PERANCANGAN APLIKASI KERAHASIAAN PESAN DENGAN ALGORITMA HILL CIPHER

Septi Maryanti [1)], Abdul Rakhman [2)], Suroso [3)]

[1),2),3)] Jurusan Teknik Elektro, Program Studi Teknik Telekomunikasi, Politeknik Negeri Sriwijaya
JL. Srijaya Negara, Bukit Besar Palembang
Email : septimaryanti3@gmail.com

Abstrak. *Dengan berjalannya waktu,perkembangan teknologi informasi kian melesat beriiringan dengan tingginya kebutuhan masyarakat akan komunikasi dan informasi. Saat ini pertukaran data atau informasi menjadi hal yang sangat sering dilakukan, sehingga pada segi keamanan pesan pun harus diperhatikan, mengingat kerap kali terjadinya penyadapan dan pembajakan terhadap suatu pesan. Pengamanan ini bisa dilakukan dengan Algoritma Kriptografi Hill Cipher. Hill Cipher bagian dari algoritma kriptografi klasik yang susah dipecahkan oleh kriptanalis jika hanya dilakukan dengan mengetahui berkas ciphertext saja. Akan tetapi, teknik ini dapat dipecahkan lumayan mudah seandainya kriptanalis memiliki berkas ciphertext dan irisan berkas plaintext.*

Kata kunci : *Sistem Keamanan, Pesan, Kriptografi, Algoritma Hill Cipher.*

1. Pendahuluan

Kriptografi merupakan studi matematika yang berkaitan dengan segi keamanan informasi seperti keutuhan sebuah data, kemurnian entitas dan kemurnian data. Kriptografi memanfaatkan beraneka macam teknik dalam upaya untuk mengamankan sebuah data. Pengiriman data dan penyimpanan data lewat media elektronik membutuhkan suatu proses yang dapat menjamin keselamatan dan keutuhan dari sebuah data yang dikirimkan. Data tersebut harus tetap rahasia selama pengiriman dan tetap utuh pada saat penerimaan ketujuan. Karena, jika tidak diamankan maka akan mudah disadap dan dibajak oleh orang yang tidak bertanggung jawab.

Menanggapi hal yang sering terjadi tersebut, maka diperlukan suatu proses penyandian (enkripsi dan dekripsi) untuk data yang akan dikirimkan. Hill Cipher sendiri adalah aritmatika modulo pada kriptografi. Teknik kriptografi ini diciptakan untuk membuat kode (*cipher*) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. Dasar dari teknik ini adalah aritmatika modulo terhadap matriks.Teori matriks yang digunakan dalam Hill Cipher antara lain yaitu perkalian antar matriks dan melakukan invers pada matriks. Matriks kunci Hill Cipher harus menggunakan matriks yang invertible. Untuk menghindari matriks kunci yang tidak invertible (*dapat dibalik)*, maka matriks kunci dibuat menggunakan koefisien binomial newton. Semakin besar suatu matriks kunci maka semakin kuat juga keamanannya. Kriptografi ini menggunakan sebuah teknik matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi.Proses enkripsi pada Hill Cipher dilakukan perblok *plaintext*. Ukuran blok tersebut sama dengan ukuran matriks kunci yaitu m x n. (Arya Widyanarko, 2009).[1]

Algoritma Hill cipher termasuk bagian dari algoritma kriptografi kunci simetris yang bekerja dengan cara penyandian blok (*block cipher).* Karena teks yang selanjutnya diproses akan dibagi menjadi blok-blok/suku kata dengan ukuran tertentu. Setiap karakter dalam satu blok akan saling mempengaruhi karakter yang lain dalam proses enkripsi dan dekripsinya, sehingga karakter yang sama tidak dipetakan menjadi karakter yang sama juga.[2]

1.1 Metodelogi Penelitian

1.Metode Eksperimen

Pada metode ini, akan dilakukan pembuatan aplikasi untuk mengekripsi dan dekripsikan sebuah pesan agar tidak mudah dimengerti oleh orang yang tidak berkepentingan. Disini akan menggunakan software Android Studio untuk membuat aplikasi.

2.Identifikasi masalah

Karena perkembangan teknologi yang semakin hari semakin pesat, teknologi dan informasi sangat dibutuhkan bagi masyarakat luas. Dengan begitu diperlukan informasi yang real. Dalam pengiriman sebuah pesan sangat dibutuhkan sebuah keamanan pada saat pengiriman berlangsung. Ini dikarenakan jika tidak adanya keamanan maka sangat mudah bagi orang-orang yang usil menyadap dan melakukan pembajakan terhadap pesan tersebut.

3.Studi Literatur

Dengan menggunakan metode ini penulis mempelajari dan mencari referensi mengenai pembuatan aplikasi kerahasiaan pesan. Referensi yang didapatkan bisa dari jurnal, buku, artikel ataupun penelitian sebelumnya.

