Akademia Nauk Stosowanych Teoretyczne i technologiczne podstawy multimediów – IS rok 3	
Imię i Nazwisko: Emilian Kochanek	**Grupa:** L2
Data: 07.10.2022	**Symbol:** TiTPM_01

Program przez mnie napisany opiera się o szyfrowanie algorytmem RSA, gdzie wykorzystywane jest klucz publiczny do zaszyfrowania wiadomości oraz klucz prywatny do odszyfrowania wiadomości.

```
public class SzyfrownieRsa {
    public static void main(String[] args){
        Scanner cin = new Scanner(System.in);
        System.out.println("Podaj tekst do zaszyfowania: ");
        String password = cin.nextLine();
        ArrayList<Integer> asciiArray = convertToAscii(password);
        System.out.println("Zakodowane: " + asciiArray);
        System.out.println("Odkodowane: " + decryptWithPrivateKey(asciiArray));
    }
```

Na początku podajemy treść jaką chcemy zaszyfrować. Następnie jest ono dzielone na pojedyncze wyrazy i zamieniane na kod ASCII.

```
private static ArrayList<Integer> convertToAscii(String password){
    ArrayList<Integer> asciiArray = new ArrayList<>();
    for(int i = 0; i<password.length(); i++){
        asciiArray.add((int) password.toUpperCase().charAt(i));
    }
    return encryptWithRsa(asciiArray);
}
```

Taka tablica z wartościami ASCII przekazywana jest do funkcji, która podnosi wartości przez pewien współczynnik i jest wyznaczana reszta z dzielenia pewnego modulo. Takie wartości zwracane są użytkownikowi jako zaszyfrowana wiadomość.

```java
private static ArrayList<Integer> encryptWithRsa(ArrayList<Integer> asciiArray){
    int k = 391;
    long s = 3;
    ArrayList<Integer> encryptedPassword = new ArrayList<>();
    for (Integer password:asciiArray) {
        double enc = Math.pow(password, s);
        encryptedPassword.add(((int)enc%k));
    }
    return encryptedPassword;
}
```

Tak zaszyfrowana wiadomość przekazywana jest do funkcji odszyfrowującej, która podnosi wartość zaszyfrowanej wiadomości o wartość klucza prywatnego i wyznacza resztę z dzielenia przez to samo modulo, co było wykorzystywane w szyfrowaniu. Tymi wartościami są znaki zapisane w systemie ASCII.

```java
private static String decryptWithPrivateKey(ArrayList<Integer> encryptedPassword){
    int d = 235;
    BigInteger k = new BigInteger( val: "391");
    ArrayList<Integer> decryptedPassword = new ArrayList<>();
    for (Integer password:encryptedPassword){
        BigInteger dec = new BigInteger(String.valueOf(password));
        dec = dec.pow(d).mod(k);
        decryptedPassword.add(dec.intValue());
    }
    return convertToString(decryptedPassword);
}
```

Te wartości są zamieniane na odpowiednie znaki i łączone w jednego stringa. String ten jest hasłem, które podał użytkownik na początku.

```java
private static String convertToString(ArrayList<Integer> decryptedPassword){
    StringBuilder password = new StringBuilder();
    for(Integer ascii:decryptedPassword){
        password.append((char) ascii.intValue());
    }
    return password.toString();
}
```

PRZYKŁAD:

```
Podaj tekst do zaszyfowania:
Teoretyczne i technologiczne podstawy multimediow
Zakodowane: [339, 69, 379, 58, 69, 339, 387, 84, 176, 269, 69, 315, 363, 315, 339, 69,
Odkodowane: TEORETYCZNE I TECHNOLOGICZNE PODSTAWY MULTIMEDIOW
```