**1.Как называется раздел науки, объединяющий криптографию и криптоанализ?**

Криптографию и криптоанализ объединяют в одну науку – криптологию

**2.Какие задачи решает криптография?**

Криптография решает следующие задачи: шифрование данных с целью защиты от несанкционированного доступа; проверка подлинности сообщений; проверка целостности передаваемых данных; обеспечение невозможности отказа.

**3.Что представляет собой криптографический алгоритм?**

Криптографические алгоритмы представляют собой алгоритмы шифрования/дешифрования, кэширования, формирования и проверки электронной цифровой подписи.

**4.Какие требования предъявляются для современных криптографических систем защиты?**

К криптографическим системам предьявляют следующие требования:

зашифрованное сообщение должно поддаваться чтению только при наличии ключа;

знание алгоритма шифрования не должно влиять на надежность защиты;

любой ключ из множества возможных должен обеспечивать надежную защиту информации;

алгоритм шифрования должен допускать как программную, так и аппаратную реализацию.

**5.В чем суть криптографического метода замены и перестановки?**

При использовании метода перестановки сообщение делится на блоки, которые переставляют на другие позиции. А метод замены заменяет символы по алфавиты на другие.

**6.Объясните метод шифрования одноконтурной обыкновенной подстановки?**

При многоалфавитной одноконтурной обыкновенной подстановке для замены символов исходного текста используется несколько алфавитов, причем смена алфавитов осуществляется последовательно циклически

**7.Объясните метод шифрования простой перестановки?**

Простейшим примером перестановки является перестановка с фиксированным периодом . В этом методе сообщение делится на блоки по определенному количеству символов и в каждом блоке производится одна и та же перестановка*.*

**8.Объясните шифрование методом гаммирования?**

Метод гаммирования подразумевает создание гаммы т.е набора случайных чисел полученных различными методами гаммирования. Далее с гаммой проводятся арифметические операции.

**9.Какова стойкость комбинированные методы шифрования?**

При использовании комбинированных методов шифрования стойкость шифра равна произведению стойкостей отдельных методов.

**10. Что является важнейшим показателем надежности криптографического закрытия?**

Важнейшим показателем надежности криптографического закрытия информации является его стойкость

**11.Как определяется трудоемкость метода шифрования?**

Трудоемкость метода - определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста

**12. Что такое маршрутная перестановка?**

Маршрутные перестановки основываются на некоторой геометрической фигуре.

**13.то называется «поворотной решеткой»?**

Отрезок открытого текста записывается в такую фигуру по некоторой траектории.

**14. Оцените количество ключей шифра вертикальной перестановки. Во сколько раз это**

Для использования шифра, называемого поворотной решеткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размера 2m´2k клеток. В трафарете вырезано m´k клеток так, что при наложении его на лист чистой бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа

**15. В чем отличие шифров простой и сложной замены?**

Шифры сложной замены – шифры сложной замены отличаются от шифров простой замены тем, что в них при шифровании используется много алфавитов.

**16. Какие шифры сложной замены вам известны?**

Шифр Гронсфельда