КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Лекция 1

Отрыванкина Татьяна Михайловна,
доцент, к.ф.-м.н.
Благовисная Анна Николаевна,
к.ф.-м.н.

Содержание дисциплины

№ 1 Введение в криптографические методы

№ 2 Основы теоретико-информационной стойкости

№ 3 Симметричное шифрование

№ 4 Асимметричное шифрование

№ 5 Электронная цифровая подпись

№ 6 Современные средства криптозащиты

ВВЕДЕНИЕ В ПРЕДМЕТ

Информация – фундаментальное, многозначное понятие.

Будем понимать под этим термином сведения, являющиеся объектом сбора (накопления), хранения, обработки (преобразования), непосредственного использования и передачи.

Простейшая модель передачи информации (рисуем)

ВВЕДЕНИЕ В ПРЕДМЕТ

Потребность гражданского общества в специалистах по защите информации.

Специалисты в области информационной безопасности необходимы и в государственных структурах, и в научных учреждениях, и в коммерческих фирмах.

ВВЕДЕНИЕ В ПРЕДМЕТ

ЗИ – совокупность мероприятий и действий, направленных на обеспечение конфиденциальности и целостности в процессе сбора, передачи, обработки и хранения.

Безопасность информации:

– конфиденциальность (секретность, смысловая и информационная скрытность),

– сигнальная скрытность (энергетическая и структурная),

– целостность (устойчивость к разрушающим, имитирующим и искажающим воздействиям и помехам).

ВВЕДЕНИЕ В ПРЕДМЕТ

Криптографическое преобразование **данных является наиболее эффективным и универсальным, а при передаче по протяженным линиям связи – *единственным* реальным средством предотвращения несанкционированного доступа к ней.**

Принципиально не обойтись без криптографии при защите данных, передаваемых по открытым электронным каналам связи, а также там, где необходимо подтверждать целостность электронной информации или доказывать ее авторство.

ВВЕДЕНИЕ В ПРЕДМЕТ

Смарт-карты,

электронная почта,

системы банковских платежей,

торговля через Интернет,

электронный документооборот,

системы электронного голосования и т.д.

ВВЕДЕНИЕ В ПРЕДМЕТ

Для тайной передачи информации есть три возможности:

Создать абсолютно надежный, недоступный для других канал связи между абонентами

Использовать общедоступный канал связи, но скрыть сам факт передачи информации

Использовать общедоступный канал связи, но передавать по нему нужную информацию в так преобразованном виде, чтобы восстановить ее мог только адресат

ВВЕДЕНИЕ В ПРЕДМЕТ

Криптография – наука о шифрах – долгое время была засекречена, так как применялась, в основном, для защиты государственных и военных секретов.

В настоящее время методы и средства криптографии используются для обеспечения информационной безопасности не только государства, но и частных лиц, и организаций.

Наиболее надежные методы защиты от таких угроз дает именно криптография.

СМЕЖНЫЕ ОБЛАСТИ КРИПТОГРАФИИ

ТЕОРИЯ ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

обеспечение целостности информации в условиях случайного воздействия

СТЕГАНОГРАФИЯ

обеспечение скрытности информации

МАТЕМАТИЧЕСКИЕ МЕТОДЫ СЖАТИЯ ДАННЫХ

ЭТАПЫ РАЗВИТИЯ КРИПТОГРАФИИ
(ПО ТЕХНОЛОГИЧЕСКИМ ХАРАКТЕРИСТИКАМ МЕТОДОВ ШИФРОВАНИЯ)

- **Наивная криптография (до начала XVI в.)**
- **Формальная криптография (конец XV в. – начало XX в.)**
- **Научная криптография (30-60 гг. XX в.)**
- **Компьютерная криптография (с 70 гг. XX в.)**

ОСНОВНЫЕ ЧЕРТЫ НАИВНОЙ КРИПТОГРАФИИ

- **Использование любых способов запутывания противника относительно содержания шифруемых текстов.**
- **Применение шифров перестановки или моноалфавитной подстановки (основной принцип — замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами).**

ШИФРЫ НАИВНОЙ КРИПТОГРАФИИ

- **Атба́ш (ивр. ש"אתב) - простой шифр подстановки .**

  Правило шифрования: замена i-й буквы алфавита буквой с номером n на $(i + 1)$-ю букву, где n — число букв в алфавите.

