

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ
ПРЕПОДАВАТЕЛЬ

ассистент

должность, уч. степень, звание

подпись, дата

М.Н. Исаева

инициалы, фамилия

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ

ИСТОРИЧЕСКИЕ ШИФРЫ

по курсу: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР.

5912

подпись, дата

В.И.Сазонова

инициалы, фамилия

Санкт-Петербург
2021

Задача

Вариант 1. Реализовать подстановочный шифр Цезаря. Провести частотный анализ. Реализация системы должна работать в двух режимах: шифрования и дешифрования, позволять вводить ключ вручную и генерировать его автоматически.

Описание алгоритма

Шифр Цезаря

В шифре Цезаря каждой букве алфавита N ставится в соответствие буква этого же алфавита со смещением вправо ключ. При этом, если ключ больше, чем расстояние до левой границы алфавита, считается, что после последней буквы с этой стороны алфавита идет первая буква с другой.

Пусть задан алфавит из N символов. Тогда шифрующее преобразование шифра Цезаря задаётся как

$$E: y = x + k \bmod N,$$

где x – номер в алфавите исходного символа, y – номер символа шифртекста, $k \in \{0, \dots, N - 1\}$ – значение ключа. Обратное преобразование задаётся как

$$D: x = y - k \bmod N$$

Описание реализации

На входе программа просит сгенерировать случайный ключ или задать ключ самостоятельно. Ключ – натуральное число. Затем программа просит выбрать, откуда считать текст, из строки или из файла, и режим работы – кодирование или декодирование. После этого программа считывает текст, кодирует/декодирует его и выводит в новый файл или строчкой ниже в консоль. Данные проведенного частотного анализа сохраняются в текстовом формате в отдельном файле. Если выбран режим генерации ключа декодирования, программа делает частотный анализ текста и на его основе считает ключ.

При шифровании заглавные буквы остаются заглавными, прописные – прописными, знаки препинания не входят в алфавит (не шифруются) и просто перезаписываются в шифртекст. Используемый алфавит – английский в кодировке ASCII.

Описание класса и функций

```
class Code
{
    int key;// ключ
    int frequency[27];//массив для подсчета частоты
    bool isKey;//введен ли ключ пользователем

public:
    Code();//конструктор по умолчанию
    Code(int k);//конструктор с известным ключом
    string Coding(string s);//функция, кодирующая строку s
    string Decoding(string s);//функция, декодирующая строку s
    string Decryption(string s);//функция декодирования строки s с
    поиском ключа
    void getFrequency(string path, string outpath);//функция вывода
    частотного анализа файлов path и outpath
private:
    char Shift(char c, bool isLow);//функция сдвига буквы на ключ
};

void ReadFile(int key, bool isCoding);// функция (де)кодирования из файла с
помощью ключа key

void ReadString(int key, bool isCoding);// функция (де)кодирования введенной
строки с помощью ключа key

void ReadFullFile();// функция декодирования файла с неизвестным ключом
```

Численные результаты

В качестве исходного текста возьмем стихотворение А.С.Пушкина «Няне»(рис.1):

```
A friend of my severe days,
Decrepit darling dove of mine!
In deep pine woods alone you wait
For me, you wait too long a time.
In your front room under the window
You grieve as if you sentry stand,
And needles linger every minute
In your fatigued and puckered hands.
You look through old forgotten gates
At a pitch-black and distant path:
Depression, premonitions, cares
Oppress incessantly your heart.
It seems to you...
```

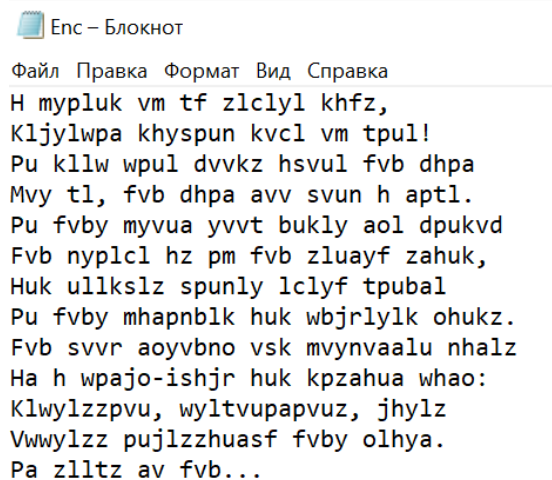
Рисунок 1. А.С.Пушкин "Няне" на английском языке

