БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

Лабораторная работа №2

«ОИсследование криптографических шифров на основе подстановки (замены) символов»

По предмету «Защита информации и надежность информационных систем»

**Выполнила:**

Студентка 3 курса 2 группы

Веракса Татьяна Анатольевна

Минск 2020

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

**Вариант 3**

Выполнить зашифрование/расшифрование текстовых документов (объемом не менее 5 тысяч знаков) созданных на основе английского алфавита; при этом следует использовать шифр Цезаря с ключевым словом, ключевое слово – собственная фамилия, таблицу Трисемуса, ключевое слово – собственное имя.

**Система шифрования Цезаря с ключевым словом (лозунгом)** является одноалфавитной системой подстановки. Особенностью этой системы является использование ключевого слова (лозунга) для смещения и изменения порядка символов в алфавите подстановки (желательно, чтобы все буквы ключевого слова были различными). Ключевое слово пишется в начале алфавита подстановки.

Пример 1. Для шифра с использованием кодового слова «VERAKS» исходный алфавит (первая строка) и алфавит подстановки (вторая строка) выглядят следующим образом:

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

Если Мi = «TANYA», то Ci = «QVGYV», если же Мi = «VERAKSA», то Ci = «UKOVGPV».

Результат зашифрования/расшифрования текстового документа на основе шифрования Цезаря с ключевым словом:

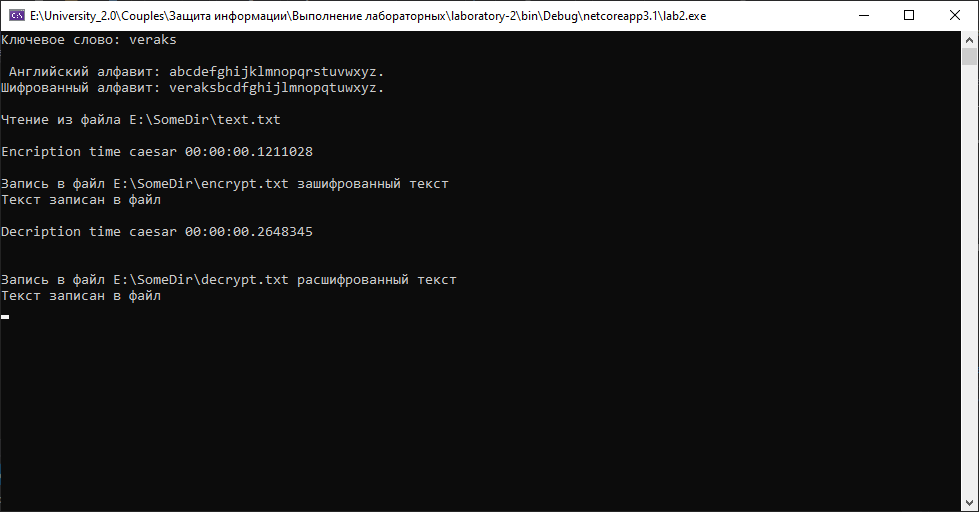


Рисунок 2.1 – Результат программы шифрования Цезаря с ключевым словом

Для примера и сравнения приведены гистограммы для исходного и зашифрованного документов.

На рисунке 2.2 представлена гистограмма исходного текстовый документ для шифрования Цезаря с ключевым словом «veraks».



Русинок 2.2 – Гистограмма для исходного текстового документа

На рисунке 2.3 представлена гистограмма зашифрованного текстового документа шифрования Цезаря с ключевым словом «veraks».



Рисунок 2.3 – Гистограмма для зашифрованного текстового документа

**Таблица Трисемуса.** Зашифрование осуществляется так: заготавливается таблица подстановки (так называемая «таблица Трисемуса» – таблица со стороной равной N, где N – мощность алфавита), где первая строка – это алфавит, вторая – алфавит, сдвинутый на один символ, и т. д. При зашифровании первая буква открытого текста заменяется на букву, стоящую в первой строке, вторая – на букву, стоящую во второй строке, и т.д. После использования последней строки вновь возвращаются к первой.

В указанной книге Трисемус впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра подстановки обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). Можно найти определенную аналогию с системой шифрования Цезаря с ключевым словом. В таблицу сначала вписывалось по стрелкам ключевое слово, причем повторяющиеся буквы также отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. Таким образом, ключом в таблицах Трисемуса является ключевое слово и размер таблицы. При шифровании буква открытого текста заменяется буквой, расположенной ниже нее в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

Указанный размер таблицы для алфавита русского языка может соответствовать 4х8 либо 8х4.

