**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?
2. Какие задачи решает криптография?
3. Что представляет собой криптографический алгоритм?
4. Какие требования предъявляются для современных криптографических систем защиты?
5. В чем суть криптографического метода замены и перестановки?
6. Объясните метод шифрования одноконтурной обыкновенной подстановки?
7. Объясните метод шифрования простой перестановки?
8. Объясните шифрование методом гаммирования?
9. Какова стойкость комбинированные методы шифрования?

10 Что является важнейшим показателем надежности криптографического закрытия?

11 Как определяется трудоемкость метода шифрования?

12 Что такое маршрутная перестановка?

13 Что называется «поворотной решеткой»?

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

15 В чем отличие шифров простой и сложной замены?

16 Какие шифры сложной замены вам известны?

* + - 1. Раздел науки, объединяющий криптографию и криптоанализ, принято называть **криптологией.**
      2. Наука, которая изучает методы сохранения содержания сообщения в тайне, принято называть **криптографией.**
      3. Набор правил, который используется для шифрования информации, чтобы ее могли прочитать только авторизованные стороны. Алгоритм позволяет генерировать зашифрованный текст, который невозможно прочитать без расшифровки
      4. 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.

5. Шифрование методом замены (подстановки).

Символы шифруемого текста заменяются другими символами, взятыми из одного алфавита (одноалфавитная подстановка) или нескольких алфавитов (многоалфавитная подстановка). Одноалфавитная подстановка.

1. 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.
2. Шифрование перестановкой заключается в том, что символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста. Данные преобразования приводят к изменению только порядка следования символов исходного сообщения.
3. Гаммирование – метод последовательного симметричного шифрования, суть которого состоит в том, что символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется гаммой.
4. 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 (времени, аппаратных средств, уменьшению пропускной способности и т. п.).

Основные требования к криптографическому закрытию информации:

Сложность и стойкость криптографического закрытия данных должны выбираться в зависимости от объема и степени секретности данных.

Надежность закрытия должна быть такой, чтобы секретность не нарушалась даже в том случае, когда злоумышленнику становится известен метод шифрования.

Метод закрытия, набор используемых ключей и механизм их распределения не должны быть слишком сложными.

Выполнение процедур прямого и обратного преобразований должно быть формальным. Эти процедуры не должны зависеть от длины сообщений.

Ошибки, возникающие в процессе преобразования, не должны распространяться по всему тексту.

Вносимая процедурами защиты избыточность должна быть минимальной.

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

1. 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 чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа. Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.

16. Шифр Виженера