Jurnal Matematika Integratif. p-ISSN:1412-6184, e-ISSN:2549-903
Vol. 16, No. 2 (2020), pp. 117-125. doi:10.24198/jmi.v16.n2.29197.117-125

Analisis Sistem Kriptografi ElGamal Untuk Membentuk Sistem Kunci Publik Berbasis Grup Non-Komutatif

Maxrizal[1], Syafrul Irawadi[2]

[1]**Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Sains Dan Bisnis Atma Luhur, Jl. Jendral Sudirman No.Kel, Selindung Baru, Pangkal Balam, Kota Pangkal Pinang, Kepulauan Bangka Belitung 33172**
[2]**Jurusan Manajemen Informatika, Fakultas Teknologi Informasi, Institut Sains Dan Bisnis Atma Luhur, Jl. Jendral Sudirman No.Kel, Selindung Baru, Pangkal Balam, Kota Pangkal Pinang, Kepulauan Bangka Belitung 33172**
Email:[1]maxrizal@atmaluhur.ac.id,[2]syafrul@atmaluhur.ac.id

Abstrak

Penelitian ini mengkaji suatu matriks persegi sebagai kunci privat pada sistem kriptografi ElGamal. Tahapan penelitian yang dilakukan adalah memodifikasi algoritma pembentukan pasangan kunci, enkripsi dan deskripsi. Hasil menunjukkan bahwa sistem kriptografi yang diusulkan dapat bekerja dengan baik untuk membangkitkan pasangan kunci, enkripsi dan deskripsi. Sistem yang diusulkan juga dibangun atas matriks-matriks persegi panjang untuk menjaga kerahasian pesan (*plaintext*) dan kunci. Selain itu, sistem kriptografi yang diusulkan juga telah diuji pada kemungkinan serangan matematis. Peretas atau penyadap dipaksa untuk melakukan *brute force attack* jika ingin meretas pesan dari sistem kriptografi yang diusulkan.

Kata kunci: kunci matriks, matriks ElGamal, kriptografi matriks, non-komutatif kriptografi, non-komutatif ElGamal.

Abstract

This study examines a square matrix as a private key in the ElGamal cryptosystem. The research stages were to modify the algorithm to generate key pairs, encryption, and descriptions. The results show that the proposed cryptosystem can work well for generating key pairs, encryption, and descriptions. The proposed system is also built on rectangular matrices to keep the message (plaintext) and keys secret. Apart from that, the proposed cryptosystem has also been tested for possible mathematical attacks. Hackers or eavesdroppers are forced to carry out brute force attacks if they want to hack messages from the proposed cryptosystem.

Keywords: *key matrix, ElGamal matrix, matrix cryptography, non-commutative cryptography, non-commutative ElGamal.*

1. Pendahuluan

Isu keamanan data (*data security*) terus menjadi perbincangan dan topik hangat pada bidang teknologi informasi. Keamanan data menjadi prioritas penting dalam bertransaksi data atau pun sekedar menyimpan data secara personal dan rahasia. Pada bidang matematika,

2000 Mathematics Subject Classification: 94A60
Submitted:2020-08-20, Revision: 2020-09-25 ; Accepted: 2020-10-27.

khususnya bidang aljabar terapan dipelajari sistem keamanan data melalui ilmu kriptografi. Ilmu ini sangat beririsan dengan bidang teknologi informasi dan komputer. Jika banyak software atau aplikasi dirancang oleh *programmer* maka para pakar dan peneliti dalam bidang matematika berperan dalam landasan-landasan teori kriptografi dan pengembangannya.

Pada bidang kriptografi dikenal algoritma kunci simetris dan kunci asimetris. Penerima dan pengirim pesan pada algoritma kunci simetris memiliki kunci yang sama, sehingga kedua belah pihak wajib menjaga kerahasian kunci. Sedangkan pada algoritma kunci asimetris, penerima dan pengirim pesan memiliki kunci yang berbeda. Pada algoritma ini juga tidak ada pertukaran kunci, masing-masing pihak akan membangun kunci dengan perhitungan matematis.

Salah satu contoh algoritma kunci asimetris adalah sistem kriptografi ElGamal. Sistem kriptografi ini bekerja pada bilangan bulat (*integer*) dengan operasi perkalian dua *integer* biasa, sehingga secara matematis sistem ini bekerja pada grup komutatif atas bilangan bulat (*integer*). Sistem kriptografi ElGamal juga telah mengalami banyak perbaikan [18, 17, 16, 9] dan penggabungan dengan algoritma kunci asimetris lainnya [4]. Pada faktanya, sistem kriptografi ElGamal dan variannya masih dapat diretas oleh peretas [5].

