ANALISIS SEKURITAS BERLAPIS DUA *CIPHE*R ABJAD TUNGGAL *CAESA*R DAN *AFFINE*

Matius Irsan Kasau*[1], ST. Aminah Dinayati Ghani[2], Nur Salman[3]
[1,2,3]Program Studi Teknik Informatika, STMIK Dipanegara Makassar
e-mail: *[1]irsan.kasau@dipanegara.ac.id, [2]dinayati.amy@dipanegara.ac.id,
[3]nursalman.halim@dipanegara.ac.id

Abstrak

Sistem keamanan komputer memiliki berbagai metode yang dapat dilakukan untuk mengenkripsi pesan plaintext menjadi pesan ciphertext pada saat pesan itu disimpan atau dikirim. Sebaliknya, mendekripsi pesan ciphertext menjadi pesan plaintext ketika pesan itu dibuka atau diterima. Penelitian ini bertujuan menganalisis tingkat keamanan dari dua buah metode Caesar dan Affine yang disusun berlapis dua disisi enkripsi dan dekripsi menggunakan dua pasang kunci simetris dan dua modulus yang sama dan berbeda. Hasil analis menunjukkan bahwa untuk dua pasang kunci yang sama dan modulus yang sama, hasil ciphertext yang diperoleh dari proses enkripsi dan dekripsi lebih mudah diserang untuk angka kunci genap daripada untuk angka kunci ganjil. Sementara untuk dua pasang kunci yang berbeda dan modulus berbeda tingkat sekuritasnya terletak diantara genap ganjil tersebut.

.

Kata kunci—: *Caesar, Affine*, Enkripsi Berlapis Dua, Dekripsi Berlapis Dua.

Abstract

Computer security systems various methods can be used to encrypt plaintext messages into ciphertext messages when they are stored or sent. Instead, decrypt the ciphertext message into a plaintext message when the message is opened or received. This study aims to analyze the security level of the two Caesar and Affine methods which are arranged in two layers alongside encryption and decryption using two pairs of symmetrical keys and two modulus that are the same and different. Analyst results show that for two pairs of the same key and the same modulus, the ciphertext results obtained from the encryption and decryption process are more easily attacked for even key numbers than for odd key numbers. While for two different pairs of keys and different modulus the level of security lies between the odd even.

Keywords— Caesar, Affine, Encryption in two layers, Decryption in two layers

1. PENDAHULUAN

Masalah keamanan komputer merupakan salah satu aspek penting dari sebuah sistem informasi terhadap berbagai ancaman seperti penghancuran sumber daya (*interruption*), pengaksesan sumber daya tanpa otorisasi *(interception*), pengubahan sumber daya *(modification*), dan pemasukan obyek obyek palsu ke sumber daya *(fabrication*)[1]. Sebagai akibatnya layanan dan lalu lintas informasi dalam sebuah organisasi dapat terganggu, macet, atau tidak berfungsi sama sekali. Kemampuan untuk menyediakan dan mengakses informasi secara cepat dan akurat menjadi sangat essensial dalam sebuah organisasi perguruan tinggi, pemerintahan, perusahaan, maupun individual. Komputer sebagai tempat memproses data menjadi informasi yang dihubungkan ke komputer lain melalui jaringan global atau internet membuka potensi terjadinya lubang keamanan (*security hole*) yang dapat dimanfaatkan oleh para penyusup jaringan[2].

Lubang keamanan ini perlu diatasi dengan mengkonversi informasi asli *(plaintext*) menjadi informasi palsu (*ciphertext*) yang tidak mudah dipahami oleh para penyusup jaringan.

Semakin tinggi tingkat keamanan, semakin sulit atau semakin tidak nyaman bagi para penyusup jaringan untuk mengakses informasi asli yang tersembunyikan dalam informasi palsu. Menurut G.J. Simons[3], keamanan informasi adalah cara bagaimana dapat mencegah penipuan *(cheating*), atau paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.

