Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет информатики и радиоэлектроники»

Факультет компьютерных технологий

Кафедра инженерной психологии и эргономики

Дисциплина: Криптографические технологии

Отчет

по Практическому заданию №1

на тему: «Криптоанализ классических шифров»

Студент: гр. 910902 Шарупич К. А.

Руководитель: Давыдович К.И.

Минск 2022

Цель работы: ознакомиться с шифром Цезаря и шифром простых замен, научиться проводить атаки на эти шифры.

Ход работы

Задание 1

Написать программу дешифрования для нахождения открытого текста, вскрыв шифр Цезаря, найти ключ шифра простой замены, используя для дешифрования известный открытый текст.

Шифртекст 1: «Srobdoskdehwlf vxevwlwxwlrq flskhuv» (для шифра Цезаря).

Шифртекст 2: «KjgyVgkcVWZqdX nsWnqdqsqdji XdkcZmn» (для шифра простой замены).

Выполнение

Шифр Цезаря. Малое пространство ключей делает простой перебор самым эффективным и простым вариантом атаки. Для вскрытия каждую букву шифртекста заменяем буквой, стоящей на один знак *левее* в алфавите, пока не получим читаемый текст.

Результат выполнения задания представлен на рисунке 1.

```
Key: 3
Final message: P o l y a l p h a b e t i c  s u b s t i t u t i o n  c i p h e r s
```

Рисунок 1 – Результат атаки (шифр Цезаря)

Полученный открытый текст: «Polyalphabetic substitution ciphers».

Ключ (количество смещений): 3.

Шифр простой замены. Ключом шифра простой замены служит перемешанный произвольным образом алфавит. Имея *зашифрованный текст* шифртекст 2 и *открытый текст* (совпадающий с открытым текстом шифра Цезаря), найдем *ключ*.

При расшифровке буква сперва ищется в ключе и затем заменяется буквой, стоящей в алфавите на той же позиции.

За основу ключа возьмем смещение влево алфавита по алгоритму дешифровки шифра Цезаря. Смещаем, пока не получим приблизительный открытый текст. Результат выполнения представлен на рисунке 2, где

– Result alphabet – ключ шифра простой замены;

– Result message – приблизительный открытый текст.

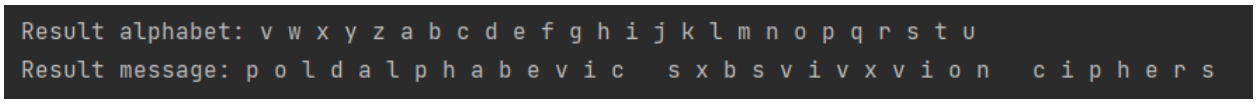

Рисунок 2 – Приблизительный открытый текст и ключ

В ходе дешифровки основной ключ подвергается небольшим изменениям (перестановка двух произвольно выбранных букв). Исходя из открытого текста «Polyalphabetic substitution ciphers» и полученного текста «Pol**d**alphabe**v**ic s**x**bs**vi**v**x**vion ciphers», необходимо переставить буквы ключа «d» и «y», «v» и «t», «x» и «u». Буква сперва ищется в *алфавите* и затем заменяется в *ключе* на той же позиции. Результат представлен на рисунке 3.

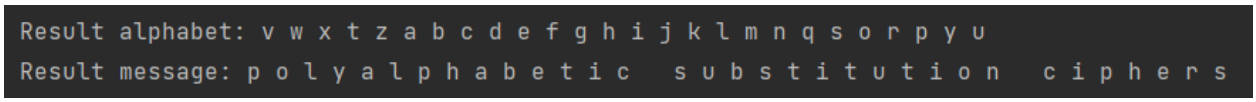

Рисунок 3 – Открытый текст и ключ

Полученный открытый текст: «Polyalphabetic substitution ciphers».
Ключ: «v w x t z a b c d e f g h i j k l m n q s o r p y u»

Задание 2

Написать программу для зашифровки ФИО, дешифровки полученного текста. Сравнить полученный текст с исходным текстом.

Выполнение

Зашифруем ФИО «Sharupich Kseniya Andreevna», используя шифр Цезаря и ключ 7. Результат представлен на рисунке 4.

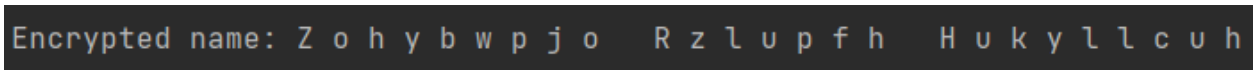

Рисунок 4 – Результат шифрования шифром Цезаря

Затем проведем дешифровку зашифрованных данных («Z o h y b w p j o R z l u p f h H u k y l l c u h»), используя тот же алгоритм, что и для первого задания. Результат работы программы на рис. 5.

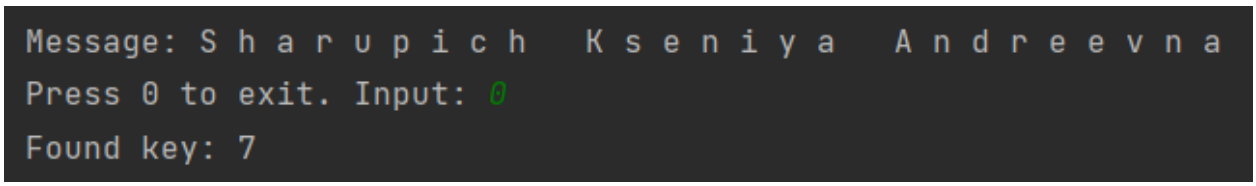

Рисунок 5 – Результат дешифровки

Результат дешифровки сходится с исходным текстом. Ключ совпадает.

Вывод. В ходе выполнения лабораторной работы был изучен шифр Цезаря и шифр простых замен, выявлены ключи для обоих шифров, а также была разработана программа для шифровки и дешифровки текста.