Secara umum, sistem-sistem kriptografi (seperti ElGamal, RSA dan ECC) masih menggunakan sifat grup komutatif. Sifat matematis ini ternyata merupakan celah bagi peretas untuk mencuri data dari sistem kriptografi yang ada. Sistem kriptografi berbasis aljabar komutatif rentan pada serangan algoritma kuantum (quantum algorithms attack). Untuk itu, para peneliti dan pakar menggunakan grup non-komutatif seperti grup matriks [11, 12, 19, 10, 1], semiring [7, 2], near-ring [8] dan polinomial dekomposisi matriks [14]. Walaupun begitu, beberapa sistem kriptografi asimetris yang dikembangkan masih dapat diretas oleh penyadap [5] [14, 13]. Salah satu pengembangan pada sistem kriptografi ElGamal adalah penggunaan Non-Abelian Groups II agar sistem bekerja atas grup non-komutatif [15].

Pada sistem kriptografi ElGamal tradisional digunakan persamaan pembangkit kunci $y = g^x \mod p$, dengan kunci privat x dan kunci publik (y, g, p). Keamanan sistem kriptografi ElGamal tradisional dan variannya terletak pada penggunaan bilangan prima p yang relatif besar yaitu mencapai 200 sampai 300 digit angka. Jika dipilih bilangan prima p yang kecil maka *brute force attack* sangat mungkin dilakukan oleh peretas, sehingga sistem kriptografi menjadi tidak aman. *Brute force attack* adalah serangan yang dilakukan oleh peretas untuk mendapatkan pesan (plainteks) atau kunci dengan mencoba semua kemungkinan kunci yang ada (*trial and error*). Pada hasil penelitian [17] [16], persamaan pembangkit pasangan kunci pada sistem kriptografi ElGamal dimodifikasi menggunakan konsep general linear group. Persamaan itu menjadi $Y = G^x \mod p$, dengan tetap menggunakan x sebagai kunci privat. Perhatikan bahwa G merupakan anggota dari himpunan semua matriks yang berukuran $n \times n$ atas lapangan berhingga (*finite field*) F_q dengan syarat determinan matriks tak nol, dinotasikan $G \in GL_n(F_p)$. Untuk itu, penelitian ini tetap menggunakan persamaan pembangkit pasangan kunci $Y = G^X \mod p$, tetapi dengan matriks G sebagai kunci privat dan (Y, x, p) sebagai kunci publik. Perbaikan konsep ini membutuhkan banyak teori aljabar linear dan aljabar abstrak [3, 6], sehingga diperoleh sistem modifikasi kriptografi ElGamal yang bekerja dengan baik. Sistem ini bekerja pada konsep grup non-komutatif. Sistem kriptografi yang diusulkan juga dianalisa dari berbagai serangan peretasan sehingga tidak rentan terhadap serangan berbasis konsep matematis.

2. Metode Penelitian

Penelitian ini merupakan jenis penelitian studi literatur. Penelitian ini menelaah teori matematika yang mendukung untuk modifikasi sistem kriptografi ElGamal tradisional. Penelitian yang diusulkan difokuskan pada algoritma pembentukan pasangan kunci, proses enkripsi dan deskripsi pesan. Jika kunci privat berbentuk matriks G maka output Y juga suatu matriks, yaitu $Y = G^x \mod p$. Hal ini menunjukkan bahwa sistem kriptografi ElGamal yang diusulkan akan bekerja pada suatu grup non-komutatif atas matriks yang memiliki invers. Peneliti juga

mengkaji serangan-serangan yang mungkin pada pembentukan kunci, enkripsi dan deskripsi sehingga dihasilkan sistem modifikasi yang cukup aman. Pada akhirnya, peneliti melakukan beberapa simulasi perhitungan menggunakan aplikasi *Mathematica 5.0* untuk memastikan bahwa sistem ini dapat bekerja dengan baik.

3. Hasil dan Pembahasan

3.1. **Sistem Kriptografi ElGamal [16].** Pada [16], sistem kriptografi ElGamal menggunakan persamaan pembangkit kunci $Y = G^x \bmod p$, dengan kunci privat x dan kunci publik (Y, G, p). Sistem kriptografi ini menggunakan konsep grup siklis yang komutatif.

