КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Введение

Основные цели курса

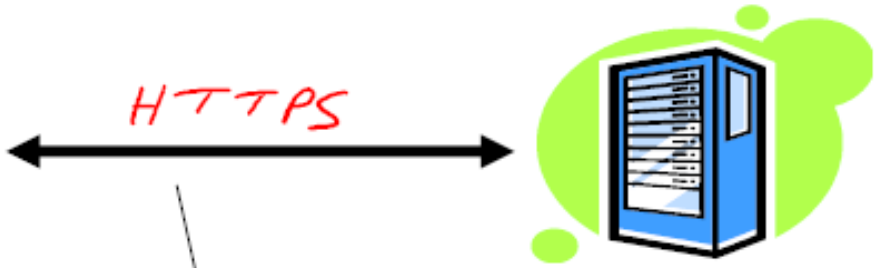
- Узнать, как работают крипто примитивы
- Узнать, как правильно их использовать
- Ввести основные понятия безопасности
- Научиться формировать протоколы из правильно подобранных крипто примитивов

Криптография повсюду

- Безопасное общение:
  - веб-трафик: HTTPS
  - беспроводной трафик: 802.11i WPA2 (и WEP), GSM, Bluetooth
- Шифрование файлов на диске: EFS, TrueCrypt
- Защита контента (например, DVD, Blu-ray): CSS, AACS
- Аутентификация пользователя

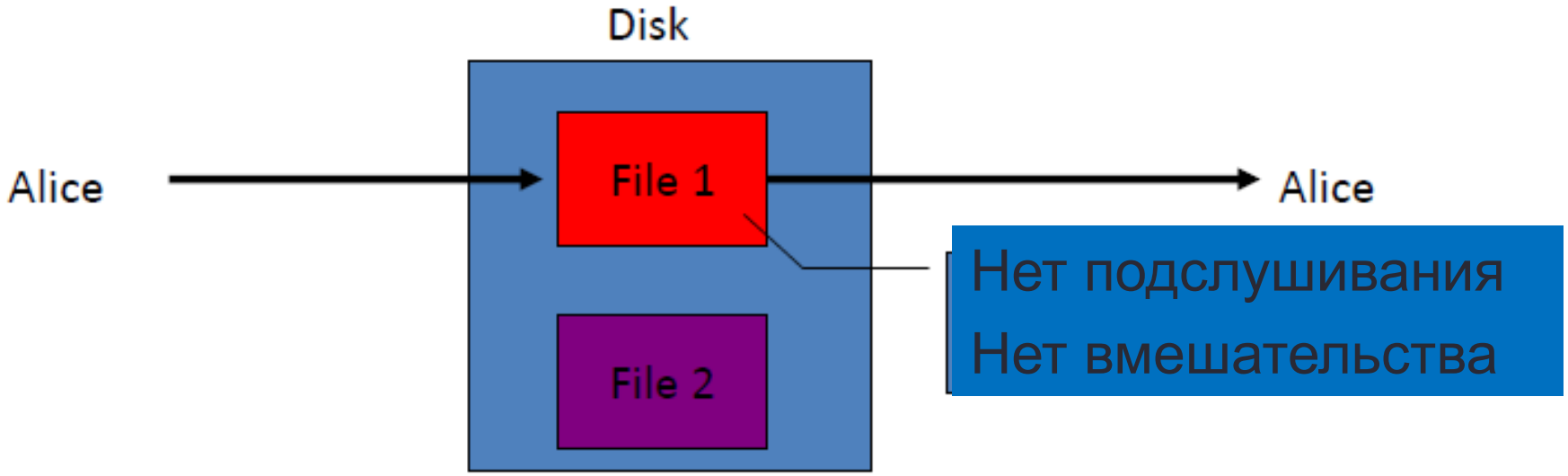
- …И многое другое

Защищенный траффик



Нет подслушивания
Нет вмешательства

Защищенное хранение



Аналогично защищенной передаче:

Алиса сегодня передает данные Алисе завтрашней

Криптология

- Криптология – наука о шифрах
- Криптология делится на
  - Крипотгафию – задача построения криптосистем
  - Криптоанализ – задача обнаружения уязвимостей

Криптография

- Криптография = крипто (тайна) + графи (письмо)
- Главный смысл: передавать сообщения между участниками криптографического протокола так, чтобы другие не смогли их понять
- Но есть и другие задачи

Основные задачи криптографии 1

- *Конфиденциальность*: как сохранить информацию в секрете от всех, кроме имеющих доступ:
  - передача данных по незащищенному каналу;
  - хранение данных на общедоступных носителях.

- *Целостность*: как обеспечить передачу данных в целости и сохранности. В частности, как заметить, менял ли кто-то данные по дороге

Основные задачи криптографии 2

- *Аутентификация*: как доказать, что данные поступают из правильного источника. Две части:
  - entity authentication: как доказать, что я это я;
  - data origin authentication: как доказать, что мое сообщение действительно от меня.

