Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Дисциплина: Теория информации (ТИ)

ОТЧЁТ

по практическому заданию №1

Тема работы: Простейшие шифры

Выполнил

Проверил: Болтак С.В.

Минск 2023

# Улучшенный столбцовый метод

## Дымовое тестирование

Тестовая фраза: «ИНФОРМАЦИОННАЯТЕОРИЯ!\*^%$#@&».

Ключевое слово: «ЯРМОЛИК».

Поскольку тестовая фраза содержит посторонние символы, при составлении таблицы они игнорируются.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Я | Р | М | О | Л | И | К |
| 7 | 6 | 4 | 5 | 3 | 1 | 2 |
| И | Н | Ф | О | Р | М |  |
| А | Ц | И | О | Н | Н | А |
| Я | Т | Е | О | Р |  |  |
| И | Я |  |  |  |  |  |

Зашифрованный текст: «МНАРНРФИЕОООНЦТЯИАЯИ»

Скриншот работы программы:

|  |  |
| --- | --- |
|  |  |

Очевидно, что результаты программы совпали с ожидаемым результатом.

## Крайние значения ключа

Крайними значениями ключа будем считать те значения, при которых его длина равна нулю или единице, а также, если ключ имеет повторяющиеся буквы.

### Длина равна нулю

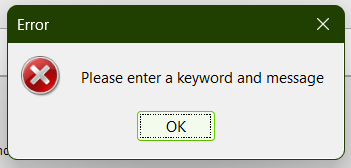
Тестовая фраза: «СУЕТАИАМОГУС!\*^%$#@&».

Ключевое слово: «»

Поскольку тестовая фраза содержит посторонние символы, при составлении таблицы они игнорируются.

Если длина ключа равна нулю, то, фактически, ключ не существует. Таблицу создать невозможно. Зашифрованный текст не получен.

Скриншот работы программы:



Очевидно, что результаты программы совпали с ожидаемым результатом.

### Длина равна единице

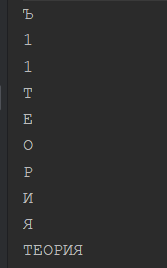
Тестовая фраза: «ТЕОРИЯ!\*^%$#@&».

Ключевое слово: «Ъ»

Поскольку тестовая фраза содержит посторонние символы, при составлении таблицы они игнорируются.

Если длина ключа равна единице, то, фактически, таблица представляет собой столбик из букв. Зашифрованный текст равен оригинальному.

Скриншот работы программы:



Очевидно, что результаты программы совпали с ожидаемым результатом.

### Ключ имеет повторяющиеся буквы

Тестовая фраза: «ИНФОРМАЦИОННАЯТЕОРИЯ!\*^%$#@&».

Ключевое слово: «ЯРМОЛИИ».

Поскольку тестовая фраза содержит посторонние символы, при составлении таблицы они игнорируются.

Ключ содержит две повторяющиеся буквы: «И» и «И». Одной из них необходимо присвоить значение «1», а другой – «2». Значения не должны повторяться.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Я | Р | М | О | Л | И | И |
| 7 | 6 | 4 | 5 | 3 | 1 | 2 |
| И | Н | Ф | О | Р | М |  |
| А | Ц | И | О | Н | Н | А |
| Я | Т | Е | О | Р |  |  |
| И | Я |  |  |  |  |  |

Зашифрованный текст: «МНАРНРФИЕОООНЦТЯИАЯИ»

Скриншот работы программы:

|  |  |
| --- | --- |
|  |  |

Очевидно, что результаты программы совпали с ожидаемым результатом.

## Ошибочные значения

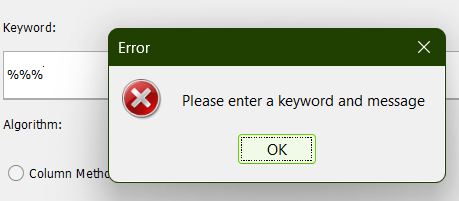
Тестовая фраза: «ОООПОВЕЗЛОПОВЕЗЛО!\*^%$#@&».

