.
60. Отставнов М. E. Финансовая инфраструктура цифрового хозяйства // Компьютерра. 1997. N 38.
61. Отставнов М. E. Электронная наличность в сетях Internet // Банковские технологии". 1996. N 2.
62. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты / А.А. Петров - М.: ДМК, 2000. – 448 с.
63. Портал ОАО «Универсальная электронная карта». [www.uecard.ru](http://www.uecard.ru/).
64. Риджуэй, А. Целую книгу закодировали в ДНК. Наука в фокусе - 2012 - №11 (013).
65. Риксон, Фред Б. Коды, шифры, сигналы и тайная передача информации / Фред Б. Риксон - М.: АСТ: Астрель, 2011. – 656 с.
66. Ростовцев А.Г. Решеточный криптоанализ // Безопасность информационных технологий. - М.: Изд. МИФИ, 1997, №3. - с. 53-55.
67. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. СПб.: АНО НПО Профессионал, 2005.
68. Ростовцев А.Г., Михайлова Н.В. Методы криптоанализа классических шифров // 1998. Опубликовано[: http://crypto.hotbox.ru/download/cryptoan.zip](http://crypto.hotbox.ru/download/cryptoan.zip)
69. Сабо. Н. Умные контракты. Четвертая революция стоимости // Компьютерра. 1998. N 38.
70. Сачков В.Н. Комбинаторные методы дискретной математики. М.: Наука, 1977.
71. Семаев И. А. О сложности вычисления логарифмов на эллиптических кривых // Вторая международная конференция по теории чисел и ее приложениям, Тула, 1993.
72. Скудис, Э. Противостояние хакерам / Эд Скудис. – М.: ДМК Пресс, 2003. – 512 с.
73. Указ Президента РФ «Перечень сведений конфиденциального характера» (№ 188 06.03.1997 г.).
74. Федеральный закон Российской Федерации «О государственной тайне» (№ 5485-1 от 06.10.1997 г.).
75. Федеральный закон Российской Федерации «О персональных данных» (№ 152 от 27.07.2006 г.).
76. Федеральный закон Российской Федерации «Об информации, информатизации и защите информации» (№ 24-03 от 20.02.1995 г.).
77. Федеральный закон Российской Федерации «Об электронной цифровой подписи» (№ 1-ФЗ от 26.12.2001 г.).
78. Фомичев, В.М. Дискретная математика и криптология / В.М. Фомичев. – М.: ДИАЛОГ-МИФИ, 2003. – 400 с.
79. Хеттинга. Р. А. Подписка на акции приватности // Компьютерра. 1999. N 33-34.
80. Хеттинга. Р. А. Финансовая криптография и геодезическое хозяйство // Компьютерра. 1998. N 7.
81. ЦИК РФ. [cikrf.ru](http://cikrf.ru/).
82. Чуров, В.Е. Российский опыт использования технических средств в ходе региональных и муниципальных выборов 2008–2011 годов / В.Е. Чуров, Н.Е. Конкин, Г.И. Райков, А.В. Иванченко. — М.: РЦОИТ, 2011. — 328 с.
83. Шелков, В.А. История "микроточки". Специальная техника и связь – 2012. – № 3.
84. Шеннон К.Э. Работы по теории информации и кибернетике // М.: И.Л., 1963.
85. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер – М.: ТРИУМФ, 2002. – 816 с.
86. Яковлев, В.В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: Учебник для вузов ж.-д. транспорта / В.В. Яковлев, А.А. Корниенко. – М.: УМК МПС России, 2002. – 328 с.
87. S. Brands. An Efficient Off-Line Electronic Cash System... Report CS-R9323, CWI, 1993.
88. Palaciosa, M.A. and etc. InfoBiology by printed arrays of microorganism colonies for timed and on-demand release of messages. [www.pnas.org/content/early/2011/09/19/1109554108](http://www.pnas.org/content/early/2011/09/19/1109554108).
89. CryptoBloG. Прикладные методы защиты информации. crypto-blog.ru.
90. D. Chaum. Security Without Identification. "Comm. ACM". v. 28. N. 10. 1985.
91. National Institute of Standards and Technology (NIST). FIPS Pub 46-3 (Federal information processing standards publication): Data Encryption Standard (DES). Oct. 1999. csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf. RFIDjournal.com www.technologyreview.com/view/515016/one-time-pad-reinvented-to-make-electronic-copying-impossible.