Сохраним стихотворение в файл *Sasha.txt*, запустим программу в режиме кодирования файла с известным ключом. Пусть ключ будет равен 7(рис.2):

```
Select:
0: you want to enter the key
1: automatic key
0
Enter the key: 7
Select:
0: you want to enter the string manually
1: text is stored in a file
1
Select:
0: Encryption
1: Decryption
0
Enter the path:
Sasha.txt
Create path for new file:
Enc.txt
```

Рисунок 2. Ввод параметров теста

В результате работы программы создастся три файла: файл с закодированным текстом и два файла частотного анализа: для исходного текста и для закодированного(рис.3, 4, 5):



Enc – Блокнот

Файл Правка Формат Вид Справка

H mypluk vm tf zlclyl khfz,
Kljylwpa khyspun kvcl vm tpul!
Pu kllw wpul dvvkz hsvul fvb dhpa
Mvy tl, fvb dhpa avv svun h aptl.
Pu fvby myvua yvvt bukly aol dpukvd
Fvb nypclcl hz pm fvb zluayf zahuk,
Huk ullkslz spunly lclyf tpubal
Pu fvby mhpnblk huk wbjrlylk ohukz.
Fvb svvr aoyvbno vsk mvynvaalu nhalz
Ha h wpajo-ishjr huk kpzahua whao:
Klwylzzpvu, wyltvupapvuz, jhylv
Vwwylzz pujlzzhuasf fvby olhya.
Pa zlltz av fvb...

Рисунок 3. Зашифрованный текст

FrequencySasha – Блокнот
 Файл Правка Формат Вид
 Frequency
 a: 23; 5.5%
 b: 1; 0.24%
 c: 6; 1.4%
 d: 20; 4.7%
 e: 40; 9.5%
 f: 8; 1.9%
 g: 8; 1.9%
 h: 7; 1.7%
 i: 24; 5.7%
 j: 0; 0%
 k: 3; 0.71%
 l: 9; 2.1%
 m: 8; 1.9%
 n: 28; 6.6%
 o: 34; 8.1%
 p: 10; 2.4%
 q: 0; 0%
 r: 23; 5.5%
 s: 20; 4.7%
 t: 25; 5.9%
 u: 14; 3.3%
 v: 4; 0.95%
 w: 5; 1.2%
 x: 0; 0%
 y: 14; 3.3%
 z: 0; 0%

Рисунок 4. Частотный анализ входного текста

FrequencyEnc – Блокнот
 Файл Правка Формат Вид
 Frequency
 a: 25; 5.9%
 b: 14; 3.3%
 c: 4; 0.95%
 d: 5; 1.2%
 e: 0; 0%
 f: 14; 3.3%
 g: 0; 0%
 h: 23; 5.5%
 i: 1; 0.24%
 j: 6; 1.4%
 k: 20; 4.7%
 l: 40; 9.5%
 m: 8; 1.9%
 n: 8; 1.9%
 o: 7; 1.7%
 p: 24; 5.7%
 q: 0; 0%
 r: 3; 0.71%
 s: 9; 2.1%
 t: 8; 1.9%
 u: 28; 6.6%
 v: 34; 8.1%
 w: 10; 2.4%
 x: 0; 0%
 y: 23; 5.5%
 z: 20; 4.7%

Рисунок 5. Частотный анализ выходного текста

По частотному анализу выходного файла отметим, что частоты буквы сдвинулись на 7 позиций, что аналогично сдвигу по ключу 7, значит, режим шифрования отработал корректно.

