**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ**

**ВЫСШЕГО ОБРАЗОВАНИЯ**

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «МИСиС»**

***ИНСТИТУТ***ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОМПЬЮТЕРНЫХ НАУК

***КАФЕДРА*** АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ И ДИЗАЙНА

***НАПРАВЛЕНИЕ*** 09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА

***ПРОФИЛЬ*** Прикладная информатика в дизайне

**ОТЧЕТ**

**о выполнении курсовой работы**

**на тему: Разработка программы для шифрования и   
дешифрования информации методом маршрутной перестановки**

|  |  |  |
| --- | --- | --- |
| *Студент группы БПИ-20-2* |  | *Бобров М. А.* |
| *Руководитель работы* |  | *ст.преп. Фейзрахманов И.Ж.* |

|  |  |  |
| --- | --- | --- |
| *Отчет защищен с оценкой* |  |  |

Москва 2022

Аннотация

Данный отчет содержит оглавление, введение, две главы, заключение, список используемых источников и приложение.

В первой главе рассматривается теоретическая часть. Приводятся алгоритмы шифрования и шифры перестановки. Рассматривается скитала или сцитала как древний инструмент для шифрования и расшифрования перестановкой. Рассматривается маршрутная перестановка.

Во второй главе рассматривается программная реализация шифрования методом маршрутной перестановки и приводятся тесты для отладки работоспособности программы.

Отчет включает 23 (двадцать три) страницы, 14 (четырнадцать) рисунков с описанием, 1 (одно) приложение. При написании было использовано 9 (девять) источников.

Оглавление

[Введение 3](#_Toc123751436)

[Глава 1. Теоретическая часть 7](#_Toc123751437)

[1.1 Алгоритмы шифрования 7](#_Toc123751438)

[1.2 Шифры перестановки 8](#_Toc123751439)

[1.2.1 Шифры перестановки без использования ключа 8](#_Toc123751440)

[1.2.2 Шифры перестановки с использованием ключа 9](#_Toc123751441)

[1.3 Скитала или сцитала как древний инструмент перестановочного шифрования 11](#_Toc123751442)

[1.3.1 Алгоритм шифрования 12](#_Toc123751443)

[1.3.2 Алгоритм расшифрования 13](#_Toc123751444)

[1.4 Маршрутная перестановка 14](#_Toc123751445)

[Глава 2. Практическая часть 16](#_Toc123751446)

[2.1 Программная реализация метода шифрования 16](#_Toc123751447)

[2.2 Алгоритм функции шифрования и дешифрования 16](#_Toc123751448)

[2.3 Алгоритм работы всей программы 17](#_Toc123751449)

[2.4 Тестирование и отладка программы 18](#_Toc123751450)

[Заключение 20](#_Toc123751451)

[Список используемых источников 21](#_Toc123751452)

[Приложения 22](#_Toc123751453)

[Приложение А 22](#_Toc123751454)

Введение

Проблемы защиты информации волновали человечество с незапамятных времен. Необходимость в этом возникла из потребностей тайной передачи, как в военных, так и дипломатических сообщений. Создание современных компьютерных систем и появление глобальных компьютерных сетей радикально изменило характер и диапазон проблем защиты информации. Криптография начала использоваться для защиты не только государственных и военных интересов, но и интересов организаций и частных лиц. В итоге криптография превратилась из секретной науки в прикладную. Современная криптография начала бурно развиваться с 1976 г [1].

Огромное влияние на развитие криптологии имела арабская цивилизация. Именно арабы первые открыли и описали метод криптоанализа. Стремительно развивающееся исламское государство испытывало потребность в хорошо налаженной системе государственного управления. Аппарат чиновников полагался на отлаженную систему обмена сообщениями, безопасность которой обеспечивалась шифрованием. Однако вклад арабов состоит не только в широком использовании шифроалфавитов, но и в создании криптоанализа (дешифрование сообщения без знания ключа). Столь высокие достижения в криптологии можно объяснить высоким уровнем развития в области математики и лингвистики. Исламские теологи активно исследовали Хадисы на предмет частотности используемых в них слов. Главным открытием стало то, что некоторые буквы в арабском языке встречаются чаще остальных. Это открытие привело к прорыву в криптографии. Позднее арабский ученый Аль-Кинди впервые описал криптосистему на основе частотного анализа в труде «Рукопись по дешифрованию криптографических сообщений» [2].

