Контрольные вопросы :

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

Раздел науки, объединяющий криптографию и криптоанализ, принято называть криптологией.

1. 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.

1. Что представляет собой криптографический алгоритм?

Набор правил, который используется для шифрования информации, чтобы ее могли прочитать только авторизованные стороны. Алгоритм позволяет генерировать зашифрованный текст, который невозможно прочитать без расшифровки.

1. Какие требования предъявляются для современных криптографических систем защиты?

Для современных криптографических систем можно сформулировать следующие требования:

- сложность и трудоёмкость процедур шифрования и дешифрования должны определяться в зависимости от требуемого уровня защиты информации (необходимо обеспечить надежную защиту информации);

- временные и стоимостные затраты на защиту информации должны быть приемлемыми при заданном уровне ее секретности (затраты на защиту не должны быть чрезмерными);

- процедуры шифрования и дешифрования не должны зависеть от длины сообщения;

- количество всех возможных ключей шифра должно быть таковым, чтобы их полный перебор с помощью современных информационных технологий (в т.ч. и распределенных вычислений) был невозможен за приемлемое для противника время;

- любой ключ из множества возможных должен обеспечивать надежную защиту информации;

- незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения;

- избыточность сообщений, вносимая в процессе шифрования, должна быть как можно меньшей (хорошим считается результат, когда длина шифрограммы не превышает длину исходного текста);

- зашифрованное сообщение должно поддаваться чтению только при наличии ключа.

1. В чем суть криптографического метода замены и перестановки? Символы шифруемого текста заменяются другими символами, взятыми из одного алфавита (одноалфавитная подстановка) или нескольких алфавитов (многоалфавитная подстановка).

1. Объясните метод шифрования одноконтурной обыкновенной подстановки?

Это прямая замена символов шифруемого сообщения другими буквами того же самого или другого алфавита ,далее после шифрования каждого символа соответствующий ему столбец алфавитов циклически сдвигается вверх на одну позицию

1. Объясните метод шифрования простой перестановки?

Это прямая замена символов шифруемого сообщения другими буквами того же самого или другого алфавита.

1. Объясните шифрование методом гаммирования?

Принцип шифрования гаммированием заключается в генерации гаммы шифра с помощью датчика псевдослучайных чисел и наложении полученной гаммы шифра на открытые данные обратимым образом

1. Какова стойкость комбинированные методы шифрования?

Одним из важнейших требований, предъявляемых к системе шифрования, является ее высокая стойкость. Однако повышение стойкости любого метода шифрования приводит, как правило, к существенному усложнению самого процесса шифрования и увеличению затрат ресурсов.

Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких различных способов шифрования, т.е. последовательное шифрование исходного текста с помощью двух или более методов.

10 Что является важнейшим показателем надежности криптографического закрытия?

Важнейшим показателем на­дежности криптографического закрытия информации яв­ляется его *криптостойкость*— тот минимальный объем зашифрованного текста, который можно вскрыть стати­стическим анализом. Таким образом, стойкость шифра оп­ределяет допустимый объем информации, зашифровывае­мый при использовании одного ключа.

11 Как определяется трудоемкость метода шифрования?

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

12 Что такое маршрутная перестановка?

Преобразования из этого шифра состоят в том, что в некоторую фигуру, обычно прямоугольник, исходный текст вписывается по ходу одного «маршрута», а затем по ходу другого выписывается с нее. Такой шифр называют **маршрутной перестановкой**.

13 Что называется «поворотной решеткой»?

Изначально **решётка** Кардано представляла собой трафарет с отверстиями, в которые записывали буквы, слоги или слова сообщения. Затем трафарет убирали, а свободное место заполняли более или менее осмысленным текстом. Такой метод сокрытия информации относится к стеганографии.

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

15 В чем отличие шифров простой и сложной замены?

В одноалфавитной (простой) замене соответствие между нормативным алфавитом и шифр-алфавитом задается один раз до начала шифрования и не меняется на всем протяжении шифрования сообщения. В многоалфавитном шифре (шифре сложной замены) буква открытого текста может быть представлена различными символами, кроме того, один и тот же символ криптограммы может обозначать разные буквы.

16 Какие шифры сложной замены вам известны?

Шифр Виженера. В шифре Виженера используется не один, а 26 различных шифр-алфавитов (для английского языка). Шифрование начинается с построения «таблицы Виженера», содержащей алфавит открытого текста с последующими алфавитами, каждый из которых циклически сдвинут влево на одну позицию относительно предыдущего.