Keamanan komputer sendiri merupakan suatu cara untuk menjamin sumber daya tidak digunakan atau dimodifikasi orang yang tidak terotorisasi[4]. Secara garis besar prinsip prinsip mendasar dari keamanan adalah enkripsi dekripsi (kriptografi), kompressi data, steganografi. Khusus untuk kriptografi terbagi atas kriptografi klasik dan kriptografi modern. Kriptografi klasik sendiri terbagi lagi menjadi abjad tunggal, abjad majemuk, homofonik, dan poligram. Kriptografi *cipher Caesar* dan *cipher Affine* merupakan jenis kriptogrfi klasik abjad tunggal[4].

Menyusun keduanya berlapis dua dimaksudkan untuk meningkatkan kesulitan penyerangan (*attack*) dari para penyusup yang tidak terotorisasi untuk mengaksesnya, dengan menyusun berlapis dua maka akan terjadi proses enkripsi bertingkat dua kali menggunakan dua kunci rahasia yang bisa dipilih sama atau berbeda. Selain itu dipilih dua angka modulus yang juga dapat sama atau berbeda sehingga serangan terhadap *ciphertext* menjadi semakin membuat frustrasi bagi para penyusup jaringan. Selain kunci dan angka modulus, kondisi akan semakin sulit dengan memilih angka konstanta *Affine* pada sisi enkripsi dan sisi dekripsi yang berkorelasi besar.

Permasalahannnya adalah bagaimana menyusun sebuah tabel kode (sandi) yang tidak hanya memuat sandi angka karakter, tetapi juga sandi angka simbol tanda lainnya, dan bagaimana memilih angka kunci, angka modulus, dan angka konstanta *Affine* yang dapat mengakses tabel kode. Susunan kode karakter dan simbol lainnya dalam tabel kode angka dan ketepatan memilih angka kunci digunakan untuk untuk menganalisis sekuritas hasil dari tabel kode (sandi) yang memuat sandi angka karakter dan kode simbol tanda lainnya sehingga jangkauan *ciphertext* dapat lebih diperluas. Selain itu, menetapkan suatu angka kunci, angka modulus, angka konstanta *Affine* sedemikian sehingga aksesnya tidak jatuh diluar wilayah tabel kode.

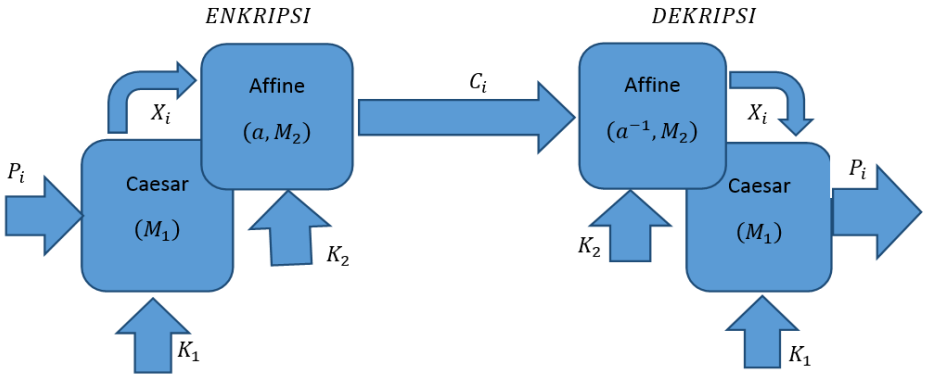
Adapun manfaat dari tabel kode dan angka kunci adalah tabel kode yang diperoleh merupakan inovasi hasil pengembangan dari table-tabel kode yang sudah ada sehingga dapat bermanfat sebagai contoh untuk pengembangan selanjutnya, dan penetapan angka kunci, angka modulus, dan angka konstanta *Affine* menentukan tingkat kesulitan terhadap upaya penyerangan oleh penyusup jaringan.

2. METODE PENELITIAN

Suatu sistem keamanan (*securitas*) terdiri atas proses enkripsi dan proses dekripsi yang pada keduanya terdapat berbagai metode yang dapat diterapkan[5]. Metode adalah suatu cara sistematis dan terstruktur untuk mengerjakan sesuatu. Urut-urutan prosedur untuk menyelesaikan masalah dikenal dengan istilah algoritma yang dapat digambarkan berbentuk *flowchart* atau diagram alir yang disusun berdasarkan dasar teori sebagai kerangka model matematik yang terbentuk dari sejumlah parameter.

