1. Криптология – объединение криптографии и криптоанализа. Криптография – наука о поиске способов преобразования информации. Криптоанализ – наука о преодолении криптографической защиты информации. Наука об обратимом преобразовании информации с целью защиты от НСД, оценкой надёжности систем шифрования и анализом стойкости шифров.
2. Направления
   1. Передача данных по отркытым каналам связи (например вотсап)
   2. Использование в банковских картах
   3. Сжача бух. Отчётов через каналы связи
   4. Банковское обслуживание предприятий
   5. Безопасное хранение файлов на ЖД (EFS)
3. Классификация криптографических методов:
   1. Шифрование
      1. С закрытым ключом (симметричное)
         1. Гаммирование
         2. Подстановки
         3. Перестановки
         4. Блочные шифры
      2. С открытым ключом (ассиметричное)
   2. Стеганография
   3. Кодирование
   4. Сжатие
4. Стеганография изучает способы передачи информации, при котором скрывается сам факт передачи информации. Стеганография может быть применима при хранении изображения, древние греки использовали стеганографический способ передачи информации, невидимыые чернила и так далее.
5. Кодирование информации - замена исходного смысла сообщения (слов, предложений) кодами. Главным отличием от шифрования является то, что для раскодирования достаточно знать правила замены, дополнительные данные (ключи) не нужны. Расшифровка же требует дополнительную информацию.
6. Сжатие информации позволяет сократить объём информации сообщения, однако надёжным криптографическим способом его назвать нельзя, так как даже если и хранить алгоритм сжатия в секрете, он может быть легко выявлен статистическими методами обработки.
7. Шифрование информации – процесс преобразования открытой информации в зашифрованную информацию (шифртекст, закрытая); Расшифрование – процесс преобразования шифртекста в открытую информацию, шифрование – процесс преобразования закрытой информацию в открытую.
8. Шифрование – процесс преобразование закрытой информации в открытую. Дешифрование – процесс криптоатаки на открытую информацию, получение закрытой информации без легально полученного ключа. Ключ – дополнительная информация, необходимая для шифрования и дешифрования сообщений.
9. Требования к методам шифрования:
   1. Открытая информация должна поддаваться чтению только при наличии ключа
   2. Знание алгоритма шифрования не должно влиять на надёжность
   3. Любой ключ должен одинаково обеспечивать защиту информации
   4. Алгоритм шифрования должен быть реализуем как аппаратно, так и программно
10. Криптостойкость – стойкость шифра к дешифрованию.
11. Методы шифрования
    1. С закрытым ключом (симметричное)
       1. Гаммирование
       2. Подстановки
       3. Перестановки
       4. Блочные шифры
    2. С открытым ключом (ассиметричное)
12. Симметричная система шифрования – метод шифрования, при котором расшифровка и шифрование требуют один и тот же ключ.
13. Ассиметричная система шифрования – метод шифрования, в которых для шифрования и расшифрования используются два разных ключа. Причём открытый ключ (при помощи которого информация шифруется) может передаваться по открытому каналу.
14. Гаммирование – метод заключается в наложении на исходный текст какой-либо псевдослучайной последовательности, генерируемой на основе ключа. Пример – наложить последовательность при помощи XOR. Наложим этот ключ на информацию. Теперь если в открытой информации стоит бит 1, значит текущий бит ключа и закрытой информации различаются, иначе – совпадают.
15. Подстановки - наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. (а это не кодирование разве???)
16. Перестановки - метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами.
17. Блочный – последовательность основных методов преобразования, применяемых к блоку (части) шифруемого текста.
18. Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию
19. Возможные способы злоумышленных действий с электронными документами с целью нарушения их аутентификации.
    1. активный перехват – нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их;
    2. маскарад – абонент С посылает документ абоненту В от имени абонента А;
    3. ренегатство – абонент А заявляет, что не посылал сообщения абоненту В, хотя на самом деле послал (или не получал сообщения от абонента В, хотя на самом деле его получил);
    4. подмена – абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента A;
    5. повтор – абонент С повторяет ранее переданный документ, который абонент А посылал абоненту В.
20. Основные функции электронной подписи
    1. удостоверяет, что подписанный текст исходит от лица, поставившего подпись;
    2. не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;
    3. гарантирует целостность подписанного текста.
21. Основные функции электронной подписи.
    1. Простая
    2. Усиленная
       1. Неквалифицированная
       2. Квалифицированная
22. Требования, предъявляемые к усиленной квалифицированной ЭП.

