**Классические симметричные методы шифрования**

Методы шифрования по типу ключей делятся на симметричные и несимметричные. Симметричные по способу преобразования бывают методы замены, методы перестановки, аналитические методы, аддитивные методы и комбинированные методы.

Симметричные методы – это способ шифрования, в котором для шифрования и расшифрования применяется один и тот же криптографический ключ. Ключ алгоритма должен сохранятся в секрете обеими сторонами и алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Метод перестановки заключается в разделении исходного текста на блоки фиксированной длины и последующей перестановки символов внутри каждого блока по определенному алгоритму. Перестановки получаются за счет разницы путей записи исходной информации и путей считывания зашифрованной информации в пределах геометрической фигуры.

Аналитические методы. Для шифрования информации могут им пользоваться наиболее распространенные методы шифрования, основанные на матричной алгебре.

Аддитивные методы шифрования заключаются в последовательном суммировании цифровых кодов соответствующих символов исходной информации, последовательности кодов, которых соответствуют некоторому картежу символов. Поэтому аддитивные методы шифрования называют гаммированием. Самым эффективным для данного метода является генератор случайных чисел.

Симметричные алгоритмы: шифрование методом Цезаря, шифр Гронсвильда, шифр Вермана, алгоритм Гамельтона, шифр Вижинера, шифр Полибе,