Generalisasi Sistem Kriptografi ElGamal Menggunakan Konsep Matriks Nonsingular

Maxrizal *[1], Maya Saftari[2], Marna[3], Sujono[4]
[1,3,4]Program Studi Sistem Informasi, STMIK Atma Luhur, Pangkalpinang
[2]Program Studi Teknik Informatika, STMIK Atma Luhur, Pangkalpinang
e-mail: *[1]maxrizal@atmaluhur.ac.id , [2]mayasaftari@atmaluhur.ac.id , [3]marna@atmaluhur.ac.id , [4]sujono@atmaluhur.ac.id

Abstrak

Sistem kriptografi ElGamal yang diperkenalkan oleh Taher ElGamal bekerja pada ring $\mathbb{Z}_p$. Penelitian ini merupakan penelitian studi literatur yang bertujuan memperkenalkan generalisasi dari sistem kriptografi ElGamal menggunakan konsep matriks nonsingular atas $\mathbb{Z}_p$. Hasil menunjukkan bahwa plaintext pada sistem kriptografi ElGamal yang diusulkan dimodelkan menjadi blok-blok bertingkat yaitu dimodelkan pada blok-blok berdasarkan panjang karakter p dan ukuran matriks G yang dipilih. Penggunaan blok-blok bertingkat pada plaintext dan perpangkatan matriks pada enkripsi akan menghasilkan ciphertext yang lebih acak dari sistem kriptografi ElGamal.

Kata kunci—Generalisasi ElGamal, matriks nonsingular, kriftografi matriks nonsingular.

Abstract

The ElGamal cryptosystem introduced by Taher ElGamal works in the ring $\mathbb{Z}_p$. This research is a literature study that aims to introduce a generalization of the ElGamal cryptosystem using the concept of a nonsingular matrix of $\mathbb{Z}_p$. The results show that the proposed plaintext on the ElGamal cryptosystem is modeled into multilevel blocks which are modeled on blocks based on character length p and the size of the selected matrix G . The use of multilevel blocks in the plaintext and the power of the matrix in encryption will produce a more random ciphertext from the ElGamal cryptosystem.

Keywords—Elgamal generalization, the nonsingular matrix, cryptosystem nonsingular matrix.

1. PENDAHULUAN

Sistem kriptografi ElGamal dikembangkan oleh Taher ElGamal pada tahun 1985. Kekuatan sistem kriptografi ini terletak pada sulitnya memfaktorkan logaritma diskrit [1], [2]. Sistem kriptografi ini menggunakan kunci asimetri dan bekerja pada ring $\mathbb{Z}_p$ (ring atas modular bilangan bulat prima). Pada sistem kriptografi ini, pihak penerima pesan harus membangkitkan pasangan kunci (kunci privat dan publik) dan melakukan deskripsi. Sedangkan pihak pengirim pesan cukup melakukan enkripsi dengan kunci publik yang diterima dari pihak penerima pesan.
Berdasarkan [1], [2], pihak penerima pesan memilih suatu generator $g \in \mathbb{Z}_p$ dan menghitung $y = g^x \bmod p$. Output dari proses membangkitkan pasangan kunci akan menghasilkan kunci publik (y, g, p) dan kunci privat (x). Selanjutnya, pihak penerima pesan mengirim kunci publik ke pihak pengirim pesan. Jika terdapat pesan *(plaintext)* m yang akan dikirim maka pihak

pengirim pesan akan melakukan enkripsi dengan persamaan $a = g^k \bmod p$ dan $b = y^k \, m \bmod p$. Selanjutnya *ciphertext* (a,b) dikirim ke pihak penerima pesan. Untuk mengembalikan *plaintext*, pihak penerima pesan menghitung $m = ba^{-x} \bmod p$.

Kunci utama sistem kriptografi ElGamal terdapat pada penggunaan ring $\mathbb{Z}_p$. Jika diperhatikan lebih lanjut, ring $\mathbb{Z}_p$ dapat digeneralisasikan pada matriks nonsingular atas $\mathbb{Z}_p$ [3]–[5]. Untuk itu, pada makalah ini akan diperkenalkan generalisasi dari sistem kriptografi ElGamal menggunakan konsep matriks nonsingular atas $\mathbb{Z}_p$.

