УНИВЕРСИТЕТ ИТМО

Факультет программной инженерии и компьютерной техники

Дисциплина «Информационная безопасность»

Лабораторная работа №1.1

Основы Шифрования данных

Вариант 2

Студент

Ершова А. И.

P34302

Преподаватель

Рыбаков С. Д.

Санкт-Петербург, 2023 г.

Цель работы: изучение основных принципов шифрования информации, знакомство с широко известными алгоритмами шифрования, приобретение навыков их программной реализации.

Вариант 2: реализовать шифрование и дешифрацию файла по методу Виженера. Ключевая фраза вводится. Реализовать в программе частотный криптоанализ зашифрованного текста.

Листинг разработанной программы

```
public class VizhenerTable {
    final String ALPHABET_RUS =
"АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ";
    final String ALPHABET_ENG = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";

    String decryptString (String str, String keyWord) {
        String finalStr = "";
        int keyWordLen = keyWord.length();
        int keyNumPointer = 0;

        for (int i = 0; i < str.length(); i++) {
            char curChar = str.charAt(i);
            if (!Character.isAlphabetic(curChar)) {
                finalStr += curChar;
                continue;
            }
            if (!isRussian(curChar) && !isEnglish(curChar)) {
                finalStr = "-";
                continue;
            }
            finalStr += decryptChar(curChar,
keyWord.charAt(keyNumPointer % keyWordLen));
            keyNumPointer++;
        }

        return finalStr;
    }

    String encryptString(String str, String keyWord) {
        String finalStr = "";
        int keyWordLen = keyWord.length();
        int keyNumPointer = 0;

        for (int i = 0; i < str.length(); i++) {
            char curChar = str.charAt(i);
            if (!Character.isAlphabetic(curChar)) {
                finalStr += curChar;
                continue;
            }
            if (!isRussian(curChar) && !isEnglish(curChar)) {
```

```
                finalStr = "-";
                continue;
            }
            finalStr += encryptChar(curChar,
keyWord.charAt(keyNumPointer % keyWordLen));
            keyNumPointer++;
        }
        return finalStr;
    }

    private char decryptChar (char wordChar, char keyChar) {
        char finalChar = '-';
        String alphabet = "";
        if (isRussian(wordChar)) alphabet = ALPHABET_RUS;
        else alphabet = ALPHABET_ENG;
        keyChar = Character.toUpperCase(keyChar);

        int alphabetWordCharNum =
findPosition(Character.toUpperCase(wordChar), alphabet);
        int alphabetCodeCharNum = findPosition(keyChar,
alphabet);

        int finalCharNum = alphabetWordCharNum -
alphabetCodeCharNum;

        if (finalCharNum < 0) finalCharNum += alphabet.length();
        finalChar = alphabet.charAt(finalCharNum);
        if (Character.isLowerCase(wordChar)) finalChar =
Character.toLowerCase(finalChar);
        else finalChar = Character.toUpperCase(finalChar);
        return finalChar;

    }

    private char encryptChar (char wordChar, char keyChar) {
        char finalChar = '-';
        String alphabet = "";
        if (isRussian(wordChar)) alphabet = ALPHABET_RUS;
        else alphabet = ALPHABET_ENG;
        keyChar = Character.toUpperCase(keyChar);

        int alphabetWordCharNum =
findPosition(Character.toUpperCase(wordChar), alphabet);
        int alphabetCodeCharNum = findPosition(keyChar,
alphabet);

        int finalCharNum = alphabetWordCharNum +
alphabetCodeCharNum;
        if (finalCharNum >= alphabet.length()) finalCharNum -=
alphabet.length();
        finalChar = alphabet.charAt(finalCharNum);
        if (Character.isLowerCase(wordChar)) finalChar =
Character.toLowerCase(finalChar);
```

```
        else finalChar = Character.toUpperCase(finalChar);

        return finalChar;
    }


    private boolean isRussian(char ch) {
        if ((ch >= 'A' && ch <= 'я') || (ch == 'ё') || (ch ==
'Ё') ) return true;
        return false;
    }

    private boolean isEnglish (char ch) {
        if ((ch >= 'A') && (ch <= 'z')) return true;
        return false;
    }

    private int findPosition (Character ch, String string) {
        int pos = -1;
        for (int i =0; i < string.length(); i++) {
            if (string.charAt(i) == ch) pos =i;
        }
        return pos;
    }
}
```

Результаты работы программы

Шифрование:

```
What do you want to do?

1. Encrypt

2. Decrypt

3. Frequency Cryptanalysis

Enter a number

1


String to encrypt:

It was nearing midnight and the Prime Minister was sitting alone in his
office, reading a long memo that was slipping through his brain without
leaving the slightest trace of meaning behind.

Key Word: Harry

Encrypted string:

Pt nrq uerigug dzbuixyr hnu kfl Pizkl Mzegztvi uhs jzraiex ysoev gu hzj
mmfztc, yerugug r cmug dvkv tyrr daj jjppgzln tyimbgy ygz birgu wzkfvuk
cchvzee ahv jjpgykczt kiyje fw klaezln bvygud.
```

input.txt

It was nearing midnight and the Prime Minister was sitting alone in his office, reading a long memo that was slipping through his brain without leaving the slightest trace of meaning behind.