Расшифруем полученный шифртекст с помощью ключа 7(рис.6):

```
Select:
0: you want to enter the key
1: automatic key
0
Enter the key: 7
Select:
0: you want to enter the string manually
1: text is stored in a file
1
Select:
0: Encryption
1: Decryption
1
Enter the path:
Enc.txt
Create path for new file:
Dec.txt
```

Рисунок 6. Ввод параметров дешифровки по ключу

В результате работы программы создается три файла: файл с раскодированным текстом и два файла частотного анализа: для входного текста и для выходного(рис. 7, 8, 9):

Dec – Блокнот
 Файл Правка Формат Вид Справка
 A friend of my severe days,
 Decrepit darling dove of mine!
 In deep pine woods alone you wait
 For me, you wait too long a time.
 In your front room under the window
 You grieve as if you sentry stand,
 And needles linger every minute
 In your fatigued and puckered hands.
 You look through old forgotten gates
 At a pitch-black and distant path:
 Depression, premonitions, cares
 Oppress incessantly your heart.
 It seems to you...

Рисунок 7. Раскодированный текст

FrequencyEnc – Блокнот
 Файл Правка Формат Вид
 Frequency
 a: 25; 5.9%
 b: 14; 3.3%
 c: 4; 0.95%
 d: 5; 1.2%
 e: 0; 0%
 f: 14; 3.3%
 g: 0; 0%
 h: 23; 5.5%
 i: 1; 0.24%
 j: 6; 1.4%
 k: 20; 4.7%
 l: 40; 9.5%
 m: 8; 1.9%
 n: 8; 1.9%
 o: 7; 1.7%
 p: 24; 5.7%
 q: 0; 0%
 r: 3; 0.71%
 s: 9; 2.1%
 t: 8; 1.9%
 u: 28; 6.6%
 v: 34; 8.1%
 w: 10; 2.4%
 x: 0; 0%
 y: 23; 5.5%
 z: 20; 4.7%

Рисунок 8. Частотный анализ входного текста

FrequencyDec – Блокнот
 Файл Правка Формат Вид
 Frequency
 a: 23; 5.5%
 b: 1; 0.24%
 c: 6; 1.4%
 d: 20; 4.7%
 e: 40; 9.5%
 f: 8; 1.9%
 g: 8; 1.9%
 h: 7; 1.7%
 i: 24; 5.7%
 j: 0; 0%
 k: 3; 0.71%
 l: 9; 2.1%
 m: 8; 1.9%
 n: 28; 6.6%
 o: 34; 8.1%
 p: 10; 2.4%
 q: 0; 0%
 r: 23; 5.5%
 s: 20; 4.7%
 t: 25; 5.9%
 u: 14; 3.3%
 v: 4; 0.95%
 w: 5; 1.2%
 x: 0; 0%
 y: 14; 3.3%
 z: 0; 0%

Рисунок 9. Частотный анализ выходного текста

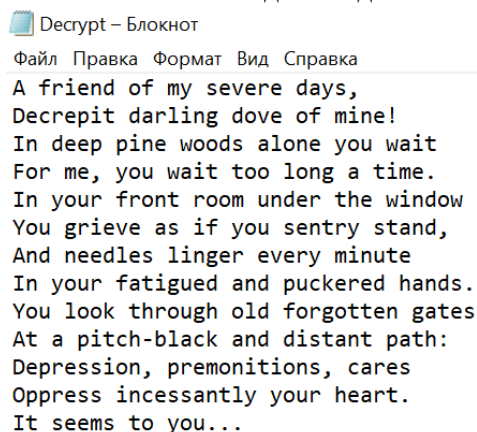
Выходной текст программы дешифровки по ключу совпадает с входным текстом программы шифровки по ключу, частотные анализы этих текстов и их зашифрованных аналогов одинаковы, значит, режим дешифровки по ключу работает корректно.