  ОТ:

  abcdefghijklmnopqrstuvwxyz

  ШТ:

  ZYXWVUTSRQPONMLKJIHGFEDCBA

ШИФРЫ НАИВНОЙ КРИПТОГРАФИИ

- **Скитала (шифр древней Спарты)**

Аполлоний Родосский (середина III века до н. э.)

Плутарх (около 45—125 н. э.)

ШИФРЫ НАИВНОЙ КРИПТОГРАФИИ

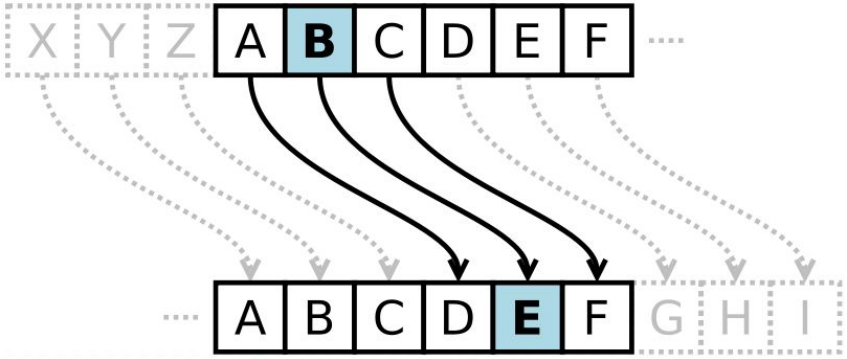
- **Квадрат Полибия**

Изобретен во II веке до н. э. в Древней Греции

Α	Β	Γ	Δ	Ε
Ζ	Η	Θ	Ι	Κ
Λ	Μ	Ν	Ξ	Ο
Π	Ρ	Σ	Τ	Υ
Φ	Χ	Ψ	Ω	

ШИФРЫ НАИВНОЙ КРИПТОГРАФИИ

- **Шифр Цезаря**



ШТ:

YYQL YLGL
YLFL

ОТ:

Veni, vidi, vici

ШИФРЫ НАИВНОЙ КРИПТОГРАФИИ

- **Тайнопись**

  Полная замена одного алфавита на другой

ОСНОВНЫЕ ЧЕРТЫ ФОРМАЛЬНОЙ КРИПТОГРАФИИ

- **Формализованные и относительно стойкие к ручному криптоанализу шифры.**

- **Шифры многоалфавитной подстановки.**

ТРУДЫ ПО КРИПТОГРАФИИ ЭПОХИ ВОЗРОЖДЕНИЯ

- **Роджер Бэкон (XIII в.) «Послание монаха Роджера Бэкона о тайных действиях искусства и природы и ничтожестве магии» (лат. *«Epistola Fratris Rog. Baconis, de secretis operibus artis et naturae et nullitate magiae»*)**
- **7 методов скрытия текста**

ТРУДЫ ПО КРИПТОГРАФИИ ЭПОХИ ВОЗРОЖДЕНИЯ

- **Леон Баттиста Альберти (1404-1472)**

  «Трактат о шифре» (1466) Идея мноноалфавитных шифров.

ТРУДЫ ПО КРИПТОГРАФИИ ЭПОХИ ВОЗРОЖДЕНИЯ

- **Иоганн Тритемий (1462-1516)**

  «Полиграфия» (1518)