Усиленная квалифицированная ЭП обладает признаками усиленной неквалифицированной подписи:

* получается в результате криптографического преобразования информации с использованием ключа электронной подписи;
* позволяет определить лицо, подписавшее электронный документ;
* позволяет обнаружить факт внесения изменений в электронный документ после его подписания;
* создается с использованием средств электронной подписи
* Использование алгоритмов RSA, встроенных в большинство операционных систем ;
* При использовании неквалифицированной электронной подписи сертификат ключа проверки электронной подписи может не создаваться, если соответствие электронной подписи признакам неквалифицированной электронной подписи, установленным настоящим Федеральным законом,

А также обладает дополнительными признаками:

* ключ проверки электронной подписи указан в квалифицированном сертификате;
* для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом.

1. Процедуру формирования электронной подписи.

Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭП получателем подписанного электронного документа.

Формируется хэш-функция документа – с помощью криптографической хэш-функции на основании документа вычисляется относительно короткая строка символов фиксированной длины (хэш). Главное свойство хэш заключается в том, что он однозначно соответствует исходному сообщению и имеет определенный размер (например 128 или 256 бит).

Затем этот хэш шифруется закрытым ключом владельца – результатом является подпись документа. Подпись прикладывается к документу, таким образом, получается подписанный документ.

1. Процедуру проверки электронной подписи.

Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭП получателем подписанного электронного документа.

Лицо, желающее установить подлинность документа, расшифровывает подпись открытым ключом владельца, а также вычисляет хэш документа. Документ считается подлинным, если вычисленный по документу хэш совпадает с расшифрованным из подписи, в противном случае документ является поддельным. В системе усиленной квалифицированной ЭП квалифицированный сертификат подтверждает принадлежность ключа проверки подписи тому или иному лицу. Его выдает удостоверяющий центр в виде электронного или бумажного документа.

1. Разновидности мошенничества с электронными подписями.

Первый вариант — могут похитить закрытый ключ, который хранится на ключевом носителе. Второй вариант – владелец может оставить подпись в общественном месте или потерять. Бывает, что компания забывает отозвать электронную подпись уволенного сотрудника: он покупает товар от имени компании и скрывается, оставив долг.

Могут быть также взломаны алгоритмы хеширования, подделаны центры сертификации и т.д.

Самое распространенное нарушение: квалифицированная электронная подпись выдается по фиктивным документам, используется для регистрации юридических лиц и индивидуальных предпринимателей. Случается, что организация сдает налоговые декларации, а когда приходит проверка и находит махинации, отрицает, что подписывала и сдавала подобную отчетность.

1. Понятие хеш-функции в электронной подписи. Хэш-функция – идентификатор документа, математически рассчитываемый на основании текста самого документа, позволяющий сравнивать документ на соответствие
2. Требования, предъявляемые к криптографическим хэш-функциям
   1. хеш-функция должна быть применима к сообщению любого размера;
   2. вычисление значения функции должно выполняться достаточно быстро;
   3. при известном значении хеш-функции должно быть трудно (практически невозможно) найти подходящий прообраз М;
   4. при известном сообщении М должно быть трудно найти другое сообщение М` с таким же значением хеш-функции, как у исходного сообщения;
   5. должно быть трудно найти какую-либо пару случайных различных сообщений с одинаковым значением хеш-функции