Міністерство освіти і науки України

Національний університет «Львівська політехніка»



**Звіт**

до лабораторної роботи № 1

«Симетричні методи шифрування інформації»

з дисципліни

«Технології захисту інформації»

**Виконав:**

студент групи IT-23

Каськів В.П.

**Прийняв:**

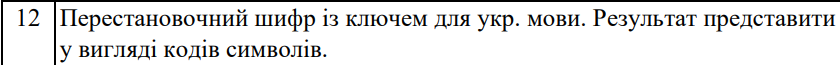
Пелещак І.Р

Львів ­­– 2022

**Мета роботи:** Навчитися опрацьовувати (шифрувати та дешифрувати) файли на основі методів симетричного шифрування..

**Хід роботи**

Написати програму на мові С++ (чи іншій за згодою викладача) яка виконує криптографічні перетворення (шифрування та дешифрування) над файлами за одним з методів симетричного шифрування відповідно до заданого варіанту приведеного в таблиці.



Виконання:

public String readFromFileToString() {

Path filePath = Path.of("D:/learn/semester 3/технологія захисту інформації/lab1/src/file.txt");

StringBuilder contentBuilder = new StringBuilder();

try (Stream<String> stream

= Files.lines(Paths.get(filePath.toUri()), StandardCharsets.UTF\_8)) {

//Read the content with Stream

stream.forEach(s -> contentBuilder.append(s).append("\n"));

} catch (IOException e) {

e.printStackTrace();

}

String fileContent = contentBuilder.toString();

return fileContent;

}

public void writeToFile(String string) throws IOException {

String path = "D:/learn/semester 3/технологія захисту інформації/lab1/src/file2.txt";

Files.write(Paths.get(path), string.getBytes());

char firstChar = string.charAt(0);

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

// access each character

int a = string.charAt(i);

System.out.print(a + ", ");

}

}

public static String encoder(char[] key, String mes) throws UnsupportedEncodingException {

String encoded1 = "";

String encoded = new String(encoded1.getBytes("Cp1251"), "UTF-8");

boolean[] arr = new boolean[26];

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

if (key[i] >= 'А' && key[i] <= 'Я') {

// To check whether the character is inserted

// earlier in the encoded string or not

if (arr[key[i] - 65] == false) {

encoded += (char) key[i];

arr[key[i] - 65] = true;

}

} else if (key[i] >= 'а' && key[i] <= 'я') {

if (arr[key[i] - 97] == false) {

encoded += (char) (key[i] - 32);

arr[key[i] - 97] = true;

}

}

}

// This loop inserts the remaining

// characters in the encoded string.

for (int i = 0; i < 26; i++) {

if (arr[i] == false) {

arr[i] = true;

encoded += (char) (i + 65);

}

}

return encoded;

}

// This function will decode the message

public static String decipheredIt(String msg, String input) throws UnsupportedEncodingException {

String plaintext0 = "абвгґдеєжзиіїйклмнопрстуфхцчшщьюя";

String decipher0 = "";

String plaintext = new String(plaintext0.getBytes("Cp1251"), "UTF-8");

String decipher = new String(decipher0.getBytes("Cp1251"), "UTF-8");

Map<Character, Integer> enc = new HashMap<>();

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

enc.put(input.charAt(i), i);

}

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

if (msg.charAt(i) >= 'А' && msg.charAt(i) <= 'Я') {

int pos = enc.get((char) (msg.charAt(i) - 32));

decipher += plaintext.charAt(pos);

} else if (msg.charAt(i) >= 'а' && msg.charAt(i) <= 'я') {

int pos = enc.get(msg.charAt(i));

decipher += plaintext.charAt(pos);

} else {

decipher += msg.charAt(i);

}

}

return decipher;