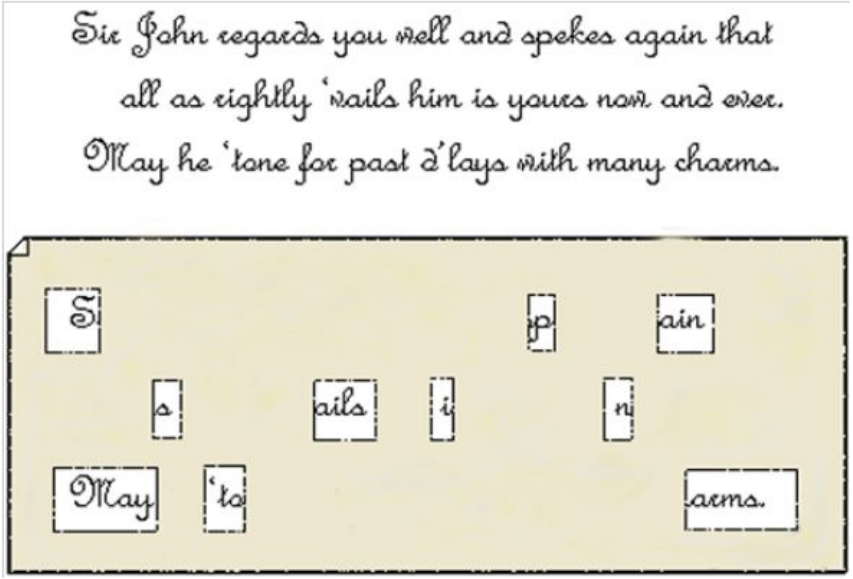
  Способ заполнения полибианского квадрата.

  Шифрование пар букв (биграмм)

Шифр Виженера

ШИФРЫ ФОРМАЛЬНОЙ КРИПТОГРАФИИ

- **Решётка Кардано**



ШИФРЫ ФОРМАЛЬНОЙ КРИПТОГРАФИИ

- **Шифр Плейфера**


Лион Плейфер

Чарльз Уитстон
(1802-1875)
Шифрование
«двойным квадратом»


Чарлз Уитстон

ШИФРЫ ФОРМАЛЬНОЙ КРИПТОГРАФИИ

- **Механические роторные машины**

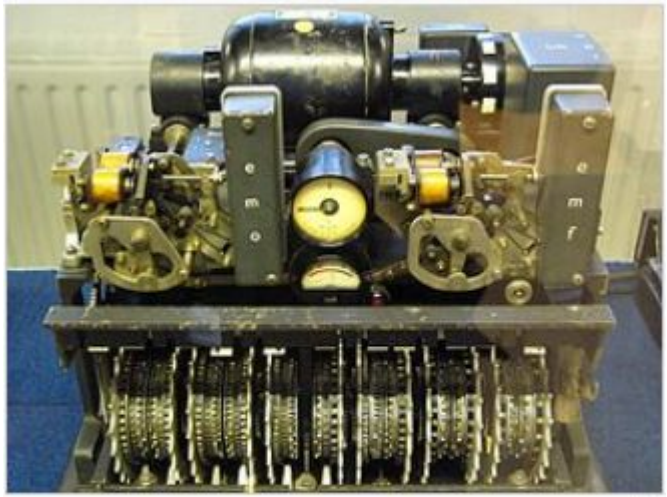
1790-е

Томас Джефферсон (1743-1826)

1817 г.

Чарльз Уитстон

ШИФРЫ ФОРМАЛЬНОЙ КРИПТОГРАФИИ



Немецкая криптомашина Lorenz использовалась во время Второй мировой войны для шифрования самых секретных сообщений

Роторная шифровальная машина Энигма, разные модификации которой использовались германскими войсками с конца 1920-х годов до конца Второй мировой войны[1]

ПРАВИЛО КЕРКХОФФА

- **Огюст Керкгоффс (1835—1903)**

«Военная криптография» (1883)

Секретность шифров должна быть основана на секретности ключа, но не алгоритма

ИСТОКИ НАУЧНОЙ КРИПТОГРАФИИ

- **Жан-Франсуа Шампольон, труд «Краткий очерк иероглифической системы древних египтян или исследования элементов этого письма», 1824 г.**
- **Публикация метода Касиски (1863).**
- **Огюст Керкгоффс, труд «Военная криптография», 1883.**
- **Уильям Ф. Фридман, «Индекс совпадения и его применение в криптографии», 1918.**
- **Введение терминов «криптология» и «криптография» (1920, Фридман).**
- **Появление электромеханических машин (1920-е).**
- **Лестер Хилл, публикация в журнале «The American Mathematical Monthly» статьи «Cryptography in an Algebraic Alphabet», 1929**

