Міністерство освіти і науки України

Національний університет «Львівська політехніка»



**Звіт**

до лабораторної роботи № 2

«Блокове шифрування інформації та шифри моноалфавітної заміни.»

з дисципліни

«Технології захисту інформації»

**Виконав:**

студент групи IT-23

Каськів В.П.

**Прийняв:**

Басюк Т.М.

Львів ­­– 2022

**Мета роботи:** Навчитися опрацьовувати (шифрувати та дешифрувати) файли з допомогою блокового шифрування інформації, методів моноалфавітної заміни та методу гамування.

Хід роботи

Написати програму на мові С++ (чи іншій за згодою викладача) яка виконує шифрування повідомлення методом накладення гамми. Гамма шифру і повідомлення вибираються згідно з варіантом.



Використовуючи алфавіт (табл. 1), дешифрувати повідомлення, яке зашифроване методом гамування. Гамма шифру та повідомлення вибираються згідно з варіантом.



Код програми

public class Lab2 {

public static void main(String[] args) throws IOException {

Scanner scan = new Scanner(System.in);

int choice;

do {

System.out.println("\nВибір: \n" +

"1. Тест із методички\n" +

"2. Тест варіанту 12\n" +

"3.Зашифрувати\n" +

"4.Дешифрувати\n" +

"5. Вихід з програми\n");

choice = scan.nextInt();

switch (choice) {

case 1: {

System.out.println("Test 1");

System.out.println(encrypt("ТИГР", "ЛЕГІОН\_27"));

System.out.println(decrypt("тигр", "хндитб4и3ї"));

break;

}

case 2:

{System.out.println("Варіант 12");

System.out.println(encrypt("БОРИМИР", "ЧОРАПНЕМОРЕ\_201"));

System.out.println(decrypt("ДИВОЗІР", "ДЗЧЦ\_РУ6ЇЗЇЕУНРЮ"));

break;}

case 3:

{

System.out.println("Шифрування\nВведіть гамму з клавіатури");

String gamma =scan.nextLine();

System.out.println("Введіть повідомлення");

String massage = scan.nextLine();

System.out.println(encrypt(gamma, massage));

break;

}

case 4:{

System.out.println("Дешифрування\nВведіть гамму з клавіатури");

String gamma =scan.nextLine();

System.out.println("Введіть повідомлення");

String massage = scan.nextLine();

System.out.println(decrypt(gamma, massage));

break;

}

case 5: System.exit(0);

default:

{System.out.println("Помилка ведіть знову\n");

break;

}

} // end of switch

} while (choice!=0); // end of loop

System.out.println();

}

public static String encrypt(String gamma, String massage) {

String res = "";

String abc = "абвгґдеєжзиіїйклмнопрстуфхцчшщьюя\_0123456789";

char[] chABC = abc.toCharArray();

char[] chMassage = massage.toLowerCase().toCharArray();// у нижньому регістрі

char[] chGamma = gamma.toLowerCase().toCharArray();

int[] m = new int[chMassage.length];

int[] g = new int[chGamma.length];

int[] c = new int[chMassage.length];

for (int i = 0; i < chGamma.length; i++) {

int index = 0;

while (chGamma[i] != chABC[index]) index++;

if (index > 43) {

index -= 43;

}

g[i] = index;

}

for (int i = 0; i < chMassage.length; i++) {

int index = 0;

while (chMassage[i] != chABC[index]) index++;

if (index > 43) {

index -= 43;

}

m[i] = index;

}

int index = 0;

for (int i = 0; i < m.length; i++) {

c[i] = (m[i] + g[index++]) % chABC.length;

if (index > chGamma.length - 1) index = 0;

}

for (int i = 0; i < c.length; i++) {

System.out.print(chABC[c[i] + 1]);

}

return "";

}

public static String decrypt(String gamma, String massage) {

String res = "";

String abc = "абвгґдеєжзиіїйклмнопрстуфхцчшщьюя\_0123456789";

char[] chABC = abc.toCharArray();

char[] chMassage = massage.toLowerCase().toCharArray();

char[] chGamma = gamma.toLowerCase().toCharArray();

int[] m = new int[chMassage.length];

int[] g = new int[chGamma.length];

int[] c = new int[chMassage.length];

for (int i = 0; i < chGamma.length; i++) {

int index = 0;

while (chGamma[i] != chABC[index]) index++;

if (index > 43) {

index -= 43;