- *Non-repudiation (*неотречение): как сделать так, чтобы человек, что-то пообещавший, потом от обещаний не отказывался

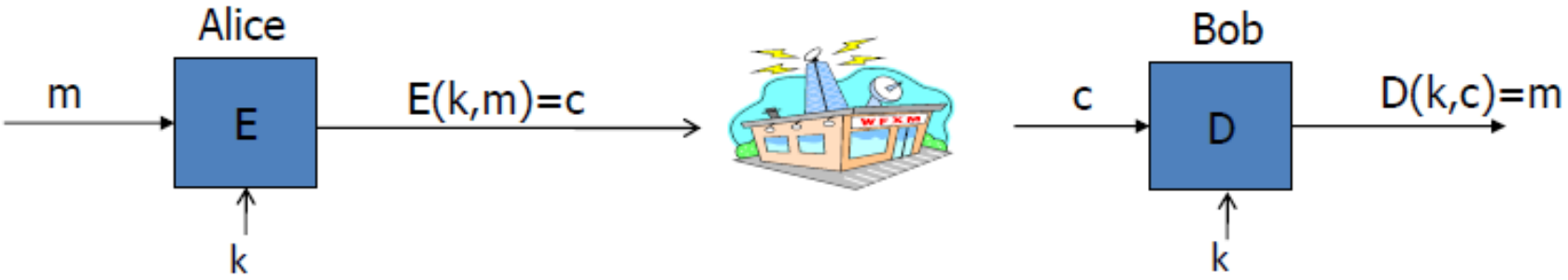
Некриптографические методы

- Если «противник» -- бездушный канал с ошибками, то есть некриптографические методы
- Передача данных -- коды, обнаруживающие ошибки и коды, исправляющие ошибки.
- Целостность данных -- контрольные суммы. CRC (cyclic redundancy code, циклический избыточный код):
  - сообщению $a_0 a_1 \dots a_{N-1}$ сопоставляем многочлен $P(x) = \sum_{i=0}^{N-1} a_i x^i$
  - значение CRC остаток от деления P(x) на G(x), которым определяется CRC.

Основные термины

- **Шифр**
- **Открытый текст (plaintext)**
- **Символ**
- **Алфавит**
- **Шифрованное сообщение** (закрытый текст, **ciphertext)**
- **Шифрование (Encryption)**
- **Расшифрование (Decryption)**
- **Ключ**

Простой пример



- E,D – шифрование, расшифрование, k – ключ
- m,c – открытый текст, закрытый текст

- Алгоритм шифрования ИЗВЕСТЕН всем
  - Никогда не используйте неизвестные шифры

Использование ключей

- Одноразовый (сессионный) ключ
  - Ключ используется однократно для шифрования единственного сообщения
    - Например: шифрование писем
- Многоразовый ключ
  - Ключ используется многократно
    - Например: шифрование диска
  - Такие ключи требуют больше внимания и сложностей алгоритмов шифрования.

Атаки

- Ciphertext only:
  - враг увидел и скопировал некоторое количество шифров, которые он теперь может анализировать;
  - у врага достаточно много таких шифров.
- Known plaintext:
  - у врага есть некоторое количество пар (сообщение, шифр), которые он теперь может анализировать;
  - например, с течением времени содержание старых сообщений становится известным.

Атаки

- Chosen plaintext:
  - враг может сам выбрать несколько сообщений и зашифровать их при помощи этого алгоритма;
  - например, шифрование -- общедоступный сервис.
- Chosen ciphertext :
  - враг может сам выбрать несколько шифроргамм и расшифровать их при помощи этого алгоритма;
  - например, использование отклика удаленного сервера.
- .

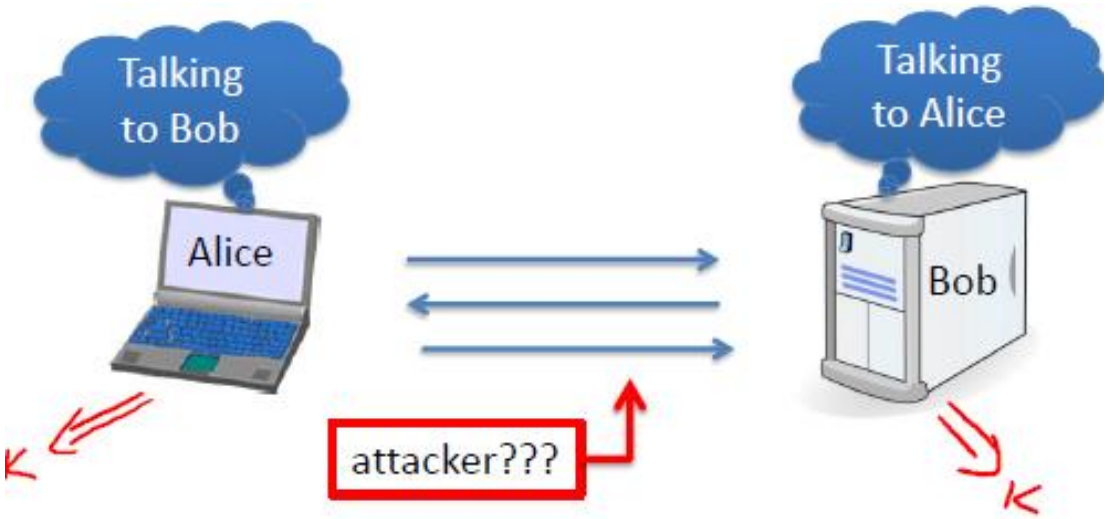
Важные моменты

- Криптография это:
  - Отличный инструмент
  - Основа для многих механизмов безопасности
- Криптография не является:
  - Решение всех проблем безопасности
  - Безусловно надежной, если реализована или используется не должным образом
  - Что-то, что вы должны попытаться изобрести

… много, очень много примеров сломанных специальных конструкций

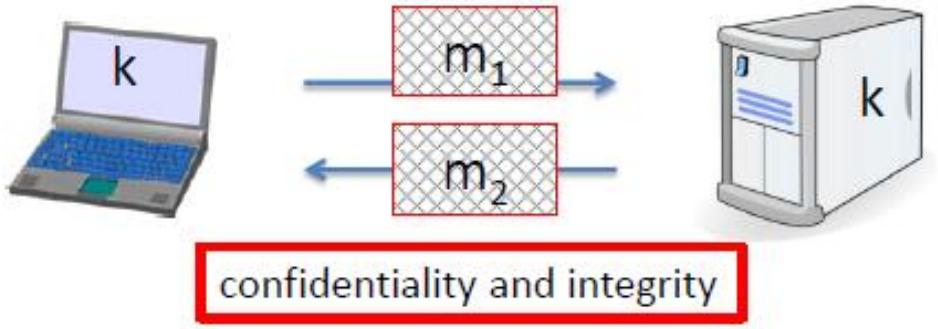
Для чего нужна криптография?

