МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра информатики и систем управления

ОТЧЕТ

по лабораторной работе №2

по дисциплине

«Средства и методы защиты информации»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_ Капранов С. Н.\_\_

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_ Сорокин Е. А. \_\_\_\_

(подпись) (фамилия, и.,о.)

\_\_\_\_\_\_\_\_ 18-В1 \_\_\_\_\_\_\_

(шифр группы)

Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород 2021

**Задание №1.1**

Реализовать алгоритм шифрования данных «Шифрование методом гаммирования» по модулю N.

**Теория**

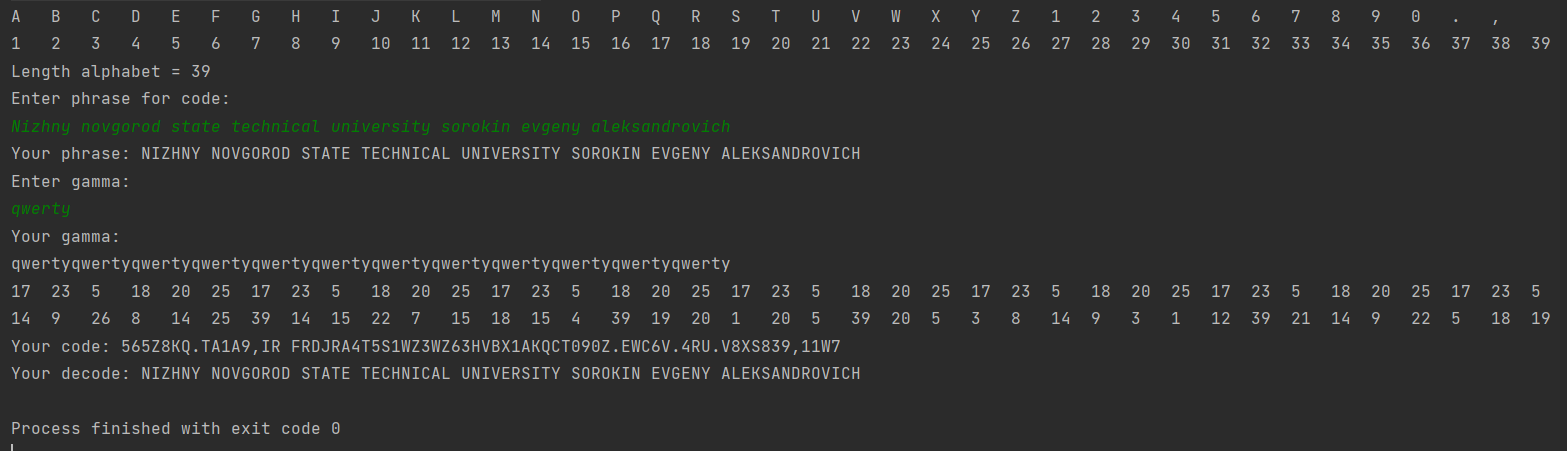
* Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, которая называется ***гаммой***

1) символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые затем складываются по модулю N, где N – число символов в алфавите, т.е.

TШ=(TО+TГ) mod N,

где ТШ, ТО ,ТГ – символы соответственно зашифрованного, исходного текста и гаммы.

**Пример работы программы**Nizhny novgorod state technical university sorokin evgeny aleksandrovich



**Код программы**

import java.util.Scanner;  
  
public class Main {  
  
 public static String convertGamma(String gamma, String phrase) {  
 StringBuilder strgamma = new StringBuilder(gamma);  
 int lenphrase = phrase.length();  
 int lengamma = strgamma.length();  
 for (int i = lengamma; i < lenphrase; i++) {  
 strgamma.append(strgamma.charAt(i%lengamma));  
 }  
 return strgamma.toString();  
 }  
  
 public static int[] convertToNumber(String phrase, String alphabet) {  
 StringBuilder strphrase = new StringBuilder(phrase);  
 StringBuilder stralphabet = new StringBuilder(alphabet);  
 int lenphrase = strphrase.length();  
 int lenalphabet = stralphabet.length();  
 int[] result = new int[lenphrase];  
 for (int i = 0 ; i < lenphrase; i++) {  
 for (int j = 0; j < lenalphabet; j++) {  
 if (strphrase.charAt(i) == stralphabet.charAt(j)) {  
 result[i] = j;  
 break;  
 }  
 }  
 }  
 return result;  
 }  
  
 public static String code(int[] phrase, int[] gamma, String alphabet) {  
 StringBuilder result = new StringBuilder();  
 int N = alphabet.length();  
 int len = phrase.length;  
 int[] res = new int[len];  
 for (int i = 0; i < len; i++) {  
 res[i] = (phrase[i]+1 + gamma[i]+1) % N;  
 if (res[i] == 0) {  
 res[i] = N;  
 }  
 }  
 StringBuilder alpha = new StringBuilder(alphabet);  
 for (int i = 0; i < len; i++) {  
 result.append(alpha.charAt(res[i]-1));  
 }  
 return result.toString();  
 }  
  
 public static String decode(int[] phrase, int[] gamma, String alphabet) {  
 StringBuilder result = new StringBuilder();  
 int N = alphabet.length();  
 int len = phrase.length;  
 int[] res = new int[len];  
 for (int i = 0; i < len; i++) {  
 res[i] = ((phrase[i]+1) - (gamma[i]+1) + N) % N;  
 if (res[i] == 0) {  
 res[i] = N;  
 }  
 }  
 StringBuilder alpha = new StringBuilder(alphabet);  
 for (int i = 0; i < len; i++) {  
 result.append(alpha.charAt(res[i] - 1));  
 }  
 return result.toString();  
 }  
  
  
 public static void main(String[] args) {  
  
 String phrase = "";  
 String gamma = "";  
 int[] resgamma;  
 int[] resphrase;  
 String result = "";  
 String alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890., ";  
  
 Scanner scan = new Scanner(System.in);  
  
 StringBuilder alpha = new StringBuilder(alphabet);  
 int length = alpha.length();  
 for (int i = 0; i < length; i++) {  
 System.out.print(alpha.charAt(i) + "\t");  
 }  
 System.out.println();  
 for (int i = 0; i < length; i++) {  
 System.out.print(i+1 + "\t");  
 }  
 System.out.println();  
  
 System.out.println("Length alphabet = " + alphabet.length());  
 System.out.println("Enter phrase for code: ");  
 phrase = scan.nextLine();  
 phrase = phrase.toUpperCase();  
 System.out.println("Your phrase: " + phrase);  
 System.out.println("Enter gamma: ");  
 gamma = scan.next();  
 System.out.println("Your gamma: ");  
  
 gamma = convertGamma(gamma, phrase);  
 System.out.println(gamma);  
 resgamma = convertToNumber(gamma.toUpperCase(), alphabet);  
  
 for (int re : resgamma) {  
 System.out.print(re+1 + "\t");  
 }  
 System.out.println();  
  
 resphrase = convertToNumber(phrase, alphabet);  
 for (int re : resphrase) {  
 System.out.print(re+1 + "\t");  
 }  
 System.out.println();  
  
 result = code(resphrase, resgamma, alphabet);  
 System.out.println("Your code: " + result);  
  
 int[] newres;  
 String newresstr;  
 newres = convertToNumber(result, alphabet);  
 newresstr = decode(newres, resgamma, alphabet);  
 System.out.println("Your decode: " + newresstr);  
  
 }  
}