Тема 2.1 Введение в криптографию. Основные понятия и определения. Виды криптосистем

- *Криптология*
  - *Криптография*
    - *Открытый текст*
    - *Криптограмма (шифртекст)*
    - *Шифр*
      - *Стойкость шифра*
    - *Ключ*
  - *Криптоанализ*

Криптография – это очень серьезная наука. Не исключаю того, что самая сложная математическая дисциплина.
– *Евгений Касперский*

Криптология

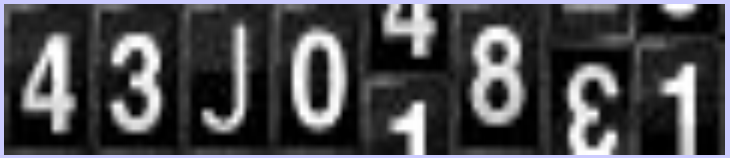
(от греч. cryptos - "тайный" и logos - "мысль") Наука, занимающаяся проблемами защиты информации

Криптография

(от греч. cryptos - тайный, сокрытый, и grapho - пишу, черчу, рисую)
Наука, изучающая методы шифрования сообщений

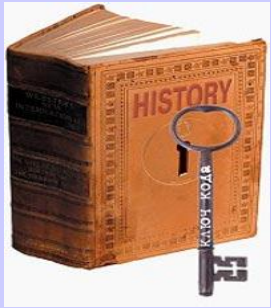
Криптоанализ - Наука, разрабатывающая методы раскрытия шифров

Шифр



(от арабского "цифра") это определенные правила преобразования открытых данных в зашифрованные и обратно.

Ключ



Секретный элемент шифра, недоступный посторонним.

Открытый текст

Исходное сообщение, которое подвергается шифрованию.

Криптограмма

Результат, полученный применением шифра к исходному сообщению.
В дальнейшем криптограмма подлежит дешифрации.

Криптограмма (шифртекст)

Расшифрование (дешифрование)

Шифр

Ключ

Стойкость шифра

это способность противостоять попыткам постороннего лица восстановить открытый текст по перехваченному шифртексту.

Три возможности

передать нужную информацию нужному адресату в тайне от других:

1. Создать абсолютно надежный, недоступный для других канал связи между абонентами.

2. Использовать общедоступный канал связи, но скрыть сам факт передачи информации.

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

Ситуация, в которой возникает задача скрытой передачи информации

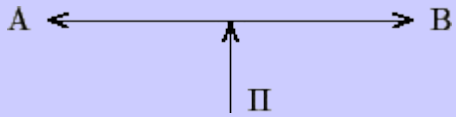


Рис. 1.1.

A и B - удаленные законные пользователи защищаемой информации;
П - незаконный пользователь (противник), который может перехватывать передаваемые по каналу связи сообщения и пытаться извлечь из них интересующую его информацию.

Решающие соображения

при выборе подходящих средств защиты информации:

1) является ли она для противника более ценной, чем стоимость атаки;
2) является ли она для вас более ценной, чем стоимость защиты.

Прокомментируем эти две возможности.

1. При современном уровне развития науки и техники сделать такой канал связи между удаленными абонентами для неоднократной передачи больших объемов информации практически нереально.

2. Разработкой средств и методов скрытия факта передачи сообщения занимается стеганография.

Стеганография – совокупность методов, предназначенных для сокрытия факта существования сообщения.

В настоящее время разработано множество программных пакетов, позволяющих осуществлять подобные операции. Преимущество стеганографии состоит в том, что она может скрывать сам факт передачи сообщений, а не только их содержимое.

Разработкой методов преобразования (шифрования) информации с целью ее защиты от незаконных пользователей занимается **КРИПТОГРАФИЯ**. Такие методы и способы преобразования информации называются шифрами. ***ШИФРОВАНИЕ (ЗАШИФРОВАНИЕ)*** — процесс применения шифра к защищаемой информации, т. е. преобразование защищаемой информации (открытого текста) в шифрованное сообщение (шифртекст, криптограмму) с помощью определенных правил, содержащихся в шифре.

ДЕШИФРОВАНИЕ — процесс, обратный шифрованию, т. е. преобразование шифрованного сообщения в открытый текст с помощью определенных правил, содержащихся в шифре.