Пример 2. Пусть Мi = «ВЕРАКСА», а ключевое слово – «ТАНЯ». Используем таблицу 8х4.

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

Следуя вышеуказанного принципу подстановки, получим Сi = «ЖЙХВПЦВ».

Результат зашифрования/расшифрования текстового документа на основе шифрования Трисемуса с ключевым словом:

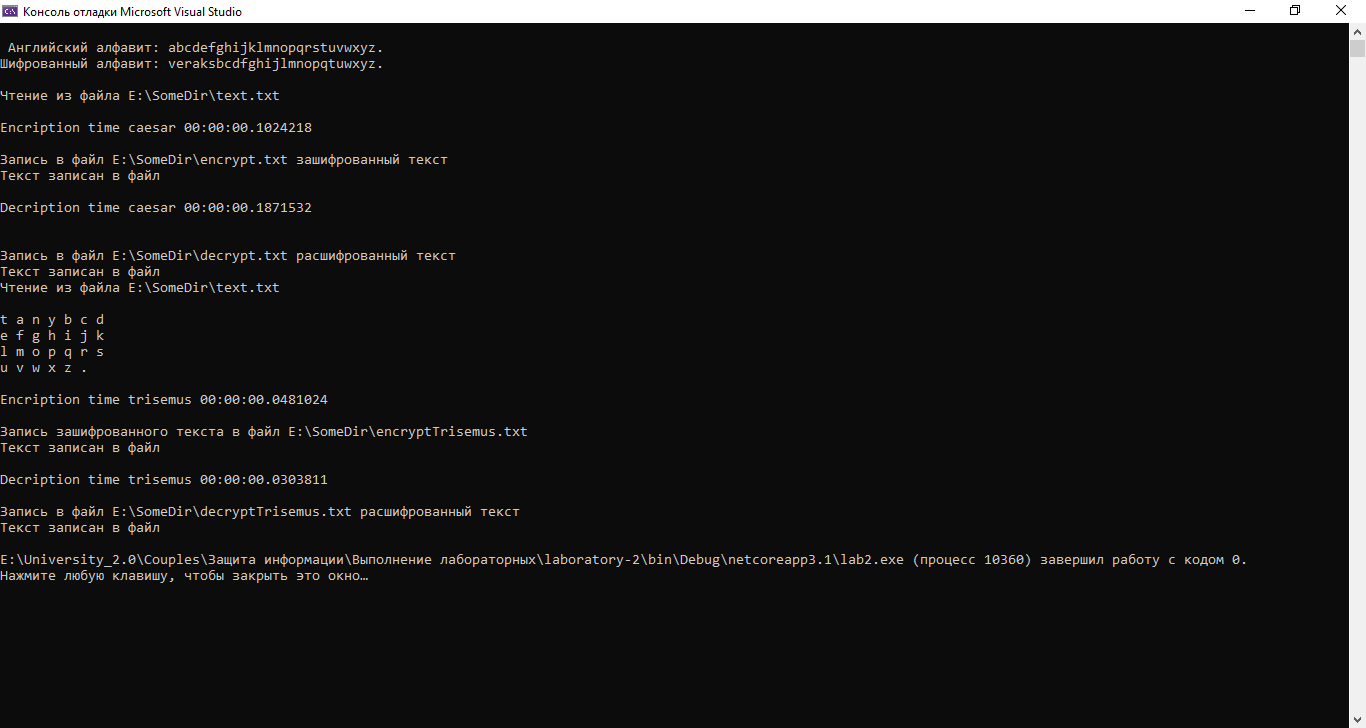


Рисунок 2.2 – Результат программы шифрования Трисемуса

На рисунке 2.3 представлена гистограмма исходного текстовый документ для шифрования Трисемуса с ключевым словом «tanya».



Русинок 2.2 – Гистограмма для исходного текстового документа

На рисунке 2.4 представлена гистограмма зашифрованного текстового документа шифрования Цезаря с ключевым словом «veraks».



Рисунок 2.4 – Гистограмма для зашифрованного текстового документа

**Вывод**: изучили и приобрели практические навыки разработки и использования приложений для реализации подстановочных шифров: шифра Цезаря и Трисемуса с ключевым словом. Оценили время выполнения операций зашифрования/расшифрования для данных шифров подстановки.