**Сущность подстановочного шифрования** состоит в том, что исходный текст (из множества М) и зашифрованный текст (из множества С) основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм подстановки.

Приведенные утверждения справедливы для следующих типов подстановочных шифров: • моноалфавитных (шифры однозначной замены или простые подстановочные); • полиграммных; • омофонических (однозвучные шифры или шифры многозначной замены); • полиалфавитных. Кратко поясним особенности указанных шифров.

**Моноалфавитные** шифры подстановки: y ≡ x + k mod N-где x, y – индекс (порядковый номер, начиная с 0) символа в используемом алфавите; k – ключ.

**Атбаш**. - шифр состоит в замене каждой буквы другой буквой, которая находится в алфавите на таком же расстоянии от конца алфавита, как оригинальная буква – от начала. Например, в русском алфавите буква А заменяется на Я.

Одним из существенных недостатков моноалфавитных шифров является их низкая **криптостойкость**. Зачастую метод криптоанализа базируется на частоте встречаемости букв исходного текста.

**Система шифрования Цезаря с ключевым словом (лозунгом).** Также является *одноалфавитной системой подстановки.* Особенностью этой системы является использование ключевого слова (лозунга) для смещения и изменения порядка символов в алфавите подстановки (желательно, чтобы все буквы ключевого слова были различными). Ключевое слово пишется в начале алфавита подстановки.

Применяя одновременно операции сложения и умножения по модулю n над элементами множества (индексами букв алфавита), можно получить систему подстановок, которую называют **аффинной системой подстановок Цезаря.** Определим процедуру зашифрования в такой системе: y ≡ ax + b mod N, где a и b – целые числа. При этом взаимно однозначные соответствия между открытым текстом и шифртекстом будут иметь место только при выполнении следующих условий: 0 ≤ a, b < N, наибольший общий делитель (НОД) чисел a, N равен 1, т. е. эти числа являются взаимно простыми.

**Полиграммные шифры-**В таких шифрах одна подстановка соответствует сразу нескольким символам исходного текста. Первым известным шифром этого типа является **шифр Порты**. Шифр представляется в виде таблицы. Наверху горизонтально и слева вертикально записывается стандартный алфавит.

Шифрование выполняется парами букв исходного сообщения. Первая буква пары указывает на строку, вторая – на столбец. В случае нечетного количества букв в сообщении Мi к нему добавляется вспомогательный символ, например «А».

Другими известными полиграммными шифрами являются **шифр Плейфера и** **шифр Хилла.** С точки зрения криптостойкости рассматриваемый тип шифров имеет преимущества перед моноалфавитными шифрами. Это связано с тем, что, во-первых, распределение частот групп букв значительно более равномерное, чем отдельных символов. Во-вторых, для эффективного частотного анализа требуется больший размер зашифрованного текста, так как число различных групп букв значительно больше, чем мощно

**Омофонические шифры**-Омофонические шифры (омофоническая замена), или однозвучные шифры подстановки, создавались с целью увеличить сложность частотного анализа шифртекстов путем маскировки реальных частот появления символов текста с помощью омофонии.

Полиалфавитные шифры-шифры состоят из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования.

**Диск Альберти**. В «Трактате о шифрах» Альберти приводит первое точное описание многоалфавитного шифра на основе шифровального диска . Он состоял из двух дисков – внешнего неподвижного и внутреннего подвижного, на которые были нанесены буквы алфавита. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замене ее на букву с внутреннего диска, стоящую под ней. После этого внутренний диск сдвигался на одну позицию, и шифрование второй буквы производилось уже по-новому шифралфавиту. Ключом данного шифра являлся порядок расположения букв на дисках и начальное положение внутреннего диска относительно внешнего.

**Таблица Трисемуса**. Зашифрование осуществляется так: заготавливается таблица подстановки (так называемая «таблица Трисемуса» – таблица со стороной, равной N, где N – мощность алфавита), где первая строка – это алфавит, вторая – алфавит, сдвинутый на один символ, и т. д. При зашифровании первая буква открытого текста заменяется на букву, стоящую в первой строке, вторая – на букву, стоящую во второй строке, и т. д. После использования последней строки вновь возвращаются к первой.( ключевое слово (или фраза))

**Шифр Виженера**. В этом шифре мы имеем дело с последовательностью сдвигов, циклически повторяющейся. Основная идея заключается в следующем. Создается таблица (таблица Виженера) размером N×N (N – число знаков в используемом алфавите). Эти знаки могут включать не только буквы, но и, например, пробел или иные знаки. В первой строке таблицы записывается весь используемый алфавит. Каждая последующая строка получается из предыдущего циклического сдвига последней на 1 символ влево. Таким образом, при мощности алфавита (английского языка), равной 26, необходимо выполнить последовательно 25 сдвигов для формирования всей таблицы. Более подробное описание шифра можно найти в [3, с. 41–43]. Листинг содержит часть кода, реализующего алгоритм шифрования Виженера.

Еще раз вспомним, что криптоанализ – это раздел криптологии, занимающийся методами взлома шифров или методами организации криптографических атак на шифры.

**Атака с известным шифртекстом** (ciphertext only attack). Предполагается, что противник знает алгоритм шифрования, у него имеется набор перехваченных шифрограмм, но он не знает секретный ключ. Разновидности такой атаки: • полный перебор ключей (лобовая атака, bruteforce attack); • атака по словарю, перебор ключей по словарю (dictionary attack); применяется часто для взлома паролей; • частотный криптоанализ – метод взлома шифра, основывающийся на предположении о существовании зависимости между частотой появления символов алфавита в открытых сообщениях и соответствующих шифрозамен в шифрограммах.

**Атака с выбором шифртекста** (chosen cipher text attack). Криптоаналитик имеет возможность выбрать необходимое количество шифрограмм и получить соответствующие им открытые тексты. Он также может воспользоваться устройством расшифрования один или несколько раз для получения шифртекста в расшифрованном виде. Используя полученные данные, он может попытаться восстановить секретный ключ.

**Адаптивная атака с выбором шифртекста** (adaptive chosen ciphertext attack). Криптоаналитик имеет возможность выбирать новые шифрограммы для расшифрования с учетом того, что ему известна некоторая информация из предыдущих сообщений. В некоторых криптографических протоколах при получении шифрограммы, несоответствующей стандарту (содержащей ошибки), отправитель получает ответное сообщение, иногда с детализированным