Тихонова Виталия Владимировна
студентка
Усманов Руслан Ирекович
студент
Додонова Наталья Леонидовна
доцент
ФГАОУ ВО «Самарский государственный аэрокосмический университет им. академика С.П. Королёва (НИУ)»
г. Самара, Самарская область

ЛАТИНСКИЕ КВАДРАТЫ И ИХ ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

Аннотация: *из года в год шифрование любого вида информации становится все сложнее и сложнее из-за прогрессивного роста киберпреступности. Именно поэтому в данной статье мы исследовали применение латинских квадратов в криптографии. Были рассмотрены основные определения латинских квадратов, свойства, которые обеспечивают наиболее высокий уровень криптостойкости. Нами был разработан новый алгоритм шифрования, основанный на шифре Виженера. Его реализация на языке программирования высокого уровня позволила оценить сильные и слабые стороны нашего шифра.*

Ключевые слова*: латинский квадрат, криптография, криптостойкость, шифрование.*

Введение

Латинский квадрат n-го порядка – таблица L=(lij) размеров n × n, заполненная n элементами множества M таким образом, что в каждой строке и в каждом столбце таблицы каждый элемент из M встречается в точности один раз [3]. Пример латинского квадрата 3-го порядка:

C	B	A
A	C	B
B	A	C

Рис. 1. Латинский квадрат 3-го порядка

Который может быть представлен в виде:

{(1,1,C),(1,2,B),(1,3,A),(2,1,A),(2,2,C),(2,3,B),(3,1,B),(3,2,A),(3,3,C)},

где первый и второй элемент – позиция элемента в матрице, а третий – значение.

Впервые латинские квадраты (4-го порядка) были упомянуты в книге «Шамс аль Маариф» написанной Ахмадом аль-Буни приблизительно в 1200 году в Египте.

Нормализованный латинский квадрат – латинский квадрат первая строка и первый столбец которого заполнены в соответствии с порядком заданным на M.

Пример:

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$$

Рисунок 2. Нормализованный латинский квадрат

Цель данной работы – разработка алгоритма шифрования/дешифрования сообщения на основе латинских квадратов, а также его программная реализация.

Применение латинских квадратов в криптографии

Латинские квадраты используются в таких областях как алгебра, теория кодов, комбинаторика, статистика и т. д. Латинские квадраты так же используются в криптографии. Впервые были применены в шифре Тритемия. Он использовал таблицу, соответствующую таблице Кэли группы (Z_{26}, +), для многоалфавитного шифрования. В многоалфавитном шифровании первая буква открытого текста шифруется первым алфавитом, т.е. первой строкой таблицы, а вторая – вторым и т. д. Со временем это шифр был модернизирован Джованни Белазо и Леоном Альберти, что привело к появлению нового шифра, основанного на квазигруппе. Это стало важным событием на пути развития криптографии.

Всю роль латинских квадратов в криптографии иллюстрирует теорема Шеннона. По теореме единственными совершенными шифрами являются шифры гаммирования, наложение гаммы в которых определяется латинским квадратом.

Стоит отметить один из примеров применения латинских квадратов для построения поточных шифров. Шифр Edon80 был предложен в 2005 году. Он дошел до 3-го тура конкурса ESTREAM. Создатели этого шифра из 576 существующих латинских квадратов 4-го порядка тщательно выбрали 4, на основе которых в криптографии строится конвейер из 80 латинских квадратов. Он используется для выработки гаммы.

Так же популярным примером использования латинских квадратов в шифровании является шифр Виженера.

Шифр Виженера – метод полиалфавитного ширфрования буквенного текста с использованием ключевого слова [4]. Впервые этот метод описал Джовани Беллазо в 1553 году, однако в XIX веке получил имя Блеза Виженера, французского дипломата. Этот метод прост для понимания и реализации, но является недоступным для простых способов криптоанализа.

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица, именуемая tabula recta или квадрат 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.