}

**Результати:**

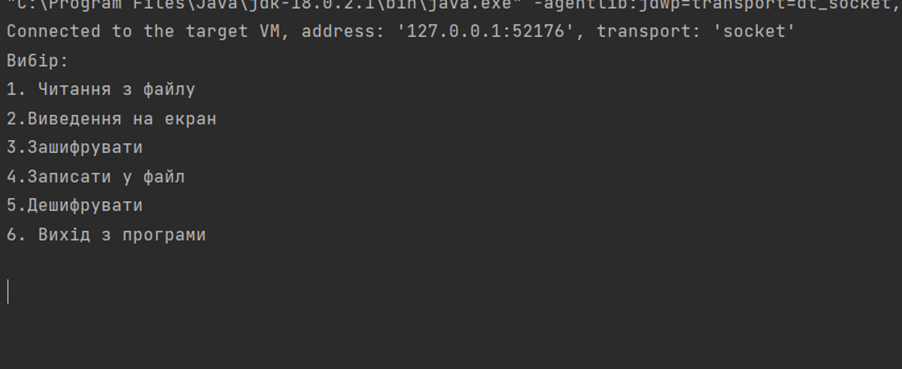
****

Рисунок 1 Компіляція програми

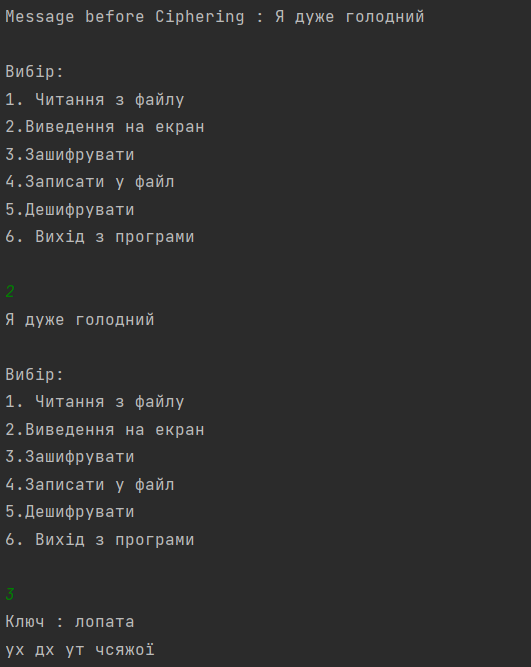
****

Рисунок 2 Читання з файлу та шифрування методом перестановки з ключем

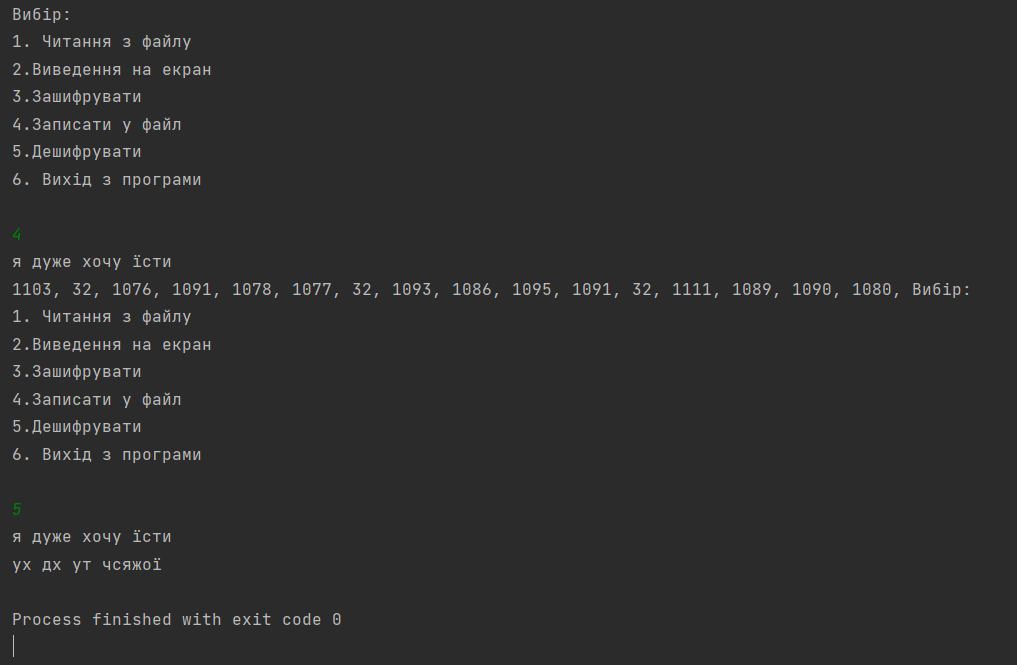
****

Рисунок 3 Демонстрація коду символів та запис у файл

В першу чергу були створені 2 методи один, для читання з файлу, а інший для запису у файл. Далі реалізовано перестановочний метод для String, яку було передано в патерн. Патерни використовуються для роботи з кирилицею. Знаходження найменшого значення по ключу хеш мапи та передача у перший рядок

Map<Character, Integer> enc = new HashMap<>();

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

enc.put(input.charAt(i), i);

}

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

if (msg.charAt(i) >= 'А' && msg.charAt(i) <= 'Я') {

int pos = enc.get((char) (msg.charAt(i) - 32));

decipher += plaintext.charAt(pos);

Записано отриманий шифр у файл та виведено на екран код символів.

**Висновок:** Під час виконання лабораторної роботи я засвоїв методику та вробив практичні навички роботі з опрацьовування (шифрувати та дешифрувати) файли на основі методів симетричного шифрування.