МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования

«БЕЛОРУССКИЙ

ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных технологий

Кафедра Информационных систем и технологий

Направление специальности Информационные системы и технологии .

**ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3**

**ПО ДИСЦИПЛИНЕ**

**«ЗАЩИТА ИНФОРМАЦИИ**

**И НАДЕЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»**

Выполнил: студент 3 курса 1 группы

Кашперко Василиса Сергеевна

Проверил: ассистент

Нистюк Ольга Александровна

Минск 2023

**Исследование криптографических шифров на основе перестановки символов**

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров.

**Теоретическая часть:**

Среди шифров рассматриваемого подкласса иногда выделяют шифры простой перестановки (или перестановки без ключа). Символы открытого текста Мi перемешиваются по каким-либо правилам. Формально каждое из таких правил может рассматриваться в качестве ключа.

Для использования шифров **одинарной перестановки** используется таблица, состоящая из двух строк: в первой строке записываются буквы, во второй – цифры J. Строки состоят из n столбцов. Буквы составляют шифруемое сообщение. Цифры J = j1, j2, …, jn, где j1 – номер позиции в зашифрованном сообщении первого символа открытого текста, где j2 – номер позиции в зашифрованном сообщении второго символа открытого текста и т. д. Таким образом, порядок следования цифр определяется используемым правилом (ключом) перестановки символов открытого текста для получения шифрограммы.

Шифры **простой блочной перестановки**. Блок должен состоять из 2-х или более символов. Если общее число таких символов в сообщении не кратно длине сообщения, то последний блок можно дополнить произвольными знаками.

Шифры **маршрутной перестановки**. Основой рассматриваемого типа является геометрическая фигура. Обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту записывается открытый текст.

Шифр **Скитала** (Сцитала). Известно, что в V веке до н. э. в Спарте существовала хорошо отработанная система секретной военной связи. Для этого использовался специальный жезл «скитала» (греч. σκυτάλη – первое, вероятно, простейшее криптографическое устройство, реализующее метод перестановки

**Организация маршрутной перестановки**. Уже упоминавшаяся маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали, зигзагом, змейкой или каким-то другим способом.

Шифр **вертикальной перестановки.** Данный шифр является разновидностью шифра маршрутной перестановки. К особенностям вертикального шифра можно отнести следующие:

- количество столбцов в таблице фиксируется и определяется длиной ключа;

- маршрут вписывания: слева-направо, сверху-вниз;

- шифрограмма выписывается по столбцам в соответствии с их нумерацией (ключом).

Шифры **множественной перестановки.** Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиваем не только столбцов (как в примере 4), но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного из них равна числу столбцов, другого – числу строк. К ключевой информацию мы можем относить также способы вписывания сообщения и считывания отдельных символов из текущего столбца матрицы.

**Практическая часть:**

В данной лабораторной работе необходимо разработать авторское приложение для шифрования с использованием английского алфавита:

• Маршрутная перестановка (маршрут: зигзагом);

• Множественная перестановка, ключевые слова – собственные имя и фамилия.

**Множественная перестановка**

Особенностью шифров данного подкласса является минимум двукратная перестановка символов шифруемого сообщения. В простейшем случае это может задаваться перемешиванием не только столбцов, но и строк. Таким образом, этот случай соответствует использованию двух основных ключей: длина одного из них равна числу столбцов, другого – числу строк.

Для реализации множественной перестановки необходимо сформировать таблицу (ключи имя и фамилия – «vasilisa» и «kashperko»). Далее записываем последовательно шифруемое сообщение в каждую ячейку слева направо: «Honesty is the best policy that you can try to practice in your life.» (Табл. 1).

Таблица 1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **v** | **a** | **s** | **i** | **l** | **i** | **s** | **a** |
| **k** | H | o | n | e | s | t | y |  |
| **a** | i | s |  | t | h | e |  | b |
| **s** | e | s | t |  | p | o | l | i |
| **h** | c | y |  | t | h | a | t |  |
| **p** | y | o | u |  | c | a | n |  |
| **e** |  | t | r | y |  | t | o |  |
| **r** | p | r | a | c | t | i | c | e |
| **k** |  | i | n |  | y | o | u | r |
| **o** |  | l | i | f | e | . |  |  |

Затем сортируем по ключу в алфавитном порядке строки (один из ключей) (Табл. 2).

