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: $y = g^x \bmod p$

$y = 3^2 \bmod 37 = 9$

2. Penghitungan Enkripsi

Rumus: $C_1 = g^k \bmod p$ $C_2 = M_i \bullet y^k \bmod p$

Plaintext: INFORMATIKA

a) I = 8
b) N = 13
c) F = 5
d) O = 14
e) R = 17
f) M = 12
g) A = 0
h) T = 19
i) K = 10

$C_1 = g^k \bmod p$
$= 3^{10} \bmod 37 = 34$

C_2 (I) = $M_i \bullet y^k \bmod p$
= 8 $(9)^{10}$ mod 37
= 8 (9) mod 37
= 72 mod 37
= 35

C_2 (N) = $M_i \bullet y^k \bmod p$
= 13 $(9)^{10}$ mod 37
= 13 (9) mod 37
= 117 mod 37
= 6

C_2 (F) = $M_i \bullet y^k \bmod p$
= 5 $(9)^{10}$ mod 37
= 5 (9) mod 37
= 45 mod 37
= 8

C_2 (O) = $M_i \bullet y^k \bmod p$
= 14 $(9)^{10}$ mod 37
= 14 (9) mod 37
= 126 mod 37
= 15

C_2 (R) = $M_i \bullet y^k \bmod p$
= 17 $(9)^{10}$ mod 37
= 17 (9) mod 37
= 153 mod 37
= 5

C_2 (M) = $M_i \bullet y^k \bmod p$
= 12 $(9)^{10}$ mod 37
= 12 (9) mod 37
= 108 mod 37
= 34

C_2 (A) = $M_i \bullet y^k \bmod p$
= 0 $(9)^{10}$ mod 37
= 0 (9) mod 37
= 0 mod 37
= 0

C_2 (T) = $M_i \bullet y^k \bmod p$
= 19 $(9)^{10}$ mod 37
= 19 (9) mod 37
= 171 mod 37
= 23

C_2 (K) = $M_i \bullet y^k \bmod p$
= 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)}

3. Penghitungan Dekripsi

Rumus:
$C_1^x = (C_1)^x \bmod p$
$M = C_2 * (C_1^x)^{-1} \bmod p$.

$C_1^x = (34)^2 \bmod 37 = 9$

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

$M(1) = C_2 * (C_1^x)^{-1} \bmod p$
$= 35 * 9^{-1} \bmod 37$
$= 35 * 33 \bmod 37$
$= 1155 \bmod 37$
$= 8$

$M(2) = C_2 * (C_1^x)^{-1} \bmod p$
$= 6 * 9^{-1} \bmod 37$
$= 6 * 33 \bmod 37$
$= 198 \bmod 37$
$= 13$

$M(3) = C_2 * (C_1^x)^{-1} \bmod p$
$= 8 * 9^{-1} \bmod 37$
$= 8 * 33 \bmod 37$
$= 264 \bmod 37$
$= 5$

$M(4) = C_2 * (C_1^x)^{-1} \bmod p$
$= 15 * 9^{-1} \bmod 37$
$= 15 * 33 \bmod 37$
$= 495 \bmod 37$
$= 14$

$M(5) = C_2 * (C_1^x)^{-1} \bmod p$
$= 5 * 9^{-1} \bmod 37$
$= 5 * 33 \bmod 37$
$= 165 \bmod 37$
$= 17$

$M(6) = C_2 * (C_1^x)^{-1} \bmod p$
$= 34 * 9^{-1} \bmod 37$
$= 34 * 33 \bmod 37$
$= 1122 \bmod 37$
$= 12$

$M(7) = C_2 * (C_1^x)^{-1} \bmod p$
$= 0 * 9^{-1} \bmod 37$
$= 0 * 33 \bmod 37$
$= 0 \bmod 37$
$= 0$

$M(8) = C_2 * (C_1^x)^{-1} \bmod p$
$= 23 * 9^{-1} \bmod 37$
$= 23 * 33 \bmod 37$
$= 759 \bmod 37$
$= 19$

$M(9) = C_2 * (C_1^x)^{-1} \bmod p$
$= 16 * 9^{-1} \bmod 37$
$= 16 * 33 \bmod 37$
$= 528 \bmod 37$
$= 10$

Konversi ke huruf:

a) 8 = I
b) 13 = N
c) 5 = F
d) 14 = O
e) 17 = R
f) 12 = M
g) 0 = A
h) 19 = T
i) 10 = K

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
2. Hitung nilai m

m = (3 – 1)(7 – 1)
m = (2)(6)
m =.12

3. 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
4. Maka diperoleh:
   - kunci publik adalah pasangan (e,n) = (5,21)
   - kunci private adalah pasangan (d,m) = (5,12)
5. Enkripsi

Rumus: Ci = Mi^e mod n

Plaintext: UNPAD

a) U = 85
b) N = 78
c) P = 80
d) A = 65
e) D = 68

Ci (U) = Mi^e mod n
= 85^5 mod 21
= 1^5 mod 21
= 1

Ci (N) = Mi^e mod n
= 78^5 mod 21
= 15^5 mod 21
= 15

Ci (P) = Mi^e mod n
= 80^5 mod 21
= 17^5 mod 21
= 5

Ci (A) = Mi^e mod n
= 65^5 mod 21
= 2^5 mod 21
= 11

Ci (D) = Mi^e mod n
= 68^5 mod 21
= 5^5 mod 21
= 17

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

6. Dekripsi

Rumus: $Mi = Ci^e \bmod m$

Ci (1) $= Ci^e \bmod m$

$= 1^5 \bmod 12$

$= 1 \bmod 12$

$= 1$

Ci (15) $= Mi^e \bmod m$

$= 15^5 \bmod 12$

$= 759375 \bmod 12$

$= 3$

Ci (5) $= Mi^e \bmod m$

$= 5^5 \bmod 12$

$= 3125 \bmod 12$

$= 5$

Ci (11) $= Mi^e \bmod m$

$= 11^5 \bmod 12$

$= 161051 \bmod 12$

$= 11$

Ci (17) $= Mi^e \bmod m$

$= 17^5 \bmod 12$

$= 1419857 \bmod 12$

$= 5$

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!!