Криптография активно развивалась в средние века и часто использовалась дипломатами и торговцами для шифрования сообщений. Одна из самых известных шифра средневековья называется Copiale - рукопись, элегантно украшенная водяными знаками, которые еще не были расшифрованы. В эпоху Возрождения Фрэнсис Бэкон описал 7 методов для скрытого текста, а также предложил метод двоичного шифрования [3].

В XIV веке увидела свет книга Чикко Симонети с описанием принципа лозунгового шифра. В XV веке вышла работа Габриэля де Лавинда «Трактат о шифрах», в которой характеризуется шифр пропорциональной замены, обеспечивающий замену букв несколькими символами, пропорционально частотности букв в исходном тексте. В Милане получает распространение миланский ключ [2].

В 1466 г. появляется «Трактат о шифрах» Леона Альберти. В нем рассматривается полуалфавитный шифр собственного изобретения, реализованный в виде шифровального диска, где для шифровки использовалось два отдельных алфавита. Альберти впервые основывал свои изыскания на принципе комбинаторики [2].

В 1518 году в Германии произошел прорыв в развитии криптографии – опубликована книга «Полиграфия» под авторством аббата Иоганнеса Тритемия, включающая несколько способов шифрования, один из которых становится основой для развития идеи полуалфавитной замены [2].

Мысли Тритемия развил Джовани Белазо. Он выпустил в 1533 году книгу «Шифр сеньора Белазо», в которой для шифрования предлагался к использованию пароль – слово или группа слов, записываемых над открытым текстом, а каждый символ пароля означал номер заменяемой буквы. Данный способ впоследствии получил название «шифр Виженера» по имени своего создателя. Блейс де Вижинер был послом, в XVI веке написал книгу «Трактат о шифрах», в которой предложил использовать для шифрования 26 алфавитов, а порядок использования шифра определялся знанием пароля. Схожий принцип был в дальнейшем применен Томасом Джефферсоном [2].

Первая мировой война способствовала дальнейшему внедрению шифрования. Так, потребности военной и оборонной сфер стали главными импульсами дальнейшего развития криптографических и криптоаналитических средств [2].

С 20-х годов ХХ века стала активно использоваться «Энигма» – шифровальная машина роторного типа, разработанная Эдвардом Хеберном и впоследствии усовершенствованная Артуром Кирхом. Наибольшее распространение получила в Германии во время Второй мировой войны. Алан Тьюринг внес большой вклад в дешифровку перехваченных сообщений и в создание электронно-механической машины Bombe [2].

Работа Клода Шеннона «Теория связи в секретных системах», выпущенная в 1949 г., является еще одной переходной точкой, когда утвердились новые теоретические принципы криптографической защиты информации. Криптография провозглашается математической наукой. К концу 1960-х появляются первые – более совершенные – блочные шифры, которые сменяли роторные системы [2].

В 80-90-е гг. прошлого века появляются новые виды шифрования: вероятностное шифрование, квантовая криптография и т. д. Развитие квантовой физики проявляет потенциальные горизонты развития криптографии. Расширяются области применения криптографии [2].

На данный момент шифрование используется везде, где ведется работа с персональными данными. Зашифрованный обмен информацией между государственными и муниципальными образованиями, а также простыми гражданами используется для того, чтобы скрыть личную информацию одной стороны от злоумышленников. Например, для передачи информации по электронным больничным листам в Фонд социального страхования используется специальное программное обеспечение по шифрованию, которое разрабатывалось самим фондом. Российский рынок позволяет пользоваться различными специализированными программными продуктами, например, ViPNet компании ИнфоТеКС [4].

**Актуальность данной работы** обусловлена необходимостью шифрования конфиденциальной информации в частном и государственном секторе для последующего хранения, передачи и защиты от кражи третьими лицами.

**Объектом исследования** является информатика.

**Предметом исследования является** шифрование информации.

**Целью** работы является разработка программы для шифрования и

дешифрования информации методом маршрутной перестановки.