Таблица 2

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **v** | **a** | **s** | **i** | **l** | **i** | **s** | **a** |
| **a** | i | s |  | t | h | e |  | b |
| **e** |  | t | r | y |  | t | o |  |
| **h** | c | y |  | t | h | a | t |  |
| **k** | H | o | n | e | s | t | y |  |
| **k** |  | i | n |  | y | o | u | r |
| **o** |  | l | i | f | e | . |  |  |
| **p** | y | o | u |  | c | a | n |  |
| **r** | p | r | a | c | t | i | c | e |
| **s** | e | s | t |  | p | o | l | i |

Затем сортируем столбцы в алфавитном порядке по второму ключу (Табл. 3).

Таблица 3

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **a** | **a** | **i** | **i** | **l** | **s** | **s** | **v** |
| **a** | s | b | t | e | h |  |  | i |
| **e** | t |  | y | t |  | r | o |  |
| **h** | y |  | t | a | h |  | t | c |
| **k** | o |  | e | t | s | n | y | H |
| **k** | i | r |  | o | y | n | u |  |
| **o** | l |  | f | . | e | i |  |  |
| **p** | o |  |  | a | c | u | n | y |
| **r** | r | e | c | i | t | a | c | p |
| **s** | s | i |  | o | p | t | l | e |

Получим зашифрованное сообщения, считывая символы по порядку по столбцам сверху вниз. На выходе получим такое сообщение: «styoilorsb r eityte f c etato.aioh hsyectp r nniuat otyu ncli cH ype».

Посмотрим, как работает шифрование и дешифрование в приложении. Результат работы программы изображен на рисунке 1.

