Nama Kelompok

Angga Kresnabayu (140810160001)

Patricia Joane (140810160065)

M. Islam Taufikurahman (140810160062)

Buat secara manual soal-soal berikut:  
a. Elgamal: p = 37, g = 3, x = 2, k = 10.  
 Plaintext: INFORMATIKA  
b. RSA: p = 3, q = 7, *e* & *d* pilih sendiri. Plaintext: UNPAD

Jawab

a. Elgamal

Diketahui:

p = 37 g = 3 x =2 k = 10

1. Pembangkitan Kunci Publik

Rumus: *y* = *gx* mod *p*

y = 32 mod 37 = 9

1. Penghitungan Enkripsi

Rumus:

C1 = *gk* mod *p*  
C2 = *Mi* • *yk* mod *p*

Plaintext: INFORMATIKA

a) I = 8 e) R = 17 i) K = 10

b) N = 13 f) M = 12

c) F = 5 g) A = 0

d) O = 14 h) T = 19

C1 = *gk* mod *p*

= 310 mod 37 = 34

C2 (I) = *Mi* • *yk* mod *p*  
 = 8 (9)10 mod 37

= 8 (9) mod 37

= 72 mod 37

= 35  
C2 (N) = *Mi* • *yk* mod *p*  
 = 13 (9)10 mod 37

= 13 (9) mod 37

= 117 mod 37

= 6

C2 (F) = *Mi* • *yk* mod *p*  
 = 5 (9)10 mod 37

= 5 (9) mod 37

= 45 mod 37

= 8

C2 (O) = *Mi* • *yk* mod *p*  
 = 14 (9)10 mod 37

= 14 (9) mod 37

= 126 mod 37

= 15  
C2 (R) = *Mi* • *yk* mod *p*  
 = 17 (9)10 mod 37

= 17 (9) mod 37

= 153 mod 37

= 5

C2 (M) = *Mi* • *yk* mod *p*  
 = 12 (9)10 mod 37

= 12 (9) mod 37

= 108 mod 37

= 34

C2 (A) = *Mi* • *yk* mod *p*  
 = 0 (9)10 mod 37

= 0 (9) mod 37

= 0 mod 37

= 0  
C2 (T) = *Mi* • *yk* mod *p*  
 = 19 (9)10 mod 37

= 19 (9) mod 37

= 171 mod 37

= 23

C2 (K) = *Mi* • *yk* mod *p*  
 = 10 (9)10 mod 37

= 10 (9) mod 37

= 90 mod 37

= 16

Chippertext: {(34,35), (34,6), (34,8), (34,15), (34,5), (34,34), (34,0), (34,23), (34,35),(34,16),(34,0)}

1. Penghitungan Dekripsi

Rumus:

C1x = (C1)x mod *p*

M = C2 \* (C1x)-1 mod *p*.

C1x = (34)2 mod 37 = 9

Mencari 9-1 = ?

GCD(9,37)