КРИПТОГРАФИЯ — прикладная наука, она использует самые последние достижения фундаментальных наук и, в первую очередь, математики. С другой стороны, все конкретные задачи криптографии существенно зависят от уровня развития техники и технологии, от применяемых средств связи и способов передачи информации

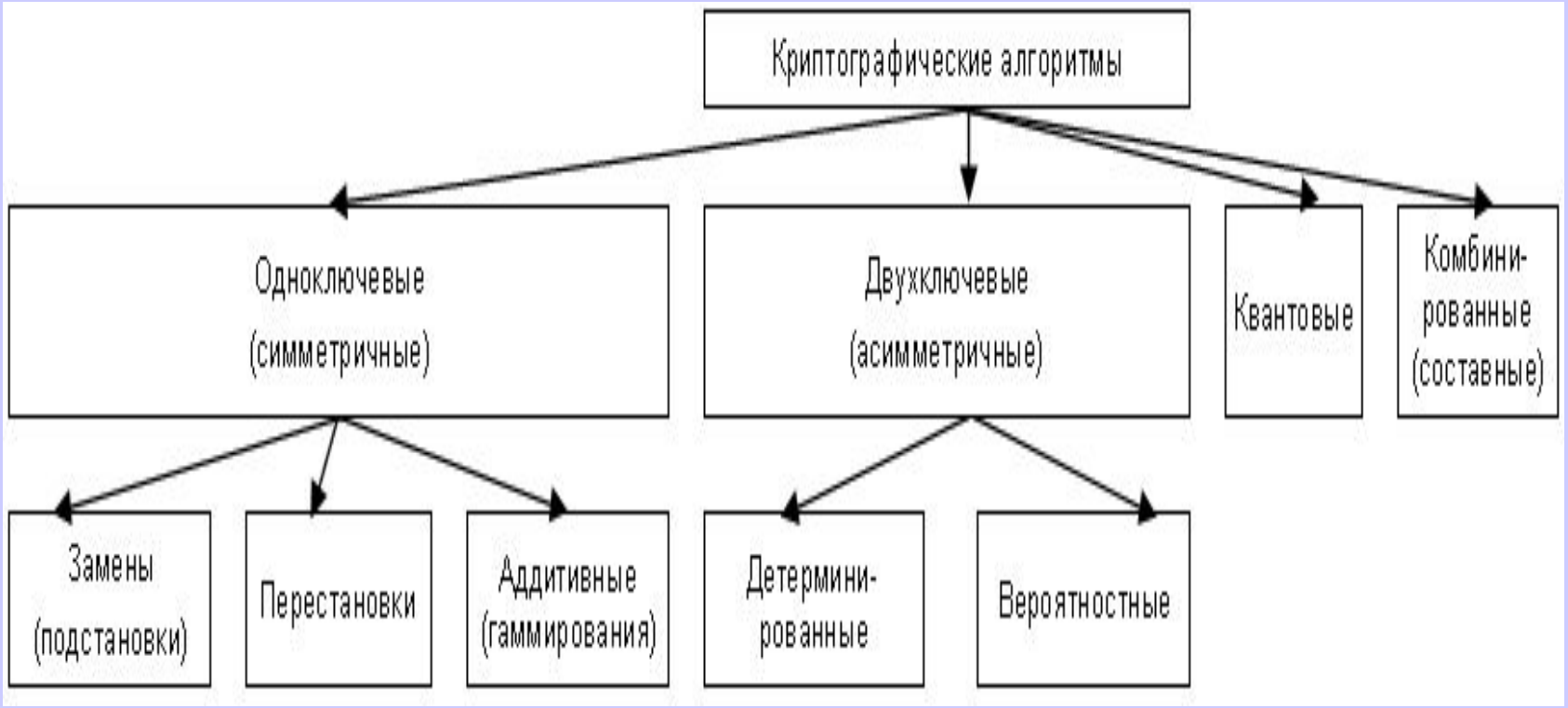
КЛАССИФИКАЦИЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ

1. По области применения шифров различают криптосистемы ограниченного и общего использования.

Стойкость **криптосистемы ограниченного использования** основывается на сохранении в секрете алгоритма криптографического преобразования в силу его уязвимости, малого количества ключей или отсутствия таковых (секретные кодовые системы).

