Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное

учреждение высшего образования

«Национальный исследовательский

Томский политехнический Университет»



Инженерная школа ядерных технологий

Направление 01.04.02 «Прикладная математика и информатика»

**Курсовая работа**

Шифр Плейфера

по дисциплине:

**Дискретная математика и теория графов**

|  |  |  |  |
| --- | --- | --- | --- |
| **Исполнитель:** |  | Е. В. Петрович | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| студент группы 0ВМ92 |  | Дата сдачи: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |  |
|  |  |  |  |
| **Руководитель:** |  | М. Л. Шинкеев | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| доцент, |  | Дата проверки: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| кандидат физико-математических наук |  |  |  |
|  |  |  |  |

Томск – 2020

Оглавление

[Введение 2](#_Toc31577617)

[Описание алгоритма 2](#_Toc31577618)

[Криптостойкость алгоритма 4](#_Toc31577619)

[Приложение «Шифр Плейфера» 5](#_Toc31577620)

[Заключение 8](#_Toc31577621)

[Список литературы и ресурсов 9](#_Toc31577622)

[Приложения 9](#_Toc31577623)

Введение

Шифр Плейфера – система шифрования сообщений, разработанная в 1854 году английским физиком Чарльзом Уинстоном. Названа именем лорда Лайона Плейфера, который способствовал внедрению этой системы шифрования на государственной службе. Шифр Плейфера использовался британскими вооруженными силами в англо-бурской войне и в первой мировой войне, а также австралийскими и немецкими войсками во второй мировой войне.

Шифр Плейфера достаточная простая система шифрования, не требующая специального оборудования. Шифрование производится подстановкой символов, но, в отличие от систем шифрования, в которых по определенному правилу производится подстановка одиночных символов, в шифре Плейфера производится подстановка пар символов. Таким образом правило подстановки одного и того же символа меняется в зависимости от того, какой символ находится с ним в паре. Этим затрудняется частотный анализ, определяющий символы по частоте появления в тексте. Частотный анализ все же возможен, но в нем анализируются частоты появления в тексте пар символов, количество которых равно квадрату количества символов в алфавите. Также для частотного анализа потребуется большие объемы зашифрованного текста. Система является симметричной, то есть для зашифровки и расшифровки используется один и тот же ключ.

Описание алгоритма

Перед зашифровкой сообщение должно быть предварительно подготовлено. В нем удаляются все пробелы, между двумя повторяющимися подряд символами вставляется разделяющий символ – в английском языке «x» или «q», в русском – «ъ» и заменяются символы «j» на «i» в английском языке и «ё» на «е» - в русском. Если количество символов в преобразованном сообщении нечетное, то в конце также добавляется разделяющий символ.

Например, сообщение «Hello world» будет преобразовано в «helxloworldx».

Далее при помощи ключевого слова создается ключ – матрица, состоящая из букв алфавита размером 5x5 в английском языке и 4x8 – в русском. Сначала в матрицу вписываются символы ключевого слова. Если в ключевом слове встречаются символы, входящие в него несколько раз, то повторные вхождения символов пропускаются. Оставшаяся часть матрицы заполняется буквами алфавита, не входящими в ключевое слово. Буквы «j» и «ё» пропускаются в английском и русском языках соответственно. Например, для ключевого слова «position» матрица будет выглядеть следующим образом:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| P | O | S | I | T |
| N | A | B | C | D |
| E | F | G | H | K |
| L | M | Q | R | U |
| V | W | X | Y | Z |

Рис.1

Далее преобразованное сообщение последовательно делится на пары символов – биграммы, определяется позиция каждого символа биграммы в матрице и, в зависимости от соотношения этих позиций, производится замена символов по следующим правилам.

* Если символы находятся на одной строке, то каждый символ заменяется на символ, находящийся справа от него. Если символ исходной биграммы находится в конце строки, то он заменяется на символ, находящийся в начале этой строки. Например, биграмма «he» будет заменена на биграмму «kf» (h→k, e→f ):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| P | O | S | I | T |
| N | A | B | C | D |
| E | F | G | H | K |
| L | M | Q | R | U |
| V | W | X | Y | Z |

Рис.2

* Если символы находятся в одном столбце матрицы, то каждый символ заменяется на символ, находящийся снизу от него. Если символ исходной биграммы находится внизу столбца, то он заменяется на символ, находящийся вверху этого столбца. Например, биграмма «wo» будет заменена на биграмму «oa» (w→o, o→a ):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| P | O | S | I | T |
| N | A | B | C | D |
| E | F | G | H | K |
| L | M | Q | R | U |
| V | W | X | Y | Z |

Рис.3

* Если ни столбцы, ни строки не совпадают, то каждый символ биграммы заменяется на символ, находящийся в этой же строке, но в столбце, в котором находится другой символ биграммы. Например, биграмма «lo» будет заменена на биграмму «mp» (l→m, o→p):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| P | O | S | I | T |
| N | A | B | C | D |
| E | F | G | H | K |
| L | M | Q | R | U |
| V | W | X | Y | Z |

Рис.4

Расшифровка сообщения производится путем замены символов биграмм при помощи этой же матрицы, и этих же правил, только направления замены символов в первом и во втором правиле заменяются на противоположные. Третье правило остается без изменений.