Tabel 1. Sistem Kriptografi ElGamal [16]

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	$M = A^{-x} B \bmod p$

Ada dua konsep yang akan menjadi modal untuk memodifikasi sistem kriptografi ElGamal yang diusulkan yaitu persamaan $Y = G^x \bmod p$ dan $M = A^{-x}B \bmod p$.

3.2. **Modifikasi Sistem Kriptografi ElGamal Yang Diusulkan.** Pada modifikasi ini dibutuhkan konsep matriks persegi panjang untuk membuat sistem kriptografi ElGamal yang diusulkan bekerja dengan baik. Perhatikan bahwa notasi $G_{3\times 2}$berarti sebarang matriks persegi panjang G yang berukuran 3×2. Pada penelitian ini diberikan sebarang $q \geq 0$ dan $r \geq 1$, dengan $q, r \in \mathbb{Z}_0^+$ yaitu q dan r merupakan anggota dari himpunan bilangan bulat positif dan nol. Kajian modifikasi ini juga membutuhkan matriks identitas (I) , sebarang matriks persegi panjang O, S, T, K, Q, U dan matriks-matriks persegi G, Y, H, P, X. Berikut ini hasil modifikasi yang diperoleh:

Tabel 2. Sistem Kriptografi ElGamal Yang Diusulkan

Pihak penerima pesan	Algoritma pembangkit pasangan kunci	$G_{(q+4)\times(q+4)} = \begin{bmatrix} G_{(q+3)\times(q+2)} & O_{(q+2)\times(q+2)} \\ O_{(q+1)\times(q+2)} & I_{(q+2)\times(q+2)} \end{bmatrix}$ $Y_{(q+4)\times(q+4)} = \left(G_{(q+4)\times(q+4)}\right)^x$ $S_{(q+2)\times(q+4)}$ Kunci privat $\left\{G_{(q+3)\times(q+2)}\right\}$ Kunci publik $\left\{x, Y_{(q+4)\times(q+4)}, S_{(q+2)\times(q+4)}\right\}$
Pihak pengirim pesan	Algoritma pembangkit pasangan kunci	$K_{(q+4)\times(q+3)}$ $H_{(q+4)\times(q+4)} = \begin{bmatrix} H_{(q+2)\times(q+2)} & O_{(q+2)\times(q+2)} \\ O_{(q+2)\times(q+2)} & I_{(q+2)\times(q+2)} \end{bmatrix}$ $T_{(q+4)\times(q+3)} = H_{(q+4)\times(q+4)} Y_{(q+4)\times(q+4)} K_{(q+4)\times(q+3)}$ Kunci privat $\left\{H_{(q+2)\times(q+2)}\right\}$ Kunci publik $\left\{T_{(q+4)\times(q+3)}, K_{(q+4)\times(q+3)}\right\}$
Pihak penerima pesan	Algoritma pembangkit pasangan kunci	$P_{(q+2)\times(q+2)} = S_{(q+2)\times(q+4)} T_{(q+4)\times(q+3)} G_{(q+3)\times(q+2)}$ Kunci publik $\left\{P_{(q+2)\times(q+2)}\right\}$
Pihak pengirim pesan	Enkripsi	$Q_{(q+2)\times r} = H_{(q+2)\times(q+2)} P_{(q+2)\times(q+2)} M_{(q+2)\times r}$ $U_{(q+2)\times(q+4)} = H_{(q+2)\times(q+2)} S_{(q+2)\times(q+4)} H_{(q+4)\times(q+4)}$
Pihak penerima pesan	Deskripsi	$X_{(q+2)\times(q+2)} = U_{(q+2)\times(q+4)} Y_{(q+4)\times(q+4)} K_{(q+4)\times(q+3)} G_{(q+3)\times(q+2)}$ $M_{(q+2)\times r} = \left(X_{(q+2)\times(q+2)}\right)^{-1} Q_{(q+2)\times r}$

Tabel di atas menunjukkan bahwa kita dapat menggunakan matriks-matriks sesuai kesepakatan antara penerima dan pengirim pesan. Semakin besar matriks kunci maka semakin banyak kemungkinan kunci yang harus dicoba pada percobaan *brute force attack* yang dilakukan oleh peretas.

Selain itu, sistem ini juga mengakibatkan plaintext $M_{(q+2)\times r}$ berbentuk matriks sehingga ciphertext yang dihasilkan $Q_{(q+2)\times r}$ akan berbentuk matriks juga. Hal ini berakibat pada output pengacakan ciphertext yang lebih rumit sehingga akan sulit diretas oleh penyadap. Jika ada beberapa elemen matriks plaintext $M_{(q+2)\times r}$ terlihat maka peretas tetap akan membutuhkan upaya ekstra untuk melakukan *chosen plaintext attack*.