Для успешного выполнения поставленной цели необходимо выполнить следующие **задачи**:

    а) анализ теории и практики в шифровании информации;

    б) анализ существующих методов шифрования;

    в) обоснование выбора метода шифрования;

    г) обоснование выбора языка программирования для реализации программы;

    д) создание программы шифрования и дешифрования информации методом маршрутной перестановки.

Глава 1. Теоретическая часть

1.1 Алгоритмы шифрования

В основном данные шифруются с помощью алгоритма и ключа шифрования. При помощи алгоритма шифрования данные становятся зашифрованными, и расшифровывают с помощью ключа шифрования [5].

Есть несколько видов алгоритмов шифрования, подразделяют их в основном как:

а) симметричные алгоритмы;

б) ассиметричные алгоритмы.

Симметричный ключ шифрования использует тот же ключ, для шифрования или дешифрования файла. Симметричный алгоритм шифрования гораздо быстрее, но при этом отправитель должен делиться обмениваться своим ключом, используемый шифрования данных с получателем, для расшифровки. Но также это означает, чтобы надежно распределять и управлять большим количеством ключей, используют симметричный алгоритм шифровки данных, при этом используют ассиметричный метод шифрования для обмена секретными ключами [5].

Ассиметричный метод шифрования известен как шифрование с открытым ключом, использует два разных, но математически связанных ключей, один общественный, другой частный. Общественный ключ может быть общим со всеми, а в то время частный хранится в секрете. RSA самый наиболее известный используемый ассиметричный метод [5].

1.2 Шифры перестановки

Шифр перестановки не заменяет один символ другим, вместо этого он изменяет местоположение символов в зашифрованном тексте. Символ в первой позиции исходного текста может появиться в десятой позиции зашифрованного текста. Символ, который находится в восьмой позиции исходного текста, может появиться в первой позиции зашифрованного текста. Другими словами, шифр перестановки ставит в другом порядке (перемещает) символы [6].

1.2.1 Шифры перестановки без использования ключа

Простые шифры перестановки, которые применялись в прошлом, не использовали ключ. Есть два метода для перестановки символов. В первом методе текст записывается в таблице столбец за столбцом и затем передаётся строка за строкой. Во втором методе текст записан в таблицы строка за строкой и затем передаётся столбец за столбцом [6].

Хороший пример шифра без использования ключа ‒ шифр изгороди (rail fence cipher). В этом шифре исходный текст размещен на двух линиях как зигзагообразный шаблон (что может рассматриваться как столбец за столбцом таблицы, которая имеет две строки); зашифрованный текст составляется при чтении шаблона строка за строкой. Например, чтобы передать сообщение Meet me at the park (Встречай меня в парке), отправитель пишет получателю текст приведенный на рисунке 1 [6].

Изображение выглядит как часы

Автоматически созданное описание

Рисунок 1 – Пример шифрования сообщения Meet me at the central park с помощью шифра изгороди

Отправитель создает зашифрованный текст MEMATEAKETETHPR, посылая первую строку, сопровождаемую второй строкой. Получатель получает зашифрованный текст и разделяет его пополам (в этом случае вторая половина имеет на один символ меньше). Первая половина формы ‒ первая строка; вторая половина ‒ вторая строка. Получатель читает результат по зигзагу. Поскольку нет никакого ключа, и номер строк установлен, криптографический анализ зашифрованного текста был бы очень прост для злоумышленника. Все, что он должен знать, ‒ это то, что используется шифр изгороди [6].

1.2.2 Шифры перестановки с использованием ключа

Бесключевые шифры перестановки переставляют символы, используя запись исходного текста одним способом (например, строка за строкой) и передачу этого текста в другом порядке (например, столбец за столбцом). Перестановка делается во всём исходном тексте, чтобы создать весь зашифрованный текст. Другой метод состоит в том, чтобы разделить исходный текст на группы заранее определенного размера, называемые блоками, а затем использовать ключ, чтобы переставить символы в каждом блоке отдельно [6].

Как пример шифра перестановки с ключом, представим, что отправитель должен передать получателю сообщение Enemy attacks tonight (Враг атакует ночью). Отправитель и получатель согласились разделить текст на группы по пять символов и затем переставить символы в каждой группе. Ниже показана группировка после добавления фиктивного символа в конце, чтобы сделать последнюю группу одинаковой по размеру с другими: Enemy attacks tonightz. Ключ, используемый для зашифрования и расшифрования - ключ перестановки, который показывает, как переставлять символы. Для этого сообщения примем, что отправитель и получатель использовали следующий ключ, представленный на рисунке 2 [6].