2.1 Blok Diagram Sistem dan Model Matematik

Untuk dapat menguraikan flowchart sistem keamanan yang dibangun, diperlukan blok diagram sistem yang memperlihatkan sejumlah parameter yang diperlukan dan hubungannya satu terhadap lainnya pada sisi enkripsi dan sisi dekripsi[6]. Adapun blok diagram *cipher Caesar* yang disusun berlapis dua dengan *cipher Affine* seperti Gambar 1.



Gambar 1 Diagram Enkripsi-Dekripsi *Caesar-Affine*

Pada sisi pengirim, *plaintext* dienkripsi secara berlapis dua menggunakan *cipher Caesar* dan kemudian *cipher Affine*. Sebaliknya, untuk memperoleh kembali *plaintext* maka pada sisi penerima, *ciphertext* yang diterima dilakukan dekripsi menggunakan *cipher Affine* dan kemudian *cipher Caesar*. Adapun rumus rumus yang digunakan pada saat enkripsi dan pada saat dekripsi[5] adalah sebagai berikut:

Enkripsi

$$X_i = (P_i + K_1) \bmod M_1 \quad (Caesar) \qquad (1)$$
$$C_i = (aX_I + K_2) \bmod M_2 \ (Affine) \qquad (2)$$

Dekripsi

$$X_i = a^{-1}(C_I - K_2) \bmod M_2 \ (Affine) \qquad (3a)$$
$$a^{-1} = \left(\frac{1+M_2 z}{a}\right) \ ; z = 0, 1, 2, 3, \ldots \ldots \qquad (3b)$$
$$P_i = (X_I - K_1) \bmod M_1 \ (\text{Caesar}) \qquad (4)$$

Prinsip kerjanya adalah *plaintext* P_i pertama kali dienkripsi dengan enkriptor *Caesar* menggunakan kunci K_1 dan angka modulus M_1sehingga melalui proses perhitungan persamaan (1) menghasilkan *ciphertext* X_i. Kemudian *ciphertext* X_i dienkripsi lebih lanjut dengan enkriptor *Affine* menggunakan kunci K_2, angka modulus M_2dan angka pengali a sehingga melalui persamaan (2) menghasilkan *ciphertext* C_i.

Selanjutnya, *ciphertext* C_i ditransmisikan melalui media kabel atau nirkabel[7] atau juga mungkin disimpan sebagai file dalam bentuk *ciphertext*. *Ciphertext* C_i yang sangat rentan terhadap serangan atau sadapan oleh para penyusup jaringan secara online atau pencuri data pada komputer secara offline[6]. Karena itu dalam menjaga keamanan komputer diperlukan proses dekripsi yang prinsip kerjanya adalah *ciphertext* C_i pertama kali didekripsi dengan dekriptor *Affine* menggunakan kunci K_2, angka modulus M_2 dan angka pengali a^{-1} sehingga menghasilkan *plaintex*t X_i melalui proses perhitungan menggunakan persamaan (3a) dan persamaan (3b). Pada *Caesar*, *plaintext* X_i yang dihasilkan *Affine* ini justru merupakan *ciphertext* yang akan didekripsi lebih lanjut menjadi *plaintext* P_i yang diproses dengan dekriptor *Caesar* kunci K_1, angka modulus M_1 menggunakan persamaan (4).