Harry

Дешифрация

```
What do you want to do?

1. Encrypt

2. Decrypt

3. Frequency Cryptanalysis

Enter a number

2

String to decrypt:

Pt nrq uerigug dzbuixyr hnu kfl Pizkl Mzegztvi uhs jzraiex ysoev gu hzj
mmfztc, yerugug r cmug dvkv tyrr daj jjppgzln tyimbgy ygz birgu wzkfvuk
cchvzee ahv jjpgykczt kiyje fw klaezln bvygud.

Key Word: Harry

Decrypted string:

It was nearing midnight and the Prime Minister was sitting alone in his
office, reading a long memo that was slipping through his brain without
leaving the slightest trace of meaning behind.
```

input.txt

Pt nrq uerigug dzbuixyr hnu kfl Pizkl Mzegztvi uhs jzraiex ysoev gu hzj mmfztc, yerugug r cmug dvkv tyrr daj jjppgzln tyimbgy ygz birgu wzkfvuk cchvzee ahv jjpgykczt kiyje fw klaezln bvygud.
Harry

Частотный криптоанализ

```
What do you want to do?

1. Encrypt

2. Decrypt

3. Frequency Cryptanalysis

Enter a number
```

```
3

String for Frequency Cryptanalysis:

Pt nrq uerigug dzbuixyr hnu kfl Pizkl Mzegztvi uhs jzraiex ysoev gu hzj
mmfztc, yerugug r cmug dvkv tyrr daj jjppgzln tyimbgy ygz birgu wzkfvuk
cchvzee ahv jjpgykczt kiyje fw klaezln bvygud.

Estimated keyword length = 5

column 0: [A = 2, B = 1, C = 0, D = 1, E = 0, F = 0, G = 0, H = 3, I = 0, J =
1, K = 0, L = 3, M = 1, N = 2, O = 0, P = 3, Q = 0, R = 0, S = 1, T = 0, U =
8, V = 2, W = 0, X = 0, Y = 1, Z = 3 ]

A = 0.0625

B = 0.03125

D = 0.03125

H = 0.09375

J = 0.03125

L = 0.09375

M = 0.03125

N = 0.0625

P = 0.09375

S = 0.03125

U = 0.25

V = 0.0625

Y = 0.03125

Z = 0.09375


column 1: [A = 2, B = 2, C = 0, D = 1, E = 3, F = 1, G = 5, H = 2, I = 2, J =
0, K = 0, L = 0, M = 1, N = 1, O = 1, P = 2, Q = 0, R = 0, S = 1, T = 5, U =
1, V = 1, W = 1, X = 0, Y = 0, Z = 0 ]

A = 0.0625

B = 0.0625

D = 0.03125

E = 0.09375

F = 0.03125

G = 0.15625

H = 0.0625

I = 0.0625

M = 0.03125

N = 0.03125

O = 0.03125

P = 0.0625
```

S = 0.03125

T = 0.15625

U = 0.03125

V = 0.03125

W = 0.03125

column 2: [A = 0, B = 0, C = 0, D = 2, E = 3, F = 1, G = 1, H = 0, I = 2, J = 2, K = 2, L = 0, M = 0, N = 1, O = 0, P = 0, Q = 0, R = 3, S = 0, T = 0, U = 1, V = 3, W = 0, X = 1, Y = 4, Z = 5]

D = 0.06451613

E = 0.09677419

F = 0.032258064

G = 0.032258064

I = 0.06451613

J = 0.06451613

K = 0.06451613

N = 0.032258064

R = 0.09677419

U = 0.032258064

V = 0.09677419

X = 0.032258064

Y = 0.12903225

Z = 0.16129032

column 3: [A = 0, B = 0, C = 2, D = 0, E = 2, F = 0, G = 0, H = 0, I = 4, J = 3, K = 3, L = 0, M = 0, N = 0, O = 0, P = 0, Q = 0, R = 3, S = 0, T = 1, U = 1, V = 2, W = 1, X = 1, Y = 3, Z = 5]

C = 0.06451613

E = 0.06451613

I = 0.12903225

J = 0.09677419

K = 0.09677419

R = 0.09677419

T = 0.032258064

U = 0.032258064

V = 0.06451613

W = 0.032258064

X = 0.032258064

```
Y = 0.09677419

Z = 0.16129032


column 4: [A = 0, B = 1, C = 3, D = 0, E = 1, F = 2, G = 7, H = 0, I = 0, J =
2, K = 3, L = 2, M = 3, N = 0, O = 0, P = 0, Q = 1, R = 3, S = 0, T = 0, U =
1, V = 0, W = 0, X = 0, Y = 2, Z = 0 ]

B = 0.032258064

C = 0.09677419

E = 0.032258064

F = 0.06451613

G = 0.22580644

J = 0.06451613

K = 0.09677419

L = 0.06451613

M = 0.09677419

Q = 0.032258064

R = 0.09677419

U = 0.032258064

Y = 0.06451613
```

Вывод

Я изучила основные принципы шифрования информации, ознакомилась с алгоритмом шифрования Виженера и приобрела навыки его программной реализации.