Изображение выглядит как стол

Автоматически созданное описание

Рисунок 2 – Ключ перестановки

Третий символ в блоке исходного текста становится первым символом в блоке зашифрованного текста, первый символ в блоке исходного текста становится вторым символом в блоке зашифрованного текста и так далее. Результаты перестановки: EEMYN TAACT TKONS HITZG [6].

Отправитель передает зашифрованный текст EEMYN TAACT TKONS HITZG получателю. получатель делит зашифрованный текст на группы по 5 символов и, используя ключ в обратном порядке, находит исходный текст [6].

1.3 Скитала или сцитала как древний инструмент перестановочного шифрования

Скитала или сцитала – инструмент, используемый для осуществления перестановочного шифрования. В криптографии известен как шифр Древней Спарты. Представляет собой цилиндр и узкую полоску пергамента, на которой писалось сообщение, обматывавшуюся вокруг него по спирали. Античные греки и спартанцы, предположительно, использовали этот шифр для обмена сообщениями во время военных кампаний [7].

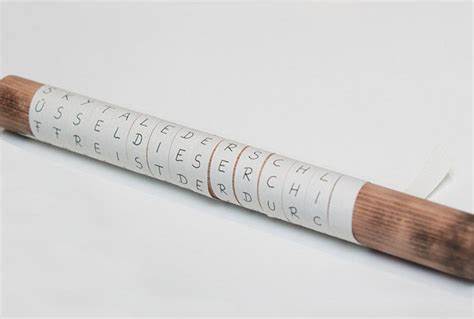


Рисунок 3 – Пример скиталы

Для шифрования сообщения использовались пергаментная лента и палочка цилиндрической формы с фиксированными длиной и диаметром. Пергаментная лента наматывалась на палочку так, чтобы не было ни просветов, ни нахлёстов. Написание сообщения производилось по намотанной пергаментной ленте по длинной стороне цилиндра. После того, как достигался конец намотанной ленты, палочка поворачивалась на часть оборота и написание сообщения продолжалось. После разматывания ленты на ней оказывалось зашифрованное сообщение. Расшифрование выполнялась с использованием палочки таких же типоразмеров. Сам процесс шифрования заключался в перестановке символов исходного текста в соответствии с длиной окружности палочки [7].

Например, используется палочка, по длине окружности которой помещается 4 символа (число строк в таблице), а длина самой палочки позволяет записать 5 символов (число столбцов в таблице), исходный текст: «это шифр древней Спарты». Схематически это можно изобразить так, как изображено на рисунке 4 [7].

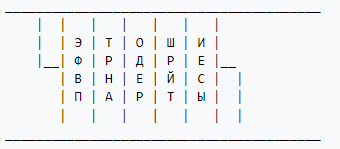


Рисунок 4 – Схематическое изображения примера

После разматывания ленты шифротекст будет следующим «ЭФВПТРНАОДЕРШРЙТИЕСЫ». Как видно из примера, получается таблица, у которой есть два параметра: n — количество столбцов, m — количество строк. Поскольку при регулярном обмене данными сообщения часто имеют разную длину, то оба этих параметра за неизменяющийся ключ взять неудобно. Поэтому обычно в качестве известного каждой стороне ключа выбирается один из них (часто это m), а второй вычисляется на основе известного и длины сообщения: n = [(k - 1) / m] +1, где [x] — целая часть числа x, а k — длина сообщения [7].

1.3.1 Алгоритм шифрования

Более подробно, алгоритм шифрования в данных обозначениях выглядит следующим образом:

    1) первые n символов выписываются в первую строку слева направо (в примере выше: «ЭТОШИ»);

    2) следующие n символов выписываем во вторую строчку пока её не заполним и т.д.;

    3) если все символы выписаны, а остались незаполненные ячейки, заполняем их пробелами или любыми другими символами по договоренности. Например, для сообщения «НАС АТАКУЮТ» мы получаем таблицу как на рисунке 5, где n=4, m=3 и звезда стоит на месте недостающего символа;

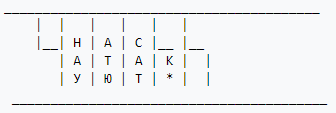


Рисунок 5 – Таблица примера для сообщения «НАС АТАКУЮТ»

    4) если выписаны не все символы, а таблица заполнена, значит, при выборе размеров допущена ошибка;

    5) теперь разворачиваем текст по столбцам - «НАУАТЮСАТ\_К» [7].