2.2 Penelitian Terdahulu

Sejauh ini terdapat sejuumlah penelitian terdahulu yang menggunakan *Caesar cipher* dan atau *Affine cipher* antara lain adalah: Yoga Religia[8] yang membahas tentang Implementasi Algoritma *Affine Cipher* dan *Viginere Cipher* untuk keamanan sistem inventory yang hanya menggunakan model standar 26 karakter saja. Kemudian penelitian yang dilakukan oleh Sasono

Wibowo[9] yang meneliti tentang Implementasi Enkripsi Dekripsi Algoritma *Affine Cipher* berbasis Android, yang mengubah voice menjadi text karakter yang juga hanya model standar 26 karakter. Selanjutnya oleh Batara Silaban[10] yang meneliti tentang Aplikasi Pembelajaran Kriptografi *Affine Cipher* dan *Viginere Cipher* menggunakan Metode *Computer Assisted Instrument* yang lagi lagi hanya terbatas pada model satandar 26 karakter. Terakhir, penelitian yang menggabungkan *Cipher Caesar* dan *Cipher Affine* seperti tulisan ini adalah penelitian yang dilakukan oleh Muhammad Lutfi dkk[11] dengan penelitian berjudul Kriptografi dengan Komposisi *Caesar Cipher* dan *Affine Cipher* untuk mengubah Pesan Rahasia, penelitian ini juga hanya menggunakan model standar 26 karakter pada *Caesar* dan pada *Affine*. Adapun penelitian yang dibahas pada tulisan ini menggunakan model yang telah dimodifikasi 26 karakter ditambah 26 kode simbol lainnya yang disusun secara berselang seling dalam Tabel Daftar kode. Selain itu pemilihan wilayah Kunci diperluas menjadi 52 angka pilihan.

3. HASIL DAN PEMBAHASAN

3.1 Menyusun Tabel Daftar Kode

Pada tulisan ini penelitian dilakukan dengan mengambil *plaintext* STMIK DIPANEGARA, yang diparsial menjadi tiga STMIK, DIPAN, dan EGARA masing-masing terdiri atas lima karakter. Enkripsi dekripsi didasarkan pada 52 kode atau sandi karakter dan tanda lainnya secara selangseling seperti daftar pada Tabel 1.
Kemudian, simulasi dilakukan untuk $K_1 = K_2 = 26(25)$, $M_1 = M_2 = 52$ dan untuk $K_1 \neq K_2$, $M_1 \neq M_2$ dimana $K_1 = 13,\ K_2 = 26$, dan $M_1 = 39, M_2 = 52$ serta $a = 5, a^{-1} = 21$

Tabel 1 Daftar kode *Plaintext* dan kode *Ciphertext* yang Digunakan

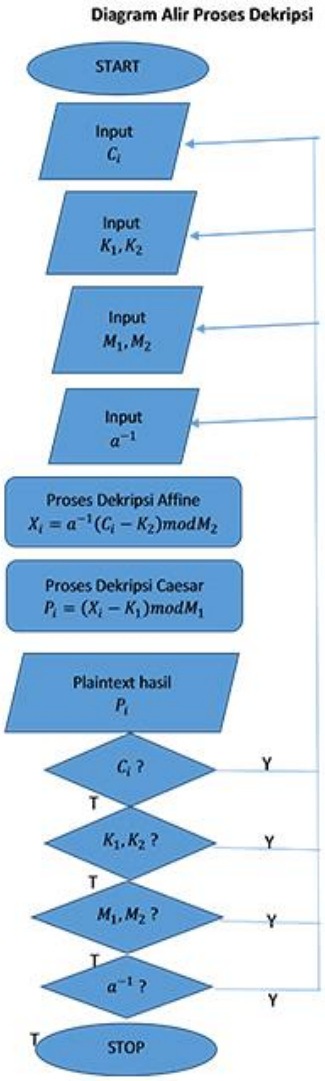
A	!	B	@	C	#	D	$	E	%	F	^	G
00	01	02	03	04	05	06	07	08	09	10	11	12
&	H	*	I	(	J	)	K	--	L	+	M	=
13	14	15	16	17	18	19	20	21	22	23	24	25
N	[	0	]	P	{	Q	}	R	:	S	;	T
26	27	28	29	30	31	32	33	34	35	36	37	38
“	U	,	V	\	W	<	X	>	Y	?	Z	/
39	40	41	42	43	44	45	46	47	48	49	50	51

Perhatikan bahwa setiap karakter dan kode simbol memiliki angka kode yang berurutan dari angka 00 (nol nol) untuk karakter A, angka 01 (nol satu) untuk kode simbol tanda seru (!), angka 02 (nol dua) untuk karakter B, angka 03 (nol tiga) untuk kode symbol at (@) dan seterusnya hingga angka 50 untuk karakter Z, angka 51 untuk kode simbol garis miring kanan (/). Semuanya berjumlah 52 karakter dan kode simbol yang disusun berselang seling dari 26 karakter dan 26 kode simbol.