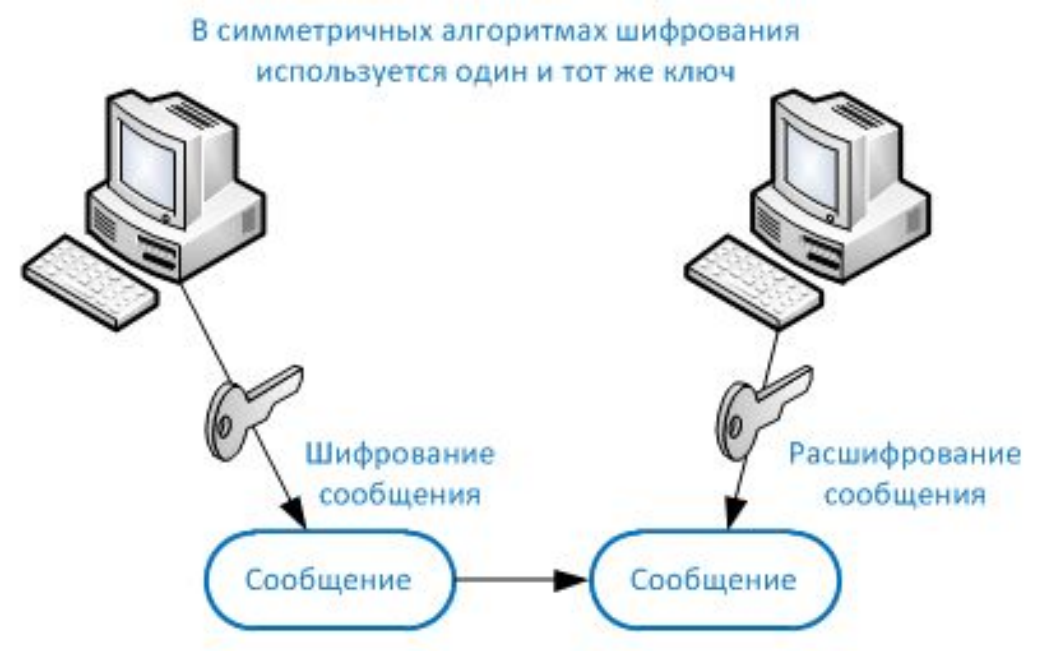
Стойкость **криптосистемы общего использования** основывается на секретности ключа и сложности его подбора потенциальным противником.

2. По особенностям алгоритма шифрования криптосистемы общего использования можно разделить на следующие виды.



Криптографические алгоритмы делятся на ***симметричные алгоритмы***, которые используют симметричные ключи (также называемые секретными ключами (secret key)), и ***ассиметричные алгоритмы***, которые используют асимметричные ключи (называемые также открытыми (public key) и закрытыми ключами (private key)).

*В **одноключевых системах*** для шифрования и дешифрования используется один и тот же ключ.



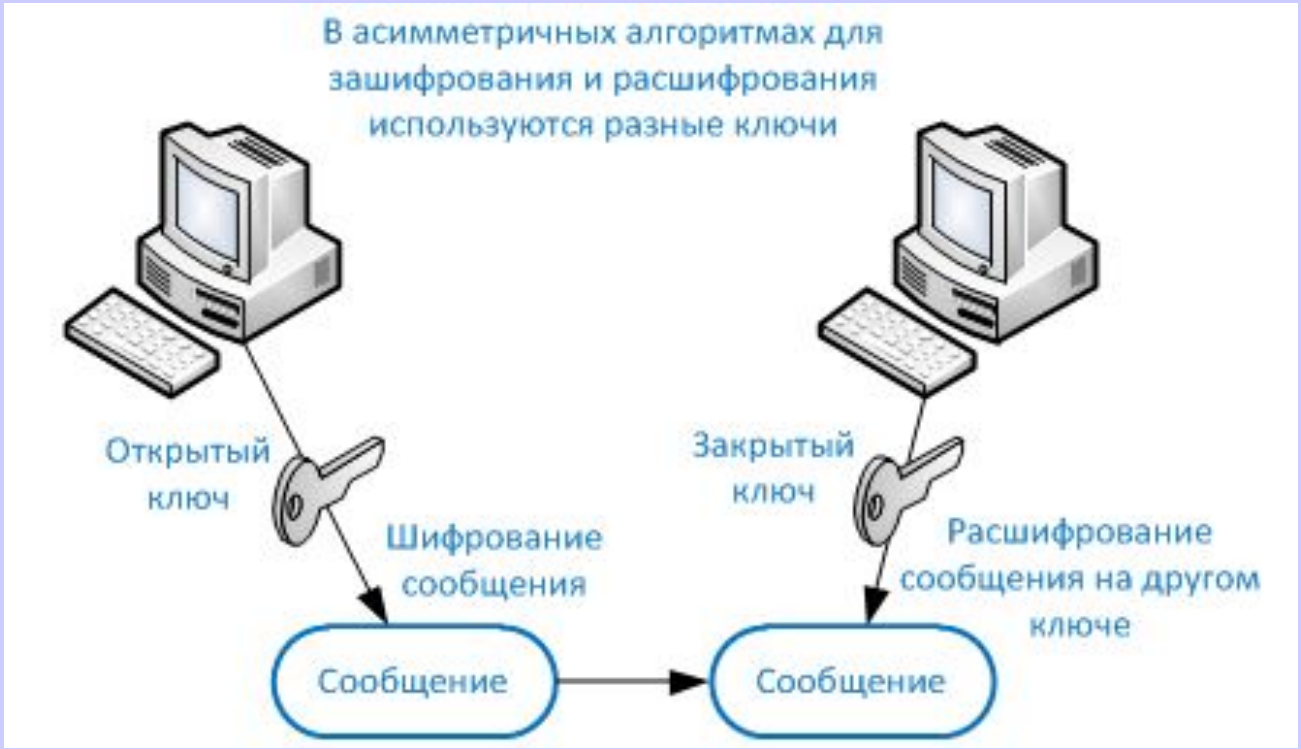
В шифрах **замены** позиции букв в шифровке остаются теми же, что и у открытого текста, но символы открытого текста заменяются символами другого алфавита.