37 = 9\*4 + 1 T2=T0 –T1\*A1 = 0 – 1\*4 = -4 mod 37 = 33

Maka 9-1 = 33

M(1) = C2 \* (C1x)-1 mod *p*  
 = 35 \* 9-1 mod 37

= 35 \* 33 mod 37

= 1155 mod 37

= 8  
M(2) = C2 \* (C1x)-1 mod *p*  
 = 6 \* 9-1 mod 37

= 6 \* 33 mod 37

= 198 mod 37

= 13  
M(3) = C2 \* (C1x)-1 mod *p*  
 = 8 \* 9-1 mod 37

= 8 \* 33 mod 37

= 264 mod 37

= 5

M(4) = C2 \* (C1x)-1 mod *p*  
 = 15 \* 9-1 mod 37

= 15 \* 33 mod 37

= 495 mod 37

= 14  
M(5) = C2 \* (C1x)-1 mod *p*  
 = 5 \* 9-1 mod 37

= 5 \* 33 mod 37

= 165 mod 37

= 17

M(6) = C2 \* (C1x)-1 mod *p*  
 = 34 \* 9-1 mod 37

= 34 \* 33 mod 37

= 1122 mod 37

= 12  
M(7) = C2 \* (C1x)-1 mod *p*  
 = 0 \* 9-1 mod 37

= 0 \* 33 mod 37

= 0 mod 37

= 0  
M(8) = C2 \* (C1x)-1 mod *p*  
 = 23 \* 9-1 mod 37

= 23 \* 33 mod 37

= 759 mod 37

= 19  
M(9) = C2 \* (C1x)-1 mod *p*  
 = 16 \* 9-1 mod 37

= 16 \* 33 mod 37

= 528 mod 37

= 10

Konversi ke huruf:  
a) 8 = I e) 17 = R i) 10 = K

b) 13 = N f) 12 = M

c) 5 = F g) 0 = A

d) 14 = O h) 19 = T

Plaintext: INFORMATIKA

b. RSA

Diketahui:

p = 3, q = 7, *e* & *d* pilih sendiri. misalkan e = 5

1. Hitung nilai n

n = p \* q

n = 3 \* 7

n = 21

1. Hitung nilai m

m = (3 – 1)(7 – 1)

m = (2)(6)

m =.12

1. Hitung *d*, kunci privat, sedemikian agar (d \* e) mod m = 1.

(d \* e) mod m = 1

(d \* e \* e-1) mod m = 1\*e-1

d = e-1 mod m

d = 5-1 mod 12

d = 5

Mencari 5-1 = ?

GCD(5,12)

12 = 5\*2 + 2 T2 = T0 –T1\*A1 = 0 – 1\*2 = -2 mod 12 = 10

5 = 2\*2 + 1 T3 = T1 – T2\*A2 = 1 – 10\*2 = -19 mod 12 = 5

Maka 5-1 = 5

1. Maka diperoleh:

* kunci publik adalah pasangan (e,n) = (5,21)
* kunci private adalah pasangan (d,m) = (5,12)

1. Enkripsi

Rumus: Ci = Mie mod n

Plaintext: UNPAD

a) U = 85 c) P = 80 e) D = 68

b) N = 78 d) A = 65

Ci (U) = Mie mod n

= 855 mod 21

= 15 mod 21

= 1

Ci (N) = Mie mod n

= 785 mod 21

= 155 mod 21

= 15

Ci (P) = Mie mod n

= 805 mod 21

= 175 mod 21

= 5

Ci (A) = Mie mod n

= 655 mod 21

= 25 mod 21

= 11

Ci (D) = Mie mod n

= 685 mod 21

= 55 mod 21

= 17

Cippertext: {1,15,5,11,17}

1. Dekripsi

Rumus: Mi = Cie mod m

Ci (1) = Cie mod m

= 15 mod 12

= 1 mod 12

= 1

Ci (15) = Mie mod m

= 155 mod 12

= 759375 mod 12

= 3

Ci (5) = Mie mod m

= 55 mod 12

= 3125 mod 12

= 5

Ci (11) = Mie mod m

= 115 mod 12

= 161051 mod 12

= 11

Ci (17) = Mie mod m

= 175 mod 12

= 1419857 mod 12

= 5

Plaintext: {1,3,5,11,5}

HAH!! MENGAPA ENKRIPSI DAN DEKRIPSINYA TIDAK KEMBALI? DIKARENAKAN NILAI M DAN N. LAH KOK BISA? NILAI M DAN N TIDAK SAMA SEKALI MENCAKUP NILAI ASCII. GIMANA MAKSUDNYA? JADI GINI, SEDERHANANYA NILAI TERSEBUT DAPAT KITA ENKRIP, PADA SAAT DEKRIPSI NILAI M ITU ADALAH 12, BERAPAPUN NILAI PERPANGKATAN CHIPERTEXT MAKA AKAN SELALU MENGHASILKAN 0 SAMPAI 11 SEDANGKAN NILAI PLANTEXT YANG KITA ENKRIP ITU NILAI RANGENYA MELEBIHI ITU. MANTAP!!