2. METODE PENELITIAN

Penelitian ini adalah penelitian studi literatur. Definisi dan proses algoritma ElGamal dikaji melalui referensi [1], [2]. Sedangkan sifat-sifat umum pada matriks nonsingular dikaji melalui referensi [4], [5]. Sedangkan referensi [3] merupakan pandangan lain mengenai matriks-matriks nonsingular atas $\mathbb{Z}_p$ yang telah diterapkan pada modifikasi *RSA*.

3. HASIL DAN PEMBAHASAN

3.1 Sistem Kriptografi ElGamal

Sistem kriptografi ElGamal menggunakan suatu grup siklis G dan bilangan prima p yang besar [1], [2]. Pada sistem ini juga dipilih suatu generator $g \in \mathbb{Z}_p$. Proses pembangkitan pasangan pasangan kunci, enkripsi dan deskripsi disajikan sebagai berikut:

Tabel 1 Sistem Kriptografi Elgamal

Pihak penerima pesan	Algoritma pembangkit pasangan kunci	$y = g^x \bmod p$ kunci publik (y, g, p) kunci privat (x)
Pihak pengirim pesan	Enkripsi	$a = g^k \bmod p$ $b = y^k \, m \bmod p$
Pihak penerima pesan	Deskripsi	$m = ba^{-x} \bmod p$

Perhatikan bahwa suatu *plaintext* M akan diblok-blok sesuai dengan panjang karakter p yang dipilih. Misalkan terdapat $P = 234567184213$ dan dipilih suatu bilangan prima $p = 2357$ maka akan terdapat $m_1 = 234$, $m_2 = 567$, $m_3 = 184$ dan $m_3 = 213$.

3.2 Sifat-Sifat Matriks Nonsingular

Suatu matriks yang memiliki determinan nol disebut matriks singular [4], [5]. Jika suatu matriks A singular maka matriks A tidak memiliki invers. Matriks nonsingular didefinisikan sebagai matriks yang memiliki invers atau determinannya tak nol. Berdasarkan [5], suatu matriks A dikatakan matriks singular jika terdapat suatu baris atau kolom nol pada matriks A. Matriks A juga dikatakan singular jika terdapat dua baris atau kolom yang sebanding pada matriks. Lebih lanjut, matriks A bersifat singular jika terdapat suatu baris atau kolom yang merupakan kombinasi linear dari baris atau kolom yang lain. Perhatikan ketiga matrik singular berikut ini.

$$A_1=\begin{bmatrix}1&0&5\\3&0&2\\4&0&10\end{bmatrix}, A_2=\begin{bmatrix}1&2&5\\3&3&15\\4&4&20\end{bmatrix}, A_3=\begin{bmatrix}1&2&7\\4&5&18\\1&1&5\end{bmatrix}$$

Matriks A_1 terdapat kolom nol. Kolom ketiga matriks A_2 merupakan lima kali kolom pertama matriks A_2. Pada matriks A_3 berlaku $K_3 = 3K_1 + 2K_2$ (K_i adalah kolom ke-i pada matirks A_3). Untuk itu, agar matriks dapat dibalik (memiliki invers) atau nonsingular maka harus dihindari ketiga syarat atau kondisi di atas dalam pembentukan matriks G pada sistem kriptografi ElGamal yang diusulkan.

3.3 Generalisasi Sistem Kriptografi ElGamal Menggunakan Matriks Nonsingular

Proses generalisasi sistem kriptografi Elgamal yang diusulkan dimulai dengan pemilihan suatu matriks G yang nonsingular. Selanjutnya, dibentuk persamaan $Y = G^x \bmod p$. Selanjutnya dibentuk $A = G^k \bmod p$ dan $B = Y^k M \bmod p$. Perhatikan bahwa

$$\begin{aligned} A^{-x}B &= \left(G^k\right)^{-x}\left(Y^k\right)M \\ &= \left(G^k\right)^{-x}\left(\left(G^x\right)^k\right)M \\ &= G^{-kx}G^{kx}M \\ &= M \end{aligned}$$