3.3. **Analisis Serangan Pada Sistem Kriptografi ElGamal Yang Diusulkan.** Pada bagian ini, kita akan menganalisa kemungkinan serangan berbasis matematis pada sistem kriptografi ElGamal yang diusulkan. Untuk itu, kita membutuhkan beberapa definisi dan teorema tentang matriks persegi panjang.

Definisi 3.1. *Matriks persegi panjang adalah matriks yang berukuran $m \times n (m \neq n)$. Matriks persegi panjang tidak memiliki balikan [3].*

Teorema 3.2. *Diberikan matriks $A_{m\times n}$ dan $B_{n\times m}$, dengan $m > n$ dan $m, n \in \mathbb{Z}^+$. Jika dibentuk $P_{m\times m} = A_{m\times n}.B_{n\times m}$maka matriks persegi $P_{m\times m}$ adalah matriks singular [3].*

Berdasarkan definisi dan teorema di atas, kita akan menjabarkan berbagai jenis serangan pada sistem kriptografi ElGamal yang diusulkan.

Serangan Pada Algoritma Pembangkit Pasangan Kunci

Serangan pertama terjadi pada persamaan $Y_{(q+4)\times(q+4)} = \left(G_{(q+4)\times(q+4)}\right)^x$. Persamaan ini merupakan ciri khas dari persamaan logaritma diskrit atas matriks pada sistem kriptografi ElGamal yang diusulkan. Pada persamaan ini, matriks $Y_{(q+4)\times(q+4)}$ tidak rahasia dan matriks $G_{(q+4)\times(q+4)}$ bersifat rahasia. Matriks $G_{(q+4)\times(q+4)}$ tidak akan mudah ditemukan karena sifat akar pada logaritma diskrit atas matriks persegi tidak berlaku. Jika diberikan $G^{10} = \begin{bmatrix} 15 & 12 \\ 8 & 5 \end{bmatrix} \bmod 17$ maka akan sangat sulit menemukan matriks G. Perhatikan bahwa pada logaritma diskrit atas matriks tidak berlaku $G = \sqrt[10]{G^{10}}$. Peretas hanya dapat melakukan brutal force attack yaitu mencoba semua kemungkinan matriks. Jika pada sistem sebelumnya (seperti ElGamal, RSA, dan ECC) kemungkinan brute force attack sebanyak p kemungkinan maka pada sistem kriptografi ElGamal yang diusulkan banyaknya percobaan brute force attack setara dengan order dari general linear grup $GL_n(F_p)$ yaitu $\prod_{k=0}^{n-1}\left(p^n - p^k\right) = \left(p^n - 1\right)\left(p^{n-1} - p\right)\ldots\left(p^n - p^{n-1}\right)$ [3] [6]. Perhatikan bahwa kemungkinan brute force attack pada sistem yang diusulkan lebih banyak sehingga lebih menyulitkan peretas. Jadi, matriks $G_{(q+4)\times(q+4)}$ sebagai kunci rahasia tetap aman.

Serangan kedua pada persamaan $T_{(q+4)\times(q+3)} = H_{(q+4)\times(q+4)}Y_{(q+4)\times(q+4)}K_{(q+4)\times(q+3)}$. Pada persamaan ini, matriks $\left\{T_{(q+4)\times(q+3)}, Y_{(q+4)\times(q+4)}, K_{(q+4)\times(q+3)}\right\}$ tidak rahasia dan matriks $H_{(q+4)\times(q+4)}$bersifat rahasia. Perhatikan bahwa berlaku

$$T_{(q+4)\times(q+3)} = H_{(q+4)\times(q+4)}(YK)_{(q+4)\times(q+3)}.$$

Berdasarkan Definisi 1, invers matriks $(YK)_{(q+4)\times(q+3)}$ tidak ada, sehingga persamaan

$$H_{(q+4)\times(q+4)} = T_{(q+4)\times(q+3)}\left((YK)_{(q+4)\times(q+3)}\right)^{-1}$$

tidak berlaku. Jadi, matriks $H_{(q+4)\times(q+4)}$ tetap aman. Selanjutnya, jika pada persamaan $T_{(q+4)\times(q+3)} = H_{(q+4)\times(q+4)}(YK)_{(q+4)\times(q+3)}$ dikalikan sebarang matriks $R_{(q+3)\times(q+4)}$ maka diperoleh $(TR)_{(q+4)\times(q+4)} = H_{(q+4)\times(q+4)}(YKR)_{(q+4)\times(q+4)}$. Perhatikan bahwa matriks

$$(YKR)_{(q+4)\times(q+4)}$$

berbentuk persegi. Berdasarkan Teorema 1, invers matriks $(YKR)_{(q+4)\times(q+4)}$ tidak ada, sehingga persamaan

$$H_{(q+4)\times(q+4)} = (TR)_{(q+4)\times(q+4)}\Big((YKR)_{(q+4)\times(q+4)}\Big)^{-1}$$

tidak berlaku. Jadi, matriks $H_{(q+4)\times(q+4)}$ tetap aman.

