**Лабораторная работа № 4**

**Шифрование с использованием системы Вижинера и шифра «двойной квадрат» Уитстона**

**1 Цель работы: изучить и закрепить умение шифровать информацию системой Вижинера и с помощью двойного квадрата Уитстона.**

**2.1 Выбрать язык программирования.**

**2.2 Изучить материал.**

**2.3 Выполнить задания.**

**2.4 Ответьте на контрольные вопросы.**

**2.4.1 Как составляется таблица в методе Виженера?**

**2.4.2 Что используется в методе Виженера для** зашифровывания **сообщения?**

**2.4.3 Отличие методов «двойной квадрат» и «полибианский квадрат».**

**2.5 Оформить отчет.**

**Теоретические сведенья:**

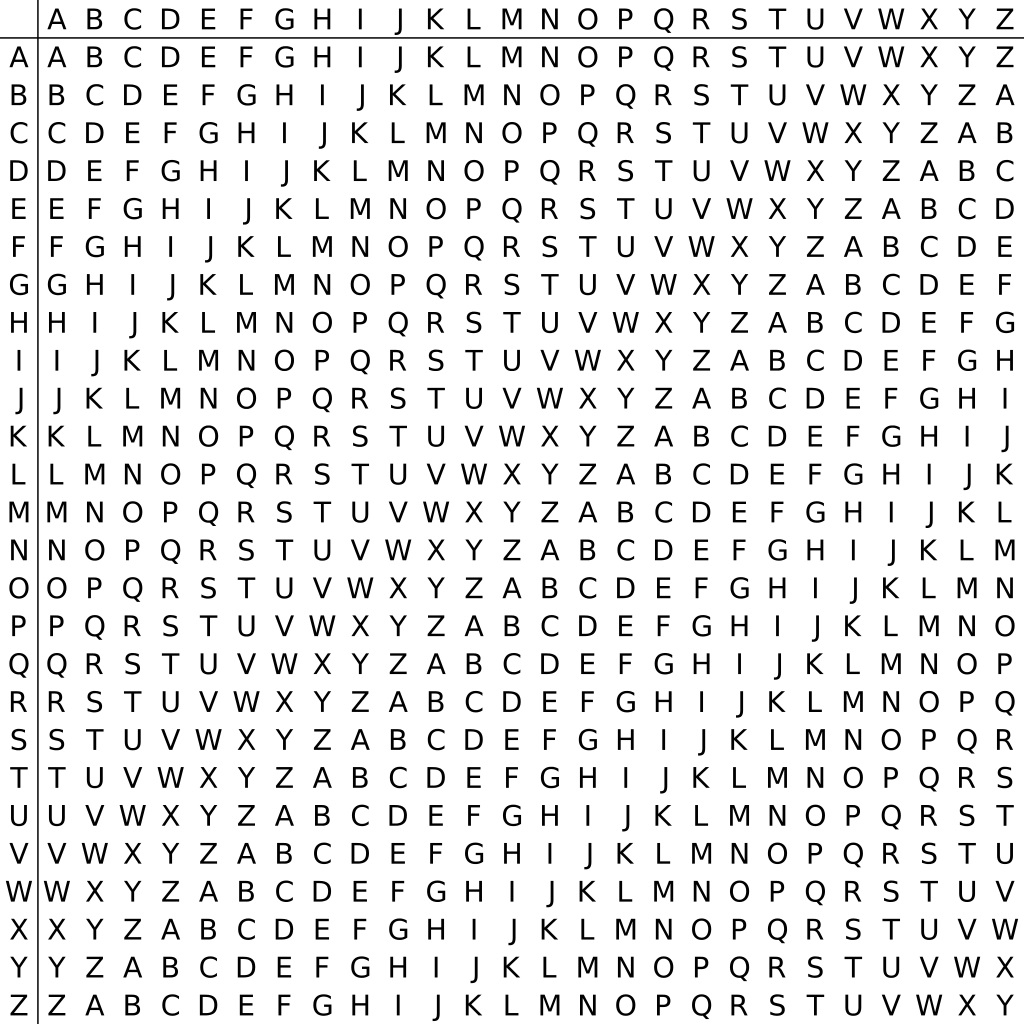
**Система Вижинера**

В [шифре Цезаря](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F) каждая буква алфавита сдвигается на несколько строк; 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 tabula recta или 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 вид:

ATTACKATDOWN

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

LEMONLEMONLE



Первый символ исходного текста A зашифрован последовательностью L, которая является первым символом ключа. Первый символ L шифрованного текста находится на пересечении строки L и столбца A в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ шифрованного текста X получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом.

Исходный текст: ATTACKATDAWN

Ключ: LEMONLEMONLE

Зашифрованный текст: LXFOPVEFRNHR

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 подобным образом.

Если буквы A—Z соответствуют числам 0-25, то шифрование Виженера можно записать в виде формулы:

Расшифровка:

**Шифр «двойной квадрат» Уитстона**

В 1854 г. англичанин Чарльз Уитстон разработал новый метод шифрования биграммами, который называют "двойным квадратом". Свое название этот шифр получил по аналогии с полибианским квадратом. Шифр Уитстона открыл новый этап в истории развития криптографии. В отличие от полибианского шифр "двойной квадрат" использует сразу две таблицы, размещенные по одной горизонтали, а шифрование идет биграммами, как в шифре Плейфейра. Эти не столь сложные модификации привели к появлению на свет качественно новой криптографической системы ручного шифрования. Шифр "двойной квадрат" оказался очень надежным и удобным и применялся Германией даже в годы второй мировой войны.