Шифр Виженера можно представить в таком виде:

m_j-буквы открытого текста

k_j -буквы ключа

n-количество букв в алфавите

Шифрование: $c_j = m_j + k_j\ (mod(n)$

Дешифрование: $c_j = m_j\text{-}k_j\ (mod(n)$

Создание собственного шифра

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Б	В	Г	Д	Е	Ё	Ж	З	И	Й	А	Л	М	Н	О	П	Р	С	Т	У	Ф	К	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	Х
В	Г	Д	Е	Ё	Ж	З	И	Й	А	Б	М	Н	О	П	Р	С	Т	У	Ф	К	Л	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	Х	Ц
Г	Д	Е	Ё	Ж	З	И	Й	А	Б	В	Н	О	П	Р	С	Т	У	Ф	К	Л	М	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	Х	Ц	Ч
Д	Е	Ё	Ж	З	И	Й	А	Б	В	Г	О	П	Р	С	Т	У	Ф	К	Л	М	Н	Щ	Ъ	Ы	Ь	Э	Ю	Я	Х	Ц	Ч	Ш
Е	Ё	Ж	З	И	Й	А	Б	В	Г	Д	П	Р	С	Т	У	Ф	К	Л	М	Н	О	Ъ	Ы	Ь	Э	Ю	Я	Х	Ц	Ч	Ш	Щ
Ё	Ж	З	И	Й	А	Б	В	Г	Д	Е	Р	С	Т	У	Ф	К	Л	М	Н	О	Р	Ы	Ь	Э	Ю	Я	Х	Ц	Ч	Ш	Щ	Ъ
Ж	З	И	Й	А	Б	В	Г	Д	Е	Ё	С	Т	У	Ф	К	Л	М	Н	О	П	П	Ь	Э	Ю	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ы
З	И	Й	А	Б	В	Г	Д	Е	Ё	Ж	Т	У	Ф	К	Л	М	Н	О	П	Р	С	Э	Ю	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
И	Й	А	Б	В	Г	Д	Е	Ё	Ж	З	У	Ф	К	Л	М	Н	О	П	Р	С	Т	Ю	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
Й	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Ф	К	Л	М	Н	О	П	Р	С	Т	У	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	К	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	Х	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	А
М	Н	О	П	Р	С	Т	У	Ф	К	Л	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	Х	Ц	В	Г	Д	Е	Ё	Ж	З	И	Й	А	Б
Н	О	П	Р	С	Т	У	Ф	К	Л	М	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	Х	Ц	Ч	Г	Д	Е	Ё	Ж	З	И	Й	А	Б	В
О	П	Р	С	Т	У	Ф	К	Л	М	Н	Щ	Ъ	Ы	Ь	Э	Ю	Я	Х	Ц	Ч	Ш	Д	Е	Ё	Ж	З	И	Й	А	Б	В	Г
П	Р	С	Т	У	Ф	К	Л	М	Н	О	Ъ	Ы	Ь	Э	Ю	Я	Х	Ц	Ч	Ш	Щ	Е	Ё	Ж	З	И	Й	А	Б	В	Г	Д
Р	С	Т	У	Ф	К	Л	М	Н	О	Р	Ы	Ь	Э	Ю	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ё	Ж	З	И	Й	А	Б	В	Г	Д	Е
С	Т	У	Ф	К	Л	М	Н	О	П	П	Ь	Э	Ю	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ж	З	И	Й	А	Б	В	Г	Д	Е	Ё
Т	У	Ф	К	Л	М	Н	О	П	Р	С	Э	Ю	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	З	И	Й	А	Б	В	Г	Д	Е	Ё	Ж
У	Ф	К	Л	М	Н	О	П	Р	С	Т	Ю	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	И	Й	А	Б	В	Г	Д	Е	Ё	Ж	З
Ф	К	Л	М	Н	О	П	Р	С	Т	У	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Й	А	Б	В	Г	Д	Е	Ё	Ж	З	И
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	Х	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	А	Л	М	Н	О	П	Р	С	Т	У	Ф	К
Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	Х	Ц	В	Г	Д	Е	Ё	Ж	З	И	Й	А	Б	М	Н	О	П	Р	С	Т	У	Ф	К	Л
Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	Х	Ц	Ч	Г	Д	Е	Ё	Ж	З	И	Й	А	Б	В	Н	О	П	Р	С	Т	У	Ф	К	Л	М
Щ	Ъ	Ы	Ь	Э	Ю	Я	Х	Ц	Ч	Ш	Д	Е	Ё	Ж	З	И	Й	А	Б	В	Г	О	П	Р	С	Т	У	Ф	К	Л	М	Н
Ъ	Ы	Ь	Э	Ю	Я	Х	Ц	Ч	Ш	Щ	Е	Ё	Ж	З	И	Й	А	Б	В	Г	Д	П	Р	С	Т	У	Ф	К	Л	М	Н	О
Ы	Ь	Э	Ю	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ё	Ж	З	И	Й	А	Б	В	Г	Д	Е	Р	С	Т	У	Ф	К	Л	М	Н	О	Р
Ь	Э	Ю	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ж	З	И	Й	А	Б	В	Г	Д	Е	Ё	С	Т	У	Ф	К	Л	М	Н	О	П	П
Э	Ю	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	З	И	Й	А	Б	В	Г	Д	Е	Ё	Ж	Т	У	Ф	К	Л	М	Н	О	П	Р	С
Ю	Я	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	И	Й	А	Б	В	Г	Д	Е	Ё	Ж	З	У	Ф	К	Л	М	Н	О	П	Р	С	Т
Я	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Й	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Ф	К	Л	М	Н	О	П	Р	С	Т	У

