2. Основные определения и термины криптологии

Цель темы: Изучить основные термины и определения криптологии и криптографии, яферы их применения. Ознакомиться с классификацией шифров.

2 Основные определения и термины криптологии

Криптология – наука о создании и анализе систем безопасности, предметом которой являются математические основания криптографии и криптоанализа.

Криптография – наука о принципах, средствах и математических методах преобразования информации, с целью сокрытия смысла или структуры данных, а также для защиты их от несанкционированного использования или подделки. Одним из основных методов криптографии является шифрование.

Криптоанализ – наука о методах раскрытия шифров или подделки данных. Поскольку проверка шифров на стойкость является обязательным элементом их разработки, криптоанализ также является частью процесса разработки.

Шифрованием называется взаимно однозначное преобразование сообщения, с целью скрытия его смысла от посторонних.

Исходный текст сообщения, который должен быть защищен называется ***открытый текст***.

Результат шифрования – шифрованный текст (***шифротекст, криптограмма***).

Совокупность данных, определяющих конкретное преобразование из множества преобразований шифра называют ***ключом***.

Открытый текст состоит из элементов, которые определяются шифрпреобразованием.

Элемент – это наименьшая часть данных, (набор битов), которая может быть зашифрована. Элементам открытого текста соответствуют элементы шифртекста.

2.1 Основные термины криптологии

Одним из основных понятий криптографии является стойкость.

Стойкость – это способность противостоять попыткам хорошо вооруженного современной техникой и знаниями криптоаналитика дешифровать перехваченный шифротекст, раскрыть ключи шифра или нарушить целостность и подлинность информации.

Криптоаналитической атакой называют использование специальных методов для раскрытия ключа шифра и/или получения открытого текста. Предполагается, что атакующей стороне уже известен алгоритм шифрования, и ей требуется только найти конкретный ключ.

Другая важная концепция связана с термином ***«взлом»*****.** Когда говорят, что некоторый алгоритм был «взломан» , это не обязательно означает, что найден практический способ раскрытия шифрованных сообщений. Может иметься в виду в виду, что найден способ существенно уменьшить ту вычислительную работу, которая требуется для раскрытия шифрованного сообщения методом «грубой силы», то есть простым перебором всех возможных ключей.

При осуществлении такого взлома практически шифр все же может оставаться стойким, поскольку требуемые вычислительные возможности будут все еще оставаться за гранью реального. Однако, хотя существование метода взлома не означает еще реальной уязвимости алгоритма, обычно такой алгоритм более не используют.

Что такое криптография?

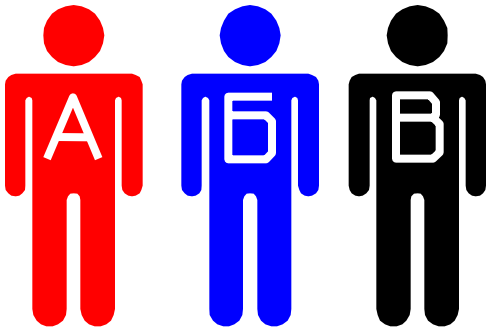
- **Наука о том**
  - как сделать информацию конфиденциальной, избирательно доступной (шифрование)
  - как обеспечить целостность данных
  - как обеспечить аутентификацию (достоверную идентификацию)
    - субъекта: аутентичность информационного источника
    - объекта: пользователя, процесса
  - как обеспечить доказательность действия (неотказуемость)
  - как обеспечить контроль доступа (авторизацию)

- **Предмет науки:**
  - криптографические алгоритмы (математика)
  - криптографические протоколы (процессы с использованием криптографических алгоритмов)
- **Принцип (Август Керхоффс, 1835-1903):**
  - вся защита должна основываться *только* на качестве (длине, энтропии) ключа
  - алгоритмы должны быть тщательно выверены и публично доступны
- **Метод:**
  - для того, чтобы выполнить криптографическую операцию (за исключением, м.б., обеспечения целостности данных), нужно знать секретную информацию (ключ)
  - незнающий ключа должен «искать иголку в стоге сена» (а «стог» должен быть достаточно большим в математическим смысле)