Perhatikan bahwa $G^{-kx}G^{kx} = I$ karena G merupakan matriks nonsingular atas $\square_p$. Secara umum, generalisasi sistem kriptografi yang diusulkan adalah:

Tabel 2 Sistem Kriptografi Elgamal Yang Diusulkan

Pihak penerima pesan	Algoritma pembangkit pasangan kunci	$Y = G^x \bmod p$ kunci publik (Y, G, p) kunci privat (x)
Pihak pengirim pesan	Enkripsi	$A = G^k \bmod p$ $B = Y^k \,\mathrm{M} \bmod p$
Pihak penerima pesan	Deskripsi	$M = A^{-x}B \bmod p$

Selanjutnya, pada sistem kriptografi ElGamal, suatu *plaintext* M akan diblok-blok sesuai dengan panjang karakter p yang dipilih. Misalkan terdapat $M = 234567184213$ dan dipilih suatu bilangan prima $p = 2357$ maka akan terdapat $m_1 = 234$, $m_2 = 567$, $m_3 = 184$ dan $m_3 = 213$. Pada sistem kriptografi yang diusulkan, blok-blok plainteks yang ada akan diblok-blok lagi berdasarkan ukuran matriks nonsingular G yang dipilih. Misalkan dipilih matriks $G = \begin{bmatrix}12&3\\27&4\end{bmatrix}$ maka bentuk *plaintext* yang ada adalah $M_1 = \begin{bmatrix}234&567\\184&213\end{bmatrix}$. Dengan demikian, sistem kriptografi yang diusulkan menggunakan konsep blok bertingkat yaitu dimodelkan pada blok-blok berdasarkan panjang karakter p dan ukuran matriks G yang dipilih. Selanjutnya, penggunaan

blok-blok bertingkat pada *plaintext* dan perpangkatan matriks atas bilangan bulat x pada saat enkripsi akan menghasilkan *ciphertext* yang lebih acak dari sistem kriptografi ElGamal.

3.4 Contoh Generalisasi Sistem Kriptografi ElGamal

Algoritma Pembangkit Pasangan Kunci

Alice akan berkirim pesan ke Bob. Pertama kali, Bob membangkitkan pasangan kunci dengan memilih $x = 5$, $p = 2357$ dan $G = \begin{bmatrix} 456 & 124 & 12 \\ 231 & 5 & 1507 \\ 421 & 511 & 1000 \end{bmatrix}$. Selanjutnya, dibentuk persamaan matematis,

$$Y = G^x \bmod p = \begin{bmatrix} 1396 & 1694 & 1568 \\ 1427 & 1036 & 1812 \\ 986 & 932 & 2116 \end{bmatrix} \bmod 2357 \ .$$

Bob memperoleh kunci publik $\left(Y = \begin{bmatrix} 1396 & 1694 & 1568 \\ 1427 & 1036 & 1812 \\ 986 & 932 & 2116 \end{bmatrix}, G = \begin{bmatrix} 456 & 124 & 12 \\ 231 & 5 & 1507 \\ 421 & 511 & 1000 \end{bmatrix} \right)$ dan kunci privat $(x = 5)$.

Enkripsi

Alice menerima kunci publik dari Bob. Alice memilih $k = 12$ dan menghitung persamaan $A = G^k \bmod p = \begin{bmatrix} 157 & 804 & 213 \\ 1921 & 654 & 1421 \\ 546 & 2198 & 247 \end{bmatrix} \bmod 2357$. Misalkan Alice akan mengirimkan sebuah pesan $M = 41212212323151115023451110045678612423456111145665432 1$. Karena $p = 2357$ memiliki 4 karakter digit dan matriks kunci privat G berukuran 3×3 maka P dimodelkan blok-blok bertingkat menjadi $M_1 = \begin{bmatrix} 412 & 122 & 123 \\ 231 & 511 & 150 \\ 234 & 511 & 100 \end{bmatrix}$ dan $M_2 = \begin{bmatrix} 456 & 786 & 124 \\ 234 & 561 & 111 \\ 456 & 654 & 321 \end{bmatrix}$.

