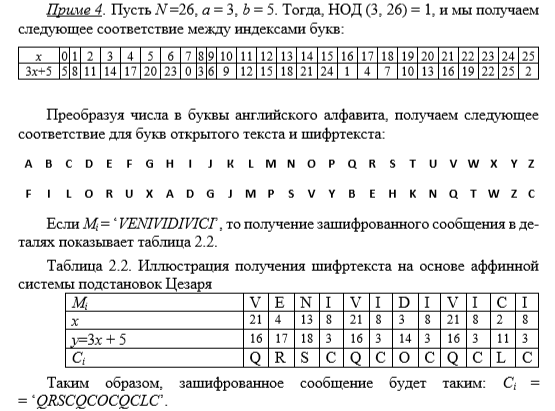
1. **Аффинная система подстановок цезаря**

Применяя одновременно операции сложения и умножения по модулю n можно получить систему подстановок – аф.сист.подст.Цезаря

**Зашифрование:**

y = (ax + b )mod N); a и b – целые числа (взаимно простые)

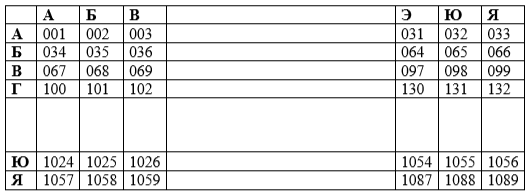


**Расшифрование:** x = a-1(y+N-b)modN

**ПОЛИГРАММНЫЕ ШИФРЫ**

1. **Шифр порты**

Шифр представляется в виде таблицы. Наверху горизонтально и слева вертикально записываются буквы алфавита. В ячейках таблицы записываются числа в опред.порядке.



Шифрование вып-ся парами букв их.сообщения. Первая пара – строка, 2 – столбец.

В случае нечетного кол-ва букв в сообщении к нему добавляется вспомогательный символ, например «А».



1. **Шифр Хилла**

С т.зр.криптостойкости имеет преимущество перед моноалфавитными. Т.к.распределение частот групп значительно более равномерное, чем отдельных символов. Во-втрых, для эффективного анализа требуется больший размер зашифрованного текста, т.к.число различных групп букв значительно больше, чем мощность алфавита.

**ОМОФОНИЧЕСКИЕ ШИФРЫ**

Создавались с целью цвеличить сложность частотного анализа шифротекстов путем маскировки реальных частот появления символов текста с помощью омофонии. (слова кот.звучат одинаково, но пишутся по разному)

1. **Книжный шифр**

Шифрозамена каждой буквы опред.набором цифр, кот.указ.на номер стр., строки и позиции в строке).

Отсутсвтие полной эл.базы изданных книг делает процедуру взлома практически невыполнимой.



**ПОЛИАЛФАВИТНЫЕ ШИФРЫ**

1. **Диск альберти**

Есть 2 диска (неподвижный и внутренний подвижный). На них нанесены буквы алфавита.

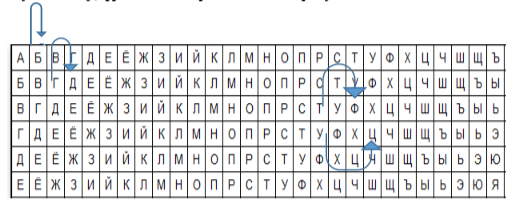
Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замене ее на буку с внутреннего диска, стоящего под ней. После этого внутренний диск сдвигался на одну позиции и шифрование 2ой буквы производилось уже по новому шарфаалфавиту.

Ключом явл.расположение букв на дисках и начальное положение внутреннего диска относительно первого.

1. **Таблица трисемуса**

Зашифрование:

Изготавливается таблица подстановки, где первая строка – алфавит, вторая – алфавит, сдвинутый на 1 символ и т.д. После исп-ния последней строки вновь возвращаемся на первую



1. **Таблица трисемуса с ключевым словом**

В таблицу сначала вписывается ключевое слово, при чем повторяющиеся буквы удаляются, затем таблица дополняется не вошедшими в ключевое слово буквами алфавита.

Ключ – ключевое слово и размер таблицы.

К.буква заменяется расположенной ниже в той же строке, если достигнули нижней стркои – заменяем первой строкой.



1. **Шифр виженера**

Имеем дело с посл-стью сдвигов, цеклически повторяющейся.

Создается таблица виженера размером N\*N (мощность)

Эти знаки м.влюч знаки препинания, пробелы и т.д.

В первой строке пишем исп-мый алфавит

К.след.строка = пред + сдвиг на 1 символ влево.

Для агнл.алф мощность 26 – 25 сдвигов.

**КИПТОАНАЛИЗ**

1. **Атака с известным шифротекстом**

Предполагается, что противник знает алгоритм, есть набор шифрограмм, но не знает ключ.

1. **Атака с выбором шифртекста**

Аналитик им.возм-сть выбрать необх.кол-во шифрограмм и получить соотв.им откр.тесты

1. **Адаптивная атака с выбором шифртекста**  
   Криптоаналитик им.возм-сть выбирать новые шифрограммы для расшифрования с учетом того, что ему известна некоторая инфа из пред. Сообщ.
2. **Атака с известным открытым текстом**

Тож., что и пред, но противник для нек.шифрограмм получается соот.им открытые тексты

1. **Атака с выбором открытого текста**
2. **На осн.связ.ключе**

Аналитик знает не ключи, а нек.различия между ними

1. **Атака с выбором кобча** (задает часть ключа, а на ост.часть вып.атаку на осн.связ.ключей)