SISTEM KRIPTOGRAFI KUNCI PUBLIK ELGAMAL DALAM Z_p^*

Oleh
Rosdiana Kumalasari
013114027

ABSTRAK

Tujuan dari penulisan skripsi ini adalah untuk mengetahui proses penentuan kunci, proses enkripsi dan proses dekripsi pada sistem kriptografi kunci publik ElGamal dalam Z_p^*, dan menyusun program simulasinya dengan menggunakan MATLAB.

Sistem kriptografi kunci publik ElGamal dalam Z_p^* diawali dengan proses penentuan kunci yang dilakukan oleh penerima pesan, yaitu menentukan bilangan prima p yang cukup besar secara random, generator g, bilangan bulat a, dengan $1 \le a \le p-2$, kemudian menghitung $b \equiv g^a \pmod p$. Hasil dari proses ini adalah kunci publik (p, g, b) dan kunci pribadi a. Proses selanjutnya adalah enkripsi yang dilakukan oleh pengirim pesan menggunakan kunci publik penerima pesan. Pada proses enkripsi *plaintext* direpresentasikan ke dalam bilangan bulat $x, x \in \{1, 2, \ldots, p-1\}$ kemudian memilih bilangan bulat s, dengan $1 \le s \le p-2$, selanjutnya menghitung $c_1 \equiv g^s \pmod p$ dan $c_2 \equiv x \cdot (b)^s \pmod p$. Hasil dari proses ini adalah *ciphertext* $c = (c_1, c_2)$. Proses dekripsi dilakukan oleh penerima pesan menggunakan kunci pribadinya. Pada proses ini *plaintext* x didapatkan kembali dengan menghitung $\left(c_1^{\,a}\right)^{-1} \cdot c_2 \pmod p$. Proses-proses pada sistem kriptografi kunci publik ElGamal dalam Z_p^* dapat diselesaikan dengan lebih mudah dan cepat menggunakan program simulasi sistem kriptografi kunci publik ElGamal dalam Z_p^*.

Proses penentuan kunci menghasilkan kunci publik (p, g, b) dan kunci pribadi a. Dalam proses enkripsi *plaintext* x yang akan dikirimkan diubah ke dalam bentuk *ciphertext* $c = (c_1, c_2)$ dengan menghitung $e_K(x, s) = (c_1, c_2)$ di mana $c_1 \equiv g^s \pmod p$ dan $c_2 \equiv x \cdot b^s \pmod p$. Untuk mendapatkan *plaintext* x kembali, pada proses dekripsi dihitung $d_K(c_1, c_2) \equiv c_2\left(c_1^{\,a}\right)^{-1} \pmod p$. Program simulasi yang dibuat dalam MATLAB *function* dapat dipanggil melalui MATLAB *Command Window* dengan cara menuliskan *Kunci*(bb, ba), *Enkripsi*(p, g, b, s, x) dan *Dekripsi*(p, a, c).