Serangan ketiga pada persamaan $P_{(q+2)\times(q+2)} = S_{(q+2)\times(q+4)}T_{(q+4)\times(q+3)}G_{(q+3)\times(q+2)}$. Pada persamaan ini, matriks $\left\{P_{(q+2)\times(q+2)}, S_{(q+2)\times(q+4)}, T_{(q+4)\times(q+3)}\right\}$ tidak rahasia dan matriks $G_{(q+3)\times(q+2)}$ bersifat rahasia. Perhatikan bahwa berlaku

$$P_{(q+2)\times(q+2)} = (ST)_{(q+2)\times(q+3)}G_{(q+3)\times(q+2)}.$$

Berdasarkan Definisi 1, invers matriks $(ST)_{(q+2)\times(q+3)}$ tidak ada, sehingga persamaan

$$G_{(q+3)\times(q+2)} = \Big((ST)_{(q+2)\times(q+3)}\Big)^{-1}P_{(q+2)\times(q+2)}$$

tidak berlaku. Jadi, matriks $G_{(q+3)\times(q+2)}$ tetap aman. Selanjutnya, jika pada persamaan $P_{(q+2)\times(q+2)} = (ST)_{(q+2)\times(q+3)}G_{(q+3)\times(q+2)}$ dikalikan sebarang matriks $R_{(q+3)\times(q+2)}$ maka diperoleh

$$(RP)_{(q+3)\times(q+2)} = (RST)_{(q+3)\times(q+3)}G_{(q+3)\times(q+2)}.$$

Perhatikan bahwa matriks

$$(RST)_{(q+3)\times(q+3)}$$

berbentuk persegi. Berdasarkan Teorema 1, invers matriks

$$(RST)_{(q+3)\times(q+3)}$$

tidak ada, sehingga persamaan

$$\Big((RST)_{(q+3)\times(q+3)}\Big)^{-1}(RP)_{(q+3)\times(q+2)} = G_{(q+3)\times(q+2)}$$

tidak berlaku. Jadi, matriks $G_{(q+3)\times(q+2)}$ tetap aman.

Serangan Pada Enkripsi

Serangan pertama pada persamaan $U_{(q+2)\times(q+4)} = H_{(q+2)\times(q+2)}S_{(q+2)\times(q+4)}H_{(q+4)\times(q+4)}$. Pada persamaan ini, matriks $\left\{U_{(q+2)\times(q+4)}, S_{(q+2)\times(q+4)}\right\}$ tidak rahasia dan matriks $H_{(q+2)\times(q+2)}$ bersifat rahasia. Karena matriks

$$H_{(q+4)\times(q+4)} = \begin{bmatrix} H_{(q+2)\times(q+2)} & O_{(q+2)\times(q+2)} \\ O_{(q+2)\times(q+2)} & I_{(q+2)\times(q+2)} \end{bmatrix},$$

maka matriks $H_{(q+4)\times(q+4)}$ bersifat rahasia juga. Jadi, matriks $H_{(q+2)\times(q+2)}$ tetap aman.

Serangan kedua pada persamaan $Q_{(q+2)\times r} = H_{(q+2)\times(q+2)}P_{(q+2)\times(q+2)}M_{(q+2)\times r}$. Pada persamaan ini matriks $\left\{Q_{(q+2)\times r}, P_{(q+2)\times(q+2)}\right\}$ tidak rahasia dan matriks $H_{(q+2)\times(q+2)}$ bersifat rahasia. Jadi, matriks $M_{(q+2)\times r}$ tetap aman.

Selanjutnya pada persamaan $Q_{(q+2)\times r} = H_{(q+2)\times(q+2)}P_{(q+2)\times(q+2)}M_{(q+2)\times r}$ disubstitusikan persamaan matriks $P_{(q+2)\times(q+2)} = S_{(q+2)\times(q+4)}T_{(q+4)\times(q+3)}G_{(q+3)\times(q+2)}$. Perhatikan bahwa diperoleh persamaan matriks

$$Q_{(q+2)\times r} = H_{(q+2)\times(q+2)}S_{(q+2)\times(q+4)}T_{(q+4)\times(q+3)}G_{(q+3)\times(q+2)}M_{(q+2)\times r}.$$

Perhatikan bahwa, karena matriks $\left\{H_{(q+2)\times(q+2)}, G_{(q+3)\times(q+2)}\right\}$ bersifat rahasia maka matriks $M_{(q+2)\times r}$ tetap aman.

Selanjutnya pada persamaan

$$Q_{(q+2)\times r} = H_{(q+2)\times(q+2)}S_{(q+2)\times(q+4)}T_{(q+4)\times(q+3)}G_{(q+3)\times(q+2)}M_{(q+2)\times r}$$

disubstitusikan persamaan matriks $T_{(q+4)\times(q+3)} = H_{(q+4)\times(q+4)}Y_{(q+4)\times(q+4)}K_{(q+4)\times(q+3)}$. Perhatikan bahwa

$$Q_{(q+2)\times r} = H_{(q+2)\times(q+2)}S_{(q+2)\times(q+4)}H_{(q+4)\times(q+4)}Y_{(q+4)\times(q+4)}K_{(q+4)\times(q+3)}G_{(q+3)\times(q+2)}M_{(q+2)\times r}.$$

Selanjutnya, kita subsitusikan persamaan $U_{(q+2)\times(q+4)} = H_{(q+2)\times(q+2)}S_{(q+2)\times(q+4)}H_{(q+4)\times(q+4)}$ sehingga diperoleh persamaan

$$Q_{(q+2)\times r} = U_{(q+2)\times(q+4)}Y_{(q+4)\times(q+4)}K_{(q+4)\times(q+3)}G_{(q+3)\times(q+2)}M_{(q+2)\times r}.$$

Perhatikan bahwa matriks $G_{(q+3)\times(q+2)}$ bersifat rahasia, sehingga matriks $M_{(q+2)\times r}$ tetap aman.

Serangan Pada Deskripsi

Serangan pada deskripsi dilakukan pada $M_{(q+2)\times r} = \left(X_{(q+2)\times(q+2)}\right)^{-1}Q_{(q+2)\times r}$. Perhatikan bahwa $X_{(q+2)\times(q+2)} = U_{(q+2)\times(q+4)}Y_{(q+4)\times(q+4)}K_{(q+4)\times(q+3)}G_{(q+3)\times(q+2)}$ hanya diketahui oleh penerima pesan, sehingga matriks

$$M_{(q+2)\times r}$$

tetap aman. Selanjutnya, pada$X_{(q+2)\times(q+2)} = U_{(q+2)\times(q+4)}Y_{(q+4)\times(q+4)}K_{(q+4)\times(q+3)}G_{(q+3)\times(q+2)}$ terdapat kunci privat $G_{(q+3)\times(q+2)}$, sehingga $X_{(q+2)\times(q+2)}$ tidak dapat dibangkitkan oleh peretas.

Berdasarkan tipe serangan pada algoritma pembangkit kunci, enkripsi dan deskripsi maka sistem kriptografi ElGamal yang diusulkan tahan terhadap serangan konsep matematis. Selain itu, karena menggunakan konsep operasi pada matriks maka sistem yang diusulkan bekerja pada grup non-komutatif.

3.4. **Contoh Modifikasi Sistem Kriptografi ElGamal Yang Diusulkan.** Bob dan Alice akan berkirim pesan. Mereka sepakat untuk membangkitkan pasangan kunci publik dan kunci privat.

Algoritma pembangkit pasangan kunci

Bob dan Alice sepakat memilih modulo $p = 2357$. Bob memilih matriks

$$G_{3\times2} = \begin{bmatrix} 11 & 2 \\ 3 & 5 \\ 7 & 14 \end{bmatrix}$$

dan membentuk matriks persegi

$$G_{4\times4} = \begin{bmatrix} G_{3\times2} & O_{2\times2} \\ O_{1\times2} & I_{2\times2} \end{bmatrix} = \begin{bmatrix} 11 & 2 & 0 & 0 \\ 3 & 5 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Ia memilih sebarang $x = 200$ dan menghitung matriks

$$Y_{4\times4} = (G_{4\times4})^{200} \bmod 2357 = \begin{bmatrix} 1454 & 142 & 0 & 0 \\ 213 & 1024 & 0 & 0 \\ 607 & 4 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Ia juga memilih matriks

$$S_{2\times4} = \begin{bmatrix} 11 & 21 & 3 & 4 \\ 1 & 2 & 11 & 4 \end{bmatrix}.$$

Jadi, Bob memiliki kunci privat $\{G_{3\times2}\}$ dan mengirimkan kunci publik $\{x, Y_{4\times4}, S_{2\times4}\}$ kepada Alice.

Selanjutnya, Alice memilih matriks

$$K_{4\times 3} = \begin{bmatrix} 1 & 22 & 3 \\ 1 & 4 & 1 \\ 1 & 51 & 3 \\ 4 & 2 & 1 \end{bmatrix}.$$

Ia memilih matriks

$$H_{2\times 2} = \begin{bmatrix} 11 & 13 \\ 3 & 4 \end{bmatrix}$$

dan membentuk

$$H_{4\times 4} = \begin{bmatrix} H_{2\times 2} & O_{2\times 2} \\ O_{2\times 2} & I_{2\times 2} \end{bmatrix} = \begin{bmatrix} 11 & 13 & 0 & 0 \\ 3 & 4 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Ia juga membentuk

$$T_{4\times 3} = H_{4\times 4}Y_{4\times 4}K_{4\times 3} \bmod 2357 = \begin{bmatrix} 691 & 1090 & 505 \\ 324 & 868 & 1324 \\ 612 & 1636 & 1828 \\ 4 & 2 & 1 \end{bmatrix}.$$

Jadi, Alice memiliki kunci privat $\{H_{2\times 2}\}$ dan mengirimkan kunci publik $\{T_{4\times 3}, K_{4\times 3}\}$ kepada Bob.

Selanjutnya, Bob membentuk matriks

$$P_{2\times 2} = S_{2\times 4}T_{4\times 3}G_{3\times 2} \bmod 2357 = \begin{bmatrix} 2263 & 159 \\ 821 & 561 \end{bmatrix}.$$

Ia mengirimkan kunci publik

$$\left\{P_{2\times 2} = \begin{bmatrix} 2263 & 159 \\ 821 & 561 \end{bmatrix}\right\}$$

ke Alice.

Enkripsi

Misalkan Alice memiliki pesan (plaintetxt)

$$M_{2\times 3} = \begin{bmatrix} 1 & 2 & 3 \\ 101 & 102 & 103 \end{bmatrix}$$

. Selanjutnya Alice menghitung matriks

$$Q_{2\times 3} = H_{2\times 2}P_{2\times 2}M_{2\times 3} \bmod 2357 = \begin{bmatrix} 1294 & 1119 & 944 \\ 2054 & 706 & 1715 \end{bmatrix}$$

,

$$U_{2\times 4} = H_{2\times 2}S_{2\times 4}H_{4\times 4} \bmod 2357 = \begin{bmatrix} 2245 & 413 & 176 & 96 \\ 620 & 765 & 53 & 28 \end{bmatrix}$$

. Alice mengirimkan *ciphertext*

$$\{Q_{2\times 3}, U_{2\times 4}\}$$

kepada Bob.

Deskripsi

Bob menghitung matriks

$$X_{2\times 2} = U_{2\times 4}Y_{4\times 4}K_{4\times 3}G_{3\times 2} \bmod 2357 = \begin{bmatrix} 211 & 1971 \\ 645 & 364 \end{bmatrix}$$

dan menentukan invers matriks

$$(X_{2\times 2})^{-1} = \begin{bmatrix} 1504 & 1569 \\ 987 & 302 \end{bmatrix}$$

. Selanjutnya, Bob membentuk matriks

$$M_{2\times 3} = (X_{2\times 2})^{-1} Q_{2\times 3} = \begin{bmatrix} 1 & 2 & 3 \\ 101 & 102 & 103 \end{bmatrix}$$

. Jadi, Bob berhasil mendapatkan pesan asli (*plaintext*)

$$M_{2\times 3}$$

dari Alice.

4. SIMPULAN

Pada penelitian ini diusulkan suatu matriks persegi sebagai kunci dari persamaan logaritma diskrit atas matriks pada sistem kriptografi ElGamal. Hasil menunjukkan bahwa sistem kriptografi yang diusulkan dapat bekerja dengan baik untuk membangkitkan pasangan kunci, enkripsi dan deskripsi. Sistem yang diusulkan juga dibangun atas matriks-matriks persegi panjang untuk menjaga kerahasian pesan (*plaintext*) dan kunci. Selain itu, sistem kriptografi yang diusulkan juga telah diuji pada kemungkinan serangan matematis. Peretas atau penyadap dipaksa untuk melakukan *brute force attack* jika ingin meretas pesan dari sistem kriptografi ElGamal yang diusulkan.

Ucapan Terima Kasih

Penelitian ini didanai oleh Kemenristek / BRIN melalui hibah Penelitian Dosen Pemula (PDP) tahun anggaran 2020. Untuk itu, peneliti mengucapkan banyak terima kasih kepada Kemristek / BRIN yang telah memberikan anggaran penelitian ini. Penulis juga mengucapkan terima kasih kepada Institut Sains Dan Bisnis Atma Luhur yang telah banyak mengadakan kegiatan pelatihan atau workshop penulisan penelitian sehingga penulis memperoleh hibah ini.

Daftar Pustaka

[1] M Andrecut. A matrix public key cryptosystem. *arXiv preprint arXiv:1506.00277*, 2015.
[2] GSGN Anjaneyulu and A Sanyasirao. Distributed group key management protocol over non-commutative division semirings. *Indian Journal of Science and Technology*, 7(6):871, 2014.
[3] Howard Anton and Chris Rorres. *Elementary linear algebra: applications version*. John Wiley & Sons, 2013.
[4] CR Bharathi. Improved elgamal encryption for elliptic curve cryptography. *International Journal of Pure and Applied Mathematics*, 118(17):341–353, 2018.
[5] Ting-Yi Chang, Min-Shiang Hwang, and Wei-Pang Yang. Cryptanalysis on an improved version of elgamal-like public-key encryption scheme for encrypting large messages. *Informatica*, 23(4):537–562, 2012.
[6] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.
[7] A Dwivedi, DB Ojha, A Sharma, and A Mishra. A model of key agreement protocol using polynomials over non-cummutative division semirings. *J. Glob. Res. Comput. Sci*, 2(3):40–43, 2011.
[8] D Ezhilmaran and V Muthukumaran. Key exchange protocol using decomposition problem in near-ring. *Gazi University Journal of Science*, 29(1), 2016.
[9] Marc Joye. Secure elgamal-type cryptosystems without message encoding. In *The New Codebreakers*, pages 470–478. Springer, 2016.
[10] Delaram Kahrobaei, Charalambos Koupparis, and Vladimir Shpilrain. Public key exchange using matrices over group rings. *Groups Complexity Cryptology*, 5(1):97–115, 2013.

[11] Zekeriya Y Karatas, Erkam Luy, and Bilal Gonen. A public key cryptosystem based on matrices. *International Journal of Computer Applications*, 975:8887.

[12] Addepalli VN Krishna, Addepalli Hari Narayana, and K Madhura Vani. A novel approach with matrix based public key crypto systems. *Journal of Discrete Mathematical Sciences and Cryptography*, 20(2):407–412, 2017.

[13] Jinhui Liu, Huanguo Zhang, and Jianwei Jia. Cryptanalysis of schemes based on polynomial symmetrical decomposition. *Chinese Journal of Electronics*, 26(6):1139–1146, 2017.

[14] Jinhui Liu, Huanguo Zhang, Jianwei Jia, Houzhen Wang, Shaowu Mao, and Wanqing Wu. Cryptanalysis of an asymmetric cipher protocol using a matrix decomposition problem. *Science China Information Sciences*, 59(5):052109, 2016.

[15] Ayan Mahalanobis. A simple generalization of the elgamal cryptosystem to non-abelian groups ii. *Communications in Algebra*, 40(9):3583–3596, 2012.

[16] Maxrizal Maxrizal, Maya Saftari, Marna Marna, and Sujono Sujono. Generalisasi sistem kriptografi elgamal menggunakan konsep matriks nonsingular. In *SENSITIf: Seminar Nasional Sistem Informasi dan Teknologi Informasi*, pages 21–26, 2019.

[17] Maxrizal Maxrizal, Maya Saftari, Eza Budi Perkasa, and Devi Irawan. Modifikasi sistem kripto elgamal hasil konstruksi marc joye menggunakan general linear group. *AKSIOMA: Jurnal Matematika dan Pendidikan Matematika*, 10(1):102–111, 2019.

[18] Fang-Yu Rao. On the security of a variant of elgamal encryption scheme. *IEEE Transactions on Dependable and Secure Computing*, 2017.

[19] M Zeriouh, A Chillali, and Abdelkarim Boua. Cryptography based on the matrices. *Boletim da Sociedade Paranaense de Matemática*, 37(3):75–83, 2019.