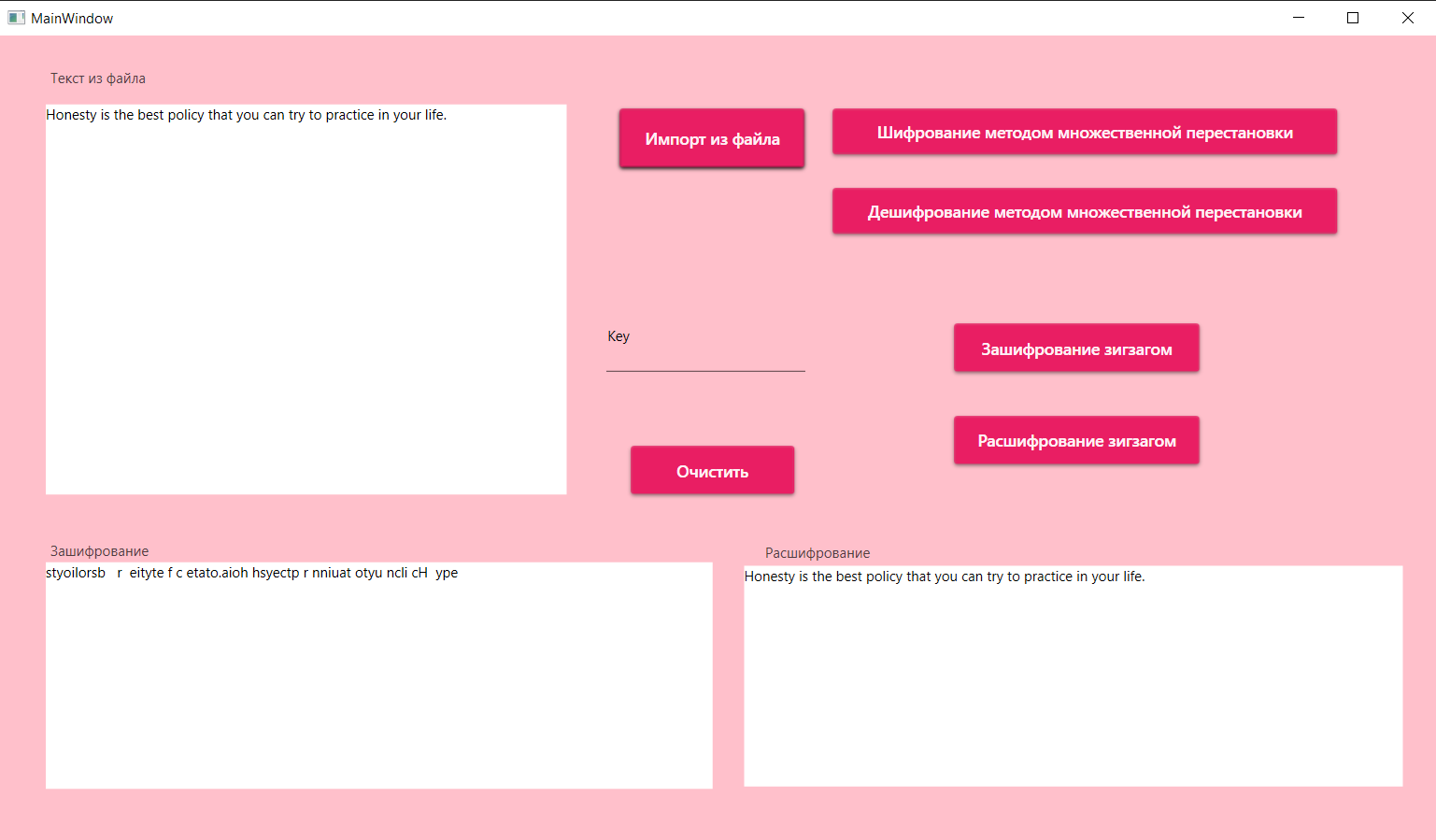


Рисунок 1 – Результат работы шифрования методом множественной перестановки

**Маршрутная перестановка (маршрут: зигзагом)**

Маршрутная перестановка (записываем сообщение по строкам, считываем – по столбцам матрицы) можно усложнить и считывать не по столбцам, а по спирали, зигзагом, змейкой или каким-то другим способом. Такие способы шифрования несколько усложняют процесс, однако усиливают криптостойкость шифра.

В соответствии с вариантом по условию лабораторной маршрутная перестановка осуществляется зигзагом. Графическое представление метода маршрутной перестановки зигзагом приведено на рисунке 2.

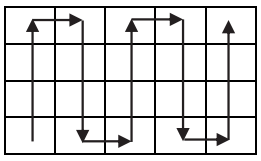


Рисунок 2 – Графическое представление метода маршрутной перестановки зигзагом

Наглядно изобразим алгоритм шифрования в виде таблицы (Табл. 4).

Таблица 4

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| H | o | n | e | s | t | y |  |
| i | s |  | t | h | e |  | b |
| e | s | t |  | p | o | l | i |
| c | y |  | t | h | a | t |  |
| y | o | u |  | c | a | n |  |
|  | t | r | y |  | t | o |  |
| p | r | a | c | t | i | c | e |
|  | i | n |  | y | o | u | r |
|  | l | i | f | e | . |  |  |

В итоге должно получится такое зашифрованное сообщение: « p y ceiHossyotrilinaru t net t yc fshphc tyeteoaatio.y ltnocu bi er ».

Посмотрим, как работает шифрование и дешифрование в приложении. Результат работы программы изображен на рисунке 3.

