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.

Alfabet : wielkie znaki ASCII numerowane od (0 do 26) (A=65ASCII, Z=90ASCII)

Klucz (cykliczny): „ADMIN"

Tekst: „ATAKOSWICIE"

```
   ATAKOSWICIE
   ADMINADMINA
+  -----------  A+A= 65-65 + 65-65 = 0+0=0 %26 =0
   AWMSBSZUKVE
```

```
   public char[] Vigenere( char[] datagram, char[] key ) throws Exception {
        char[] chars = new char[ datagram.length ];
        for (int i=0, j=0; i<datagram.length;i++,j++) {
            int A=datagram[i]; A=A-65;
            if ( j>key.length ) {j=0;}
            int K=key[j];      K=K-65;
            chars[i] = (char) (((A+K) %26)+65);
        }
        return chars;
    }

           String fileName = "myFile.txt";
            char[] chars = zad3.fileToCharAry(fileName);
            char[] key = "ADMIN".toUpperCase().toCharArray();

            char[] C = zad3.Vigenere(chars, key);

            String fileNameOut = "myFile.out";
            zad3.charAryToFile(fileNameOut, C );
```

```
myFile.txt
ATAKOSWICIE

myFileOut.txt
AWMSBSZUKVE
```

```
// nudny kod czytania pliku
```

```
public char[] fileToCharAry( String fileName ){
    try {
        File f = new File( fileName );
        int len = (int) f.length();
        char[] c = new char[len];
        FileReader fr = new FileReader( fileName );
        fr.read( buf );
        fr.close();
        return buf;
    } catch (Throwable e) { throw new RuntimeException(e); }
}
public void charAryToFile( String fileName , char[] buf ){
    try {
        FileWriter fw = new FileWriter( fileName );
        fw.write( buf );
        fw.close();
    } catch (Throwable e) { throw new RuntimeException(e); }
}
```

```
MOJPLIKTEKSTOWY
```

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.

Szyfr z kluczem niesymetrycznym, czyli mamy klucz publiczny i klucz prywatny.
Krok 1: wybranie liczb p i q, oraz małej liczby e=10-12 bitów losowe względnie pierwsze.
obliczamy n=p*q;
obliczamy ø(n)= ø((p-1)(q-1))=(p-1)*(q-1);
ø(n) - jest elementem prywatnym; a n publicznym;

Krok 2: klucz publiczny to n oraz e
Krok 3: obliczenie $d=e^{-1}(\text{mod } ø(n))$ - klucza prywatnego.
Krok 4: obliczenie szyfrogramu: $C=m^e \text{ (mod n)}$; gdzie m - tekst jawny, C szyfrowany;
Krok 5: odszyfrowanie: $m=C^d \text{ (mod n)}$

Zadanie 6
Pokazać, że w systemie kryptograficznym RSA rozkład liczby n na czynniki pierwsze łamie RSA.
klucz publiczny to znane n (oraz e);
klucz prywatny wymaga znajomości ø(n); a to można wyliczyć -> ø(n) = ø(a*b) = ø((p-1)(q-1));
jeśli znamy rozkład n na a i b to wyliczymy ø(n);
dalej policzymy $d=e^{-1}(\text{mod } ø(n))$;
a d jest kluczen prywatnym.
Zatem bezpieczeństwo klucza prywatnego polega na trydności znalezienia a i b (lub p i q)

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

niech n=p*q gdzie p=3(mod 4) i q=3(mod 4);
funkcja Rabina $f(x) = x^2 \text{(mod n)}$ i jest podobna do szyfru RSA przy wybraniu liczby e=2

szyfrowanie $C = m^e \text{ (mod n)}$
deszysfowanie $m=C^d \text{ (mod n)}$ gdzie $d=e^{-1}(\text{mod } ø(n))$

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

pojedyncza runda powtórzona k razy zapewnia, że prawdopodobieństwo fałszywego uwierzytelnienia nie przekracza 2^{-k} razy.
a zatem ponieważ 10 < 2*2*2*2 to:
$(2*2*2*2)^{-100} = 2^{-103}$
zatem musimy zastosować k=103 rundy.

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.

```
                Rsa4096 rsa = new Rsa4096( “C:\\Users\\John\\Desktop\\AlgorytmyIBezpieczenstwo\\CodeInJava\\OpenS-
SL\\private_key_rsa_4096_pkcs8-generated.pem”, “C:\\Users\\John\\Desktop\\AlgorytmyIBezpieczenstwo\\CodeInJava\\
OpenSSL\\public_key_rsa_4096_pkcs8-exported.pem” );


                String expected = getFileAsString(“C:\\Users\\John\\Desktop\\AlgorytmyIBezpieczenstwo\\CodeInJava\\
OpenSSL\\file_unencrypted.txt”);
                String encryptedAndEncoded = getFileAsString(“C:\\Users\\John\\Desktop\\AlgorytmyIBezpieczenstwo\\
CodeInJava\\OpenSSL\\file_encrypted_and_encoded.txt”);

                System.out.println( rsa.encryptToBase64(expected) );
                //String actual = rsa.decryptFromBase64( encryptedAndEncoded );
                }
```

// crypted:

```
Y60tZhMXQh92BQ867kqHDaDSHcvw90s++zovApSutzrDXd3W3K00z6bPs4J7hUIGGKAJ4kkpDDGyyIBRSaYHwwU+e08UoYoFui-
FRyV3pi95Eyg2rlyHawvQZ5zx6LjMCbtcPeCVT0vBR2LZNCcIvS+19gb5R1WgcnhFRq3O3em2QAFIIOc9CwPrCG6059fCYtnZuy-
cdOuUoQOLYex+XKKL4N5lHOn+9e96LR9YBqt25jPaWmoMWiW5kVzmN4ZbP8Dc4GJjWz7IVgsZMZzvKN4B+8K/LoEBieehVQgS/
TGKSbwEEuG2uh20Q4Jq7vxl5wZXmBQtpDum5ul0YrunHP1yubqYZ2m9ul9qZ4GJiFccxOPkt57hQJ8ANdL1wDQ3I56/bMwEmJ94CyL+iA2NIr8ZCTQ-
JFO6KHaeH7wsQzzinu9YTk7+4nmF4nCw31U1EFE9GxpOGI+Xe++tDXLK3pQxOc2Uahn/X793jhcGM1234RCqRq5RRF+ibuUeFHMIR+OL4VjqyYZD-
15KZ/51BTiNdnX+SAoDbUaPVJhrk7rXGil1kFSPpPM3vGlKAaBR5deg99/6ghA2bviu+Ja0q5h59Y/NKTzb2iIAev344b+jpjcVGqaxAD/DvkC-
MO5MSVJ06I4U7fFvVfogU4dgR5T+hQYgbGp+cG2sMLpiszdx/w=
```


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

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

Krótko, ale niezbyt jasno:
„jeśli podstawa potęgi i m są względnie pierwsze to na wykładnikach pracujemy modulo $\varphi(m)$”.

jeśli podstawy a i m względnie pierwsze w pierścieniu to ich wymnożenie da jakieś “przesunięcie” b
pomnożenie tego przesunięcia o b*m mod(m)=b

a zatem oczywiste że
jeśli a^n = b (mod m)
    to b*m (mod m) = b;