Криптостойкость алгоритма

Взлом шифра Плейфера прямым перебором всех возможных вариантов ключа не эффективен, так как количество вариантов ключа равно количеству перестановок в матрице 5x5 – 25! Оптимальным методом взлома может оказаться алгоритм имитации отжига:

* Выбирается произвольная последовательность символов в ключе, производится расшифровка текста и вычисляется коэффициент соответствия расшифрованного текста языку
* В ключе производятся небольшие изменения и снова выполняется расшифровка и расчет коэффициента
* Если коэффициент увеличился, то изменения ключа принимаются
* Если коэффициент уменьшился, то изменения ключа принимаются с вероятностью, зависящей от разницы между коэффициентами.

Таким образом, алгоритм позволяет дойти до наилучшей степени соответствия расшифрованного сообщения естественному языку, не застревая в локальных минимумах. С использованием современных компьютеров и вычислительных технологий шифр Плейфера может быть взломан в течение нескольких секунд.

Приложение «Шифр Плейфера»

Для реализации алгоритма шифрования Плейфера разработано приложение на языке С++.

Окно приложения содержит поля ввода для ключевого слова и исходного сообщения, поля для выводя зашифрованного и расшифрованного сообщений и кнопки управления (Рис.5).

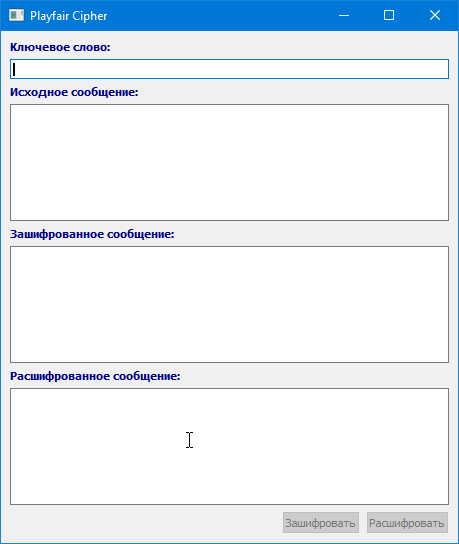


Рис.5

Для получения зашифрованного сообщения нужно ввести ключевое слово и исходное сообщение. Кнопка «Зашифровать» станет активной. Нажав на кнопку «Зашифровать», получаем зашифрованное сообщение в соответствующем окне вывода. Кнопка «Расшифровать» станет активной. Нажав на кнопку «Расшифровать», получаем расшифрованное сообщение в соответствующем окне вывода (Рис.6).

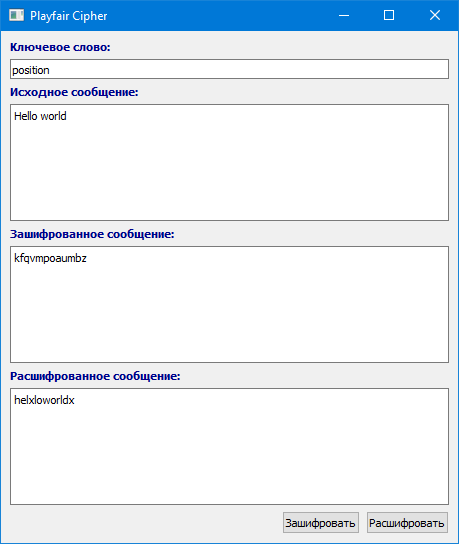


Рис.6

В приложении поддерживается также и русский язык (Рис.7).

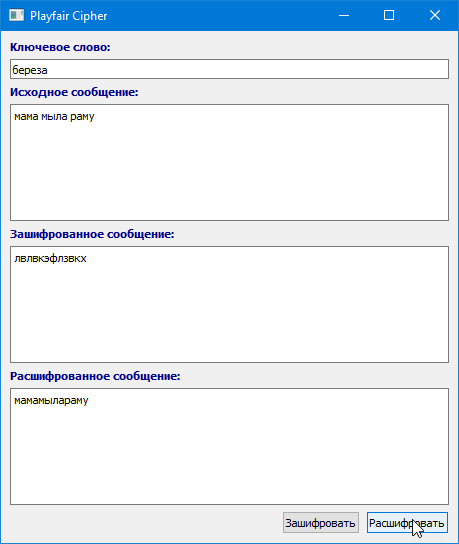


Рис.7

Заключение

В работе изучен алгоритм шифрования текстовых сообщений «Шифр Плейфера». Проведена оценка его криптостойкости и разработано приложение, реализующее этот алгоритм шифрования.

Список литературы и ресурсов

* Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009 – 576 с. ISBN 978-5-9775-0319-8.
* <https://ru.wikipedia.org/wiki/>Шифр\_Плейфера

Приложения

Исходный код приложения на языке C++:

<https://github.com/petrovicheugene/PlayfairCipher.git>