**Лабораторная 4**

Классификация шифров:

1. **на основе процедуры шифрования**
   1. подстановочные
   2. перестановочные
2. **на основе генерирования и использования ключа**
   1. блочные
   2. поточные(потоковые)
3. **на основе типа ключа**
   1. симметричные(с тайным ключом)
   2. асимметричные(с открытым ключом)

Подстановочные шифры:

1. ***моноалфавитные*** - замена производится раздельно над каждым одиночным символом сообщения(***шифр Цезаря***(с ключевым словом), ***аффинный шифр цезаря*** на основе уравнения y = ax+b mod N) - низкая криптостойкость
2. ***полиграммные шифры*** - одна подстановка соответствует нескольким символам исходного текста(шифра Порты(АВВА - 003 067))
3. ***омофонические***
4. ***полиалфавитные*** - состоит из нескольких шифров однозначной замены(***Таблица Трисемуса*** - таблица NxN первая стока это алфавит, последующие сдвигаются на один символ, первая буква в первой строке, вторая во второй и т.д; ***Шифр Виженера*** - используется таблица Трисемуса, сообщение шифруется с помощью ключевого слова. Ключ смотрится в верхней строке которая соответствует исходному алфавиту, шифруемое слово в левом столбце соответствующем исходному алфавиту, Если ключ действительно случайный, его длина равна длине сообщения и он использовался единожды, то шифр Виженера теоретически будет невзламываемым)

**Шифр Плейфера**

матрица 5х5 - для латиницы, 4х8 - для кириллицы

матрицу заполняем сначала ключевым словом без повторения символов, потом оставшимся алфавитом

Сообщение разбивается на биграммы и ищем их в таблице

Если символы совпадают разделяются х

В одной строке - заменяются ближайшими символами в столбце

В одном столбце - заменяются символом который стоит ниже

**Лабораторная 5**

Сущность ***перестановочного шифрования*** состоит в том, что исходный текст (М) и зашифрованный текст (С) основаны на использовании одного и того же алфавита, а тайной или ключевой информацией является алгоритм перестановки.

Шифры перестановки относятся к классу симметричных.

Элементами текста могут быть отдельные символы, пары, тройки букв и т.д.

**Шифры перестановки:**

1. **Простой или одинарной, перестановки** - при зашифровании символы перемещаются с исходных позиций в новые только один раз
   1. **Простая перестановка** - фактически каждый символ будет являться ключем, тк мы указывае индекс каждого символа.
   2. **Блочная перестановка** - работает таким же образом только мы шифруем не один символ из сообщения.
   3. **Маршрутная перестановка** - записывают символы в таблицу и считываются по определенному маршруту, усложнение маршрута считывания символов увеличивает криптостойкость шифра
   4. **шифр вертикальной перестановки** - разновидность маршрутной перестановки(кол-во столбцов в таблице фиксируется и определяется длиной ключа; маршрут - слева направо, сверху вниз; шифрограмма выписывается по столбцам в соответствии с их нумерацией
2. **Сложной или множественной, перестановки** - при зашифровании символы перемещаются с исходных позиций в новые несколько раз.

**Лабораторная 6**

Машина «Энигма» – это электромеханическое устройство. Как и другие роторные машины, «Энигма» состоит из комбинации механических и электрических подсистем.

Механическая часть включает в себя клавиатуру, набор вращающихся дисков – роторов, которые расположены вдоль вала и прилегают к нему, и ступенчатого механизма, двигающего один или несколько роторов при каждом нажатии на клавишу.

Электрическая часть, в свою очередь, состоит из электрической схемы, соединяющей между собой клавиатуру, коммутационную панель, лампочки и роторы (для соединения роторов использовались скользящие контакты).

Замкнутую цепь составляют: батарея 1 (это могут быть и иные источники питания), нажатая двунаправленная буквенная клавиша 2, разъем коммутационной панели 3 (как видим, в одном случае – буква «а» – коммутационного перехода на другую букву нет), входной разъем (входное колесо) роторного модуля 4, роторный модуль 5 (состоит из трех роторов, как в версии «Энигмы» для Вермахта, Wehrmacht Enigma М3, или четырех – в версии «Энигмы» для военно-морского флота, Kriegsmarine Enigma M4), рефлектор 6. Последний возвращает ток (цепь) по другому пути через те же узлы, «зажигая» на ламповой панели букву «D», к другому полюсу батареи. Обратим внимание, что обратная часть цепи уже проходит с учетом выполненной коммутации (7 и 8).

Чтобы оценить криптостойкость шифра, нужно учитывать все возможные настройки машины. Для этого необходимо рассмотреть следующие свойства «Энигмы»: • выбор и порядок роторов; • разводку (коммутацию) роторов; • настройку колец на каждом из роторов; • начальное положение роторов в начале сообщения; • отражатель; • настройки коммутационной панели.