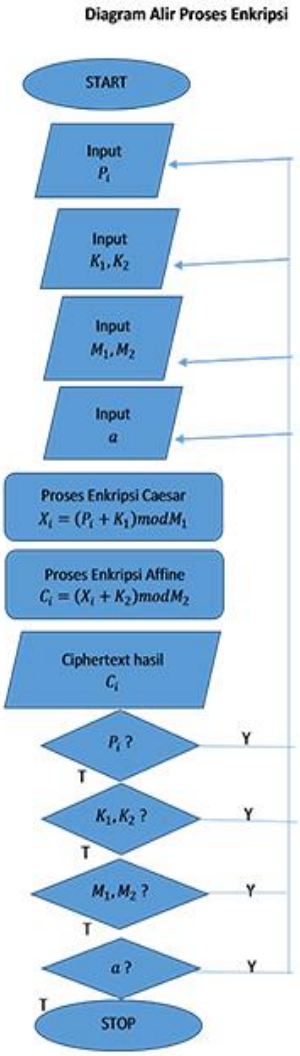
Angka pada setiap karakter dan kode symbol merupakan identitas diri dari setiap karakter dan kode symbol. Dalam proses enkripsi menggunakan matematik persamaan (1) untuk *cipher Caesar* dan persamaan (2) untuk *cipher Affine*, angka angka identitas diri tersebut yang akan diproses mewakili karakter dan kode simbol. Penentuan besarnya angka kunci yang dipilih sebaiknya terletak diantara angka 0 (nol) dan angka 52 (lima dua), lebih besar angka kunci yang dipilih dalam *range* tersebut adalah lebih baik dan lebih sulit diserang *ciphertext* yang dihasilkannya. Perhatikan bahwa Tabel 1 hanya berisi 52 karakter kapital dan sejumlah kode simbol, belum termasuk karakter kecil dan kode simbol lainnya yang jumlahnya masih banyak, bahkan sepuluh simbol angka juga belum termasuk. Karena itu Tabel 1 dapat dikembangkan menjadi lebih besar, sehingga tingkat sekuritasnya lebih handal. Semakin banyak jenis karakter dan kode simbol yang digunakan semakin sulit dan semakin kecil kemungkinan serangan berhasil.

3.2 Diagram Alir Enkripsi dan Dekripsi

Untuk dapat mengeksekusi model matematik pada persamaan (1) sampai persamaan (4) diperlukan langkah langkah sebagai tuntunan alur logika proses eksekusi program dalam komputer. Pada enkripsi dekripsi berlapis dua ini pertama tama dilakukan empat kali pengimputan secara berturut turut, mula mula input *plaintext*, lalu angka kunci yang dipilih pada *cipher Caesar* dan *cipher Affine*, kemudian angka modulus yang dipilih, dan angka input terakhir adalah angka konstanta *Affine*. Setelah itu dilanjutkan dengan proses perhitungan matematik persamaan (1) dan persamaan (2) yang menghasilkan *ciphertext* sebagai output. Jika proses pengulangan diinginkan untuk *plaintext*, angka kunci, angka modulus dan angka konstanta yang lain, maka langkah langkah tersebut terulang kembali. Adapun proses dekripsi langkah langkahnya mirip, hanya yang menjadi masukan awal adalah *ciphertext* dan angka angka korelasi *Affine* harus dihitung menggunakan persamaan (3b). Struktur diagram alir alur logika terdiri atas input, proses, output seperti ditunjukkan pada Gambar 2 dan Gambar 3.