- Базовое понятие:



- 1. Выработка секретного ключа

2. Обмен данными по защищенному каналу



Криптография может гораздо больше!

- Цифровая подпись

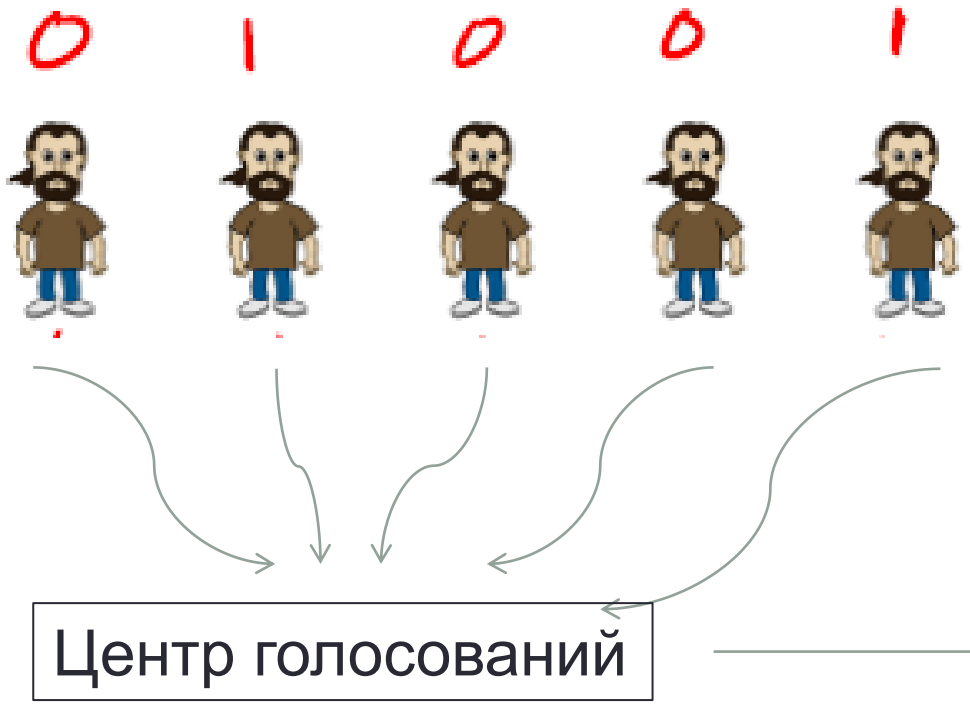
- Анонимное общение

- Цифровые деньги
  - Можно ли оплатить товары и услуги не сообщая кто я?
  - Как избежать дублирования и двойных трат е-денег