Ключевое слово: «%%%»

Поскольку тестовая фраза и ключ содержат посторонние символы, при составлении таблицы они игнорируются.

Оказалось, что ключ состоит исключительно из недопустимых символов, то есть на выходе остался пустой ключ (отсутствие ключа). Таблицу составить невозможно, зашифрованный текст не получен.

Скриншот работы программы:



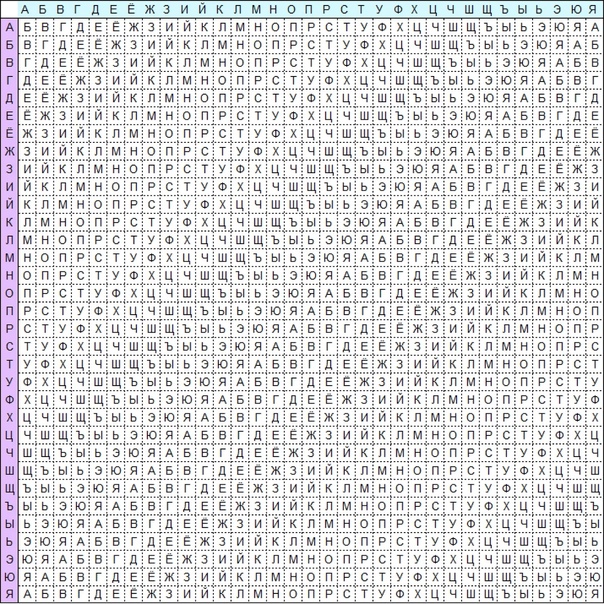
Очевидно, что результаты программы совпали с ожидаемым результатом.

# Шифр Виженера (автогенерирующийся ключ)

Формула шифрования: «PosC = (Size + PosM + PosK) % Size»

Формула дешифрования: «PosM = (Size + PosC - PosK) % Size»

Помимо формул, можно воспользоваться квадратом Виженера:



## Дымовое тестирование

Тестовая фраза: «ЁЛКИПАЛКИ!\*^%$#@&».

Ключевое слово: «АМОГУС».

Автогенерирующийся ключ: «АМОГУСЁЛК»

Поскольку тестовая фраза содержит посторонние символы, при составлении таблицы они игнорируются.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ё | Л | К | И | П | А | Л | К | И |
| А | М | О | Г | У | С | Ё | Л | К |
| Ё | Ш | Щ | Л | Г | С | С | Ц | У |

Зашифрованный текст: «ЁШЩЛГССЦУ»

Скриншот работы программы:

|  |  |
| --- | --- |
|  |  |

Очевидно, что результаты программы совпали с ожидаемым результатом.

## Буква Ё

Корректная обработка буквы ё была продемонстрирована в предыдущем разделе. Программа реализована таким образом, чтобы буква ё ничем не отличалась от других букв по методам обработки.

## Ошибочные значения

Если ключ содержит недопустимые символы, то их необходимо игнорировать, оставляя только символы заданного алфавита. Если же окажется, что ключ состоит из недопустимых символов целиком, то на выходе окажется пустой ключ (отсутствие ключа), что неверно. В таком случае программа должна вывести сообщение об ошибке.

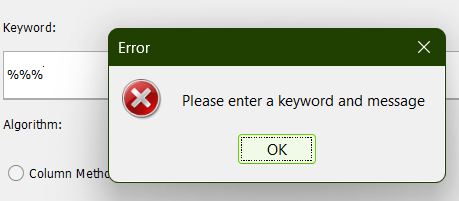
Тестовая фраза: «ТЕСТСЛОВО!\*^%$#@&».

Ключевое слово: «%%%»

Поскольку тестовая фраза и ключ содержат посторонние символы, при составлении таблицы они игнорируются.

Оказалось, что ключ состоит исключительно из недопустимых символов, то есть на выходе остался пустой ключ (отсутствие ключа). Учитывая, что ключ автогенерирующийся, зашифровать текст получится, а вот дешифровать – нет.

Скриншот работы программы:



Очевидно, что результаты программы совпали с ожидаемым результатом.