Gambar 2 Diagram Alir Proses Enkripsi



Gambar 3 Diagram Alir Proses Deskripsi

3.3 Memilih Angka Kunci, Angka Modulus, dan Angka Konstanta Affine

Untuk maksud analisis sekuritas, diperlukan variasi pemilihan besarnya angka kunci, angka modulus, dan angka konstanta *Affine*. Berikut ini diperlihatkan dua kali simulasi yang berbeda.

1. Simulasi PERTAMA dilakukan untuk $K_1 = K_2 = 26(25), M_1 = M_2 = 52, a = 5, a^{-1} = 21$ Dalam simulasi pertama ini dipilih kunci yang sama pada *Caesar* dan *Affine*, mula-mula 26 dan kemudian 25 untuk melihat perbedaan ciphertext yang terjadi dengan hanya menurunkan satu angka. Angka modulus dipilih 52 sesuai dengan jumlah karakter dan kode simbol dalam Tabel 3.1. Sedangkan angka konstanta Affine dipilih 5 dan 21 (hasil perhitungan korelasi). Hasil simulasinya adalah sebagai berikut:

PLAINTEXT CAESAR ⟺ CIPHERTEXT CAESAR / PLAINTEXT AFFINE ⟺ CIPHERTEXT AFFINE

STMIK (36,38,24,16,20)$K_1 = 26$ 10,12,50,42,46 (FGZVX) $K_2 = 26$ 24,34,16,28,48 (MRI0Y)
STMIK (36,38,24,16,20) $K_1 = 25$ 09,11,49,41,45 (%^?,<) $K_2 = 25$ 23,33,15,27,47 (+}*[>)

DIPAN (06,16,30,00,26)$K_1 = 26$ 32,42,04,26,00 (QVCNA) $K_2 = 26$ 30,28,46,00,26 (POXAN)
DIPAN (06,16,30,00,26)$K_1 = 25$ 31,41,03,25,51 ({,@=/) $K_2 = 25$ 29,27,45,51,25 (][</=)

EGARA(08,12,00,34,00)$K_1 = 26$ 34,38,26,08,26(RTNEN) $K_2 = 26$ 40,08,00,14,40(UEAHU)
EGARA (08,12,00,34,00)$K_1 = 25$ 35,37,25,07,25 (:;=$=) $K_2 = 25$ 39,07,51,13,39 (“$/&”)

2. Simulasi KEDUA dilakukan untuk $K_1 \neq K_2, M_1 \neq M_2$ dimana $K_1 = 13(12), K_2 = 26$, dan $M_1 = 39, M_2 = 52$ serta $a = 5, a^{-1} = 21$

Dalam simulasi kedua ini dipilih kedua kunci berbeda, mula mula kunci Caesar dipilih 13, modulus 39 berpasangan dengan kunci Affine 26, modulus 52. Kemudian kunci Caesar diganti dengan 12, modulus 39, berpasangan dengan kunci Affine dan angka konstanta Affine yang tetap seperti sebelumnya. Hasil simulasinya adalah sebagai berikut:

PLAINTEXT CAESAR ⟺ CIPHERTEXT CAESAR / PLAINTEXT AFFINE ⟺ CIPHERTEXT AFFINE

STMIK(36,38,24,16,20)$K_1 = 13$ 10,12,37,29,33(FG[]})$K_2 = 26$ 24,34,13,15,09(MR&*%)
STMIK(36,38,24,16,20)$K_1 = 12$ 09,11,36,28,32(%^SOQ)$K_2 = 26$ 19,29,50,10,30()]ZFP)

DIPAN (06,16,30,00,26)$K_1 = 13$ 19,29,04,13,00 ()]C&A) $K_2 = 26$ 17,15,46,39,13 ((*X”&)
DIPAN (06,16,30,00,26)$K_1 = 12$ 18,28,03,12,51 (JO@G/) $K_2 = 26$ 12,10,41,34,11(GF,R^)

EGARA(08,12,00,34,00)$K_1 = 13$ 21,25,13,08,13(--=&E&)$K_2 = 26$ 27,47,39,14,39([>”H”)
EGARA(08,12,00,34,00)$K_1 = 12$ 20,24,12,07,12(KMG&G)$K_2 = 26$ 22,42,34,09,34 (LVR%R)

