**Контрольные вопросы:**

Как называется раздел науки, объединяющий криптографию и криптоанализ?

Интегральный криптоанализ

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.

Что представляет собой криптографический алгоритм?

Криптографический алгоритм - код — совокупность алгоритмов криптографических преобразований (шифрования), отображающих множество возможных открытых данных на множество возможных зашифрованных данных, и обратных им преобразований.

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.

В чем суть криптографического метода замены и перестановки?

Шифр перестано́вки — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее.

Объясните метод шифрования одноконтурной обыкновенной подстановки?

При полиалфавитной одноконтурной обыкновенной подстановке для замены символов исходного текста используются несколько алфавитов, причем смена алфавитов осуществляется последовательно и циклически, т.е. первый символ заменяется соответствующим символом первого алфавита, второй – символом второго алфавита и т. д. до тех пор, пока не будут использованы все выбранные алфавиты. После этого использование алфавитов повторяется.

Объясните метод шифрования простой перестановки?

перестановка букв исходного элементаю

Пример 1. Открытый текст: "ШИФРОВАНИЕ\_ПЕРЕСТАНОВКОЙ".

Ключ (правило перестановки): группы из 8 букв с порядковыми номерами 1.2.....8 переставить в порядок 3-8-1-5-2-7-6-4.

Шифртекст: "ФНШОИАВР\_СИЕЕЕРПННТВАОКО".

Объясните шифрование методом гаммирования?

гаммирование. В этом способе шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите.

Какова стойкость комбинированные методы шифрования?

стойкость комбинированных методов шифрования открытого текста гораздо выше, так - как с усложнением процесса шифровки усложняются способы определения

Что является важнейшим показателем надежности криптографического закрытия?

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

Как определяется трудоемкость метода шифрования?

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

Что такое маршрутная перестановка?

маршрутная перестановка - Преобразования состоят в том, что отрезок открытого текста записывается в такую фигуру по некоторой траектории, а выписывается по другой траектории. Пример данного шифра — шифр Скиталы.

Что называется «поворотной решеткой»?

решётка Кардано

В чем отличие шифров простой и сложной замены?

Одноалфавитные (простые) и многоалфавитные (сложные) замены.

Какие шифры сложной замены вам известны?

шифры гронсфельда, виженера