MATHEMATICAL SCIENCES AND APPLICATIONS JOURNAL

Volume 4, Number 1 | ISSN: 2986-4180

https://online-journal.unja.ac.id/msa

Article

Implementasi Matriks *Skew-symmetric* dalam Metode Kriptografi Affine-Hill Cipher

Putri Nisa Pratiwi, Sisilia Sylviani*

Departemen Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Padjadjaran, Sumedang 45363, Indonesia

*Corresponding author e-mail: sisilia.sylviani@unpad.ac.id

Article Info
Received October 2023
Accepted October 2023
Published October 2023

Keyword:
Modular operation
Affine-Hill Cipher
Skew-symmetric matrix

Abstract

The concept of cryptography is widely used to reduce data security threats along with developments in information technology. Affine Cipher is an example of classic cryptography that utilizes modular operations and shifts on characters. On the other hand, Hill Cipher method is more dependent on matrix operations. The combination of the two methods, Affine-Hill Cipher, creates a more complex and superior method in terms of security. In this research, we utilize a square skew-symmetric matrix with an order corresponds to the secret key to construct the key matrix. The encryption and decryption processes are carried out using the Affine-Hill Cipher and adding the key exchange concept into the algorithm. The results indicate that this algorithm's complexity can effectively reduce data security threats.

1. Pendahuluan

Seiring dengan perkembangan teknologi informasi, keamanan data merupakan hal yang krusial. Konsep kriptografi berperan dalam mengurangi ancaman dalam dunia teknologi dan keamanan data seperti pencurian data, peretasan, dan lain sebagainya [1]. Kriptografi adalah salah satu aplikasi dari teori bilangan yang menerjemahkan suatu teks ke dalam bentuk unik yang sulit dipahami.

Secara umum, kriptografi bertujuan untuk mengubah teks biasa (*plaintext*) menjadi teks ber-enkripsi (*ciphertext*), dan sebaliknya, yang tidak dapat dipahami oleh orang yang tidak memiliki akses terhadap teks tersebut [2]. Metode kriptografi yang paling sederhana menerapkan pergeseran atau substitusi huruf-huruf alfabet, seperti Caesar Cipher yang diperkenalkan oleh kaisar Romawi kuno, Julius Caesar [3]dan Affine Cipher yang melibatkan transformasi matematis sederhana pada huruf-huruf *plaintext* dengan operasi modular. Akan tetapi, metode-metode tersebut menghasilkan *ciphertext* yang dapat dipecahkan dengan mudah.

Hill Cipher merupakan salah satu metode kriptografi klasik yang memiliki kompleksitas tinggi sehingga lebih kuat dalam hal keamanan dibandingkan metode substitusi sederhana seperti Caecar Cipher dan Affine Cipher. Hill Cipher pertama kali diperkenalkan oleh matematikawan bernama Lester Hill pada tahun 1929. Keamanan dalam Hill Cipher sangat bergantung pada operasi matriks kunci yang meningkatkan kompleksitas dalam proses enkripsi dan dekripsi. Namun demikian, matriks kunci dalam Hill Cipher bersifat *invertible* sehingga diperlukan waktu yang lama untuk menguji apakah matriks berorde tinggi memiliki *inverse* atau tidak [4]. Beberapa jenis matriks digunakan untuk mengatasi masalah *inverse* dari matriks kunci seperti penggunaan matriks *self-invertible* [5], matriks persegi panjang [6], matriks skew-symmetric [3], dan matriks ortogonal [7]. Selain itu, dilakukan penelitian mengenai variasi baru dari Hill Cipher sehingga dekripsi dari *ciphertext* dapat dicari walau dengan matriks kunci yang tidak *invertible* [8]. Namun, penelitian tersebut belum dibuktikan secara matematis.

Kombinasi dari Affine Cipher dan Hill Cipher disebut sebagai Affine-Hill Cipher. Hill Cipher yang berfokus pada operasi matriks dan Affine Cipher yang melibatkan transformasi matematis sederhana pada huruf-huruf *plaintext* menciptakan kombinasi metode yang lebih

https://doi.org/10.22437/msa.v4i1.28864

unggul dalam hal kemanan dan memungkinkan proses enskripsi dan deskripsi dengan kompleksitas tinggi. Modifikasi dari metode Affine-Hill Cipher sudah diteliti seperti konsep kriptografi *public key* dalam Affine-Hill Cipher [9], Affine-Hill Cipher dengan matriks kunci Fibonacci dan konsep *public key* [10–14], serta penggunaan matriks rekursif lain seperti matriks Lucas [15] . Konsep *public key* juga sudah digunakan dalam metode Hill-Cipher [16].

Algoritma dalam menentukan matriks kunci dari matriks *skew-symmetric* oleh [3] sangat menarik untuk dipelajari karena algoritma yang digunakan dapat memudahkan pencarian *inverse* tanpa mengurangi kompleksitas algoritma. Selain itu, konsep *public key* dalam Affine-Hill Cipher dapat meningkatkan keamanan pesan. Oleh karena itu, pada penelitian ini matriks *skew-symmetric* digunakan untuk mengonstruksi matriks kunci dalam metode Affine-Hill Cipher dengan konsep *public key*.

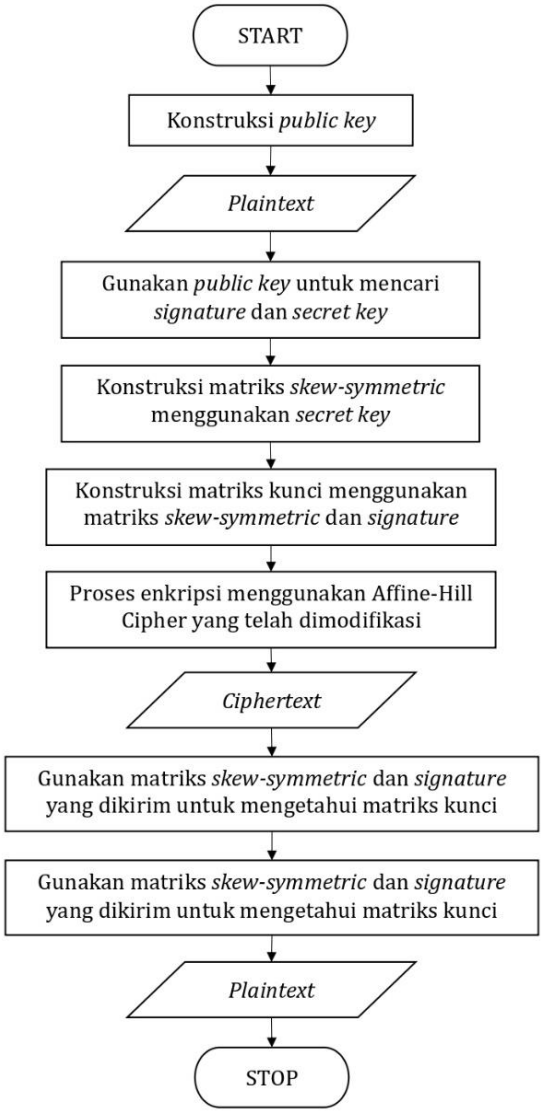
2. Metode Penelitian

Metode penelitian ini berdasarkan algoritma [3] untuk memilih matriks kunci dari matriks *skew-symmetric* dan algoritma [10, 16] untuk melakukan proses enkripsi dan dekripsi. Sebelum melakukan proses enkripsi, *public key* akan dikonstruksi terlebih dahulu oleh penerima pesan. *Public key* digunakan oleh pengirim untuk mencari nilai *signature* dan *secret* key. *Secret key* digunakan untuk menentukan orde matriks *skew-symmetric* yang elemen-elemennya sembarang bilangan bulat. Matriks *skew-symmetric* dan *signature* digunakan untuk mengonstruksi matriks kunci. Setelah matriks kunci diperoleh, proses enkripsi dapat dilakukan. Untuk melakukan proses dekripsi, penerima pesan akan mengirimkan matriks *skew-symmetric* dan *signature* untuk menentukan matriks kunci yang digunakan dalam proses dekripsi oleh penerima pesan. Diagram alir penelitian ini ditunjukkan pada Gambar 1.

2.1. Matriks *Skew-symmetric*

Pada bagian ini dijelaskan definisi dan teorema mengenai matriks *skew-symmetric* yang digunakan dalam proses konstruksi matriks kunci dalam penelitian ini.

Definisi 1. *Matriks* $A = [a_{ij}]$ *berukuran* $n \times n$ *dikatakan skew-symmetric jika* $A^T = -A$. *Sehingga untuk setiap* i *dan* j, $a_{ij} = -a_{ji}$.



Gambar 1. Diagram Alir Penelitian

Teorema 1. *Jika* A *merupakan matriks skew-symmetric berukuran* $n \times n$, *maka matriks* $(I + A)$ *dan* $(I - A)$ *invertible* [3].

Bukti. Misalkan A matriks *skew-symmetric* berukuran $n \times n$. Asumsikan suatu skalar λ sebagai nilai eigen untuk A sedemikian sehingga $Ax = \lambda x$ untuk suatu vektor $x \neq 0$. Berdasarkan hal tersebut, 1 merupakan nilai eigen untuk matriks identitas I karena $Ix = 1x$ untuk suatu vektor $x \neq 0$. Perhatikan bahwa, $Ix + Ax = 1x + \lambda x \Rightarrow (I + A)x = (1 + \lambda)x$ dan $Ix - Ax = 1x - \lambda x \Rightarrow (I - A)x = (1 - \lambda)x$. Terlihat bahwa masing-masing nilai eigen untuk $(I + A)$ dan $(I - A)$ adalah $(1 + \lambda)$ dan $(1 - \lambda)$. Karena A *skew-symmetrci*, nilai eigen untuk A pasti nol atau bilangan imajiner bi sehingga nilai eigen $(1 \pm \lambda) \neq 0$. Oleh karena itu, determinan matriks $(I + A)$ dan $(I - A)$ pasti ada dan tidak nol sehingga matriks $(I + A)$ dan $(I - A)$ *invertible*. ■

Teorema 2. *Misalkan A suatu matriks skew-symmetric berukuran $n \times n$ dan I matriks identitas. Matriks $(I + A)$ dan $(I - A)$ komutatif atau $(I - A)(I + A) = (I + A)(I - A)$* [3].

Bukti. Misalkan A matriks *skew-symmetric* berukuran $n \times n$ dan I matriks identitas. Perhatikan bahwa,

$$\begin{aligned}(I + A)(I - A) &= (I + A)I - (I + A)A \\ &= I^2 + AI - IA - A^2 \\ &= I^2 - A^2 \end{aligned} \quad (1)$$

dan

$$\begin{aligned}(I - A)(I + A) &= (I - A)I + (I - A)A \\ &= I^2 - AI + IA - A^2 \\ &= I^2 - A^2 \end{aligned} \quad (2)$$

Terlihat bahwa, persamaan (1) dan (2) sama. Dengan demikian, $(I - A)(I + A) = (I + A)(I - A)$ atau $(I + A)$ dan $(I - A)$ komutatif. ■

Teorema 3. *Misalkan A suatu matriks skew-symmetric berukuran $n \times n$ dan I matriks identitas. Jika $L = (I - A)(I + A)^{-1}$merupakan matriks ortogonal, maka $L^T L = LL^T = I$* [3].

Bukti. Misalkan A matriks *skew-symmetric* berukuran $n \times n$ dan I matriks identitas. Misalkan $L = (I - A)(I + A)^{-1}$ suatu matriks ortogonal, maka

$$\begin{aligned}L^T L &= \left((I - A)(I + A)^{-1}\right)^T \left((I - A)(I + A)^{-1}\right) \\ &= ((I + A)^{-1})^T (I - A)^T \left((I - A)(\alpha I + A)^{-1}\right) \\ &= ((I + A)^T)^{-1} (I - A)^T \left((I - A)(I + A)^{-1}\right) \\ &= (I + A^T)^{-1} (I - A^T) \left((I - A)(I + A)^{-1}\right) \\ &= \left((I - A)^{-1}(I + A)\right)\left((I - A)(I + A)^{-1}\right) \\ &= \left((I - A)^{-1}(I - A)\right)\left((I + A)(I + A)^{-1}\right) \\ &= I.I \\ &= I. \end{aligned}$$

Sehingga, terbukti $L = (I - A)(I + A)^{-1}$ matriks ortogonal.■

2.2. Affine-Hill Cipher

Affine-Hill Cipher merupakan perluasan konsep metode kriptografi Affine Cipher dan Hill Cipher. Proses enkripsi didefinisikan sebagai

$$E(P) = C_i \equiv (P_i M + B) (\text{mod } p) \quad (3)$$

dan proses dekripsi didefinisikan sebagai

$$D(C) = P_i \equiv (C_i - B) M^* (\text{mod } p). \quad (4)$$

P_i, C_i, dan B adalah matriks berukuran $1 \times n$ serta M adalah matriks kunci berukuran $n \times n$. Dengan P_i matriks untuk *plaintext*, C_i matriks untuk *ciphertext*, dan B matriks pergeseran. p merupakan bilangan prima yang lebih besar dari jumlah karakter berbeda dalam *plaintext*.

2.3. Algoritma *Key Exchange*

Misalkan p bilangan prima. Pilih *private key* d sedemikian sehingga $1 < d < \phi(p)$ lalu suatu akar primitif dari p, misalkan sebagai β. Tetapkan $T_1 = \beta$ dan $T_2 = T_1^d (\text{mod } p)$. Konstruksi (p, T_1, T_2) sebagai *public key*. *Key exchange* dalam proses enkripsi menggunakan *public key* (p, T_1, T_2) yang sudah diterima untuk menghasilkan *signature* $k = T_1^e (\text{mod } p)$ dimana $e \in \mathbb{Z}$ sembarang dan $1 < e < \phi(p)$ dan *secret key* $\xi = T_2^e (\text{mod } p)$.

3. Hasil dan Pembahasan

Pada bagian ini diberikan algoritma lengkap dalam proses kriptografi dalam penelitian ini. Selain itu, diberikan proposisi berikut.

Proposisi 1. *Misalkan A suatu matriks skew-symmetric berukuran $n \times n$ dan I matriks identitas. Jika $M = (\alpha I - A)(\alpha I + A)^{-1}$ untuk suatu $\alpha \in \mathbb{Z}$ merupakan matriks ortogonal, maka $M^T M = MM^T = I$.*

Bukti. Misalkan A matriks *skew-symmetric* berukuran $n \times n$ dan I matriks identitas. Misalkan $M = (\alpha I - A)(\alpha I + A)^{-1}$ suatu matriks ortogonal, maka

$$\begin{aligned}M^T M &= \left((\alpha I - A)(\alpha I + A)^{-1}\right)^T \left((\alpha I - A)(\alpha I + A)^{-1}\right) \\ &= ((\alpha I + A)^{-1})^T (\alpha I - A)^T \left((\alpha I - A)(\alpha I + A)^{-1}\right) \\ &= ((\alpha I + A)^T)^{-1} (\alpha I - A)^T \left((\alpha I - A)(\alpha I + A)^{-1}\right) \\ &= (\alpha I + A^T)^{-1} (\alpha I - A^T) \left((\alpha I - A)(\alpha I + A)^{-1}\right) \\ &= \left((\alpha I - \boldsymbol{A})^{-1}(\alpha I + \boldsymbol{A})\right)\left((\alpha I - A)(\alpha I + A)^{-1}\right) \\ &= \left((\alpha I - A)^{-1}(\alpha I - A)\right)\left((\alpha I + A)(\alpha I + A)^{-1}\right) \\ &= I.I \\ &= I. \end{aligned}$$

Sehingga, terbukti $M = (\alpha I - A)(\alpha I + A)^{-1}$ matriks ortogonal. ■

Selanjutnya diberikan algoritma untuk mengonstruksi *public key* dan enkripsi dan dekripsi menggunakan Affine-Hill Cipher.

Algoritma 1: *Public key*

1. Pilih bilangan prima p.
2. Pilih *private key* d sedemikian sehingga $1 < d < \phi(p)$.
3. Pilih β, yaitu akar primitif dari p.
4. Tentukan $T_1 = \beta$ dan $T_2 = T_1^d (\text{mod } p)$.

5. Konstruksi $pk(p, T_1, T_2)$ sebagai *public key*.

Algoritma 2: Enkripsi
1. Pilih bilangan e, sehingga $1 < e < \phi(p)$.
2. Hitung signature $k = T_1^e \pmod p$.
3. Hitung secret key $\xi = T_2^e \pmod p$.
4. Tetapkan A sebagai matriks skew-symmetric berukuran $\xi \times \xi$ dengan entri-entri sembarang bilangan bulat. Matriks A bersifat rahasia.
5. Hitung matriks kunci $M = (kI - A)(kI + A)^{-1} \pmod p$.
6. Lakukan enkripsi dengan persamaan (3).

Algoritma 3: Dekripsi
1. Tetapkan matriks kunci $M^* = (kI + A)(kI - A)^{-1} \pmod p$.
2. Lakukan dekripsi dengan menggunakan persamaan (4).

Berikut contoh penerapan algoritma-algoritma yang ditunjukkan. Misalkan "Alice" sebagai pengirim pesan dan "Bob" penerima pesan. Dalam hal ini, 26 huruf berkorespondensi dengan angka-angka 0 sampai 25 dan tiga simbol "?", ",", "!" berkorespondensi dengan angka 26, 27, dan 28 secara berturut sehingga modulo $p = 29$.

Contoh 1. (*Public key*) Misalkan $p = 29$ dan *private key* Bob adalah $d = 17$. Selanjutnya Bob memilih akar primitif dari p, misalkan $\beta = 2$. Sehingga dapat diperoleh

$$T_1 = \beta = 2$$

dan

$$T_2 = T_1^d \pmod p = 2^{17} \pmod{29} = 21.$$

Sehingga konstruksi *public key* dari Bob adalah $pk(29,2,21)$.

Contoh 2. (Enkripsi) Alice akan mengirimkan pesan plaintext yaitu **PLEASE BE AWARE!**, dengan *public key* $pk(29,2,21)$ dan pergeseran $B = [13 \quad 23 \quad 19 \quad 17]$. Berdasarkan Algoritma 1, maka pilih $e = 10$ sehingga $1 < e < \phi(29)$. Selanjutnya hitung *signature* $k = T_1^e \pmod p = 2^{10} \pmod{29} = 9$ dan *secret key* $\xi = T_2^e \pmod p = 21^{10} \pmod{29} = 4$.

Selanjutnya, tetapkan matriks kunci berukuran 4×4 yang skew-symmetric dengan entri-entri sembarang bilangan bulat, yaitu

$$A = \begin{bmatrix} 0 & 7 & 6 & -9 \\ -7 & 0 & 5 & 8 \\ -6 & -5 & 0 & -3 \\ 9 & -8 & 3 & 0 \end{bmatrix}.$$

Menggunakan persamaan $M = (9I - A)(9I + A)^{-1} \pmod{29}$, diperoleh matriks kunci

$$M = \begin{bmatrix} 20 & 19 & 25 & 6 \\ 9 & 10 & 28 & 15 \\ 19 & 18 & 23 & 11 \\ 0 & 17 & 8 & 24 \end{bmatrix}.$$

Kemudian *plaintext* $\mathbf{P} = \mathbf{PLEASEBEAWARE!}$ dibagi ke dalam matriks berukuran 1×4. Karena jumlah karakter pada plaintext adalah 14, tambahkan 2 karakter dummy menjadi $\mathbf{P_D} = \mathbf{PLEASEBEAWARE!!!}$ sehingga diperoleh

$$P_1 = [\boldsymbol{P} \quad \boldsymbol{L} \quad \boldsymbol{E} \quad \boldsymbol{A}] = [15 \quad 11 \quad 4 \quad 0],$$
$$P_2 = [\boldsymbol{S} \quad \boldsymbol{E} \quad \boldsymbol{B} \quad \boldsymbol{E}] = [18 \quad 4 \quad 1 \quad 4],$$
$$P_3 = [\boldsymbol{A} \quad \boldsymbol{W} \quad \boldsymbol{A} \quad \boldsymbol{R}] = [0 \quad 22 \quad 0 \quad 17], \; dan$$
$$P_4 = [\boldsymbol{E} \quad ! \quad ! \quad !] = [4 \quad 28 \quad 28 \quad 28].$$

Enkripsikan matriks P_i menggunakan persamaan (3), maka:

$$C_1 = (P_1 M + B) \equiv \left([15 \quad 11 \quad 4 \quad 0] \begin{bmatrix} 20 & 19 & 25 & 6 \\ 9 & 10 & 28 & 15 \\ 19 & 18 & 23 & 11 \\ 0 & 17 & 8 & 24 \end{bmatrix} + [13 \quad 23 \quad 19 \quad 17] \right) \pmod{29}$$
$$= [24 \quad 26 \quad 11 \quad 26] = [\mathbf{Y} \quad \mathbf{Z} \quad \mathbf{L} \quad \mathbf{Z}].$$

$$C_2 = (P_2 M + B) \equiv \left([18 \quad 4 \quad 1 \quad 4] \begin{bmatrix} 20 & 19 & 25 & 6 \\ 9 & 10 & 28 & 15 \\ 19 & 18 & 23 & 11 \\ 0 & 17 & 8 & 24 \end{bmatrix} + [13 \quad 23 \quad 19 \quad 17] \right) \pmod{29}$$
$$= [22 \quad 27 \quad 27 \quad 2] = [\mathbf{W} \quad ? \quad ? \quad \mathbf{C}].$$

$$C_3 = (P_3M + B) \equiv \left([0 \quad 22 \quad 0 \quad 17] \begin{bmatrix} 20 & 19 & 25 & 6 \\ 9 & 10 & 28 & 15 \\ 19 & 18 & 23 & 11 \\ 0 & 17 & 8 & 24 \end{bmatrix} + [13 \quad 23 \quad 19 \quad 17] \right) (\text{mod } 29)$$
$$= [8 \quad 10 \quad 17 \quad 1] = [\mathbf{I} \quad \mathbf{K} \quad \mathbf{R} \quad \mathbf{B}].$$

$$C_4 = (P_4M + B) \equiv \left([4 \quad 28 \quad 28 \quad 28] \begin{bmatrix} 20 & 19 & 25 & 6 \\ 9 & 10 & 28 & 15 \\ 19 & 18 & 23 & 11 \\ 0 & 17 & 8 & 24 \end{bmatrix} + [13 \quad 23 \quad 19 \quad 17] \right) (\text{mod } 29)$$
$$= [7 \quad 25 \quad 2 \quad 20] = [\mathbf{H} \quad \mathbf{Z} \quad \mathbf{B} \quad \mathbf{U}].$$

Sehingga diperoleh *ciphertext* YZLZW??CIKRBHZBU. Selanjutnya Alice akan mengirimkan pesan berupa *ciphertext* $\mathbf{C} = \mathbf{YZLZW??CIKRBHZBU}$ kepada Bob dengan menyertakan matriks A dan *signature* k.

Contoh 3. (Dekripsi) Bob menerima *ciphertext* **C** beserta matriks A dan *signature* k dari Alice. Menggunakan Algoritma 3, bob akan mencari matriks kunci $M^* = (9I + A)(9I - A)^{-1} (\text{mod } 29)$, yaitu

$$M^* = \begin{bmatrix} 20 & 9 & 19 & 0 \\ 19 & 10 & 18 & 17 \\ 25 & 28 & 23 & 8 \\ 6 & 15 & 11 & 24 \end{bmatrix}.$$

Jelas bahwa $MM^* = M^*M \equiv I (\text{mod } 29)$. Kemudian ciphertext $\mathbf{C} = \mathbf{YZLZW??CIKRBHZBU}$ dibagi ke dalam matriks berukuran 1×4, yaitu

$C_1 = [\mathbf{Y} \quad \mathbf{Z} \quad \mathbf{L} \quad \mathbf{Z}] = [24 \quad 26 \quad 11 \quad 26]$,
$C_2 = [\mathbf{W} \quad ? \quad ? \quad \mathbf{C}] = [22 \quad 27 \quad 27 \quad 2]$,
$C_3 = [\mathbf{I} \quad \mathbf{K} \quad \mathbf{R} \quad \mathbf{B}] = [8 \quad 10 \quad 17 \quad 1]$, dan
$C_4 = [\mathbf{H} \quad \mathbf{Z} \quad \mathbf{B} \quad \mathbf{U}] = [7 \quad 25 \quad 2 \quad 20]$.

Dekripsikan matriks C_i menggunakan persamaan (4), maka:

$$P_1 = (\mathrm{C}_1 - B)M^* \equiv \left(([24 \quad 26 \quad 11 \quad 26] - [13 \quad 23 \quad 19 \quad 17]) \begin{bmatrix} 20 & 9 & 19 & 0 \\ 19 & 10 & 18 & 17 \\ 25 & 28 & 23 & 8 \\ 6 & 15 & 11 & 24 \end{bmatrix} \right) (\text{mod } 29)$$
$$= [15 \quad 11 \quad 4 \quad 0] = [\mathbf{P} \quad \mathbf{L} \quad \mathbf{E} \quad \mathbf{A}].$$

$$P_2 = (\mathrm{C}_2 - B)M^* \equiv \left(([22 \quad 27 \quad 27 \quad 2] - [13 \quad 23 \quad 19 \quad 17]) \begin{bmatrix} 20 & 9 & 19 & 0 \\ 19 & 10 & 18 & 17 \\ 25 & 28 & 23 & 8 \\ 6 & 15 & 11 & 24 \end{bmatrix} \right) (\text{mod } 29)$$
$$= [18 \quad 4 \quad 1 \quad 4] = [\mathbf{S} \quad \mathbf{E} \quad \mathbf{B} \quad \mathbf{E}].$$

$$P_3 = (\mathrm{C}_3 - B)M^* \equiv \left(([8 \quad 10 \quad 17 \quad 1] - [13 \quad 23 \quad 19 \quad 17]) \begin{bmatrix} 20 & 9 & 19 & 0 \\ 19 & 10 & 18 & 17 \\ 25 & 28 & 23 & 8 \\ 6 & 15 & 11 & 24 \end{bmatrix} \right) (\text{mod } 29)$$
$$= [0 \quad 22 \quad 0 \quad 17] = [\mathbf{A} \quad \mathbf{W} \quad \mathbf{A} \quad \mathbf{R}].$$

$$P_4 = (\mathrm{C}_4 - B)M^* \equiv \left(([7 \quad 25 \quad 2 \quad 20] - [13 \quad 23 \quad 19 \quad 17]) \begin{bmatrix} 20 & 9 & 19 & 0 \\ 19 & 10 & 18 & 17 \\ 25 & 28 & 23 & 8 \\ 6 & 15 & 11 & 24 \end{bmatrix} \right) (\text{mod } 29)$$
$$= [4 \quad 28 \quad 28 \quad 28] = [\mathbf{E} \quad ! \quad ! \quad !].$$

Sehingga *plaintext* berhasil dipulihkan, yaitu **PLEASE BE AWARE!!!**.

4. Kesimpulan

Implementasi matriks *skew-symmetric* dalam algoritma Affine-Hill Cipher dengan konsep *public key* yang diusulkan dapat meningkatkan keamanan data. Hal tersebut disebabkan oleh matriks *skew-symmetric* A dan *signature* k yang hanya diketahui oleh pengirim (Alice) dan penerima (Bob). Selain itu, matriks *skew-symmetric* A diubah terlebih dahulu menjadi matriks ortogonal M sehingga yang menjadi matriks kunci dalam algoritma ini adalah matriks M. Berdasarkan hal tersebut, keamanan dapat diminimalisir jika matriks *skew-symmetric* A diketahui penyusup. Untuk penelitian selanjutnya, algoritma ini dapat dikembangkan dengan mengonstruksi matriks *skew-symmetric* dengan entri-entri matriks yang dapat ditentukan dengan suatu pola sehingga meningkatkan kompleksitas dan keamanan data.

Daftar Pustaka

1. Maulana, K., Nofrianto, D., & and others. 2023. Hill-Cipher Method with Matrice In Text Coding Processing. *Klik-Kumpulan Jurnal Ilmu Komputer*, *10*(1), 51–61.
2. Alawiyah, T., Hikmah, A. B., Wiguna, W., Kusmira, M., Sutisna, H., & Simpony, B. K. 2020. Generation of Rectangular Matrix Key for Hill Cipher Algorithm Using Playfair Cipher. *Journal of Physics: Conference Series*, *1641*(1), 012094. https://doi.org/10.1088/1742-6596/1641/1/012094.
3. Liew, K. J., & Nguyen, V. 2020. Hill Cipher Key Generation Using Skew-symmetric Matrix.
4. Chen, Y., Xie, R., Zhang, H., Li, D., & Lin, W. 2023. Generation of high-order random key matrix for Hill Cipher encryption using the modular multiplicative inverse of triangular matrices. *Wireless Networks*. https://doi.org/10.1007/s11276-023-03330-8.
5. Acharya, B., Rath, G., Patra, S., & Panigrahy, S. K. 2007. Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm. *International Journal of Security*, *1*.
6. Hidayat, A., & Alawiyah, T. 2013. Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang. *Jurnal Matematika Integratif*, *9*(1), 39. https://doi.org/10.24198/jmi.v9.n1.10196.39-52.
7. Kanwal, S., Inam, S., Othman, M. T. Ben, Waqar, A., Ibrahim, M., Nawaz, F., Hamam, H. 2022. An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices. *Sensors*, *22*(12), 4359. https://doi.org/10.3390/s22124359.
8. Sharma, N., & Chirgaiya, S. 2014. A Novel Approach to Hill Cipher. *International Journal of Computer Applications*, *108*, 34–37. https://doi.org/10.5120/18958-0285.
9. Sundarayya, P., & Vara Prasad, G. 2019. A public key cryptosystem using Affine Hill Cipher under modulation of prime number. *Journal of Information and Optimization Sciences*, *40*(4), 919–930. https://doi.org/10.1080/02522667.2018.1470751.
10. Prasad, K., & Mahato, H. 2022. Cryptography using generalized Fibonacci matrices with Affine-Hill cipher. *Journal of Discrete Mathematical Sciences and Cryptography*, *25*(8), 2341–2352. https://doi.org/10.1080/09720529.2020.1838744.
11. Billore, V., & Patel, N. 2023. Cryptography utilizing the Affine-Hill cipher and Extended Generalized Fibonacci matrices. *Electronic Journal of Mathematical Analysis and Applications*, *11*(2), 1–11. https://doi.org/10.21608/ejmaa.2023.295792.
12. Kumari, M., & Tanti, J. 2023. Cryptography using multinacci block matrices. *International Journal of Nonlinear Analysis and Applications*. https://doi.org/10.22075/ijnaa.2023.29918.4295.
13. Mohanta, K. K., & Sharanappa, D. S. 2022. A Public-Key Cryptographic Model Based on Hybrid Key Exchange Technique using Affine-Hill Cipher. *Communications in Combinatorics, Cryptography & Computer Science*, *2022*(2), 94–104.
14. Kumari, M., & Tanti, J. 2020. A public key cryptography using multinacci block matrices. *arXiv preprint arXiv:2003.08634*.
15. Prasad, K., Mahato, H., & Kumari, M. 2022, October. A novel public key cryptography based on generalized Lucas matrices.
16. Viswanath, M. K., & Kumar, M. R. 2015. A Public Key Cryptosystem Using Hiil's Cipher. *Journal of Discrete Mathematical Sciences and Cryptography*, *18*(1–2), 129–138. https://doi.org/10.1080/09720529.2014.962856.