TUGAS PRAKTIKUM KRIPTORAFI

1. Elgamal

P = 37; g = 3 ; x = 2; k = 10.

PT = MENCINTAIMU

M = 12; E = 4; N = 13; C = 2; I = 8; T = 19; A= 0; U = 20.

Encryption

$Y = g^x \bmod p$

$Y = 3^x \bmod 37$

$Y = \bmod 37$

Y = 9.

$C_1 = g^k \bmod p$

$C_1 = 3^{10} \bmod 37$

$C_1 = 34$

$C_2(1) = M \times Y^k \bmod p$

$C_2(1) = 12 \times 9^{10} \bmod 37 = 34$

$C_2(2) = 4 \times 9^{10} \bmod 37 = 36$

$C_2(3) = 13 \times 9^{10} \bmod 37 = 6$

$C_2(4) = 2 \times 9^{10} \bmod 37 = 18$

$C_2(5) = 8 \times 9^{10} \bmod 37 = 35$

$C_2(6) = 19 \times 9^{10} \bmod 37 = 23$

$C_2(7) = 0 \times 9^{10} \bmod 37 = 0$

$C_2(8) = 20 \times 9^{10} \bmod 37 = 32$

CT = (34,34),(34,46),(34,6),(34,18),(34,18),(34,35),(34,23),(34,0),(34,32)

Decryption

$C_1^x = (C_1)^x \bmod p$

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

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

$= 34 * 9^{-1} \bmod 37$

gcd(37,9)

37 = 9*4 + 1

to = 0

t1 = 1

t2 = 0 – 1 (4) mod 37 = -4 mod 47 = 33

M(1) = 34 * 33 mod 37 = 12 (M)

M(2) = 36 * 33 mod 37 = 4 (E)

M(3) = 6 * 33 mod 37 = 13 (N)

M(4) = 18 * 33 mod 37 = 2 (C)

M(5) = 35 * 33 mod 37 = 8 (I)

M(6) = 23 * 33 mod 37 = 19 (T)

M(7) = 0 * 33 mod 37 = 0 (A)

M(8) = 32 * 33 mod 37 = 20 (U)

PT = MENCINTAIMU

RSA

PT = TEMAN

P = 17; q = 11;

n = p*q = 17*11 = 187.

m = (p – 1) x (q – 1)

m = (17-1) x (11-1)

m = 160

e = 17

gcd(17,160)

160 = 17 * 9 + 7

17 = 7 * 2 + 3

7 = 3 * 2 + 1

T0 = 0

T1 = 1

T2 = 0 – 1(9) mod 160 = 151

T3 = 1 – 151(2) mod 160 = 19

T4 = 151 – 19(2) mod 160 = 113

$d = e^{-1} \bmod m$

d = 113 mod 160 = 113

Kunci public = (17,187); Privat = (117, 187).

Enkripsi

$Ci = Mi^e \bmod n$

T = 19; e = 4; M = 12; A = 0; N = 13;

$C1 = 19^{17} \bmod 187 = 2$

$C2 = 4^{17} \bmod 187 = 38$

$C3 = 12^{17} \bmod 187 = 12$

$C4 = 0^{17} \bmod 187 = 0$

$C5 = 13^{17} \bmod 187 = 183$

Dekripsi

$Mi = Ci^d \bmod n$

CT = 2,38,12,0,183

$M1 = 2^{113} \bmod 187 = 19$

$M2 = 38^{113} \bmod 187 = 4$

$M3 = 12^{113} \bmod 187 = 12$

$M4 = 0^{113} \bmod 187 = 0$

$M5 = 183^{113} \bmod 187 = 13$