TUGAS 6

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

Kerjakan secara manual Enkripsi & Dekripsi algoritma Elgamal, dengan diketahui :

p = 37, g = 3, x = 2, k = 15.

Plaintext: KRIPTOGRAFI

Jawaban

Plaintext:

[K,R,I,P,T,O,G,R,A,F,I] = [10,17,8,15,19,14,6,17,0,5,8]

p = 37, g = 3, x = 2, k = 15

Kunci Publik (y): g^x mod p = 3^2 mod 37 = 9

- Enkripsi E(x)
  - Mencari nilai C1
    - C1 = g^k mod p = 3^15 mod 37 = 11
  - Mencari nilai C2
    - C2 = M . y^k mod p = M . 9^15 mod 37
      - C2(1) = 10 . 9^15 mod 37 = 26
      - C2(2) = 17 . 9^15 mod 37 = 22
      - C2(3) = 8 . 9^15 mod 37 = 6
      - C2(4) = 15 . 9^15 mod 37 = 2
      - C2(5) = 19 . 9^15 mod 37 = 5
      - C2(6) = 14 . 9^15 mod 37 = 29
      - C2(7) = 6 . 9^15 mod 37 = 23
      - C2(8) = 17 . 9^15 mod 37 = 22
      - C2(9) = 0 . 9^15 mod 37 = 0
      - C2(10) = 5 . 9^15 mod 37 = 13
      - C2(11) = 8 . 9^15 mod 37 = 6
  - Hasil Enkripsi (CipherText):
    [(11,26),(11,22),(11,6),(11,2),(11,5),(11,29),(11,23),(11,22),(11,0),(11,13),(11,6),]

- Dekripsi D(x)
  - Mencari nilai C1^x
    - C1^x = 11^2 mod 37 = 10
  - Mencari nilai M
    - M = C2 . (C1^x)^-1 mod p
      - M(1) = 26 . 10^-1 mod 37 = 10
      - M(2) = 22 . 10^-1 mod 37 = 17
      - M(3) = 6 . 10^-1 mod 37 = 8
      - M(4) = 2 . 10^-1 mod 37 = 15
      - M(5) = 5 . 10^-1 mod 37 = 19
      - M(6) = 29 . 10^-1 mod 37 = 14
      - M(7) = 23 . 10^-1 mod 37 = 6
      - M(8) = 22 . 10^-1 mod 37 = 17
      - M(9) = 0 . 10^-1 mod 37 = 0
      - M(10) = 13 . 10^-1 mod 37 = 5
      - M(11) = 6 . 10^-1 mod 37 = 8
  - Hasil Dekripsi D(x):

    [10,17,8,15,19,14,6,17,0,5,8] = KRIPTOGRAFI