ИСТОКИ НАУЧНОЙ КРИПТОГРАФИИ

- **К началу 30-х годов окончательно сформировались разделы математики, являющиеся научной основой криптологии - общая алгебра, теория чисел, теория вероятностей и математическая статистика.**
- **К концу 1940-х годов построены первые программируемые счётные машины, заложены основы теории алгоритмов, кибернетики**

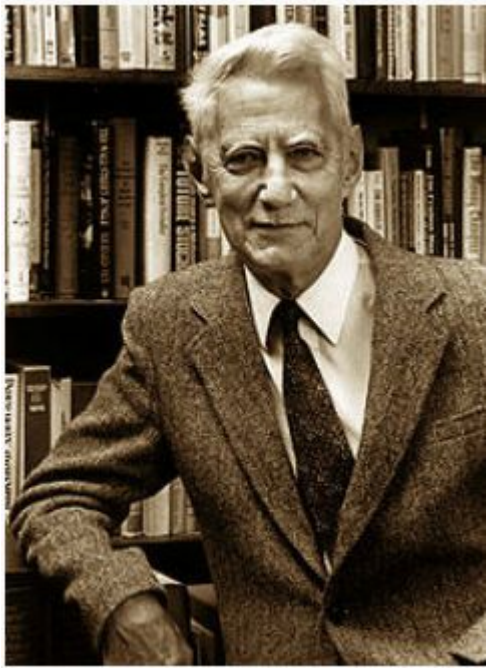
ОСНОВНЫЕ ЧЕРТЫ НАУЧНОЙ КРИПТОГРАФИИ

- **Появление криптосистем со строгим математическим обоснованием криптостойкости**
- **Появление теоретических принципов криптографической защиты информации**

ПОДХОД К КРИПТОГРАФИИ КАК МАТЕМАТИЧЕСКОЙ НАУКЕ

- **Клод Шеннон**

«Теория связи в секретных системах» (*Communication Theory of Secrecy Systems*) — секретный доклад, представленный автором в 1945 г., опубликован в «Bell System Technical Journal» в 1949 г.



ВВЕДЕНИЕ В ПРЕДМЕТ

Криптография как научная дисциплина молода:

строгое математическое обоснование криптостойкости появилось только в 30-60 годах XX века, а возможность большой скорости шифрования и увеличения криптостойкости в разы обеспечили вычислительные системы с 70-х годов XX века.

ВВЕДЕНИЕ В ПРЕДМЕТ

Клод Шеннон

Доклад "Математическая теория криптографии" (1945 г.)

Рассекречен и опубликован в 1948 г.

Переведен на русский язык в 1963 г.

Шеннон смог получить верхнюю оценку на длину шифртекста, которую необходимо учитывать для того, чтобы при криптоанализе достичь любого требуемого уровня достоверности его раскрытия.

ВВЕДЕНИЕ В ПРЕДМЕТ

Для профессионального понимания криптографических алгоритмов и умения оценивать их сильные и слабые стороны необходима серьезная математическая подготовка (на уровне математических факультетов университетов).

Это объясняется том, что современная криптография основана на глубоких результатах таких разделов математики, как

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ

общая алгебра **теория чисел**

теория вероятностей и математическая статистика

теория алгоритмов **теория информации**

теория вычислительной сложности

кибернетика

Криптология

Криптография

обеспечение конфиденциальности, аутентичности

Криптоанализ

нарушение конфиденциальности, аутентичности

Конфиденциальность – невозможность получения интересующей информации без знания дополнительной информации.

Аутентичность – подлинность авторства и целостности.

