**Тема Симметричные криптосистемы**

**Цель:** Изучить симметричные блочные криптоалгоритмы

**Вопросы практического занятия:**

*Основные понятия и термины современной криптографии. Классификация современных криптосистем. Классическая сеть Фейстеля. Потоковые шифры. Блочные шифры. Методы криптоанализа. Способы реализации стеганографических системе их достоинства и недостатки.*

**Задания практического занятия:**

1 Подготовьте конспект по вопросам практического занятия

2 Ответьте на контрольные вопросы.

**Контрольные вопросы:**

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

**Криптология**

1. Какие задачи решает криптография?

**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**

1. Какие требования предъявляются для современных криптографических систем защиты?

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

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

**- зашифрованное сообщение должно поддаваться чтению только при наличии ключа.**

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

1. В чем суть криптографического метода замены и перестановки?

**Метод перестановки - шифрование проводится в следующем порядке:**

**1)Шифруемый текст записывается последовательными строками под числами ключевой последовательности, образуя блок шифрования размером nxm.**

**2) Зашифрованный текст выписывается колонками в порядке возрастания номеров колонок, задаваемых ключевой последовательностью.**

**3)Заполняется новый блок и т.д.**

**Метод замены - символы шифруемого текста заменяются другими символами, взятыми из одного алфавита (одноалфавитная подстановка) или нескольких алфавитов (многоалфавитная подстановка).**

1. Объясните метод шифрования одноконтурной обыкновенной подстановки?

**Для замены символов используются несколько алфавитов, причем смена алфавитов проводится последовательно и циклически: первый символ заменяется на соответствующий символ первого алфавита, второй - из второго алфавита, и т.д. пока не будут исчерпаны все алфавиты. После этого использование алфавитов повторяется.**

1. Объясните метод шифрования простой перестановки?

**1. Сообщение записывается в таблицу по столбцам.**

**2. После этого, как открытый текст записан колонками, для образования шифровки он считывается по строкам. Для использования этого шифра отправителю и получателю нужно договориться об общем ключе в виде размера таблицы.**

1. Объясните шифрование методом гаммирования?

**Шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите. Если в исходном алфавите, например, 33 символа, то сложение производится по модулю 33.**

1. Какова стойкость комбинированные методы шифрования?

**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?

***Стойкость* - тот минимальный объем зашифрованного текста, который можно вскрыть статистическим анализом**

11 Как определяется трудоемкость метода шифрования?

**Числом элементарных операций, необходимых для шифрования одного символа исходного текста**

12 Что такое маршрутная перестановка?

**Преобразование в некоторую фигуру, обычно прямоугольник, исходный текст вписывается по ходу одного «маршрута», а затем по ходу другого выписывается с нее**

13 Что называется «поворотной решеткой»?

**Трафарет, изготовленный из квадратного листа клетчатой бумаги размера n×n**

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

15 В чем отличие шифров простой и сложной замены?

**Шифр сложной замены состоит из нескольких простых подстановочных шифров.**

16 Какие шифры сложной замены вам известны?

**Шифр Виженера, Гронсфельда, Шифр «двойной квадрат» Уитстона**