Rok akademicki 2022 -2023, półsemestr letni

TEST 3

**Zadanie 1**

Podać przykład szyfrowania szyfrem Vernama (szyfr idealny) .
Napisać program szyfrujący szyfrem Vernama np.w C lub Pythonie.

```
public class Main {
    public static void main(String[] args) throws Exception {
        Zad3 zad3 = new Zad3();
        char[] datagram=new char[28];
            datagram="SchowalemKluczPodWycieraczka".toCharArray(); // dont use UTF-8

        char[] key=new char[28];
            key="@1To2JesT3Moj4TajnY5Klucz6@!".toCharArray();

        char[] zaszyfrowany = zad3.vernam(  datagram, key );
        char[] cos = zad3.vernam(  datagram, zaszyfrowany );

        System.out.println(  zaszyfrowany  ); // R< E9x!□       N<?>9 V"         L+@
        System.out.println( cos ); //@1To2JesT3Moj4TajnY5Klucz6@!  coś = klucz

    }

public class Zad3 {

    public char[] vernam( char[] datagram, char[] key ) throws Exception {
        if ( datagram.length!=key.length ) throw new Exception("niezgodne długości");
        char[] chars = new char[ datagram.length ];
        for (int i=0;i<datagram.length;i++) {
            int A=datagram[i];
            int K=key[i];
            chars[i] = (char) (A^K);
        }
    return chars;
    }

    String bytesToString ( char[] chars ){
        return String.valueOf(chars);
    }

}
```

**Zadanie 2**

Wiadomo, że Alicja i Bob posługują się szyfrem Vernama. P
rzechwycono wiadomość jawną , gdzie  i szyfrogram , gdzie . Znaleźć klucz ;  jakim posłużyli się Alicja i Bob.

wykonanie szyfrowania Vernama dla szyfrogramu i jawnego zwraca (ujawnia) klucz
dla każdego $m_i$, $k_i$ i $c_i$
$m_i$ XOR $k_i$ = $c_i$
$m_i$ XOR $c_i$ = $k_i$

**Zadanie 3**
Podaj przykład szyfrowania i deszyfrowania szyfrem Vigenere'a. Napisać przykładowy program w Pythonie szyfrowania i deszyfrowania plików tekstowych szyfrem Vigenere'a.

**Zadanie 4**
Podać przykład systemu kryptograficznego ElGamala dla ciała ***F19*** oraz podać przykład szyfrowania i deszyfrowania tym szyfrem.

**Zadanie 5**
Podać przykład systemu kryptograficznego RSA dla n=11*13 i podać przykład szyfrowania i deszyfrowania tym szyfrem.

**Zadanie 6**
Pokazać, że w systemie kryptograficznym RSA rozkład liczby n na czynniki pierwsze łamie RSA.

**Zadanie 7**
Podać przykład systemu kryptograficznego Rabina dla n=13*17 i podać przykład szyfrowania i deszyfrowania tym szyfrem.

**Zadanie 8**
Ile razy trzeba wykonać protokół uwierzytelniania Fiata-Shamira by prawdopodobieństwo oszustwa było mniejsze od $10^{-100}$

**Zadanie 9**
Wykorzystując bibliotekę Open SSL napisać skrypt szyfrujący szyfrem AES i skrypt deszyfrujący szyfrem AES (w trybach CBC, CFB, ECB, OFB). Podać przykłady szyfrowania dla różnych plików i kluczy.

**Zadanie 10**
Pokazać, że jeśli NWD(a,m)=1 (gdzie a z ***Z***, m z ***N, m>=2***) to dla dowolnego n z ***Z***

$$a^n \equiv a^{[n]\varphi(m)} \pmod m$$ - równoważne z pierścieniem ***Zm***

Krótko, ale niezbyt jasno: „jeśli podstawa potęgi i m są względnie pierwsze to na wykładnikach pracujemy modulo *φ(m)*".