}

g[i] = index;

}

for (int i = 0; i < chMassage.length; i++) {

int index = 0;

while (chMassage[i] != chABC[index]) index++;

if (index > 43) {

index -= 43;

}

m[i] = index;

}

int index = 0;

for (int i = 0; i < m.length; i++) {

c[i] = ((m[i] - g[index++]) + 43) % chABC.length;

if (c[i] == 0) c[i] = 44;

if (index > chGamma.length - 1) index = 0;

}

for (int i = 0; i < c.length; i++) {

System.out.print(chABC[c[i]]);

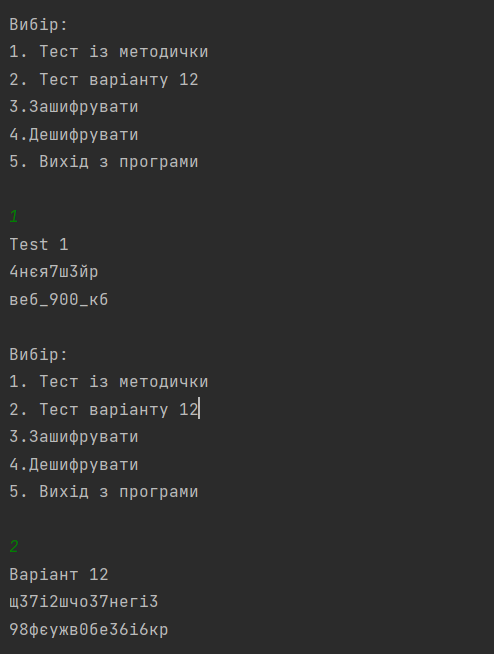
}

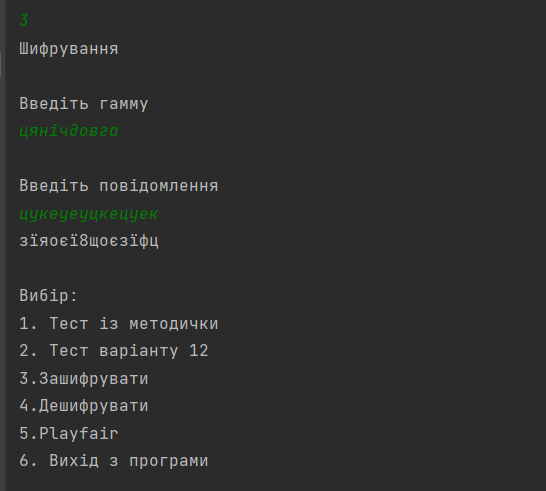
return "";

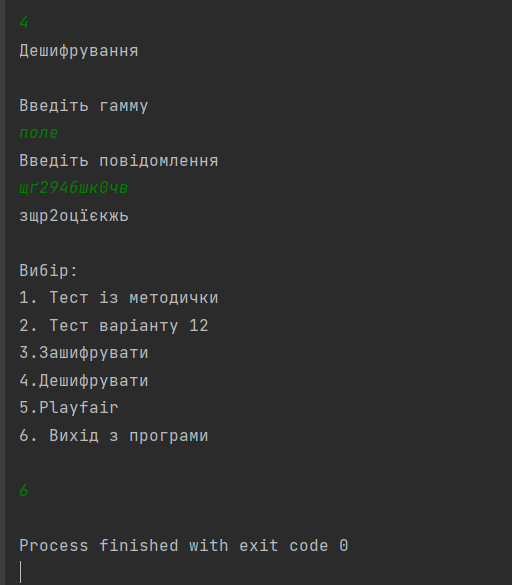
}

}

Результати виконання







Реалізована два методи в класі для шифрування та дешифрування методом гамування. Проведені тести для тесту верхнього на нижнього регістру.

**Висновок:** Під час виконання лабораторної роботи я навчився шифрувати та дешифрувати з допомогою блокового шифрування інформації, методів моноалфавітної заміни та методу гамування.