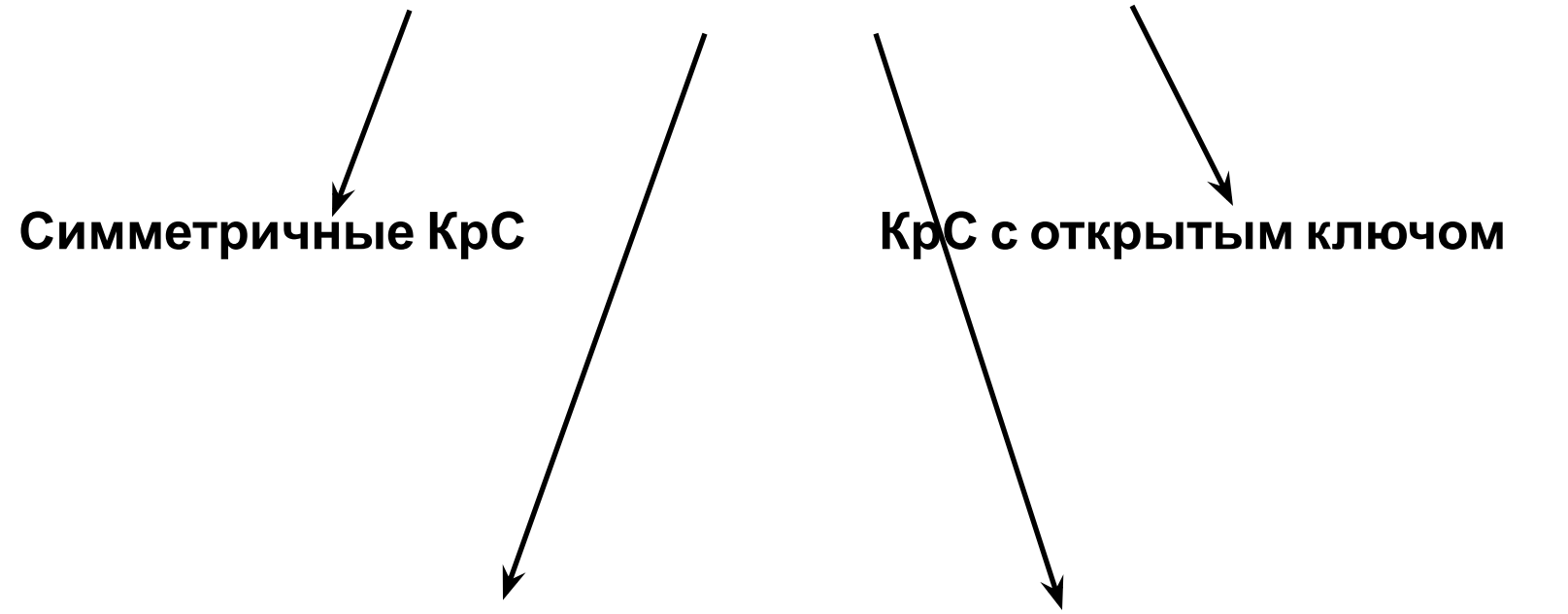
СТОЙКОСТЬ КРИПТОСИСТЕМЫ

Количество усилий, потраченных квалифицированными криптоаналитиками при неудачных попытках ее раскрытия

Теория информации:
Криптограф уповает на то, что криптоаналитик не будет располагать достаточной информацией для того, чтобы дешифровать криптограмму

Теория сложности вычислений:
Криптограф рассчитывает только на то, что у криптоаналитика не хватит времени, чтобы дешифровать криптограмму

РАЗДЕЛЫ СОВРЕМЕННОЙ КРИПТОГРАФИИ



СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Фомичев В.М. Дискретная математика и криптология. Курс лекций. – М.: ДИАЛОГ-МИФИ, 2003. – 400 с.
2. Смарт Н. Криптография. – М.: Техносфера, 2005.
3. Нечаев В.И. Элементы криптографии (Основы теории защиты информации). – М.: Высшая школа, 1999. – 109 с.
4. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002
5. Биркгоф Г., Барти Т. Современная прикладная алгебра. – СПб.: Лань, 2005.
6. Акритас А. Основы компьютерной алгебры (с приложениями). – М.: Мир, 1994.
7. Ван Тилборг **Х.К.А.** Основы криптологии. – М.: Мир, 2006.
8. Виноградов И.М. Основы теории чисел. – Спб.: Лань, 2004.
9. Судоплатов С.В., Овчинникова Е.В. Элементы дискретной математики: Учеб. для вузов / С.В. Судоплатов. – Новосибирск: НГТУ, 2002.
10. Лидл Р., Пильц Г. Прикладная абстрактная алгебра. – Екатеринбург, 1996.