Tabel 2 Rangkuman Hasil Simulasi

KUNCI	PLAINTEX (P_i) ⟷ CIPHERTEXT (X_i)	⟷CIPHERTEXT (C_i)	
$K_1 = K_2 = 26$	STMIK	FGZVZ	MRIOY
$a = 5, a^{-1} = 21$	DIPAN	QVCNA	POXAN
$M_1 = M_2 = 52$	EGARA	RTNEN	UEAHU
$K_1 = K_2 = 25$	STMIK	%^?,<	+}*[>
$a = 5, a^{-1} = 21$	DIPAN	{,@=/	][</=
$M_1 = M_2 = 52$	EGARA	:;=$=	“$/&”
$K_1 = 13, K_2 = 26$	STMIK	FG[]}	MR&*%

$a = 5, a^{-1} = 21$ $M_1 = 39, M_2 = 52$	DIPAN EGARA	)]C&A --=&E&	(*X”& [>”H”
$K_1 = 12, K_2 = 26$ $a = 5, a^{-1} = 21$ $M_1 = 39, M_2 = 52$	STMIK DIPAN EGARA	%^SOQ JO@G/ KMG&G	)]ZFP GF,R^ LVR%R

3.4 Pembahasan Hasil Penelitian

Hasil simulasi menunjukkan bahwa untuk pemilihan kunci yang sama dengan angka genap (26), dan angka modulus yang sama sebesar jumlah karakter dan kode simbol penuh (52), maka hasil enkripsi dari *cipher Caesar* seluruhnya berbentuk karakter. Demikian halnya hasil enkripsi lebih lanjut dengan *cipher Affine* seluruhnya juga berbentuk karakter. Berbeda dengan pemilihan kunci dengan angka ganjil (25), dan angka modulus sebesar jumlah karakter dan kode simbol penuh (52), maka hasil enkripsi dari *cipher Caesar* seluruhnya berbentuk kode simbol. Demikian halnya hasil enkripsi lebih lanjut dengan *cipher Affine* seluruhnya juga berbentuk kode simbol.

Sementara itu, untuk pemilihan kunci yang berbeda dengan angka kunci *cipher Caesar* ganjil (13) dan angka kunci *cipher Affine* genap (26), angka modulus yang berbeda untuk *Caesar* ganjil (39) dan modulus untuk *Affine* genap (52), maka hasil enkripsi dari *cipher Caesar* bercampur aduk antara karakter dengan kode simbol dengan perbandingan satu banding empat (1:4) hingga dua berbanding tiga (2:3). Enkripsi lebih lanjut dengan *cipher Affine* diperoleh komposisi perbandingan yang sama. Selanjutnya, jika angka kunci *cipher Caesar* dikurangi satu menjadi angka genap (12) sementara yang lainnya tetap, maka *ciphertext* yang juga bercampur aduk baik *cipher Caesar* maupun *cipher Affine* menghasilkan perbandingan tiga banding dua (3:2) hingga perbandingan empat berbanding satu (4:1).

Berdasarkan komposis perbandingan tersebut diperoleh bahwa paling sulit diserang penyusup jika *ciphertex* berupa kode simbol seluruhnya. Semakin tinggi jumlah kode simbol dari jumlah kode karakter dalam *ciphertex* semakin sulit diserang oleh penyusup jaringan. Sebaliknya, semakin tinggi jumlah kode karakter daripada kode simbol dalam suatu *ciphertext* semakin mudah diserang oleh penyusup jaringan.