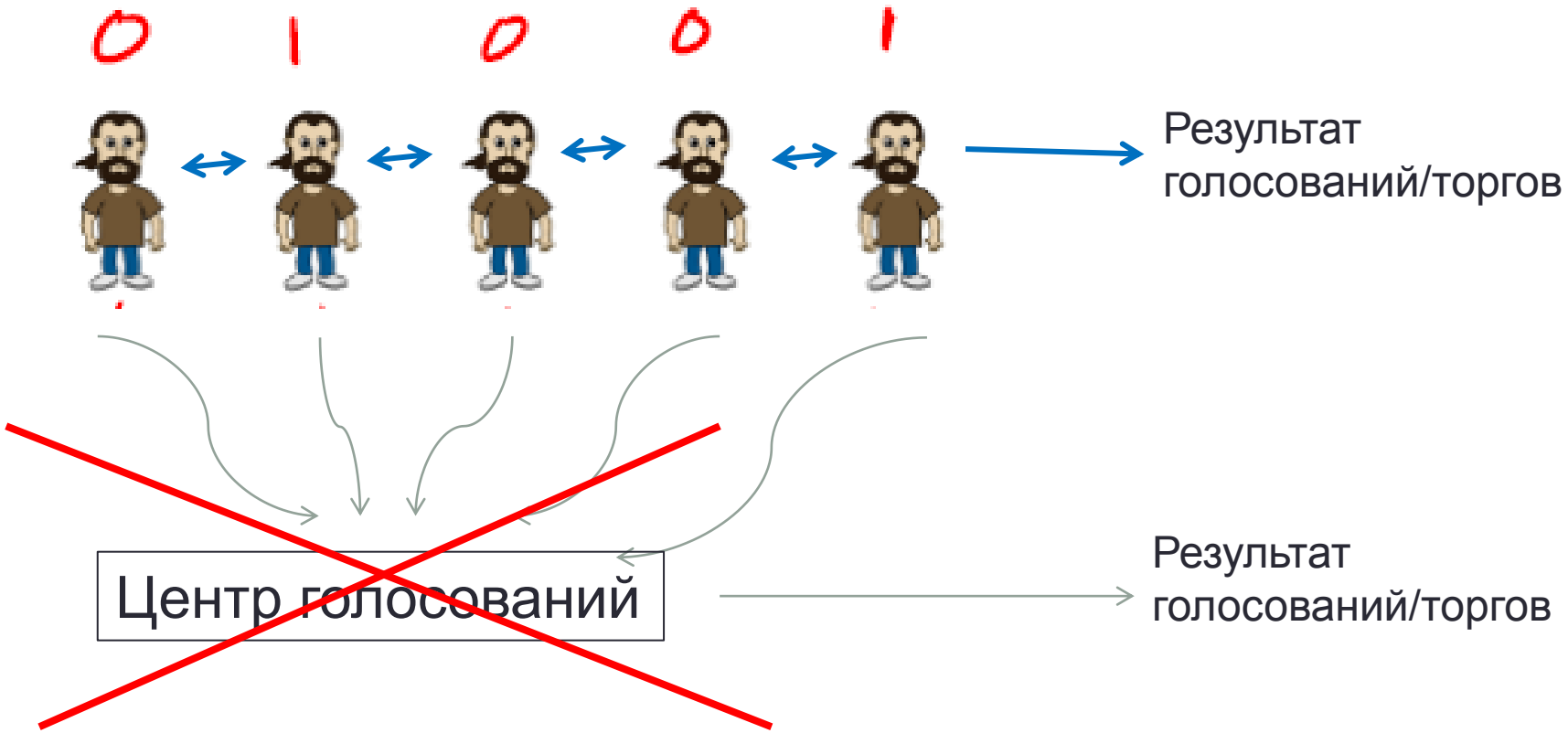
Протоколы

- Выборы

- Электронные аукционы

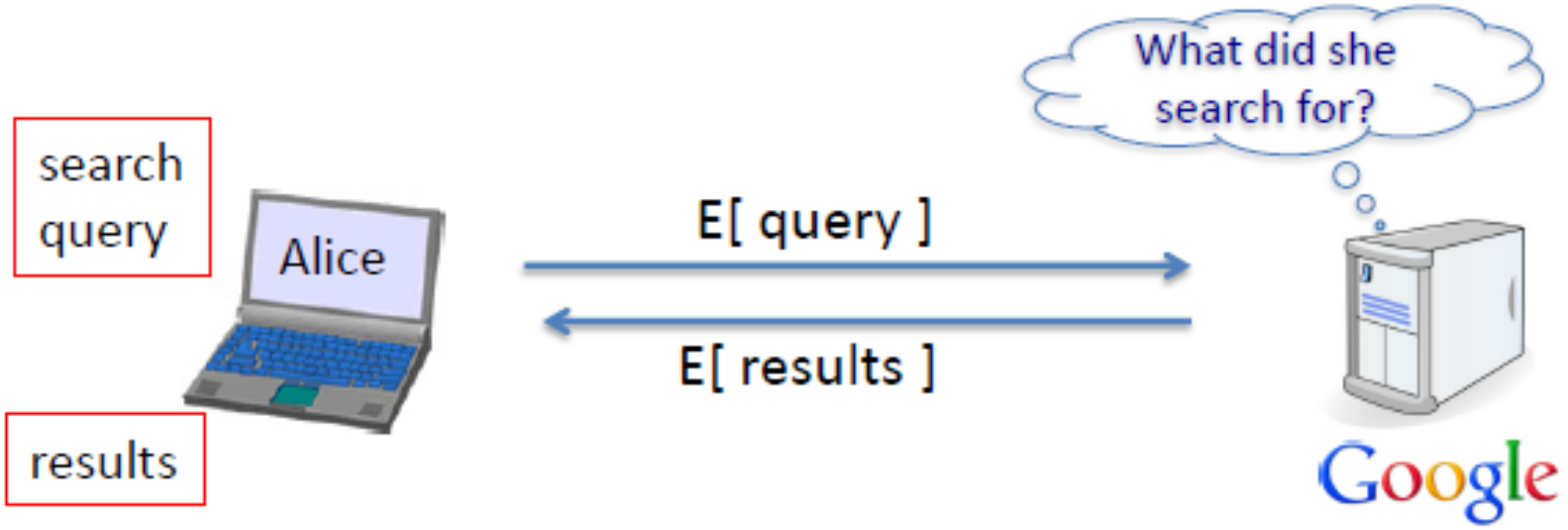


- Многосторонние вычисления

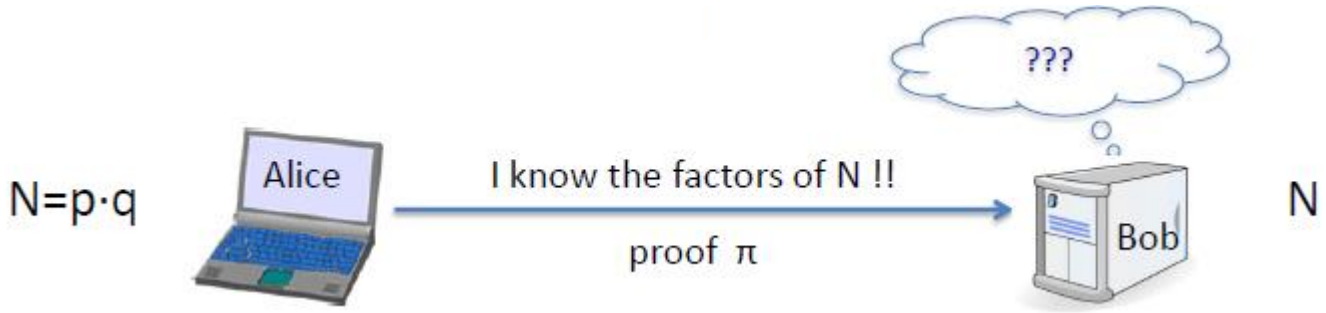


И просто магия

- Защищенные удаленные вычисления



- Доказательства с нулевым разглашением



Строгая наука

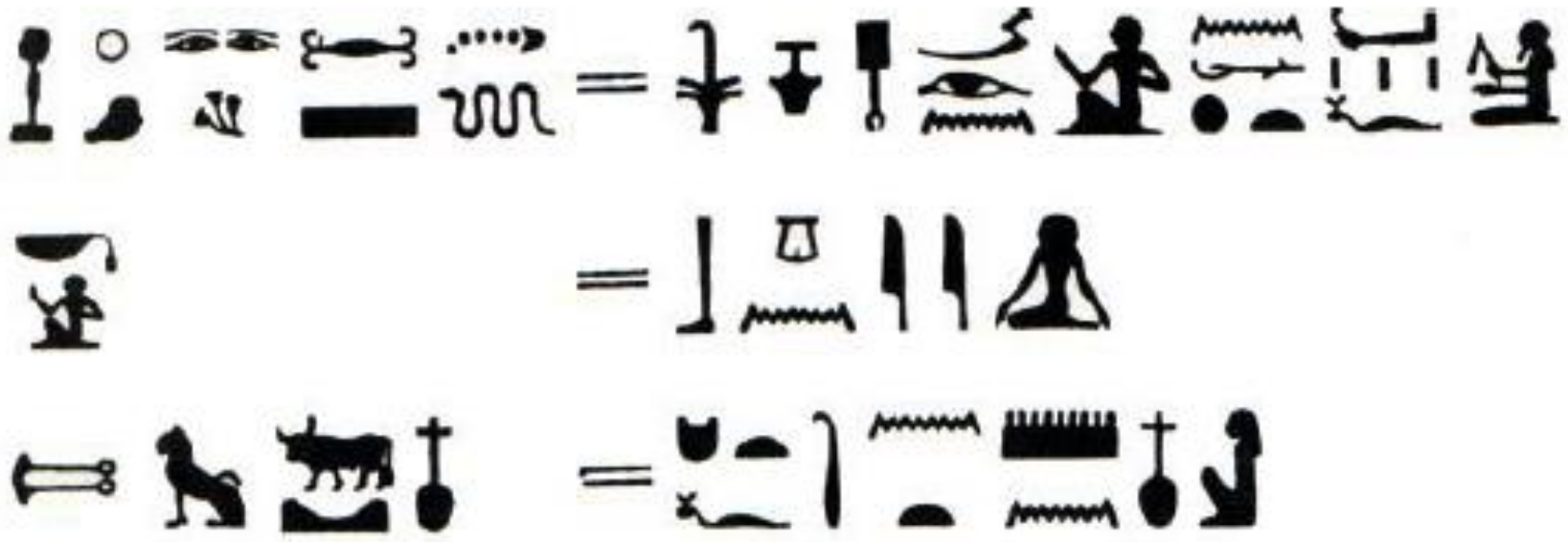
- Три шага в криптографии:
  - Точно указать модель угрозы
  - Предложить криптопримитив
  - Доказательство, что успешное вскрытие предложенного примитива в рамках модели угроз решит сложную проблему

История криптографии

- Криптография древности
- Криптография нового времени
- Криптография в XX веке до 1976 года
- Современная криптография

Криптография древности

- Около 4000 лет назад египтяне заменяли некоторые иероглифы в важных текстах на другие.
- Их было нетрудно расшифровать; видимо, цель была не в сокрытии информации.



- Китай: Ву Джинг Зонг Яо (1044) содержал не только формулу пороха, но и небольшой код для военных целей, но вообще не развито было шифрование
- Индия
- Курды

Греция

- Лисандр – скитала

Греция

- Диск Энея (Эней Тактик, 4 в. до н.э.): на диске просверливаются дырки, соответствующие буквам, через них продевается в нужном порядке нить. Расшифровка тривиальна, но сообщение можно мгновенно уничтожить. Он же — книжный шифр: незаметные пометки над буквами книги (первая стеганография).
- Квадрат Полибия: в квадрат выписываются буквы, каждая буква заменяется на ту, что под ней. Шифр — порядок букв в этом квадрате.
- Ещё стеганография: Геродот упоминает, как сообщение о планирующейся атаке персов было записано на основе восковых табличек, которые потом опять покрыли воском.

Шифр Цезаря

- Шифр Цезаря — простой вариант шифра подстановки. Буквы сдвигаются на фиксированное число позиций: A – D, B – E, C – F и т.д.
- Талмуд — *атбаш* (алеф–таф, бет–шин): первая буква заменяется на последнюю, вторая — на предпоследнюю и т.д. В Библии: «лев камай» (сердце моих противников) — «халдеи», «Шешах» — «Вавилон».

