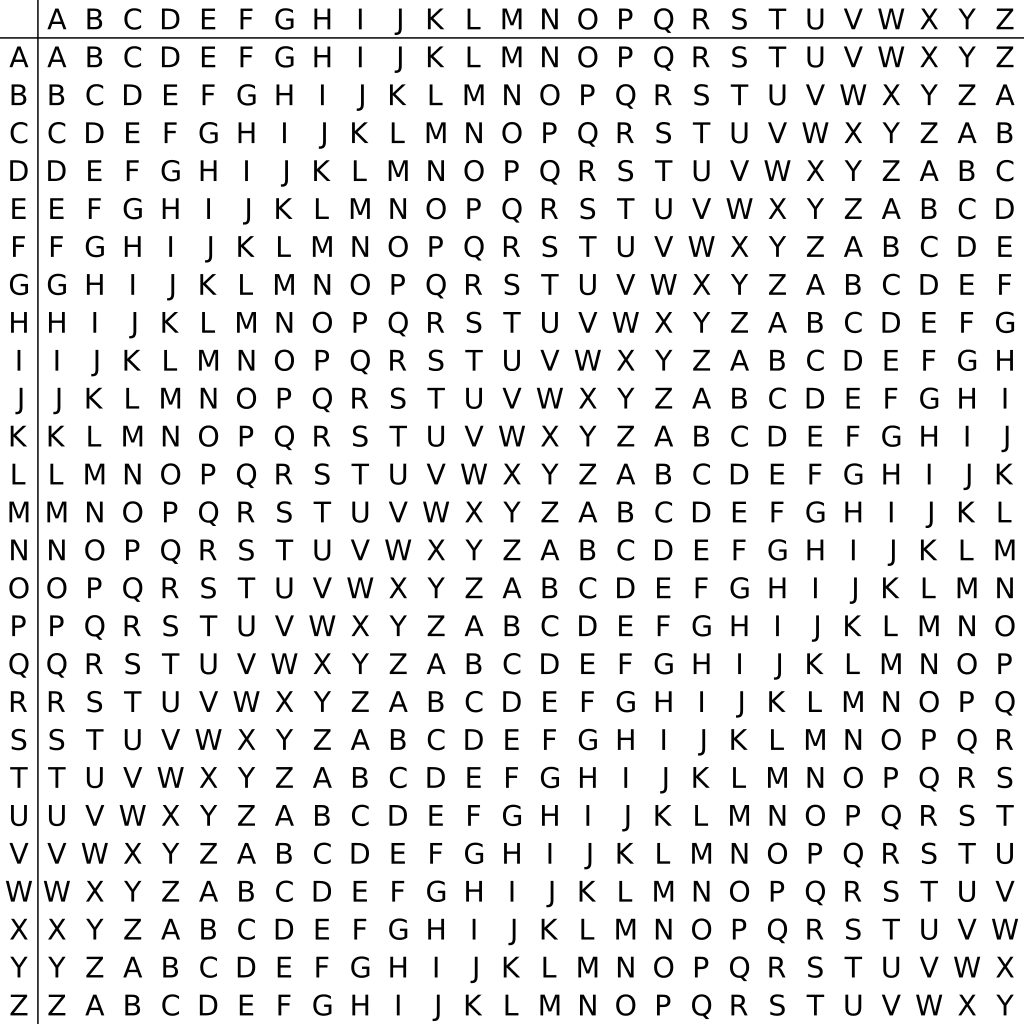
**Шифр Виженера** — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Этот метод является простой формой многоалфавитной замены.

Шифр Виженера имел репутацию исключительно стойкого к «ручному» взлому. Известный писатель и математик Чарльз Лютвидж Доджсон ([Льюис Кэрролл](https://ru.wikipedia.org/wiki/Льюис_Кэрролл)) назвал шифр Виженера невзламываемым в своей статье «Алфавитный шифр», опубликованной в журнале в 1868 году. В 1917 году также отозвался о шифре Виженера как о не поддающемся взлому. Это представление было опровергнуто после того, как [Касиски](https://ru.wikipedia.org/wiki/Касиски,_Фридрих) полностью взломал шифр в XIX веке, хотя известны случаи взлома этого шифра некоторыми опытными криптоаналитиками ещё в XVI веке.

