TUGAS 8

PRAKTIKUM KRIPTOGRAFI

Disusun oleh:

Muhamad Rumi Rifai - 140810220026

PROGRAM STUDI S-1 TEKNIK INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PADJADJARAN

JATINANGOR

2024

Soal

1. Kerjakan secara manual Enkripsi, dan Dekripsi algoritma RSA, dengan diketahui :
   p = 19, q = 13
   Plaintext: HIMATIF
2. Enkripsikan huruf paling depan nama kalian (KAPITAL) dengan terlebih dahulu mengkonversikan ke ASCII (M: 77 = 01001101). Sebagai kunci gunakan huruf terakhir nama kalian (HURUF KECIL) yang telah dikonversi ke ASCII dan tambahkan 01 di belakangnya (l: 108 = 01101100+01 = 0110110001)
   (Contoh: Pt = M, Ct = l)
3. Dekripsikan kembali hingga didapatkan kedua huruf tersebut (M dan l), dengan mengerjakan soal yang sama dan tuliskan juga langkah pengerjaannya.

Jawab

1. Key Generation
   n = 19*13 = 247
   m = (19-1)*(13-1) = 216
   Cari e yang relatif dengan 216, didapat e = 11

   Hitung d = e^-1 mod m
   gcd(11,216) = 1
   216 = 11***19**+7
   11 = 7***1**+4
   7 = 4***1**+3
   4 = 3***1**+2
   3 = 1***3**+0

   t0 = 0; t1 = 1
   t2 = (0-(19*1)) mod 216
      = (-19) mod 216
      = 197
   t3 = (1-(1*197)) mod 216
      = (-196) mod 216
      = 20
   t4 = (197-(1*20)) mod 216
      = 177 mod 216
      = 177
   t5 = (20-(1*177)) mod 216
      = (-157) mod 216
      = 59
   e^-1 = 59
   Maka d = 59

```
Publik (e,n) = (11,247)
Private (d,n) = (59,247)

Enkripsi
Plaintext: [H,I,M,A,T,I,F] = [72,73,77,65,84,73,70]
e = 11; n = 247
C1 = 72^11 mod 247 = 41
C2 = 73^11 mod 247 = 161
C3 = 77^11 mod 247 = 77
C4 = 65^11 mod 247 = 221
C5 = 84^11 mod 247 = 50
C6 = 73^11 mod 247 = 161
C7 = 70^11 mod 247 = 21
Ciphertext: [41,161,77,221,50,161,21]

Dekripsi
d = 59; n = 247
M1 = 41^59  mod 247 = 72
M2 = 161^59 mod 247 = 73
M3 = 77^59  mod 247 = 77
M4 = 221^59 mod 247 = 65
M5 = 50^59  mod 247 = 84
M6 = 161^59 mod 247 = 73
M7 = 21^59  mod 247 = 70
Plaintext: [72,73,77,65,84,73,70] = HIMATIF
```

2. Plaintext : R (ASCII: 82 -> 01010010)
   Master Key : i (ASCII: 105 -> 01101001 + 01 -> 0110100101)
   P10   : 3 5 2 7 4 10 1 9 8 6
   P8   : 6 3 7 4 8 5 10 9
   P4   : 3 4 3 1

   Mencari K1
   Key = 0 1 1 0 1 0 0 1 0 1
   Acak sesuai P10
   P10 : 3 5 2 7 4 10 1 9 8 6
   Key : 1 0 1 0 1 1 0 0 0 0
   Bagi 2 P10, geser kiri hasil P10 sebanyak 1 kali
   Ls1 : 1 0 1 0 1 || 1 0 0 0 0
   Ls1 diacak dengan P8, hasilnya adalah K1
   P8 : 6 3 7 4 8 5 10 9
   K1 : 0 1 1 0 0 1 0 0

   Mencari K2
   Ls1 digeser 2 kali menjadi Ls2
   Ls2 : 1 0 1 0 1 || 0 0 0 1 0
   Acak hasil Ls dengan P8, hasilnya adalah K2
   P8 : 6 3 7 4 8 5 10 9
   K2 : 0 1 0 0 1 0 1 0

   Enkripsi
   Plaintext 8 bit diacak dengan IP
   Plaintext : 0 1 0 1 0 0 1 0
   IP   : 2 6 3 1 4 8 5 7
                1 0 0 0 0 1 1 0
   Ambil 4 bit **paling kanan**, lakukan expansion permutation (Ep)
   lalu XOR dengan K1
   Ep   : 4 1 2 3 2 3 4 1
         : 0 0 0 1 1 1 0 1
   K1   : 0 1 1 0 0 1 0 0
          ———————————————— XOR
           0 1 1 1 1 0 0 1