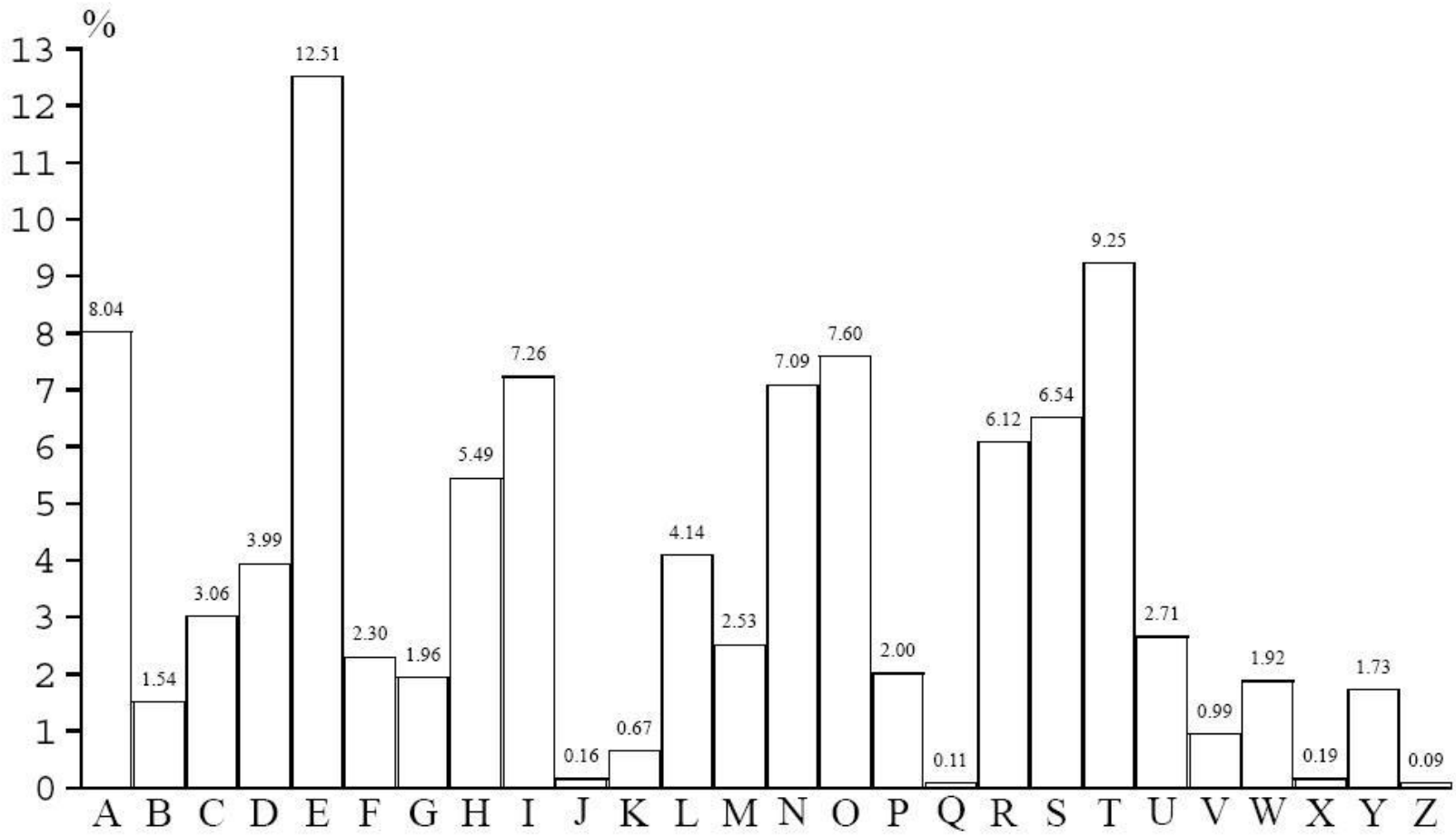
Моноалфавитные шифры

- Шифр Цезаря и атбаш частные случаи моноалфавитных шифров.
- В них каждой букве алфавита ставится в соответствие
  другая буква или символ другого алфавита.
- Т.е. моноалфавитный шифр перестановка букв
  алфавита или биекция с другим алфавитом.
- Как взломать моноалфавитный шифр?

