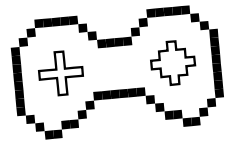
Praktikum Kriptografi

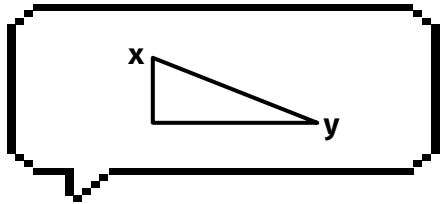
Pertemuan - 06

Topik: Elgamal

Review



- **Vigenere Cipher**
- **Autokey**
- **Permutasi**



01

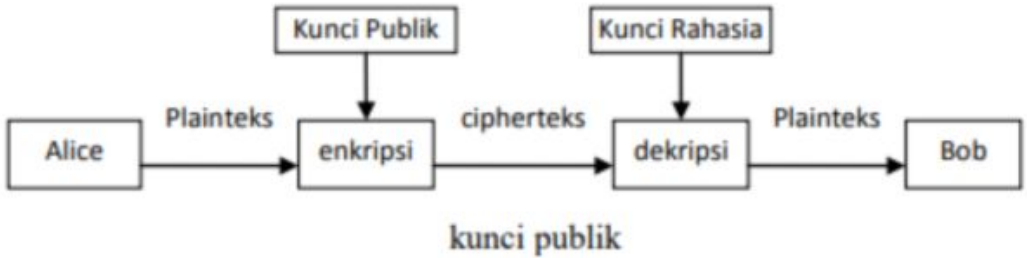
Elgamal

Elgamal

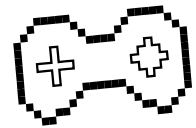
Algoritma ElGamal ditemukan oleh ilmuwan Mesir, yaitu Taher ElGamal pada tahun 1985, merupakan algoritma kriptografi kunci publik.

Algoritma Elgamal terdiri dari 3 proses :

Proses pembentukan kunci, enkripsi, dan dekripsi.



Key Generation



1. **Pilih sembarang bilangan prima p**

   Ambil bilangan p yang cukup besar

2. **Pilih bilangan acak g, dengan g < p**

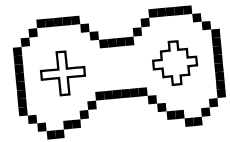
3. **Pilih bilangan acak x (untuk private key)**

   dengan $1 \leqslant x \leqslant p - 1$

   (ada referensi lain yang menulis p– 2 [R Munir]).

4. **Hitung kunci publik y = g^x mod p.**

Enkripsi



1. Mengambil nilai **k secara acak**, dengan k bernilai

   $1 \leqslant k \leqslant p - 1$ (juga ada yang menulis sampai p-2)

2. Menghitung nilai **C1 dan C2**, yang mana :

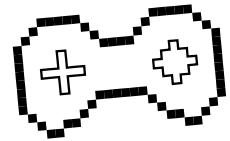
   $C1 = g^k \bmod p$

   $C2 = M.y^k \bmod p$

3. Jadi, ciphertext C yang dikirimkan adalah satu pasangan dengan dua nilai C_1 dan C_2 (terpisah).

   Ada juga yang menuliskan bahwa plaintext disusun terlebih dahulu dalam blok-blok tertentu.

Contoh Enkripsi



Diketahui :

p = 29
g = 2
k = 11

Private key :
x = 6
PT : HALO

Jawab :

Pembangkitan Kunci Publik

$y = g^x \bmod p$

$y = 2^6 \bmod 29$

$= 6$

Perhitungan Enkripsi :

H=7, A=0, L=11, O=14

$C_1 = g^k \bmod p$

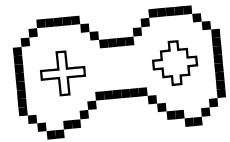
$= 2^{11} \bmod 29 = 18$

$C_2 = M.y^k \bmod p$

$C_2\ (1) = 7.(6)^{11} \bmod 29 = 5$
$C_2\ (2) = 0.(6)^{11} \bmod 29 = 0$
$C_2\ (3) = 11.(6)^{11} \bmod 29 = 12$
$C_2\ (4) = 14.(6)^{11} \bmod 29 = 10$

CT = (18,5),(18,0),(18,12),(18,10)

Dekripsi



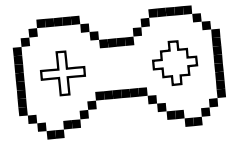
1. Menghitung nilai C_1^x , yang mana :

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

2. Menghitung nilai $M = C_2(C_1^x)^{-1} \bmod p$

Jadi, plaintext yg dikirimkan adalah satu huruf dari pasangan chipertext C_1 dan C_2 yaitu nilai **M**

Contoh Dekripsi



Diketahui :
p = 29
g = 2
k = 11

Private key :
x = 6

CT =
(18,5),(18,0),
(18,12),(18,10)

Perhitungan Dekripsi :

$C_1^x = (18)^6 \bmod 29 = 9$

$M(1) = C_2 * (C_1^x)^{-1} \bmod p$
$= 5 * (9)^{-1} \bmod 29 = \mathbf{7}$

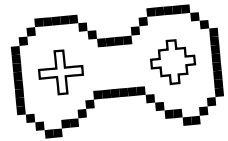
$M(2) = C_2 * (C_1^x)^{-1} \bmod p$
$= 0 * (9)^{-1} \bmod 29 = \mathbf{0}$

$M(3) = C_2 * (C_1^x)^{-1} \bmod p$
$= 12 * (9)^{-1} \bmod 29 = \mathbf{11}$

$M(4) = C_2 * (C_1^x)^{-1} \bmod p$
$= 10 * (9)^{-1} \bmod 29 = \mathbf{14}$

Hasil : HALO

Tugas



1. Kerjakan secara manual Enkripsi & Dekripsi algoritma Elgamal, dengan diketahui :
2. p = 37, g = 3, x = 2, k = 15.

   Plaintext: KRIPTOGRAFI

Format: Tugas6_NPM.pdf

Deadline Tugas: H-1 Praktikum Berikutnya, 23.59

Thank You!!

Kalau misalkan ada pertanyaan,
yaudah tanya aja

Praktikum Kriptografi 2023