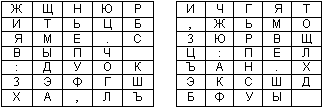
Поясним процедуру шифрования этим шифром на примере. Пусть имеются две таблицы со случайно расположенными в них русскими алфавитами (рис.). Перед шифрованием исходное сообщение разбивают на биграммы. Каждая биграмма шифруется отдельно. Первую букву биграммы находят в левой таблице, а вторую букву - в правой таблице. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.

Рис. Две таблицы со случайно расположенными символами русского алфавита для шифра "двойной квадрат"

Предположим, что шифруется биграмма исходного текста ИЛ. Буква И находится в столбце 1 и строке 2 левой таблицы. Буква Л находится в столбце 5 и строке 4 правой таблицы. Это означает, что прямоугольник образован строками 2 и 4, а также столбцами 1 левой таблицы и 5 правой таблицы. Следовательно, в биграмму шифртекста входят буква О, расположенная в столбце 5 и строке 2 правой таблицы, и буква В, расположенная в столбце 1 и строке 4 левой таблицы, т.е. получаем биграмму шифртекста ОВ.

Если обе буквы биграммы сообщения лежат в одной строке, то и буквы шифртекста берут из этой же строки. Первую букву биграммы шифртекста берут из левой таблицы в столбце, соответствующем второй букве биграммы сообщения. Вторая же буква биграммы шифртекста берется из правой таблицы в столбце, соответствующем первой букве биграммы сообщения. Поэтому биграмма сообщения ТО превращается в биграмму шифртекста ЖБ. Аналогичным образом шифруются все биграммы сообщения:

Сообщение ПР ИЛ ЕТ АЮ \_Ш ЕС ТО ГО

Шифртекст ПЕ 0В ЩН ФМ ЕШ РФ БЖ ДЦ

Шифрование методом "двойного квадрата" дает весьма устойчивый к вскрытию и простой в применении шифр. Взламывание шифртекста "двойного квадрата" требует больших усилий, при этом длина сообщения должна быть не менее тридцати строк.

**Задание №1**

Зашифровать системой Вижинера индивидуальный текст.

Ключ и текст брать из таблицы.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Текст для шифрования | | Ключ |
| 1 | Скажи-ка, дядя, ведь не даром Москва, спаленная пожаром, Французу отдана? Ведь были ж схватки боевые, | | буйвол |
| 2 | Да, говорят, еще какие! Недаром помнит вся Россия Про день Бородина! - Да, были люди в наше время, | | мальта |
| 3 | Не то, что нынешнее племя: Богатыри - не вы! Плохая им досталась доля: Немногие вернулись с поля. | | портрет |
| 4 | Не будь на то господня воля, Не отдали б Москвы! Мы долго молча отступали, Досадно было, боя ждали, | | архив |
| 5 | Ворчали старики: "Что ж мы? на зимние квартиры? Не смеют, что ли, командиры Чужие изорвать мундиры | | совершенство |
| 6 | О русские штыки?" И вот нашли большое поле: Есть разгуляться где на воле! Построили редут. | удар | |
| 7 | У наших ушки на макушке! Чуть утро осветило пушки И леса синие верхушки - Французы тут как тут. | знакомство | |
| 8 | Забил заряд я в пушку туго И думал: угощу я друга! Постой-ка, брат мусью! Что тут хитрить, пожалуй к бою; | советник | |
| 9 | Уж мы пойдем ломить стеною, Уж постоим мы головою За родину свою! Два дня мы были в перестрелке. | мгновенье | |
| 10 | Что толку в этакой безделке? Мы ждали третий день. Повсюду стали слышны речи: "Пора добраться до картечи!" | гвардейцы | |

**Задание №2**

Зашифровать системой двойного квадрата Уитстона индивидуальный текст.

Шифрующие таблицы сделать самому.

|  |  |
| --- | --- |
| № | Текст для шифрования |
| 1 | И вот на поле грозной сечи Ночная пала тень. Прилег вздремнуть я у лафета, И слышно было до рассвета, |
| 2 | Как ликовал француз. Но тих был наш бивак открытый: Кто кивер чистил весь избитый, Кто штык точил, ворча сердито, |
| 3 | Как ликовал француз. Но тих был наш бивак открытый: Кто кивер чистил весь избитый, Кто штык точил, ворча сердито, |
| 4 | Полковник наш рожден был хватом: Слуга царю, отец солдатам... Да, жаль его: сражен булатом, Он спит в земле сырой. |
| 5 | И молвил он, сверкнув очами: "Ребята! не Москва ль за нами? Умремте же под Москвой, Как наши братья умирали!" |
| 6 | И умереть мы обещали, И клятву верности сдержали Мы в Бородинский бой. Ну ж был денек! Сквозь дым летучий |
| 7 | Французы двинулись, как тучи, И всё на наш редут. Уланы с пестрыми значками, Драгуны с конскими хвостами, |
| 8 | Все промелькнули перед нам, Все побывали тут. Вам не видать таких сражений!.. Носились знамена, как тени, |
| 9 | В дыму огонь блестел, Звучал булат, картечь визжала, Рука бойцов колоть устала, И ядрам пролетать мешала |
| 10 | Гора кровавых тел. Изведал враг в тот день немало, Что значит русский бой удалый, Наш рукопашный бой!.. |

**Оформите отчет. Запишите результаты выполнения заданий в отчет.**