   0 1 1 1 1 0 0 1
   S0 : 0111 S1 : 1001
   Rn : 11   Rn : 00
   Cn : 10   Cn : 01

```
  0 1 2 3
0 1 0 3 2
1 3 2 1 0
2 0 2 1 3
3 3 1 3 2
Hasil = 11

  0 1 2 3
0 0 1 2 3
1 2 0 1 3
2 3 0 1 0
3 2 1 0 3
Hasil = 10
```

Hasil Box diacak oleh P4 dan di XOR oleh 4 bit **kiri dari hasil ip di awal** 1110

```
P4 : 3 4 3 1
   : 1 0 0 1
     1 1 1 0
    —--------- XOR
     0 1 1 1
```

Gabungkan dengan 4 bit **kanan hasil IP** lalu lakukan Swap (SW)

```
0 0 1 0 1 0 0 1
SW : 1 0 0 1 0 0 0 0
```

Lanjutkan langkah serupa dengan K2

```
Sw: 1 0 0 1 0 0 0 0
```

Ambil 4 bit **paling kanan,** lakukan expansion permutation (Ep) lalu XOR dengan K2

```
Ep : 4 1 2 3 2 3 4 1
   : 1 0 0 0 0 0 1 0
   : 0 1 0 1 1 1 0 0
    —---------------- XOR
     1 1 0 1 1 1 1 0

S0 : 1110  S1 : 1110
Rn : 10    Rn : 00
Cn : 11    Cn : 01
```

```
  0 1 2 3
0 1 0 3 2
1 3 2 1 0
2 0 2 1 3
3 3 1 3 2
Hasil = 11

  0 1 2 3
0 0 1 2 3
1 2 0 1 3
2 3 0 1 0
3 2 1 0 3
Hasil = 01
```

Hasil Box diacak oleh P4 dan di XOR oleh 4 bit **kiri dari hasil IP di awal** 1101

```
P4 : 2 4 3 1
   : 1 0 1 1
   : 1 1 0 1
    ---------- XOR
     0 1 1 0

IP^-1 : 4 1 3 5 7 2 8 6
CT    : 0 1 1 0 0 1 0 1
```

3. Ubah 8-bit plaintext/ciphertext dengan initial permutation IP
   CT : 0 1 1 0 0 1 0 1
   IP : 2 6 3 1 4 8 5 7
      : 1 1 0 0 0 1 1 0

   Ambil 4 bit **bagian kanan,** lalu lakukan Expansion Permutation (Ep)
   Ep : 4 1 2 3 2 3 4 1
      : 1 0 0 0 0 1 1 0
   K2 : 0 1 0 1 0 1 1 0
       ———————————————— XOR
        1 1 0 1 0 0 0 0

   Bagi hasil XOR menjadi 2 bagian
   S0: 1101   S1: 0000
   Rn: 10   Rn: 00
   Cn: 11   Cn: 00

     0 1 2 3
   0 1 0 3 2
   1 3 2 1 0
   2 0 2 1 3
   3 3 1 3 2
   Hasil = 11

     0 1 2 3
   0 0 1 2 3
   1 2 0 1 3
   2 3 0 1 0
   2 3 0 1 0
   3 2 1 0 3
   Hasil = 00

   Hasil S-Box diacak oleh P4
   1101
   P4 : 2 4 3 1
      : 1 1 0 0
      : 0 1 1 0 (4 bit kiri dari IP)
       ————————— XOR
        1 0 1 0

   Gabungkan dengan 4 bit **kanan hasil IP**
   1 0 1 0 0 0 0 1
   SW: 1 0 1 0 0 1 1 0

Ambil 4 bit bagian **kanan,** lakukan Expansion Permutation
Ep : 4 1 2 3 2 3 4 1
   : 1 0 1 1 0 0 1 0
K1 : 0 1 1 0 0 1 0 0
    —————————————— XOR
     1 1 0 1 0 1 0 0

Bagi hasil XOR menjadi 2 bagian
S0 : 1101 S1 : 0100
Rn : 11   Rn : 00
Cn : 10   Cn : 10

  0 1 2 3
0 1 0 3 2
1 3 2 1 0
2 0 2 1 3
3 3 1 3 2
Hasil = 11

  0 1 2 3
0 0 1 2 3
1 2 0 1 3
2 3 0 1 0
3 2 1 0 3
Hasil = 10

Hasil S-Box diacak oleh P4
1110
P4 : 2 4 3 1
   : 1 0 1 1
   : 1 0 1 0 (4 bit kiri dari hasil SW)
    ——————— XOR
     0 0 0 1 (Gabungkan dengan 4 bit **kanan hasil SW**)

IP^-1 : 4 1 3 5 7 2 8 6
PT   : 0 1 0 1 0 0 1 0 (R)

0 1 0 1 0 0 1 0 -> 82 -> R
i -> Master Key - 01 -> 0110100101 - 01 -> 105 -> i