Selanjutnya, Alice menghitung

$$B_1 = Y^k M_1 \bmod p = \begin{bmatrix} 1589 & 817 & 497 \\ 747 & 819 & 1137 \\ 354 & 853 & 2067 \end{bmatrix} \bmod 2357$$

$$B_2 = Y^k M_2 \bmod p = \begin{bmatrix} 1065 & 733 & 1046 \\ 146 & 1940 & 540 \\ 281 & 513 & 1123 \end{bmatrix} \bmod 2357$$

Dari perhitungan di atas diperoleh *ciphertext*

$$\left(A = \begin{bmatrix} 157 & 804 & 213 \\ 1921 & 654 & 1421 \\ 546 & 2198 & 247 \end{bmatrix}, B_1 = \begin{bmatrix} 1589 & 817 & 497 \\ 747 & 819 & 1137 \\ 354 & 853 & 2067 \end{bmatrix}, B_2 = \begin{bmatrix} 1065 & 733 & 1046 \\ 146 & 1940 & 540 \\ 281 & 513 & 1123 \end{bmatrix} \right),$$

Deskripsi

Setelah menerima *ciphertext* dari Alice, Bob melakukan perhitungan matematis dengan bantuan kunci privat (x), yaitu

$$M_1 = A^{-x}B_1 \bmod p = \begin{bmatrix} 412 & 122 & 123 \\ 231 & 511 & 150 \\ 234 & 511 & 100 \end{bmatrix}$$

$$M_2 = A^{-x}B_2 \bmod p = \begin{bmatrix} 456 & 786 & 124 \\ 234 & 561 & 111 \\ 456 & 654 & 321 \end{bmatrix}$$

Dari perhitungan ini diperoleh *plaintext*

$$M = 412122123231511150234511100456786124234561111456654321$$

4. KESIMPULAN

Dari hasil dan pembahasan di atas, diperoleh kesimpulan bahwa sistem kriptografi ElGamal yang bekerja pada ring $\square_p$ dapat digeneralisasi menjadi sistem kriptografi Elgamal pada matriks nonsingular atas $\square_p$. Hasil menunjukkan bahwa *plaintext* pada sistem kriptografi ElGamal yang diusulkan dimodelkan menjadi blok-blok bertingkat yaitu dimodelkan pada blok-blok berdasarkan panjang karakter p dan ukuran matriks G yang dipilih. Penggunaan blok-blok bertingkat pada *plaintext* dan perpangkatan matriks pada enkripsi akan menghasilkan *ciphertext* yang lebih acak dari sistem kriptografi ElGamal.

5. SARAN

Fokus dari penelitian ini adalah menggeneralisasi sistem kriftografi ElGamal yang bekerja pada ring $\square_p$ menjadi sistem kriptografi ElGamal pada matriks nonsingular atas $\square_p$. Penelitian ini belum membandingkan seberapa cepat dan efisien proses komputasi pada sistem kriftografi yang diusulkan dengan sistem kriftografi ElGamal. Untuk itu, penelitian ini dapat dilanjutkan untuk mengukur kecepatan dari proses komputasi pada sistem kriftografi yang diusulkan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada STMIK Atma Luhur yang telah memberi dukungan financial terhadap penelitian ini. Penulis juga berterima kasih kepada rekan-rekan peneliti yang telah berkolaborasi untuk menyelesaikan penelitian ini dengan baik.

DAFTAR PUSTAKA

[1] Castleman, [1] T. ElGamal, 1985, “A Public Key Cryptosystem and A Signature Based on Descrete Logarithms,” *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472.

[2] F.-Y. Rao, 2017, “On the Security of a Variant of ElGamal Encryption Scheme,” *IEEE Trans. Dependable Secur. Comput.*, vol. 14, no. 8, pp. 1–1.

[3] A. D. Hartanto, D. Junia, and E. Palupi, 2016 ,“Konstruksi Sistem Kriptografi Menggunakan General Linear Group,” *Pros. Semin. Nas. Aljabar USD 2016*, pp. 203–214.

[4] D. S. Dummit and R. M. Foote, 2004, *Abstract Algebra*, 3rd ed. John Wiley & Sons Inc.

[5] H. Anton and C. Rorres, 2010, *Elementary Linear Algebra: Applications Version*. Wiley eGrade.