1.3.2 Алгоритм расшифрования

Для расшифрования сообщения адресат использовал палочку, аналогичную по размерам палочки отправителя, на которую он наматывал пергамент [7].

Преимущество данного шифра в простоте и отсутствии ошибок. Однако, он может быть легко дешифрован. Способ дешифрования алгоритма, например, был предложен Эдгаром Алланом По в работе «A Few Words on Secret Writing». Суть метода в том, что, не зная точного диаметра палочки, можно использовать конус, имеющий переменный диаметр и перемещать пергамент с сообщением по его длине до тех пор, пока текст не начнёт читаться — таким образом дешифруется ключ — диаметр скиталы [7].

Пусть имеется зашифрованный текст: «РНОАЫЙКЕСЕ\_КТВА». Применялся шифр скитала с количеством строк: 3, столбцов: 5. То есть m=3, n=5. При шифровании считывание велось по столбцам, а в каждом столбце было по 3 символа [7].

    1) Разобьём наш зашифрованный текст по m букв, учитывая пробелы («РНО АЫЙ КЕС Е\_К ТВА»).

    2) Сначала восстановим первый столбец, для этого первую группу букв запишем в первый столбец сверху вниз. Пример на рисунке 6.

    3) По следующим m символам восстановим второй столбец. Пример на рисунке 7.

    4) После восстановления всех столбцов можно будет прочитать текст — «РАКЕТНЫЕ ВОЙСКА». Пример на рисунке 8 [7].



Рисунок 6 – Пример этапа 2



Рисунок 7 – Пример этапа 3

Изображение выглядит как текст, антенна

Автоматически созданное описание

Рисунок 8 – Пример этапа 4

1.4 Маршрутная перестановка

Широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру. Преобразования из этого шифра состоят в том, что в фигуру исходный текст вписывается по ходу одного «маршрута», а затем по ходу другого выписывается с нее. Такой шифр называют маршрутной перестановкой. Например, можно вписывать исходное сообщение в прямоугольную таблицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево. Выписывать же сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх [8].

Зашифруем, например, указанным способом фразу ПРИМЕРМАРШРУТНОЙПЕРЕСТАНОВКИ используя прямоугольник размера четыре на семь, пример на рисунке 9 [8].

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 9 – Прямоугольник с шифром

Зашифрованная фраза выглядит так: МАСТАЕРРЕШРНОЕРМИУПВКЙТРПНОИ [8].

Теоретически маршруты могут быть значительно более изощренными, однако запутанность маршрутов усложняет использование таких шифров. В данном примере видно, что шифр состоит из двух перестановок:

    а) выбор маршрута, как вписывать сообщение в таблицу;

    б) выбор маршрута, записи шифр текста [8].

Так как можно произвольно вписывать буквы сообщения в таблицу, то мы получим маршрутов P(28) = 28! в первой перестановке. Во второй тоже 28!. И в итоге получаем 28! \* 28! = (28!)2 вариантов шифрования одного сообщения. Но какое бы ни было число вариантов, шифр можно взломать [8].

Глава 2. Практическая часть

2.1 Программная реализация метода шифрования

В данной работе реализовано шифрование методом табличной маршрутной перестановки. Программа реализована на языке программирования Python 3.10.8. Средой разработки, использованной для разработки программного кода, была выбрана Visual Studio Code. Полный код программы приведен в приложении А.