В [шифре Цезаря](https://ru.wikipedia.org/wiki/Шифр_Цезаря) каждая буква алфавита сдвигается на несколько позиций; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее.

 Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Например, предположим, что исходный текст имеет такой вид:

SHIFROVANIE

Человек, посылающий сообщение, записывает ключевое слово («LEMON») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

LEMONLEMONL

Первый символ исходного текста («S») зашифрован последовательностью L, которая является первым символом ключа. Первый символ зашифрованного текста («D») находится на пересечении строки L и столбца S в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ зашифрованного текста («L») получается на пересечении строки E и столбца H. Остальная часть исходного текста шифруется также:

Исходный текст: SHIFROVANIE

Ключ: LEMONLEMONL

Зашифрованный текст: DLUTEZZMBVP

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются идентично.

Если N – количество букв в алфавите, Mj – буквы открытого текста, Kj – буквы ключа, то шифрование Виженера можно записать следующим образом:

Сj = (Mj+Kj) mod N

расшифрование:

Mj = (Cj+N-Kj) mod N

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по модулю N.

Если таблица будет более сложной, чем циклическое смещение строк, то шифр станет надежнее. Например, если менять ее чаще, допустим, от слова к слову. Но составление таких таблиц, представляющих собой латинские квадраты, где любая буква встречается в строке или столбце один раз, трудоемко и его стоит делать лишь на ЭВМ. Для ручного же многоалфавитного шифра полагаются лишь на длину и сложность ключа, используя приведенную таблицу, которую можно не держать в тайне, а это упрощает шифрование и расшифровывание.

Итак, шифр Виженера получается как повторяющаяся комбинация сдвигов. В общем случае этот шифр не сохраняет частоту встречающихся букв и по этой причине не может напрямую подвергаться статистическому анализу.

Существует много других легкозапоминающихся квадратов, которые могут применяться в качестве основы для многоалфавитной системы так же, как и квадрат Виженера. Одним из наиболее известных является [квадрат Бофора](https://ru.wikipedia.org/wiki/Шифр_Бофора). Его строками являются строки квадрата Виженера, записанные в обратном порядке. Он назван в честь адмирала сэра [Френсиса Бофора](https://ru.wikipedia.org/wiki/Фрэнсис_Бофорт) — создателя шкалы для определения скорости ветра. Если в квадрате Виженера первая строка и столбец указывают на строки и столбцы соответственно, то в квадрате Бофора этим целям служат первая строка и последний столбец.

Версия шифра Виженера running key (бегущий ключ) использует в качестве ключа блок текста, равный по длине исходному тексту. Так как ключ равен по длине сообщению, то методы, предложенные Фридманом и Касиски, не работают (так как ключ не повторяется). В 1920 году Фридман первым обнаружил недостатки этого варианта. Проблема с running key шифра Виженера состоит в том, что криптоаналитик имеет статистическую информацию о ключе (учитывая, что блок текста написан на известном языке) и эта информация будет отражаться в шифрованном тексте. Если ключ действительно случайный, его длина равна длине сообщения и он использовался единожды, то этот вариант будет уже шифром Вернама-Виженера, для которого доказана абсолютная криптостойкость.

Несмотря на очевидную стойкость шифра Виженера, он широко не использовался в Европе. Большее распространение получил [шифр Гронсфельда](https://ru.wikipedia.org/wiki/Шифр_Гронсфельда), созданный графом Гронсфельдом, идентичный шифру Виженера, за исключением того, что он использовал только 10 различных алфавитов (соответствующих цифрам от 0 до 9). Преимущество шифра Гронсфельда состоит в том, что в качестве ключа используется не слово, а цифровая последовательность, которая повторяется до тех пор, пока не станет равной длине шифруемого сообщения. Шифр Гронсфельда широко использовался по всей Германии и Европе.