В шифрах **перестановки** все буквы открытого текста остаются в зашифрованном сообщении, но меняют свои позиции.

В **аддитивных** шифрах буквы алфавита заменяются числами, к которым затем добавляются числа секретной случайной (псевдослучайной) числовой последовательности (гаммы). Состав гаммы меняется в зависимости от используемого ключа. Обычно для шифрования используется логическая операция «Исключающее ИЛИ» (XOR). При дешифровании та же гамма накладывается на зашифрованные данные. Гаммирование широко используется в военных криптографических системах.

Двухключевых системах для шифрования и дешифрования используется два совершено разных ключа.

.



При этом два отличающихся асимметричных ключа связаны между собой математически. Если сообщение зашифровано одним ключом, для его расшифрования требуется другой ключ.
В системах с открытыми ключами, создается пара ключей, один из которых является закрытым, другой – открытым. ***Открытый ключ*** (public key) может быть известен всем, а ***закрытый ключ*** (private key) должен знать только его владелец. Часто открытые ключи хранятся в каталогах и базах данных адресов электронной почты, общедоступных всем желающим использовать эти ключи для зашифрования и расшифрования данных при взаимодействии с отдельными людьми.
Открытый и закрытый ключи асимметричной криптосистемы математически связаны, однако наличие у кого-то открытого ключа другого человека не позволяет узнать соответствующий ему закрытый ключ. Таким образом, если злоумышленник получит копию открытого ключа Боба, это вовсе не значит, что он с помощью какого-то математического волшебства сможет получить соответствующий ему закрытый ключ Боба. Однако, если кто-то получит закрытый ключ Боба, возникнет большая проблема. Поэтому никто кроме владельца не должен иметь доступа к закрытому ключу.

При использовании **детерминированного** алгоритма шифрование и расшифрование посредством соответствующей пары ключей возможно только единственным способом.

Вероятностный алгоритм при шифровании одного и того же исходного сообщения с одним и тем же ключом может давать разные шифртексты, которые при расшифровке дают один и тот же результат.

Квантовая криптография вносит в процесс шифрования естественную неопределенность квантового мира. Процесс отправки и приёма информации выполняется посредством объектов квантовой механики, например, при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи. Самым ценным свойством этого вида шифрования является то, что при посылке сообщения отправляющая и принимающая сторона с достаточно большой вероятностью (99.99…%) могут установить факт перехвата зашифрованного сообщения.

Комбинированные *(составные) методы* предполагают использование для шифрования сообщения сразу нескольких методов (например, сначала замена символов, а затем их перестановка).

Все шифры по алгоритму преобразования также делят на **потоковые и блочные.** В **потоковых** шифрах преобразование выполняется отдельно над каждым символом исходного сообщения. Для **блочных** шифров информация разбивается на блоки фиксированной длины, каждый из которых шифруется и расшифровывается отдельно.

Домашние задание:

Конспект (оформить в виде реферата)

-Периоды развития и этапы криптографии.

-Эни́гма.

-Скитала.