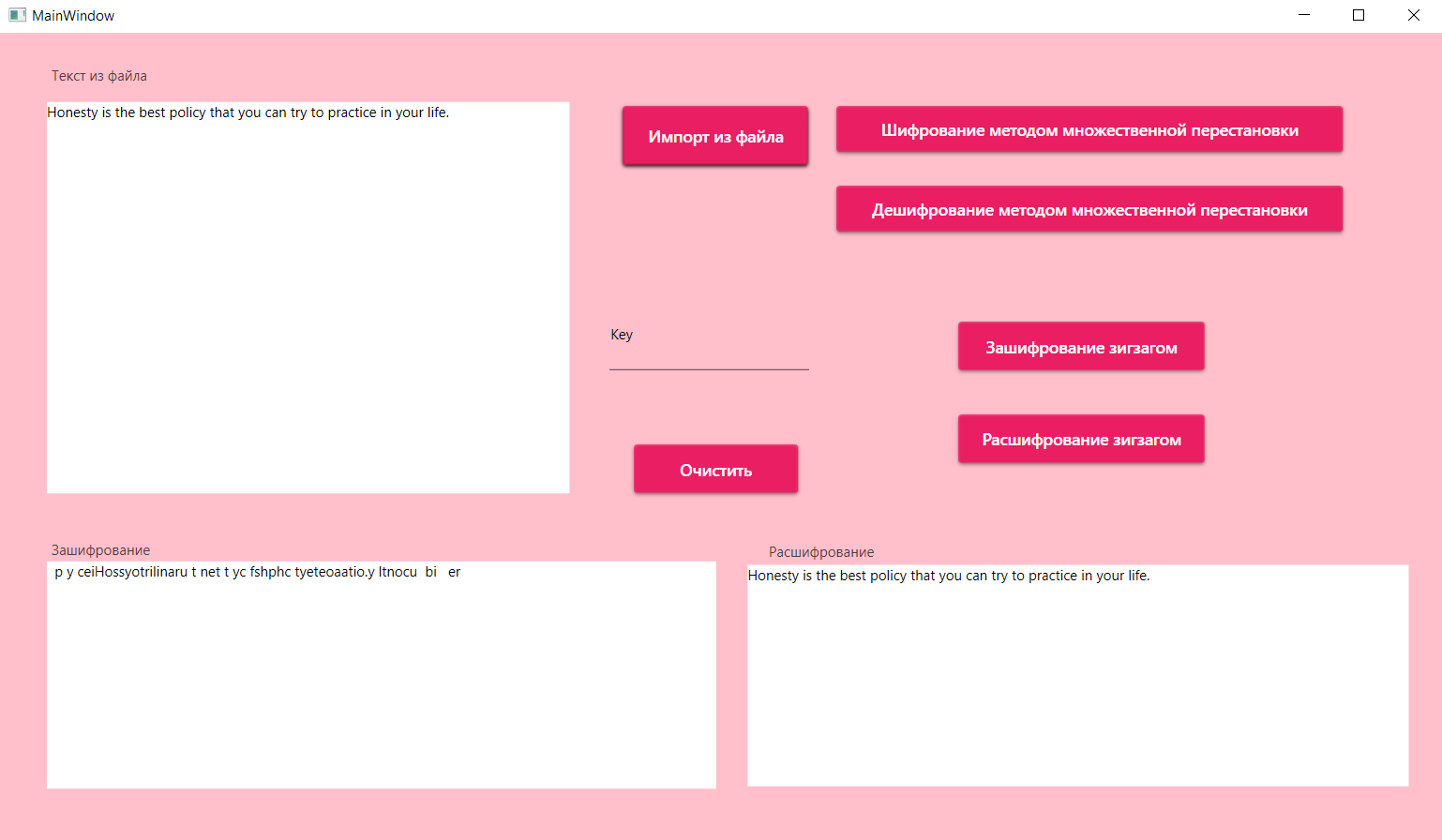


Рисунок 3 – Результат работы шифрования методом маршрутной перестановки зигзагом

Результаты времени выполнения операций зашифрования и расшифрования приведены на рисунках 4, 5, 6 и 7.

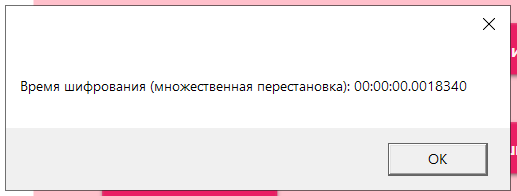


Рисунок 4 – Результат времени зашифрования множественной перестановкой

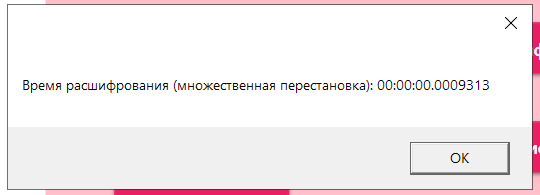


Рисунок 5 – Результат времени расшифрования множественной перестановкой

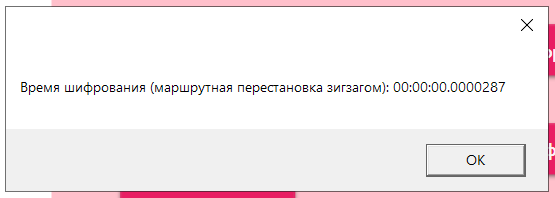


Рисунок 6 – Результат времени зашифрования маршрутной перестановкой зигзагом

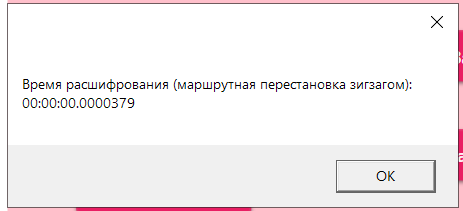


Рисунок 7 – Результат времени расшифрования маршрутной перестановкой зигзагом

Гистограммы частот появления символов для исходного и зашифрованного сообщений методом маршрутной перестановки зигзагом совпадают, и приведены на рисунке 8. А также были сравнены диаграммы алфавитов до и после шифрования. По результату анализа видно: символы лишь перемешиваются, меняются местами между собой, но не заменяются, поэтому встречаемость символов в обоих алфавитах остается одинаковой.



