Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерного проектирования

Кафедра инженерной психологии и эргономики

КРИПТОГРАФИЧЕСКИЕ ТЕХНОЛОГИИ
Практическая работа №1
Криптоанализ классических шифров

Проверил:
Давыдович К. И.

Выполнили:
Мисевич А. С.

Минск 2023

Цель работы

Изучение и криптоанализ шифра перестановки, шифра замены.

Задача

1. Ниже два шифртекста одного и того же сообщения, зашифрованные с помощью классических шифров:
   - **a.** Цезарь - Шифртекст 1.

   Srobdoskdehwlf vxevwlwxwlrq flskhuv
   - **b.** простой замены - Шифртекст 2.

   KjgyVgkcVWZqdX nsWnqdqsqdji XdkcZmn

   Напишите программу дешифрования, используя любой известный вам язык программирования:
   - найдите соответствующий открытый текст, вскрыв шифр Цезаря,
   - а затем найдите *ключ шифра простой замены*, используя для дешифрования известный открытый текст.

   Обе атаки должны быть полностью описаны.
2. Напишите программу, используя любой известный вам язык программирования:
   - зашифруйте свою фамилию, имя отчество
   - дешифруйте полученный текст
   - сравните с исходным текстом

Листинг кода

```
import java.util.Arrays;
import java.util.Scanner;

public class Main {

    public static void main(String[] args) {
        Scanner scan = new Scanner(System.in);

        String originalMessage = "";
        String messageCaesar = "Srobdoskdehwlf vxevwlwxwlrq
flskhuv";
        String messageReplacement = "KjgyVgkcVWZqdX
nsWnqdqsqdji XdkcZmn";
        int keyCaesar;
        char[] keyReplacement = new char[52];

        String name = "";
        String nameReplacement = "";

        //Расшифровки шифра цезаря для всех 26 вариантов
сдвига
        for(int j = 25; j > 0; j--) {
```

```
                System.out.print("Смещение = " + (26 - j) + ",
оригинал текста: ");
                for (int i = 0; i < messageCaesar.length(); i++) {

System.out.print(letterShift(messageCaesar.toCharArray()[i], j));
                }
                System.out.println();
            }

            System.out.print("Введите смещение, при котором
оригинал текста имеет смылс: ");
            keyCaesar = scan.nextInt();

            //Восстановление оригинального сообщения
            for (int i = 0; i < messageCaesar.length(); i++) {
                originalMessage +=
letterShift(messageCaesar.toCharArray()[i], 26 - keyCaesar);
            }

            System.out.print("Оригинальное сообщение: ");
            System.out.println(originalMessage);

            //Восстановление ключа для шифра простой замены
            Arrays.fill(keyReplacement, '?');
            for (int i = 0; i < originalMessage.length(); i++) {
                char letter = originalMessage.toCharArray()[i];
                if((int)letter < 91 && (int)letter > 64) {
                    keyReplacement[(int)letter - 65] =
messageReplacement.toCharArray()[i];
                } else if((int)letter < 123 && (int)letter > 96) {
                    keyReplacement[(int)letter - 97 + 26] =
messageReplacement.toCharArray()[i];
                } else {
                    continue;
                }
            }

            //Вывод таблицы шифра простой замены
            System.out.println("Таблица шифра простой замены:");
            for (int i = 65; i < 91; i++) {
                System.out.print((char)i);
            }
            for (int i = 97; i < 123; i++) {
                System.out.print((char)i);
            }
            System.out.println();
            System.out.println(keyReplacement);
```

```
            //Ввод ФИО
            scan.nextLine();
            System.out.print("Введите ваше ФИО: ");
            name = scan.nextLine();

            //Шифрование ФИО шифром простой замены с ключом,
полученным ранее
            for (int i = 0; i < name.length(); i++) {
                nameReplacement +=
letterReplace(name.toCharArray()[i], keyReplacement);
            }
            System.out.print("ФИО после шифрования: ");
            System.out.println(nameReplacement);

            //Дешифрование ФИО шифром простой замены с ключом,
полученным ранее
            System.out.print("ФИО после дешифрования: ");
            for (int i = 0; i < nameReplacement.length(); i++) {

System.out.print(letterReplaceReverse(nameReplacement.toCharArray()
[i], keyReplacement));
            }
        }

        //Метод для замены буквы по шифру цезаря. Принимает букву
и величину сдвига, возвращает букву
        public static char letterShift(char letter, int shift){
            if((int)letter < 91 && (int)letter > 64) {
                if((int)letter + shift > 90) {
                    return (char)(letter - 26 + shift);
                } else {
                    return (char)(letter + shift);
                }
            } else if((int)letter < 123 && (int)letter > 96) {
                if((int)letter + shift > 122) {
                    return (char)(letter - 26 + shift);
                } else {
                    return (char)(letter + shift);
                }
            } else {
                return letter;
            }
        }

        //Метод замены буквы по шифру простой замены. Принимает
букву и ключ, возвращает букву
        public static char letterReplace(char letter, char[] key){
            if((int)letter < 91 && (int)letter > 64) {
```

```
                return key[(int)letter - 65];
            } else if((int)letter < 123 && (int)letter > 96) {
                return key[(int)letter - 97 + 26];
            } else {
                return letter;
            }
        }

        //Метод восстановления буквы по шифру простой замены.
Принимает букву и ключ, возвращает букву
        public static char letterReplaceReverse(char letter,
char[] key){
            if(((int)letter < 91 && (int)letter > 64) ||
((int)letter < 123 && (int)letter > 96)) {
                int index = 0;

                for (int i = 0; i < key.length; i++) {
                    if (key[i] == letter) index = i;
                }

                if (index < 26) {
                    return (char)(index + 65);
                } else {
                    return (char)(index - 26 + 97);
                }
            } else {
                return letter;
            }
        }
    }
```

Результат работы программы

```
Смещение = 24, оригинал текста: Utqdfqumfgjynh xzgxyhyzynts hhumjwx
Смещение = 25, оригинал текста: Tspceptlefixmg wyfwxmxyxmsr gmtlivw
Введите смещение, при котором оригинал текста имеет смылс: 3
Оригинальное сообщение: Polyalphabetic substitution ciphers
Таблица шифра простой замены:
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
????????????????K??????????VWX?Z??cd??g?ijk?mnqs???y?
Введите ваше ФИО: Misevich Arseniy Sergeevich
ФИО после шифрования: ?dnZ?dXc ?mnZidy ?Zm?ZZ?dXc
ФИО после дешифрования: ?ise?ich ?rseniy ?er?ee?ich
```

Вывод

Были изучены шифры перестановки и замены.