Python – [высокоуровневый язык программирования](https://ru.wikipedia.org/wiki/%D0%92%D1%8B%D1%81%D0%BE%D0%BA%D0%BE%D1%83%D1%80%D0%BE%D0%B2%D0%BD%D0%B5%D0%B2%D1%8B%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F) общего назначения с [динамической](https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D0%BD%D0%B0%D0%BC%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%82%D0%B8%D0%BF%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) [строгой](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D0%BE%D0%B3%D0%B0%D1%8F_%D1%82%D0%B8%D0%BF%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) типизацией и автоматическим управлением памятью, ориентированный на повышение производительности разработчика, читаемости [кода](https://ru.wikipedia.org/wiki/%D0%98%D1%81%D1%85%D0%BE%D0%B4%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%B4) и его качества, а также на обеспечение переносимости написанных на нём программ. Язык является полностью [объектно-ориентированным](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%8A%D0%B5%D0%BA%D1%82%D0%BD%D0%BE-%D0%BE%D1%80%D0%B8%D0%B5%D0%BD%D1%82%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F) в том плане, что всё является [объектами](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%8A%D0%B5%D0%BA%D1%82_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)) [9].

Для взаимодействия с пользователем используется консольный ввод и вывод. Пример взаимодействия представлен на рисунке 10.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 10 – Пример взаимодействия

2.2 Алгоритм функции шифрования и дешифрования

Программа использует созданную для реализации программы функцию «script», принимающую в себя строковую переменную и выводящую строковую переменную как результат. Она шифрует и расшифрует сообщение, переданное пользователем. Функция вызывается в программе два раза. Первый раз для шифровки и второй раз для расшифровки. Внутри функции создается матрица, в которую переносятся символы сообщения. Длина определяется взятием длины изначальной строки под корень. При этом происходит проверка, где квадрат корня сравнивается с длиной строки. Если квадрат корня меньше длины строки, то значение корня увеличивается на 1. Символы перебираются таким образом, что при шифровке под конец создания матрицы текст в ней можно читать по столбцам сверху вниз слева направо, а при дешифровке матрица, которую можно читать по столбцам сверху вниз слева направо, после обработки можно читать построчно слева направо сверху вниз. Далее содержание матрицы построчно выводится в строчную переменную, которая выводит результат из функции. Блок схема работы функции представлена на рисунке 11.

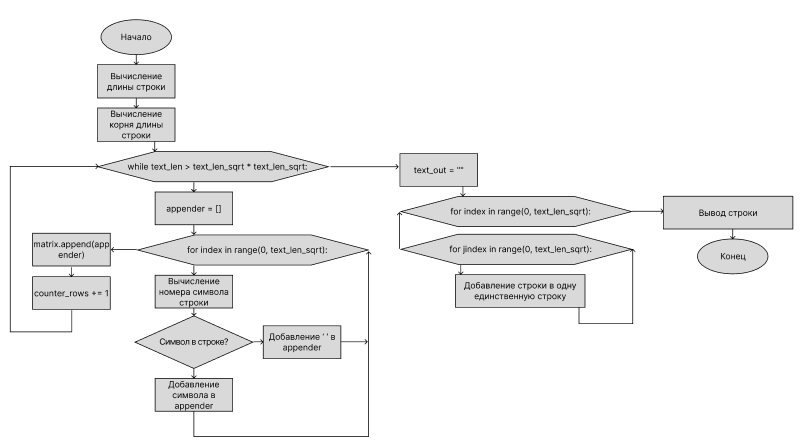


Рисунок 11 – Блок схема функции «script»

2.3 Алгоритм работы всей программы

В начале программы импортируется библиотека math, используемая для функции «script» для возможности использования возведения в корень. Затем задается определение функции «script». Дальше идет главная часть, в которой программа ожидает ввод от пользователя, сохраняет ввод в переменной, дальше отправляется как вводные данные в функцию «script», результат которой записывается в отдельную переменную для зашифрованного результата и выводится пользователю в консоль. Далее зашифрованная строка отправляется как вводные данные в функцию «script», результат которой сохраняется в переменной для расшифрованной строки и впоследствии выводится пользователю в консоль. Блок схему всей программы можно увидеть на рисунке 12.