Рисунок 8 – Гистограмма частот появления для исходного и зашифрованного алфавитов

**Вывод:** в данной лабораторной работе я закрепила теоретические знания по перестановочным шифрам. Также было разработано приложение для работы с множественной и маршрутной перестановками. Была проведен анализ времени шифрования и расшифрования, в результате которого было выяснено, что шифрование методом множественной перестановки занимает больше времени из-за сортировок строк и столбцов (ключей) по алфавиту. Были изучены гистограммы алфавитов до и после шифрования.

**Контрольные вопросы**

*1. В чем заключается основная идея криптографических преобразований на основе шифров перестановки?*

Сущность перестановочного шифрования состоит в том, что исходный текст зашифрованный текст основаны на использовании одного и того же или разных алфавитов, а тайной или ключевой информацией является алгоритм перестановки

*2. Привести классификационные признаки и дать сравнительную характеристику разновидностям перестановочных шифров.*

Простой перестановки/Простой блочной перестановки: при больших значениях n приходится работать с таблицами, состоящими из большого числа столбцов; для сообщений разной длинны необходимо создавать разные таблицы перестановок – не очень удобен.

Маршрутной перестановки: геометрическая фигура, обычно прямоугольник или прямоугольная матрица. В ячейки этой фигуры по определенному маршруту (слева направо, сверху вниз или каким-либо иным образом) записывается открытый текст. Для получения шифрограммы нужно записать символы этого сообщения в иной последовательности, т. е. по иному маршруту.

Множественная перестановка: минимум двукратная перестановка символов шифруемого сообщения (перемещения не только столбцов, но и строк); использует 2 основных ключа (для строк и столбцов), а также к ключевой информацию мы можем относить также способы вписывания сообщения и считывания отдельных символов из текущего столбца матрицы.

*3. Сколько разновидностей шифров, подобных шифру Цезаря, можно составить для алфавитов русского и белорусского языков?*

Существует 4 разновидности шифра Цезаря, но так как мы можем комбинировать несколько шифров, необходимо найти сумму сочетаний, умноженную на 2, так как 2 алфавита:

N=(i=14Ci4)\*2 =4+6+4+1\*2=30

*4. Охарактеризовать криптостойкость перестановочных и подстановочных шифров.*

Простой подстановочный шифр (моноалфавитный шифр) – это шифр, заменяющий каждый символ открытого текста соответствующим символом шифр-текста. Такие шифры взламываются без труда, поскольку не скрывают частоту использования различных символов в открытом тексте. Омофонический подстановочный шифр подобен простому подстановочному, но одному символу открытого текста может быть сопоставлен один из нескольких символов шифр-текста. Сложнее для вскрытия чем простые подст-ые, но не скрывают всех статистич. Свойств открытого текста. Без труда взламываются путем вскрытия с известным открытым текстом. Полиграмный (n-граммный) подстановочный шифр – шифрует блоки символов по группам. Подобный шифр использовался британцами во время Первой мировой войны. Перестановочный шифр с множественной перестановкой является наиболее криптостойким, в связи с тем, что используется 2 ключа-слова.

*5. Привести примеры и дать характеристику перестановочным шифрам, не рассмотренным в материалах к данной лабораторной работе.*

Например, существует шифр с названием «поворотная решётка»: изначально решётка Кардано представляла собой трафарет с отверстиями, в которые записывали буквы, слоги или слова сообщения. Затем трафарет убирали, а свободное место заполняли более или менее осмысленным текстом.

*6. Имеются ли предпочтения в выборе размеров используемой таблицы для перестановочных шифров?*

Да. Например, при использовании метода простой перестановки, при больших значениях *n* приходится работать с таблицами, состоящими из большого числа столбцов, что неудобно. Если мы используем маршрутный метод, то для считывания информации определенным алгоритмом (зигзагом, по спирали), так же имеет значение, возьмём мы таблицу размерностью 2х5 или 5х5.

*7. Охарактеризовать основные методы взлома перестановочных шифров.*

Для взлома используются различные алгоритмы перестановки.