В основу нашего шифра был положен шифр Виженера. Для упрощения описания алгоритма шифрования используем таблицу, которая представляет собой латинский квадрат 3х3, который назовем главным:

I	II	III
II	III	I
III	I	II

Каждый элемент главного латинского квадрата представляет собой латинские квадраты 11х11, которые назовем дочерними.

Суть алгоритма состоит в следующем:

1. Задается 64-х разрядный ключ.

2. Ключ делится пополам, вторая половина используется как ключ при шифровании первой.

3. Полученный 32-х разрядный ключ делится пополам.

4. Первое шифрование текста, при этом используется первая 16-разрядная половина ключа.

5. Повторное шифрование текста, получившегося на предыдущем этапе. При шифровании используется вторая 16-разрядная половина ключа.

Процесс шифрования:

1. Путем повторения ключа необходимое количество раз, размерность ключа увеличивается до размерности сообщения. Каждой букве сообщения ставим в соответствие букву ключа.

2. При помощи первой строки главного латинского квадрата определяем к какому дочернему латинскому квадрату относится буква текста.

3. Так же определяем к какому дочернему квадрату относится буква ключа.

4. Определяем порядковый номер буквы сообщения в дочернем латинском квадрате.

5. К порядковому номеру буквы ключа прибавляем порядковый номер буквы сообщения по модулю 11.

6. Повторяем шаги 2–5 до тех пор, пока все сообщение не будет зашифровано.

Графически процесс шифрования можно изобразить следующим образом:

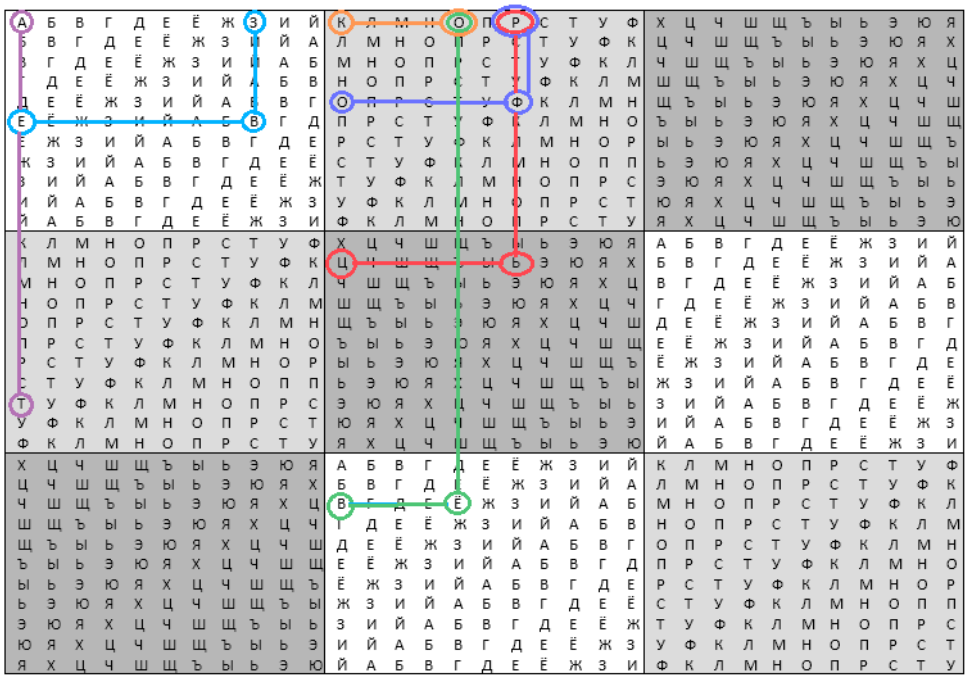

Рисунок 3. Процесс шифрования

Ключ: РОЗА
Сообщение: ЦВЕТОК

Р	О	З	А	Р	О
Ц	В	Е	Т	О	К
Ь	Ё	В	Т	Ф	О

Зашифрованное слово: ЬЁВТФО

Рисунок 4. Пример шифрования

По составленному алгоритму была написана программа, позволяющая шифровать и дешифровать сообщения.

```
Шифрование
Введите сообщение мама мыла раму маша читала книгу
Введите ключ ключшифра
рарг нысд фгнф тдшд шйтёпа нойго

Process finished with exit code 0
```

Рисунок 5. Шифрование

```
Дешифрование
Введите сообщение рарг нысд фгнф тдщд шйтёпа нойго
Введите ключ ключшифра
мама мыла раму маша читала книгу
Process finished with exit code 0
```

Рисунок 6. Дешифрование

Оценка криптографической стойкости

Криптостойкость шифра является его основным показателем эффективности. Она измеряется временем или стоимостью средств, необходимых криптоаналитику для получения исходной информации по шифртексту, при условии, что ему неизвестен ключ [2].

Сохранить в секрете широко используемый алгоритм шифрования практически невозможно. Поэтому алгоритм не должен иметь скрытых слабых мест, которыми могли бы воспользоваться криптоаналитики. Если это условие выполняется, то криптостойкость шифра определяется длиной ключа, так как единственный путь вскрытия зашифрованной информации – перебор комбинаций ключа и выполнение алгоритма расшифрования. Таким образом, время и средства, затрачиваемые на криптоанализ, зависят от длины ключа и сложности алгоритма шифрования.

Для начала отметим, что вычислительная сложность нашего алгоритма шифрования и шифра Виженера равна $O(n^2)$ [1]. Но при равных сложностях, наш алгоритм более надежный, это и постараемся доказать.

Оценим криптостойкость нашего шифра при помощи теоретических рассуждений:

1. При шифровании и дешифровании используется один ключ, но отправляемое сообщение шифруется не исходным ключом, а новой ключевой комбинацией, полученной в следствии шифровальных преобразований исходного ключа.

2. Путем экспериментальных и логических рассуждений был сделан вывод, что зашифрованное сообщение не поддается частотному анализу, так как при

шифровании каждой буквы сообщения используется своя ключевая буква. Таким образом символы зашифрованного текста равновероятны

3. Зашифрованное сообщение получается путем двукратного шифрования с различными ключевыми последовательностями. Это создает значительную сложность при расшифровке сообщения, так как необходимо воспользоваться двукратным дешифрованием.

4. Несомненным плюсом нашего алгоритма является нетипичное построение самого латинского квадрата, с помощью которого и производится процесс шифрования.

Из всех вышеприведенных рассуждений можно сделать вывод, что данный шифр является достаточно надежным.

Вывод

В результате проделанной работы, были изучены основные определения, свойства латинских квадратов, а также их применение в криптографии. Что позволило обобщить уже имеющиеся знания о методах шифрования и криптоанализе. Модификацией уже известного шифра Виженера был получен новый алгоритм. Его реализация на языке программирования высокого уровня позволила оценить вычислительную сложность и криптостойкость шифра. Сравнительный анализ показал, что новый алгоритм шифрования в отличие от шифра Виженера имеет некоторые преимущества в надежности.

Список литературы

1. Временная сложность алгоритма. Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%BC-%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%BB%D0%BE%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%D0%B0 (дата обращения 25.04.2019).

2. Криптографическая стойкость. Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%-BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%

D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%81%D1%82%D0%BE%D%B9%D0%BA%D0%BE%D1%81%D1%82%D1%8C (дата обращения 28.04.2019).

3. Латинский квадрат. Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%9B%D0%B0%D1%82%D0%B8%D0%BD%D1%81%D0%BA%D0%B8%D0%B9_%D0%BA%D0%B2%D0%B0%D0%B4%D1%80%D0%B0%D1%82 (дата обращения 12.03.2019).

4. Шифр Виженера. Википедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%92%D0%B8%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%B0 (Дата обращения 14.03.2019).