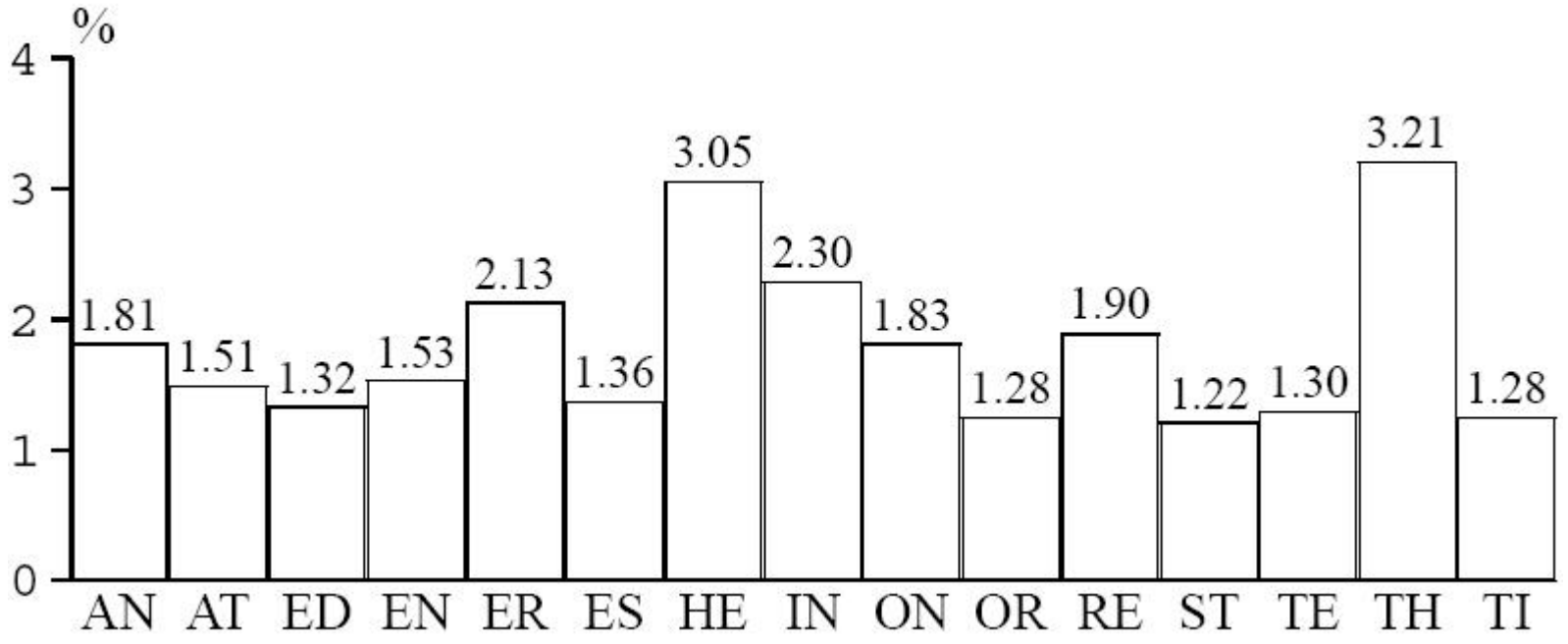
Арабы

- Частотный анализ появился в Аравии.
  - 14-томная энциклопедия Ахмада аль-Калькашанди (1412) содержала раздел по криптологии.
  - Таблицы сочетаемости букв арабского языка, какая после какой наиболее вероятна, какие буквы самые частые (алиф и лам, конечно). Все это на основе Корана.
- Частотным анализом можно взломать моноалфавитные шифры;
- с биграммами уже сложнее, но тоже можно.

Частотный анализ



Частотный анализ биграммы



Новое время

- До Возрождения криптография считалась «темным искусством» и смешивалась с Каббалой.
- С XVI века появилась дипломатия, которой понадобились секретные сообщения.
- Франсуа Виет был в том числе и криптоаналитиком, помогал Генриху IV.
- Английские криптоаналитики на службе Уолсингема расшифровали письма Марии Стюарт и обвинили ее в измене.
- И так далее...

Полиалфавитные шифры

- Леон Батиста Альберти архитектор, художник, композитор, писатель.
- Первый полиалфавитный шифр: внутри код, снаружи сообщение.
- Время от времени

двигаем внутренний диск,

изменяя тем самым код.

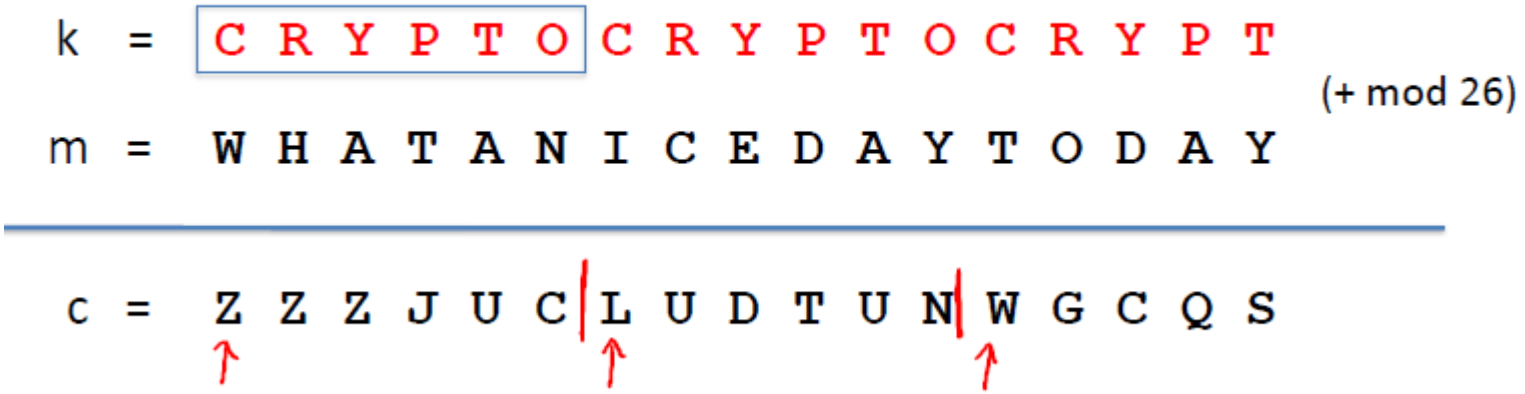
Полиалфавитные шифры

- Иоганн Трисемус, 1508: «Полиграфия», первый труд покриптологии.
- Шифр Трисемуса квадрат, tabula recta, в котором записан алфавит со смещением. Первая буква кодируется по первой строке, вторая по второй и т.д.

- Стали появляться секретные отделы криптологов при дворах.

Шифр Вижинера

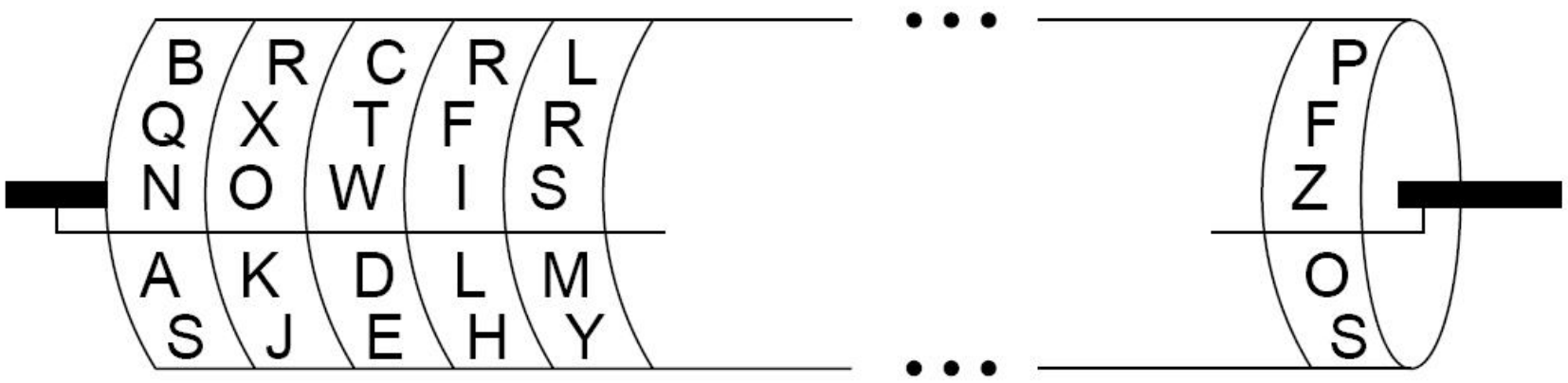
- Блез де Виженер, 1586 первым предложил кодировать сообщение им самим: первая расшифрованная буква используется для декодирования второй и т.д.



