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.