Расшифруем шифртекст с помощью генерации ключа(рис.10):

```
Select:
0: you want to enter the key
1: automatic key
1
Select:
0: you want to enter the string manually
1: text is stored in a file
1
Select:
0: Encryption
1: Decryption
1
Enter the path:
Enc.txt
Create path for new file:
Decrypt.txt
```

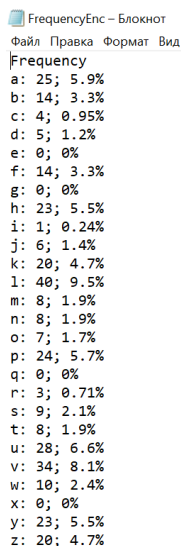
Рисунок 10. Ввод параметров дешифровки без ключа

В результате работы программы создается три файла: файл с раскодированным текстом и два файла частотного анализа: для входного текста и для выходного(рис. 11, 12, 13):



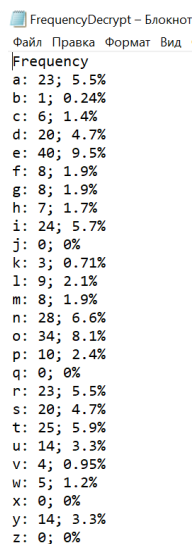
Decrypt – Блокнот
Файл Правка Формат Вид Справка
A friend of my severe days,
Decrepit darling dove of mine!
In deep pine woods alone you wait
For me, you wait too long a time.
In your front room under the window
You grieve as if you sentry stand,
And needles linger every minute
In your fatigued and puckered hands.
You look through old forgotten gates
At a pitch-black and distant path:
Depression, premonitions, cares
Oppress incessantly your heart.
It seems to you...

Рисунок 11. Расшифрованный текст



FrequencyEps – Блокнот
Файл Правка Формат Вид
Frequency
a: 25; 5.9%
b: 14; 3.3%
c: 4; 0.95%
d: 5; 1.2%
e: 0; 0%
f: 14; 3.3%
g: 0; 0%
h: 23; 5.5%
i: 1; 0.24%
j: 6; 1.4%
k: 20; 4.7%
l: 40; 9.5%
m: 8; 1.9%
n: 8; 1.9%
o: 7; 1.7%
p: 24; 5.7%
q: 0; 0%
r: 3; 0.71%
s: 9; 2.1%
t: 8; 1.9%
u: 28; 6.6%
v: 34; 8.1%
w: 10; 2.4%
x: 0; 0%
y: 23; 5.5%
z: 20; 4.7%

Рисунок 12. Частотный анализ входного текста



FrequencyDecrypt – Блокнот
Файл Правка Формат Вид
Frequency
a: 23; 5.5%
b: 1; 0.24%
c: 6; 1.4%
d: 20; 4.7%
e: 40; 9.5%
f: 8; 1.9%
g: 8; 1.9%
h: 7; 1.7%
i: 24; 5.7%
j: 0; 0%
k: 3; 0.71%
l: 9; 2.1%
m: 8; 1.9%
n: 28; 6.6%
o: 34; 8.1%
p: 10; 2.4%
q: 0; 0%
r: 23; 5.5%
s: 20; 4.7%
t: 25; 5.9%
u: 14; 3.3%
v: 4; 0.95%
w: 5; 1.2%
x: 0; 0%
y: 14; 3.3%
z: 0; 0%

Рисунок 13. Частотный анализ выходного текста

Выходной текст программы дешифровки с помощью генерации ключа совпадает с входным текстом программы шифровки по ключу, частотные анализы этих текстов и их зашифрованных аналогов одинаковы, значит, режим дешифровки с помощью генерации ключа работает корректно.

Таким образом, во всех режимах программа вывела ожидаемые результаты, значит, отработала корректно.

Выводы

В реальной жизни рассмотренный способ шифрования не является вычислительно стойким для любых алфавитов естественных языков. Шифр Цезаря является моноалфавитным шифром замены, поэтому он обладает всеми уязвимостями этого класса шифров.

В случае шифрования сообщений на английском языке (т.е. $N = 26$) существует 25 нетривиальных ключей, а значит, для взлома такого шифра не требуется много времени. С помощью частотного анализа или даже простого перебора ключей из зашифрованного таким образом текста можно получить исходный достаточно быстро, поэтому в современном мире данный метод шифрования либо не используется вовсе, либо используется, но как основа для других, более сложных, шифров.

Список литературы

1. **А.А.Овчинников.** *ОИБ. Исторические шифры.* Санкт-Петербург : ГУАП, 2018.
2. **Р.Черчаус.** *Коды и шифры. Юлий Цезарь, "Энигма" и Интернет.* б.м. : Весь мир, 2005.