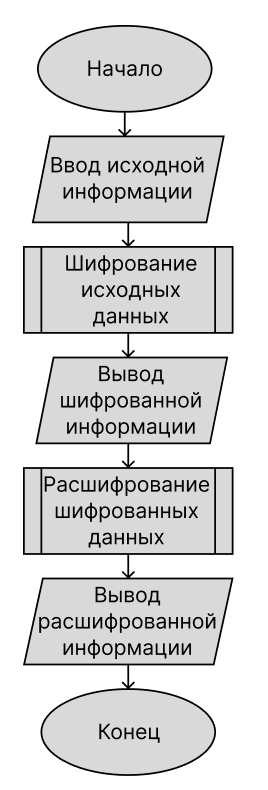


Рисунок 12 – Блок схема алгоритма всей программы

2.4 Тестирование и отладка программы

Для тестирования программы взято два сообщения: сообщение «Пример работы программы» и отрывок из стихотворения В. В. Маяковского “Ночь”: «Багровый и белый отброшен и скомкан, в зеленый бросали горстями дукаты, а черным ладоням сбежавшихся окон раздали горящие желтые карты.». Результаты представлены на рисунках 13 и 14. По ним видно, что программа правильно шифрует и дешифрует сообщения.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 13 – Работа программы с сообщением «Пример работы программы»

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 14 – Работа программы с сообщением в виде отрывка из стиха В. В. Маяковского «Ночь»

Заключение

В ходе выполнения данной работы была изучена теория относительно краткой истории криптографии, теория перестановки, маршрутной перестановки. По результатам изучения теоретической части были разработаны алгоритм и программа для выполнения шифрования и дешифрования по методу маршрутной перестановки с реализацией на языке программирования Python.

В ходе выполнения курсовой работы были выполнены все поставленные задачи и достигнута основная цель данной работы.

Список используемых источников

1. Антонов Ю. С., Занимательная криптография, текст научной статьи из журнала «Наука и техника в Якутии» №2(9) – 2005, стр. 112.

2. Фикс А. С., История криптографии и новый этический статус информации, текст научной статьи из журнала «Философские проблемы информационных технологий и киберпространства» №2(8) – 2014, стр. 65–76. eISSN: 2305–3763.

3. Дьяченко Н. В., Отакулов А. С., Шатомиров И. С., Виды криптографического шифрования, текст научной статьи из журнала «MODERN SCIENCE» №5(3) – 2019, стр. 232–235. ISSN: 2414–9918.

4. Иванов А. А., Криптография в современном мире, текст научной статьи из сборника трудов конференции «Сборник материалов Х всероссийской, научно-практической конференции молодых ученых с международным участием “Россия Молодая”» - 2018, стр. 31530.1–31530.3. УДК: 003.26.09.

5. Alan Konheim, Computer Security and Cryptography, текст из учебного материала – 2007, стр. 45.

6. Ахмедов Б. А., Корченко А. Г., Сиденко В. П., Дрейс Ю. А., Сейлова Н. А., Прикладная криптология: методы шифрования, текст из учебного материала – 2015, стр. 91–94. УДК 004.056.55 (075.8).

7. Википедия - свободная энциклопедия, Скитала, электронный ресурс. Дата обращения – 29.12.2022. URL: https://ru.wikipedia.org/wiki/%D0%A1%D0%BA%D0%B8%D1%82%D0%B0%D0%BB%D0%B0.

8. Ященко В. В., Введение в киптографию, текст из учебного материала – 2012, стр. 189-197. ISBN 978-5-4439-0026-1.

9. Википедия - свободная энциклопедия, Python, электронный ресурс. Дата обращения – 29.12.2022. URL: https://ru.wikipedia.org/wiki/Python.

Приложения

Приложение А

Листинг А.1 – программа шифрования и дешифрования сообщения

import math

def script(text):

text\_len = len(text)

text\_len\_sqrt = int(math.sqrt(text\_len))

while text\_len > text\_len\_sqrt \* text\_len\_sqrt:

text\_len\_sqrt+=1

matrix = []

counter\_rows = 0

while counter\_rows < text\_len\_sqrt:

appender = []

for index in range(0, text\_len\_sqrt):

number = text\_len\_sqrt \* index + counter\_rows

if number < text\_len:

appender.append(text[number])

else:

appender.append(' ')

matrix.append(appender)

counter\_rows += 1

text\_out = ""

for index in range(0, text\_len\_sqrt):

for jindex in range(0, text\_len\_sqrt):

text\_out+=str(matrix[index][jindex])

return text\_out

#Шифровка

user\_text = input("\n Введите текст: ")

output\_s = script(user\_text)

print("\n Зашифрованная строка: ", output\_s)

#Расшифровка

output\_r = script(output\_s)

print("\n Расшифрованная строка: ", output\_r)