XIX век

- Многое изменилось с изобретением телеграфа.
- Теперь нужно было кодировать большие объемы сообщений.
- Прежние шифры были слишком трудоемки. Перешли на простые коды, секретность достигалась частой сменой кодовых слов. Но были и новые шифры.
- Чарльз Уитстон Playfair cipher.

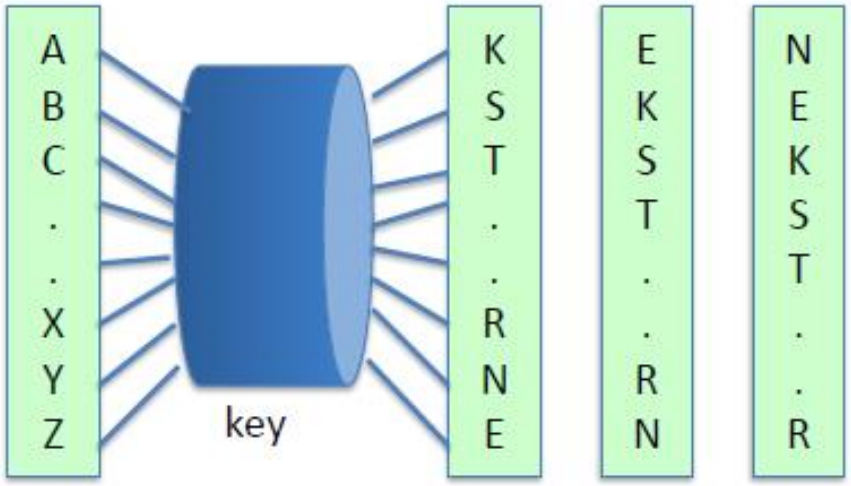
Цилиндр Джеферсона



- Устройство представляло собой деревянный цилиндр, разрезанный на 36 дисков. Эти диски насаживались на одну общую ось таким образом, чтобы они могли независимо вращаться на ней.

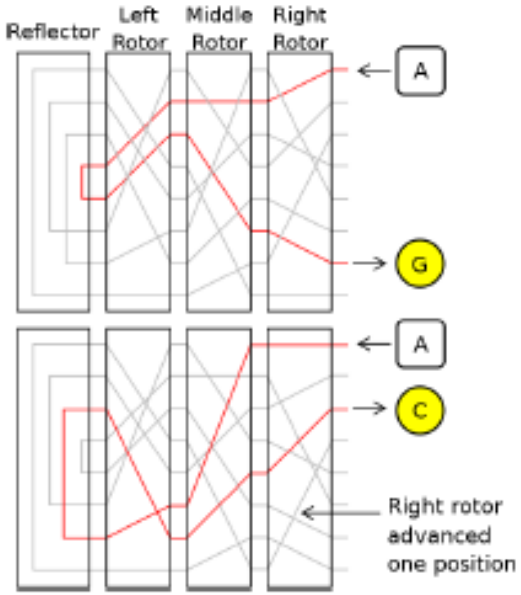
Роторные машины

Early example: the Hebern machine (single rotor)



Энигма

- 3-5 роторов



keys = $26^4 = 2^{18}$ (actually 2^{36} due to plugboard)

Криптоанализ

- Фридрих Касиски (1863) метод взлома полиалфавитных шифров.
- Август Керхкоф (1883) «La Cryptographic militaire»; принципы шифрования:
  - система должна быть невзламываема если не в теории, то на практике;
  - алгоритм шифрования может стать известным противнику, и это не должно привести ко взлому системы;
  - ключ должно быть легко запомнить и легко изменить;
  - криптограммы должно быть возможно передавать по телеграфу;
  - кодирование и декодирование должен быть в состоянии делать один человек.
- Удивительно современные принципы.

Мировые войны (XX век)

- Во время мировых войн криптоанализ сыграл важнейшую роль.
- Еще больше, чем телеграф, на криптографию повлияло радио. Теперь можно было перехватывать большие евражеских сообщений.
- WWI: Британия, Room 40. Из-за блокады перехватывали все немецкие сообщения, и многие шифры успешно декодировали.
- В частности, декодировали и показали американцам планы Германии заключить союз с Мексикой, после чего США вошли в войну.
- WWII: Bletchley Park. Работали многие математики и криптографы (Алан Тьюринг).

Шифр Вернама

- 1910-е годы: Гильберт Вернам:
  - улучшил шифр Виженера;
  - разработал шифр, который невозможно взломать. Как это?
- Одноразовый блокнот: используем одноразовый секретный ключ k, который просто складываем побитово с сообщением:

$$c = m \text{ xor } k.$$

- Без знаний о ключе и сообщении враг, перехвативший сообщение, получил ровно ноль информации.
- Это, конечно, доказал уже Шеннон в конце 1940-х.

Появление криптографии с публичным ключем

- Whiteld Dieffy, Martin Hellman, 1976: «New directions in cryptography”.
- Ralph Merkle..
- Ron Rivest, Adi Shamir, Leonard Adleman, 1978: