JOURNAL OF FUNDAMENTAL MATHEMATICS
AND APPLICATIONS (JFMA), Vol. 1, No. 2 (Nov 2018)
Available online at www.jfma.matematika.undip.ac.id

BEBERAPA MODIFIKASI PADA ALGORITMA KRIPTOGRAFI AFFINE CIPHER

Dian Eka Wijayanti

Program Studi Matematika Universitas Ahmad Dahlan, Yogyakarta, Indonesia
Email: dian@math.uad.ac.id

Abstract. Affine Cipher Cryptography Technique is one of the techniques in classical cryptography which is quite simple so it is very vulnerable to cryptanalysis. Affine cipher's advantage is having an algorithm that can be modified with various techniques. The modifications that can be made to Affine Cipher is to combine Affine cipher's algorithm with other ciphers, replace Affine cipher's key with various functions and matrices and expand the space for plaintext and ciphertexts on Affine cipher. Affine cipher can also be applied to the stream cipher as a keystream generator. This research discusses several modifications of Affine cipher algorithm and performs several other modifications. These modifications are combining Affine Chiper and Vigenere Cipher on $\mathbb{Z}_{29}$, combining Affine, Vigenere and Hill Cipher with invertible matrix applications on $M_{2x2}(\mathbb{Z}_{29})$. Furthermore, a comparison of the three modifications will be carried out to obtain a new cryptographic method that is more resilient to the cryptanalysis process.
Keywords: affine cipher, vigenere cipher, hill cipher, stream cipher, cryptanalysis.

Abstrak. Teknik Kriptografi Affine *Cipher* merupakan salah satu tehnik dalam kriptografi klasik yang cukup sederhana sehingga sangat rentan terhadap kriptanalisis. Kelebihan Affine *cipher* adalah mempunyai algoritma yang dapat dimodifikasi dengan berbagai teknik. Modifikasi yang dapat dilakukan pada Affine Cipher adalah menggabungkan algoritma Affine *cipher* dengan *cipher* lain, mengganti kunci Affine *cipher* dengan berbagai fungsi dan matriks dan memperluas ruang plainteks dan cipherteks pada Affine *cipher*. Affine *cipher* juga dapat diaplikasikan pada *stream cipher* sebagai pembangkit *keystream*. Penelitian ini membahas beberapa modifikasi yang telah dilakukan kriptografi affine *cipher* dan melakukan beberapa modifikasi lain yaitu mengkombinasikan Affine chiper dan Vigenere *Cipher* pada $\mathbb{Z}_{29}$, mengkombinasikan Affine, Vigenere dan Hill *Cipher* dengan aplikasi matriks invertibel pada $M_{2x2}(\mathbb{Z}_{29})$ dan mengganti kunci Affine-Hill *cipher* dengan *keystream* matriks-matriks invertibel. Selanjutnya akan dilakukan perbandingan dari ketiga modifikasi untuk memperoleh sebuah metode kriptografi baru yang lebih tangguh terhadap proses kriptanalisis.
Kata kunci: affine *cipher,* vigenere *cipher*, hill *cipher*, stream *cipher*, *cryptanalysis*.

I. PENDAHULUAN

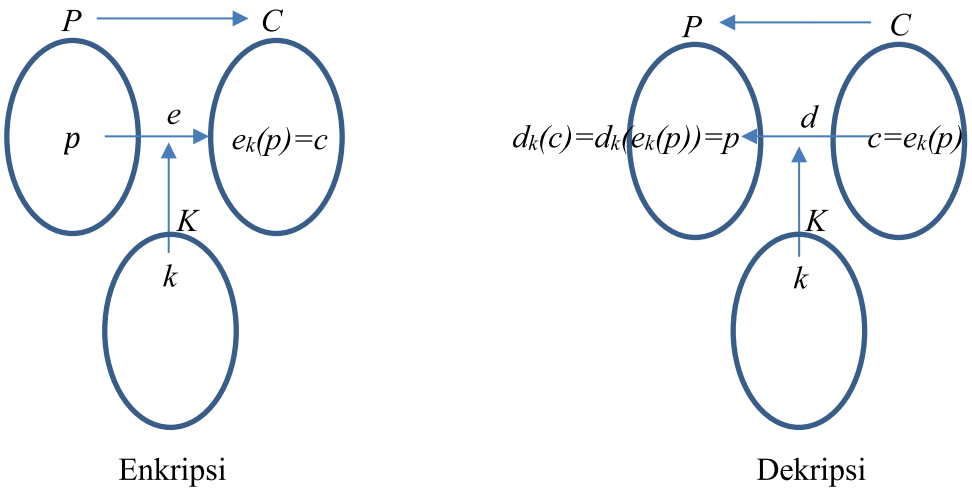
Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan (*confidentiality*), integritas data (*data integrity*), autentikasi (*authentication*), anti penyangkalan (*non-repudiation*)[1][2]. Tujuan mendasar kriptografi adalah untuk memungkinkan dua pihak berkomunikasi melalui media yang tidak aman tetapi pihak lain yang tidak berkepentingan tidak mengerti apa isi komunikasi kedua pihak tersebut [3]. Pesan awal (plainteks) diubah ke bentuk pesan rahasia (cipherteks). Proses ini disebut enkripsi dan proses kebalikannya untuk mengubah cipherteks kembali

menjadi plainteks disebut dekripsi . Proses enkripsi dan dekripsi ini memerlukan suatu mekanisme dan kunci tertentu yang dilakukan menggunakan suatu algoritma dengan berbagai tehnik yang menggunakan konsep-konsep dalam bidang matematika [4][5]. Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara himpunan yang beranggotakan elemen-elemen plainteks dengan himpunan yang beranggotakan elemen-elemen cipherteks [1][6]. Teknik untuk mencoba memecahkan sistem kriptografi ini tanpa mengetahui kunci enkripsinya dinamakan kriptanalisis [7].

Sejarah awal mula kriptografi sebelum era komputerisasi menggunakan pena, kertas dibantu dengan alat mekanik sederhana. Kriptografi pada era ini dinamakan kriptografi klasik. Beberapa contoh dari kriptografi klasik antara lain shift cipher, subtitusi cipher, permutasi cipher, Vigenere cipher dan Affine cipher . Pada teknik enkripsi klasik sederhana seperti Affine cipher, sangatlah mudah untuk dipecahkan dengan kriptanalisis sehingga diperlukan modifikasi untuk membuatnya layak digunakan dalam kriptografi modern. Berbagai ilmu matematika seperti aljabar, teori bilangan dan teori koding telah digunakan untuk mengembangkan dan melakukan modifikasi pada kriptografi affine cipher. Paper ini membahas beberapa modifikasi yang sudah dilakukan pada Affine cipher dan melakukan beberapa modifikasi pada Affine *cipher*. Lebih lanjut, akan dilakukan perbandingan algoritma Affine cipher yang telah dimodifikasi guna memperoleh tehnik enkripsi baru yang lebih tangguh dan mempunyai banyak kelebihan untuk kemudian dibuat program komputasi dalam sebagai algoritma cipher baru [5].

II. KONSEP DASAR MODIFIKASI PADA AFFINE CIPHER

Misalkan P adalah himpunan yang beranggotakan elemen-elemen plainteks dan C adalah himpunan yang beranggotakan elemen-elemen cipherteks. Fungsi enkripsi e memetakan anggota P ke C dan fungsi dekripsi d memetakan anggota C ke P. Karena proses enkripsi $e(p)=c$ kemudian dekripsi $d(c)= p$ mengembalikan pesan acak ke pesan semula maka berlaku $d(e(p))=p$. Kunci (*key*) k, adalah parameter berupa *string* atau deretan bilangan yang digunakan untuk transformasi enkripsi dan dekripsi [8][9].



Gambar 1. Skema Enkripsi dan Dekripsi dalam Kriptografi

Pada Affine *cipher*, $P = C = \mathbb{Z}_{26}$ dengan $K = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\}$. Untuk $k = (a, b) \in K$ didefinisikan [10][11]:

$$e_k(x) = (ax + b)\ mod\ 26$$
$$d_k(y) = a^{-1}(y - b)\ mod\ 26 \quad (1)$$

untuk setiap $x, y \in \mathbb{Z}_{26}$ dan a^{-1} adalah invers modulo 26 dari a. Algoritma enkripsi dan dekripsi ini memungkinkan kita untuk melakukan modifikasi-modifikasi pada himpunan plainteks dan cipherteks yaitu dengan memperluasnya dari $\mathbb{Z}_{26}$ ke $\mathbb{Z}_n$ dimana *n* adalah suatu bilangan prima. Modifikasi ini sebenarnya sangat sederhana akan tetapi efektif untuk dilakukan karena selain memperluas ruang kunci juga menambah banyak kemungkinan cipherteks yang dihasilkan. Nilai *n* yang prima berakibat berapapun nilai *a* yang dipilih pastilah memenuhi $\gcd(a, n) = 1$. Penggunaan matriks sebagai kunci juga efektif dalam melakukan modifikasi karena pola bilangan dalam pemilihan kunci akan lebih acak. Konsep stream cipher pun juga bisa diaplikasikan pada algoritma Affine cipher, yaitu dengan mengganti kunci *k* dengan kunci aliran (keystream)[12][7].

III. BEBERAPA MODIFIKASI PADA AFFINE CIPHER

3.1 Modifikasi Yang Telah Dilakukan Pada Affine Cipher

Banyak modifikasi yang telah dilakukan pada Affine *cipher*. Untuk menambah keacakan kunci yang digunakan dilakukan perluasan ruang kunci pada generator kuncinya yaitu dengan menggunakan matriks berordo 3 yang dicerminkan pada garis sembarang.

$$e(X) = (AX + B) \bmod 26 \quad (2)$$

(A, B) adalah pasangan kunci matriks berordo 3x3 [13]. Pada modifikasi affine cipher yang digunakan untuk password maka modifikasi sederhana dilakukan pada ruang plainteks dan cipherteks yaitu dari $\mathbb{Z}_{26}$ menjadi $\mathbb{Z}_{36}$ sehingga fungsi enkripsinya menjadi

$$e(\mathrm{x}) = (\mathrm{ax} + \mathrm{b}) \bmod 36 \quad (3)$$

dan fungsi dekripsinya menjadi

$$\mathrm{d_K(y)} = \mathrm{a^{-1}(y - b)} \bmod 36 \quad (4)$$

dengan nilai a dan b yang relatif prima terhadap 36 [14]. Modifikasi yang dilakukan Hartini ini dapat lebih maksimal jika nilai n yang diambil bukanlah 36 melainkan suatu bilangan prima seperti 37. Modifikasi pada Affine juga dapat dilakukan dengan penggabungan tehnik enkripsi Affine dengan Hill *cipher* menggunakan matriks 4 x 4 pada proses enkripsi Affine *cipher* yaitu dengan mengganti bilangan kunci dengan matriks dan menggunakan *invers* modulo untuk mendekripsikan kembali cipherteks menjadi plainteks [15]. Penggabungan lainnya yaitu Affine cipher dengan Vigenere cipher dengan nilai *n* = 40. Modifikasi ini sebenarnya juga efektif, akan tetapi pemilihan nilai *a* yang harus relatif prima dengan 40 mempersempit kemungkinan nilai *a* yaitu salah satu bilangan bulat anggota {1, 3, 7, 9, 11, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39} yang berjumlah 16 bilangan. Hal ini berakibat kombinasi kunci (*a, b*) sebanyak 16 x 40 = 640 kemungkinan [16]. Fungsi Gamma dan Hiperbolik juga dapat digunakan dalam modifikasi algoritma Affine *Cipher* yaitu dengan mensubtitusi fungsi gamma sebagai nilai *a* dan fungsi hiperbolik sebagai nilai *b* [17]. Modifikasi lainnya dapat dilakukan pada transformasi Affine tergeneralisir berdasarkan matriks *Circulant* [18].

3.2 Modifikasi Kombinasi Affine *Cipher* Dan Vigenere *Cipher* Pada $\mathbb{Z}_{29}$

Vigenere *cipher* adalah metode kriptografi *polyalphabetic* (*polyalphabetic cryptosystem)* yang mengenkripsi plainteks dengan menambahkan numerik pada kata kunci ke numerik alphabet plainteks yang bersesuaian. Kriptosistem vigenere *cipher* dijelaskan sebagai berikut ,

Definisi 1 [2]. *Misalkan m bilangan bulat positif. Definisikan* $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. *Untuk kunci* $\mathcal{K} = \{k_1, k_2, \dots, k_m\}$ *didefinisikan*

$$e_K(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m) \; mod \; 26$$

dan

$$d_K(y) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m) \; mod \; 26$$

untuk setiap $x, y, k \in \mathbb{Z}_{26}$.

Affgenere (Affine Vigenere) *cipher* dapat dilakukan dengan mengkombinasikan fungsi enkripsi dan dekripsi Affine *cipher* dengan vigenere *cipher* dan memperluas ruang plainteks dan cipherteks dalam $\mathbb{Z}_{29}$. menjadi :

$$e_K(x_1, x_2, \dots, x_m) = (ax_1 + k_1, \; ax_2 + k_2, \dots, ax_m + k_m) \bmod 29 \qquad (4)$$

dan

$$d_K(y) = (a^{-1}y_1 - k_1, a^{-1}y_2 - k_2, \dots, a^{-1}y_m - k_m) \bmod 29 \qquad (5)$$

Bilangan $p = 29$ diperoleh dari jumlah 26 abjad dari A sampai Z ditambah dengan spasi, koma dan titik.

Tabel 2. Proses Enkripsi Modifikasi Kombinasi Affine *Cipher* dan Vigenere *Cipher* pada $\mathbb{Z}_{29}$ dengan $a = 3$

Plainteks	x_i	Proses enkripsi $y_i = (ax_i + k_i) \text{Mod } 29$	y_i	Cipherteks
U	20	$y_1 = (3.20 + 12) \text{Mod } 29$	14	O
A	0	$y_1 = (3.0 + 8) \text{Mod } 29$	8	I
D	3	$y_1 = (3.3 + 15) \text{Mod } 29$	24	Y
Spasi	26	$y_1 = (3.26 + 0) \text{Mod } 29$	20	U
H	7	$y_1 = (3.7 + 26) \text{Mod } 29$	18	S
E	4	$y_1 = (3.4 + 9) \text{Mod } 29$	21	V
B	1	$y_1 = (3.1 + 0) \text{Mod } 29$	3	D
A	0	$y_1 = (3.0 + 24) \text{Mod } 29$	24	Y
T	19	$y_1 = (3.19 + 0) \text{Mod } 29$	28	,

Contoh 1. Jika dipilih nilai $a = 3$ dan kata kunci MIPA JAYA sebagai nilai k_i maka hasil konversi kunci dan plainteks UAD HEBAT diberikan pada Tabel 1.

Tabel 1. Konversi Nilai Plainteks dan Kunci

Plainteks	x_i	Kunci	k_i
UAD HEBAT	20 0 3 26 7 4 1 0 19	MIPA JAYA	12 8 15 0 26 9 0 24 0

Diperoleh hasil enkripsi plainteks pada Tabel 2.

3.3 Modifikasi Kombinasi Affine, Vigenere Dan Hill *Cipher* (Affgenere-Hill *Cipher*) Dengan Aplikasi Matriks Invertibel Pada $M_{2x2}(\mathbb{Z}_{29})$

Modifikasi pada Affine cipher akan dilakukan dengan mengkombinasikan affine cipher dengan hill cipher lalu mengaplikasikan penggunaan matriks invertibel sebagai kuncinya. Hill *cipher* adalah kriptografi dengan kriptosistem *polyalphabetic* yang mengenkripsi kombinasi linear dari m karakter alphabet sebagai satu elemen pada plainteks yang kemudian menghasilkan m karakter alphabet dalam satu elemen cipherteks. Kriptosistem dari Hill *cipher* dapat dijelaskan dalam definisi berikut.

Definisi 2 [3][11]. *Misalkan bilangan bulat,* $m \geq 2$ *dan misalkan* $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ *dan misalkan* $\mathcal{K} = \{m \times m\,;\, matriks\ yang\ invertibel\ pada\ \mathbb{Z}_{26}\}$. *Untuk* $K \in \mathcal{K}$ *didefinisikan:*

$$e_K(x) = xK \tag{6}$$

dan

$$d_K(y) = y\,K^{-1} \tag{7}$$

dengan semua operasi pada $\mathbb{Z}_{26}$ *dan invers matriks yang dimaksud adalah invers matriks modulo pada* $\mathbb{Z}_{26}$.

Secara umum, Kriptosistem Affgenere-Hill *Cipher* dapat dirumuskan sebagai berikut :

Jika diberikan $\mathcal{P} = \mathcal{C} = M_{2x2}(\mathbb{Z}_{29})$ dan $\mathcal{K} = \{(A, B_i) | A, B_i, \mathrm{A}^{-1} \in M_{2x2}(\mathbb{Z}_{29})\}$ maka fungsi enkripsi dan dekripsi untuk setiap $\mathrm{K} = (\mathrm{A}, \mathrm{B}) \in \mathcal{K}$, didefinisikan berturut-turut sebagai :

$$Y_i = e_K(X_i) = (AX_i + B_i)\ mod\ 29 \tag{8}$$

dan

$$X_i = d_K(X_i) = A^{-1}(Y_i - B_i)\ mod\ 29 \tag{9}$$

$X_i, Y_i, B_i, A \in M_{2x2}(\mathbb{Z}_{29})$, A invertibel dengan A^{-1} adalah invers modulo dari A. Langkah-langkah pembangkitan dilakukan sebagai berikut :

1. Susunlah barisan bilangan plainteks kedalam matriks ukuran 2x2 sebagai berikut $x_1, x_2, x_3, x_4, \ldots, x_n$ menjadi $X_1 = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}, \cdots, X_{n/4} = \begin{bmatrix} x_{n-3} & x_{n-2} \\ x_{n-1} & x_n \end{bmatrix}$. Jika panjang barisan plainteks bukan kelipatan 4 maka tambahkan spasi dibelakangnya sampai menjadi kelipatan 4.
2. Tentukan kunci $\mathrm{K} = (A, B_i) \in \mathcal{K}$,
   definisikan $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ dan $B_1 = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}, \cdots, B_{n/4} = \begin{bmatrix} b_{n-3} & b_{n-2} \\ b_{n-1} & b_n \end{bmatrix}$.

Matriks A yang dipilih haruslah matriks invertibel dan matriks B sama banyak dengan matriks X.

3. Dengan fungsi enkripsi pada persamaan 6 maka

$$\begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} + \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$$

Dan diperoleh cipherteks sebagai berikut

$$y_1 = \left((a_{11}x_1 + a_{12}x_3) + b_1\right) \bmod 29$$
$$y_2 = \left((a_{11}x_2 + a_{12}x_4) + b_2\right) \bmod 29$$
$$y_3 = \left((a_{21}x_1 + a_{22}x_3) + b_3\right) \bmod 29$$
$$y_4 = \left((a_{21}x_1 + a_{22}x_3) + b_4\right) \bmod 29$$

Contoh 2. Dengan menggunakan hasil modifikasi ini, plainteks UAD HEBAT dengan pemilihan kunci $A = \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}$ dan kata kunci MIPA JAYA akan dienkripsi dengan proses sebagai berikut :

Tabel 3. Proses Enkripsi Modifikasi Kombinasi Affgenere-Hill *Cipher* pada $\mathbb{Z}_{29}$

Plain teks	x_i	Kata Kunci	b_i	X_i , A dan B_i	y_i	Cipher teks
U	$x_1 = 20$	M	$b_1 = 1$	$X_1 = \begin{bmatrix} 20 & 0 \\ 3 & 26 \end{bmatrix}$	$y_1 = (1.20 + 3.3 + 12) \bmod 29 = 12$	M
A	$x_2 = 0$	I	$b_2 = 8$	$X_2 = \begin{bmatrix} 7 & 4 \\ 1 & 0 \end{bmatrix}$	$y_2 = (1.0 + 3.26 + 8) \bmod 29 = 28$	.
D	$x_3 = 3$	P	$b_3 = 1$		$y_3 = (2.20 + 5.3 + 15) \bmod 29 = 12$	M
	$x_4 = 26$	A	$b_4 = 0$	$X_3 = \begin{bmatrix} 19 & 26 \\ 26 & 26 \end{bmatrix}$	$y_4 = (2.0 + 5.26 + 0) \bmod 29 = 14$	O
H	$x_5 = 7$		$b_5 = 26$	$A = \begin{bmatrix} 1 & 3 \\ 2 & 5 \end{bmatrix}$	$y_5 = (1.7 + 3.1 + 26) \bmod 29 = 7$	H
E	$x_6 = 4$	J	$b_6 = 9$		$y_6 = (1.4 + 3.0 + 9) \bmod 29 = 13$	N
B	$x_7 = 1$	A	$b_7 = 0$	$B_1 = \begin{bmatrix} 12 & 8 \\ 15 & 0 \end{bmatrix}$	$y_7 = (2.7 + 5.1 + 0) \bmod 29 = 19$	U
A	$x_8 = 0$	Y	$b_8 = 24$	$B_2 = \begin{bmatrix} 26 & 9 \\ 0 & 24 \end{bmatrix}$	$y_8 = (2.4 + 5.0 + 24) \bmod 29 = 3$	D
T	$x_9 = 19$	A	$b_9 = 0$	$B_3 = \begin{bmatrix} 0 & 12 \\ 8 & 15 \end{bmatrix}$	$y_9 = (1.19 + 3.26 + 0) \bmod 29 = 10$	K
	$x_{10} = 2$	M	$b_{10} = 1$		$y_{10} = (1.26 + 3.26 + 12) \bmod 29 =$	A
	$x_{11} = 2$	I	$b_{11} = 8$		$y_{11} = (2.19 + 5.26 + 8) \bmod 29 = 2$	C
	$x_{12} = 2$	P	$b_{12} = 1$		$y_{12} = (2.26 + 5.26 + 15) \bmod 29 = 23$	X

3.4 Modifikasi Affine-Hill *Cipher* Dengan *Keystream* Matriks-Matriks Invertibel

Modifikasi Affine-Hill *Cipher* dengan keystream matriks-matriks invertibel dapat dilakukan sebagai berikut :
Pilih dua matriks yang invertibel, $A, B \in M_{2x2}(\mathbb{Z}_{29})$ dan bangkitkan himpunan $\mathcal{A} = \langle A \rangle = \{A_i = A^i \,|1 \leq i \leq 28\} = \{A^i\}$ dan $\mathcal{B} = \langle B \rangle = \{B_i = B^i \,|1 \leq i \leq 28\}$. Lebih lanjut, bentuk

$$\mathcal{K} = \{(A_i, B_i) | A_i \in \mathcal{A}, B_i \in \mathcal{B}\}$$

maka fungsi enkripsi dan dekripsi untuk setiap $K = (A_i, B_i) \in \mathcal{K}$, didefinisikan berturut-turut sebagai :

$$Y_i = e_K(X_i) = (A_i X_i + B_i) \; mod \; 29 \tag{10}$$

dan

$$X_i = d_K(X_i) = {A_i}^{-1}(Y_i - B_i) \; mod \; 29 \tag{11}$$

$X_i, Y_i, B_i, A_i \in M_{2x2}(\mathbb{Z}_{29})$, A_i invertibel dengan ${A_i}^{-1}$ adalah invers modulo dari A_i.

Contoh 3. Dengan menggunakan hasil modifikasi ini, plainteks UAD HEBAT dengan pemilihan kunci $A = \begin{bmatrix} 1 & 3 \\ 7 & 5 \end{bmatrix}$ dan $B = \begin{bmatrix} 2 & 5 \\ 4 & 1 \end{bmatrix}$ akan dienkripsi dengan prosesnya diberikan pada Tabel 4.

Tabel 4. Proses Enkripsi Modifikasi Kombinasi Affine-Hill *Cipher* dengan Keystream Matriks-matriks Invertibel pada $\mathbb{Z}_{29}$

Plain teks	x_i	X_i , A_i dan B_i	y_i	Cipher teks
U	$x_1 = 20$	$X_1 = \begin{bmatrix} 20 & 0 \\ 3 & 26 \end{bmatrix}$	$y_1 = (1.20 + 3.3 + 2) \text{mod } 29 = 2$	M
A	$x_2 = 0$	$X_2 = \begin{bmatrix} 7 & 4 \\ 1 & 0 \end{bmatrix}$	$y_2 = (1.0 + 3.26 + 5) \text{mod } 29 = 25$	Z
D	$x_3 = 3$	$X_3 = \begin{bmatrix} 19 & 26 \\ 26 & 26 \end{bmatrix}$	$y_3 = (7.20 + 5.3 + 4) \text{mod } 29 = 14$	O
	$x_4 = 26$		$y_4 = (7.0 + 5.26 + 1) \text{mod } 2 = 15$	P
H	$x_5 = 7$	$A_1 = A^1 = \begin{bmatrix} 1 & 3 \\ 7 & 5 \end{bmatrix}$	$y_5 = (22.7 + 18.1 + 24) \text{mod } 29 = 22$	W
E	$x_6 = 4$	$A_2 = A^2 = \begin{bmatrix} 22 & 18 \\ 13 & 17 \end{bmatrix}$	$y_6 = (22.4 + 18.0 + 15) \text{mod } 29 = 16$	Q
B	$x_7 = 1$	$A_3 = A^3 = \begin{bmatrix} 3 & 11 \\ 16 & 8 \end{bmatrix}$	$y_7 = (13.7 + 17.1 + 12) \text{mod } 29 = 4$	E
A	$x_8 = 0$		$y_8 = (13.4 + 17.0 + 21) \text{mod } 29 = 15$	P
T	$x_9 = 19$	$B_1 = B^1 = \begin{bmatrix} 2 & 5 \\ 4 & 1 \end{bmatrix}$	$y_9 = (3.19 + 11.26 + 21) \text{mod } 29 = 16$	Q
	$x_{10} = 26$	$B_2 = B^2 = \begin{bmatrix} 24 & 15 \\ 12 & 21 \end{bmatrix}$	$y_{10} = (3.26 + 11.26 + 19) \text{mod } 29 = 6$	G
	$x_{11} = 26$	$B_3 = B^3 = \begin{bmatrix} 21 & 19 \\ 21 & 23 \end{bmatrix}$	$y_{11} = (16.19 + 8.26 + 21) \text{mod } 29 = 11$	L
	$x_{12} = 26$		$y_{12} = (16.26 + 8.26 + 23) \text{mod } 29 = 9$	J

3.5 Perbandingan Hasil Modifikasi Affine *Cipher*

Cipherteks yang dihasilkan dengan menggunakan fungsi enkripsi hasil modifikasi yang diperoleh dengan menggabungkan metode Affine cipher dengan Vigenere cipher (Affgenere cipher) lebih acak jika dibandingkan dengan cipherteks yang dihasilkan dengan metode Affine atau Vigenere *cipher*. Sebagai salah satu cipher subtitusi, Affine cipher sangat rentan terhadap kriptanalisis dengan metode analisa frekuensi sedangkan metode Affgenere cipher tangguh terhadap analisa frekuensi. Hal disebabkan pada Affine cipher, plainteks yang sama akan dienkripsi menjadi cipherteks yang sama sedangkan pada metode Affgenere, plainteks yang sama belum tentu dienkripsi menjadi cipherteks yang sama.

Tabel 4. Perbandingan hasil enkripsi Metode Affgenere *Cipher*, Affgenere-Hill *Cipher* dan Keystream Affine-Hill *Cipher* pada $\mathbb{Z}_{29}$

Plain teks	Cipherteks			
	Affine *Cipher* (2,1)	Affgenere *Cipher*	Affgenere-Hill *Cipher*	Keystream Affine Hill Cipher
U	M	O	M	M
A	B	I	.	Z
D	H	Y	M	O
	Y	U	O	P
H	P	S	H	W
E	J	V	N	Q
B	D	D	U	E
A	B	Y	D	P
T	U	,	K	Q
			A	G
			C	L
			X	J

Hasil ini jauh lebih acak dibandingkan dengan metode affine cipher ataupun vigenere cipher. Pemilihan nilai 29 dilakukan karena 29 merupakan bilangan prima sehingga berapapun nilai *a* yang dipilih selalu ada invers dari fungsi enkripsi yang menjadi fungsi untuk mengambalikan cipherteks ke plainteks. Untuk kriptografi modern, nilai p dapat dipilih berdasarkan jumlah bit yang digunakan.Kebebasan untuk memilih nilai *a* ini membuat hasil enkripsi lebih bervariasi. Kemungkinan nilai *a* yaitu salah satu bilangan bulat anggota {1, ..., 29} yang berjumlah 29 bilangan. Hal ini berakibat kombinasi kunci (*a, b*) sebanyak 29 x 29 =

841 kemungkinan. Penggabungan dengan Vigenere *cipher* membuat kemungkinan kunci *b* sebanyak jumlah karakter pada kata kunci yaitu 9 sehingga jumlah total kemungkinan kunci adalah $29^9 = 14.507.145.975.869$ kemungkinan.

Modifikasi Affine yang dikombinasikan dengan hill cipher dengan menggunakan keystream matriks-matriks invertible pada $\mathbb{Z}_{29}$ menghasilkan cipherteks yang lebih acak dari pada affine *cipher*, Hill *cipher* bahkan Affgenere *cipher*. Modifikasi ini selain memperluas ruang ciphertext juga membuat transformasi enkripsi menjadi lebih acak sehingga sulit untuk dikriptanalis. Bila dibandingkan secara analisa matematis, dari ketiga modifikasi yang dilakukan pada affine cipher maka modifikasi yang dilakukan dengan mengkombinasikan affine cipher dengan hill cipher lalu mengaplikasikan penggunaan barisan matriks invertibel sebagai kuncinya yang menghasilkan cipherteks paling acak.

IV. KESIMPULAN

Dari hasil ketiga modifikasi dapat dianalisa dari sisi matematisnya bahwa dengan memilih nilai $p = 29$ yang merupakan bilangan prima berakibat ruang plainteks dan cipherteks yaitu $\mathbb{Z}_{29}$ mempunyai struktur aljabar *field*. Artinya berapapun nilai $a \in \mathbb{Z}_{29}$ yang diambil akan mempunyai invers terhadap perkalian didalam $\mathbb{Z}_{29}$. Hal ini berakibat pengguna dapat bebas untuk memilih kunci K sehingga menghasilkan cipherteks yang lebih random dan bervariasi. Modifikasi yang dilakukan dengan mengkombinasikan Affine cipher dengan cipher lain menyebabkan cipherteks yang dihasilkan jauh lebih acak. Hal ini pula mengakibatkan plainteks yang sama dapat dienkripsi menjadi cipherteks yang berbeda sehingga tahan terhadap kriptanalisis dengan metode analisa frekuensi.

Perlu penelitian lebih lanjut untuk membuat algoritma dan protokol kriptografi dari hasil modifikasi Affine *cipher* ini, kemudian menguji sejauh mana ketahanan *cipher* hasil modifikasi ini secara kriptografi. Karena secara analisa matematis *cipher* modifikasi ini kuat terhadap metode known plaintext attack dan analisa statistik, perlu diujicoba apakah cipher ini juga bisa bertahan terhadap kriptanalisis dengan brute force search attack.

REFERENSI

[1] Goutam, Paul, Maitra, Subhamoy, Rossen Rosen, Kenneth H., 2012, RC4 Stream Cipher and Its Varians, Taylor & Francis Group, USA.
[2] Meijer, Alko R., 2016, Algebra for Cryptologist, Springer International Publishing, Switzerland.
[3] Howard Anton, et. All., 2014 Elementary Linear Algebra ; ApplicationsVersion, John Wiley & Sons, Inc., USA.
[4] Buchmann, Johannes A., 2000, Introduction to Cryptography , Springer-Verlag New York, Inc., USA.
[5] Hoffstein Jeffrey, et. All., 2008, An Introduction to Mathematical Cryptography, Springer Science + Business Media, LLC.
[6] Kenneth H. Rosen, 2011, Elementary Number Theory & Its Applications, 6th. E. Pearson Education, Inc., Boston M.A. 02116.

[7] Oorcshot Menezes, Vanstone, 1996 , Handbook of Applied Cryptography , CRC Press, Inc. USA.
[8] D.S. Malik, John N. Mordeson, M.K. Sen. Introduction to Abstract Algebra, United States, 2007.
[9] Hari Om, Rahul Patwa, 2008, Affine Transformation in Chryptography, Journal of Discrete Mathematical Sciences and Cryptography, 11.1, 59-65, Taru Publications.
[10] Christof Paar, Jan Pelzl, 2010, Understanding Cryptography, A Textbook for Students and Practitioners, Springer-Verlag Berlin Heidelberg.
[11] Douglass R. Stinson, 2006, Cryptography Theory And Practice, Chapman & Hall, CRC, New York, USA .
[12] Hanif Khan , Fozia, Shams, Rehan, Qazi, Farheen, Agha, Dure-E-Shawar, 2015, Hill Cipher Key Generation Algorithm by Using Orthogonal Matrix, International Journal of Innovative Science and Modern Engineering (IJISME), Volume-3 Issue-3, Blue Eyes Intelligence Engineering & Sciences Publication Pvt. Ltd.
[13] M.G.Vara Prasad, P.Pari Purna Chari, K.Pydi Satyam, 2016. Affine Hill Cipher Key Generation Matrix Of Order 3 By Using Reflects In An Arbitrary Line y=a x+ b, International Journal of Science, Technology and Manajemen, Vol. No. 5 Issue. 08.
[14] Hartini, Sri Primaini, Kriptografi Password Menggunakan Modifikasi Metode Affine Ciphers, Jurnal Sigmata, Volume 2 : Nomor : 1 Edisi : Oktober 2013 – Maret 2014.
[15] Dian Eka Wijayanti, 2016, Modifikasi Tehnik Transformasi Affine dalam Kriptografi, Prosidding URECOL 2016.
[16] Juliadi, Prihandono, Bayu, Kusumastuti, Nilamsari, 2013, Kriptografi Klasik Dengan Modifikasi Affine Cipher yang diperkuat dengan Vigenere Cipher, Buletin Ilmiah Mat. Stat dan Terapannya (Bimaster) Vol.02, N0. 2.
[17] Ricky Djoko, , Alz Danny Wowor, Dian Widiyanto Chandra, 2014, Modifikasi Affine Cipher Menggunakan Fungsi Gamma Dan Fungsi Hiperbolik, Jurnal KNS&I STIKOM Bali, Vol. 8 No. 1.
[18] Adi Narayana Reddy K a, Vishnuvardhan B b, Durga Prasad Kc, September 2012. Generalized Affine Transformation Based On Circulant Matrices, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.5.