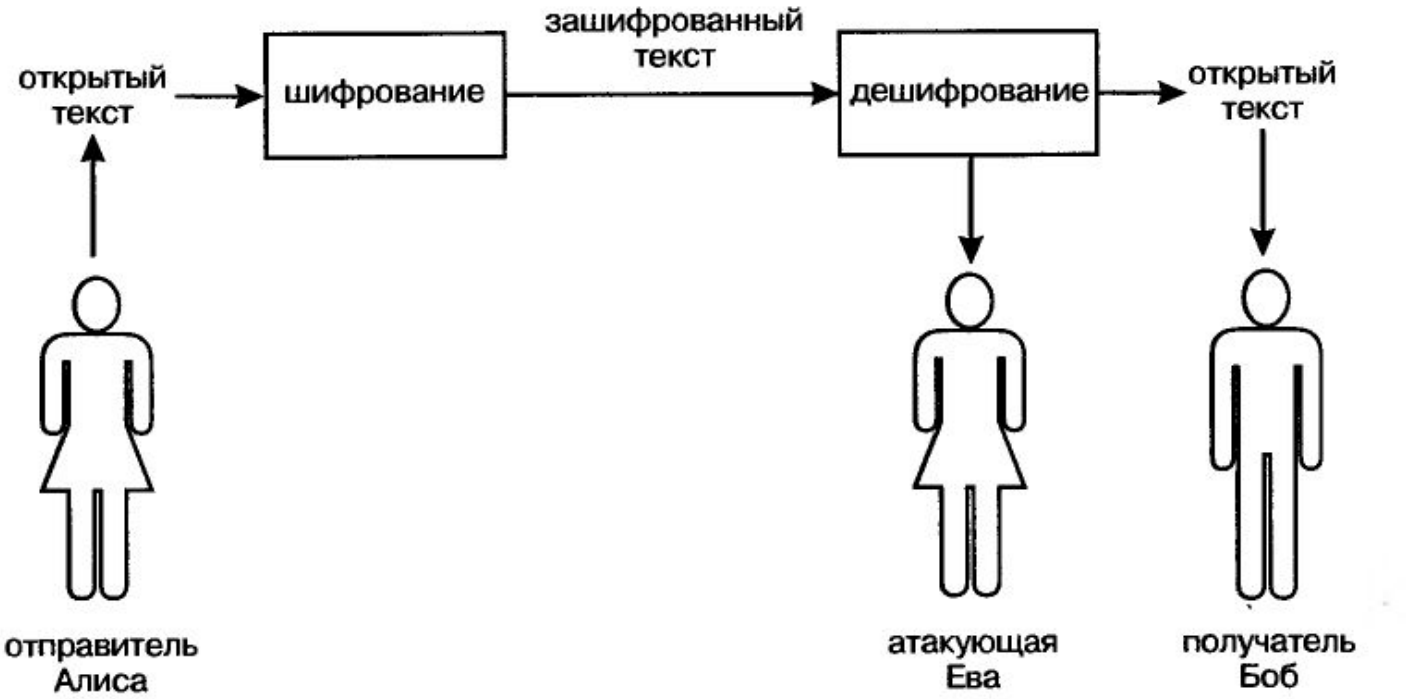
2.2 Основные задачи криптографии

- В узком контексте сетевой безопасности основными задачами криптографии являются
  - *конфиденциальность* данных:
    - цель: сделать данные «нечитаемыми» для непосвященных
    - метод: шифрование
  - *целостность* и *имитостойкость* данных
    - цель: исключить возможность умышленного и неумышленного изменения (искажения) данных неуполномоченными лицами
    - метод: хэш, имитовставка, электронно-цифровая подпись
  - *аутентификация субъекта* – доказательство того, что субъект действия является именно тем, за кого себя выдает
  - *аутентификация источника данных* – доказательство того, что данные изданы определенным субъектом и являются подлинными (т.е. никем другим не искажены; в этом смысле – аутентификация источника данных автоматически обеспечивает их целостность)
  - обеспечение *безотказности* – невозможности для субъекта, выполнившего некоторое действие, впоследствии отказаться от факта выполнения этого действия

2.3 Алиса и Боб



- В криптографических протоколах часто приходится строить примеры взаимодействия двух объектов А и Б
- Криптографы (математики!) придумали для этих объектов имена – Алиса и Боб
  - это удобно произносится
  - герои разнополые, поэтому когда о них говорят в третьем лице – он или она – ясно, о ком речь
- Иногда в криптографических теоремах появляется третий герой – злоумышленник, его обозначим «В», враг



2.4 Классификация систем шифрования

2.5 Контрольные вопросы и задания

1. Поясните значения терминов «криптология» и «криптография», охарактеризуйте сферы их применения.
2. Какова основная задача криптоанализа?
3. Приведите примеры «элементов» шифруемого сообщения.
4. Приведите известные примеры «ключей».
5. Что понимается под термином «стойкость»?
6. Как определить, считается ли шифр взломанным?
7. Перечислите и охарактеризуйте основные задачи криптографии.
8. Приведите и охарактеризуйте основные виды шифров.