4. KESIMPULAN

1. *Ciphertext* hasil enkripsi yang seluruhnya karakter paling mudah diserang dan *ciphertext* yang seluruhnya kode simbol paling sulit diserang, maka diperoleh tingkat sekuritas dari yang paling mudah diserang sampai yang paling sulit diserang dengan penamaan tingkat kesulitan adalah: paling mudah, mudah, sulit, paling sulit, sebagai berikut:
   a. Paling mudah diserang jika pemilihan angka kunci dan angka modulus sama yang genap pada *cipher Caesar* dan *cipher Affine*.
   b. Mudah diserang jika pemilihan angka kunci genap berbeda, dan angka modulus berbeda; ganjil pada *cipher Caesar*, dan genap pada *cipher Affine*.
   c. Sulit diserang jika pemilihan angka kunci berbeda, dan angka modulus berbeda; angka kunci ganjil pada *cipher Caesar*, dan angka kunci genap pada *cipher Affine*.
   d. Paling sulit diserang jika pemilihan angka kunci dan angka modulus sama yang ganjil pada *cipher Caesar* dan *cipher Affine*.
2. Pemilihan kunci angka ganjil baik pada *cipher Caesar* maupun pada *cipher Affine* lebih sulit diserang daripada pemilihan kunci genap sehingga sekuritas sistem keamanan lebih terjamin. Tingkat sekuritas dapat lebih ditingkatkan lagi dengan memilih angka konstanta dari *cipher Affine* yang lebih besar dan angka konstanta korelasinya pada sisi dekripsi yang sulit diketahui posisinya.

5. SARAN

Penelitian dilakukan dengan memilih karakter kapital sebanyak 26 buah dari A sampai Z dan kode simbol juga sebanyak 26 buah yang disusun secara berselang seling. Posisi karakter menempati kode angka genap, sementara posisi kode simbol menempati kode angka ganjil. Untuk dapat semakin lebih meningkatkan sekuritas terhadap serangan, disarankan hal hal berikut:

1. Selain memilih semua karakter kapital, juga pilih semua karakter kecil dan semua kode simbol yang ada dalam ASCII.
2. Susun tabel daftar kode yang acak, semakin lebih acak semakin lebih aman tingkat sekuritasnya.

DAFTAR PUSTAKA

[1] John D. Haward. 1995, *Analysis of Security Incidents on the Internet,* Prentice-Hall.Inc.

[2] Zelvos C. Belauger P.R. 2000, *A hacker's Guide to Protecting Your Linux Server and Workstation Maximum Linux Security,* John Wiley & Son.

[3] Hartini dkk. 2014, Kriptografi Password Menggunakan Modifikasi Metode Affine Cipher, Prosiding Snatif, vol.2, no.1.

[4] Sadikin.2012. *Kriptografi untuk Keamanan Jaringan,* Penerbit Andi, Yogyakarta.

[5] Sing A. Ttiebel A.W. 2015. *Network Security,* John Wiley & Son Tanembaum S.A, Prentice-Hall. Inc.

[6] Hans K.M. 2002. Keamanan Komputer, Diktat Kuliah pada STMIK Dipanegara, Makassar.

[7] Tanembaum S.A, 2001, *Computer Network,* Prentice-Hall. Inc.

[8] Yoga Religia, 2015, *Implementasi Algoritma Affine Cipher Dan Vigenere Cipher Untuk Keamanan Login Sistem Inventori Tb Mita Jepara, Karya Ilmiah Kriptografi 06/03/2015,* Universitas Dian Nuswantoro Semarang.

[9] Sasono Wibowo, Florentina Esti Nilawati, Suharnawi Suharnawi, 2014, *Implementasi Enkripsi Dekripsi Algoritma Affine Cipher Berbasis Android*, Jurnal Teknologi Informasi, Vol 13, No 4**,** e-issn: 2356-2579, p-issn: 1412-2693.

[10] Batara Silaban, Tonni Limbong, 2017, Aplikasi Pembelajaran Pengenalan Kriptografi Algoritma Affine Cipher dan Vigenere Cipher Menggunakan Metode Computer Assisted Instruction, *Jurnal Ilmiah Program Studi Sistem Informasi*, Volume 2 Nomor *2*, e-issn: 2599-3089, p-issn: 2547-6985.

[11] Muhammad Lutfi Lutfi Wijaya, Kartika Yulianti, Husty Serviana Husain, 2017, *Kriptografi Dengan Komposisi Caesar Cipher Dan Affine Cipher Untuk Mengubah Pesan Rahasia***,** Jurnal EurekaMatika, Volume 5 Nomor 1**,** e-issn: 2528-4231,