1.2 Tinjauan Pustaka

A. Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Algoritma kriptografi dapat diabedakan menjadai dua jenis, yaitu algoritma simitris dan asimetris.[3] Alogaritma simetris adalah alogaritma yang menggunakan kunci untuk proses enskripsi sama dengan kunci untuk proses deskripsi. Alogaritma asimetris adalah alogaritma yang menggunakan kunci yang berbeda untuk enskripsi dan deskripsinya. Alogaritma ini disebut juga alogaritma kunci umum (*public key)* yang mana dapat diketahui oleh setiap orang, tetapi kunci untuk deskripsinya hanya diketahui oleh orang yang berhak mengetahui data yang disandikan atau sering disebut kunci pribadi *(private key)*.[4][7]

B. Aspek Keamanan Kriptografi

Kriptografi memiliki beberapa aspek keamanan antara lain :

1. Kerahasiaan (confidentiality), menjamin bahwa data-data tersebut hanya bisa diakses oleh pihak-pihak tertentu saja. Kerahasiaan bertujuan untuk melindungi suatu informasi dari semua pihak yang tidak berhak atas informasi tersebut.[5]
2. Otentikasi (authentication), merupakan identifikasi yang dilakukan oleh masing – masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengidentifikasi satu sama lainnya. Informasi yang didapat oleh suatu pihak dari pihak lain harus diidentifikasi untuk memastikan keaslian dari informasi yang diterima.[5]
3. Integritas (integrity), menjamin setiap pesan yang dikirim pasti sampai pada penerimanya tanpa ada bagian dari pesan tersebut yang diganti, diduplikasi, dirusak, diubah urutannya, dan ditambahkan. Integritas data bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berhak atas informasi tersebut. Untuk menjamin integritas data ini pengguna harus mempunyai kemampuan untuk mendeteksi terjadinya manipulasi data oleh pihak-pihak yang tidak berkepentingan. Manipulasi data yang dimaksud di sini meliputi penyisipan, penghapusan, maupun penggantian data.[5]
4. Nirpenyangkalan (Nonrepudiation), mencegah pengirim maupun penerima mengingkari bahwa mereka telah mengirimkan atau menerima suatu pesan. Jika sebuah pesan dikirim, penerima dapat membuktikan bahwa pesan tersebut memang dikirim oleh pengirim yang tertera. Sebaliknya, jika

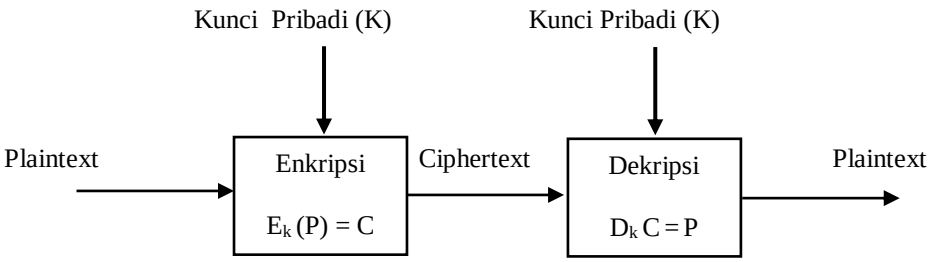
sebuah pesan diterima, pengirim dapat membuktikan bahwa pesannya telah diterima oleh pihak yang ditujunya.[5]

2. Pembahasan

Pada pembahasan kali ini, peneliti akan menguraikan tahap-tahap analisis, perancangan dan uji coba berdasarkan pada tujuan dan alur penelitian.

2.1 Analisis dan Rancangan Enkripsi dan Dekripsi Kriptografi Simetris

Pada bagian ini akan digambarkan tahapan dari proses enkripsi teks dengan Kriptografi. Digambarkan seperti dibawah ini :



Gambar 1. Gambaran umum skema algoritma simetri

2.2 Algoritma Hill Cipher

Algoritma hill cipher diciptakan oleh Lester S.Hill pada tahun 1929. Hill cipher merupakan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Teknik ini diciptakan bertujuan untuk dapat menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. Algoritma ini tidak mengganti setiap abjad yang sama pada plaintext dengan abjad laiinya yang sama pada ciphertext, karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya.[6]

Secara matematis, proses enkripsi pada Hill Cipher adalah :

$$C = K \,.\, P$$

Dimana :
C = Cipertext
K = Kunci
P = Plaintext

Tabel Konversi

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
0	1	2	3	4	5	6	7	8	9	!	@	#	$	%	^	&	*	(	)	¯	-	+	=	{	}
52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77
[	]	<	>	.	,	;	“	‘	`	\	/	?	:	~	|										
78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93										

-Enkripsi

Dimisalkan P : Password=950. Maka nilai plaintext dari kata tersebut adalah :
15,26,44,44,48,40,43,29,75,61,57,52

Pembagian blok/suku kata :

C (Pa) : 15	C (ss) : 44	C (wo) : 48	C (rd) : 43	C (=9) : 75	C (50) : 57
26	44	40	29	61	52

Kunci K = $\begin{bmatrix}7 & 3\\3 & 3\end{bmatrix}$

Proses enkripsi : matriks kunci x matriks P

C (Pa) :

$$\begin{bmatrix}7 & 3\\3 & 2\end{bmatrix}\begin{bmatrix}15\\26\end{bmatrix} = \begin{bmatrix}183\\97\end{bmatrix} mod\ 94 = \begin{bmatrix}89\\3\end{bmatrix}$$

C (ss) :

$$\begin{bmatrix}7 & 3\\3 & 2\end{bmatrix}\begin{bmatrix}44\\44\end{bmatrix} = \begin{bmatrix}440\\220\end{bmatrix} mod\ 94 = \begin{bmatrix}64\\32\end{bmatrix}$$

C (wo) :

$$\begin{bmatrix}7 & 3\\3 & 2\end{bmatrix}\begin{bmatrix}48\\40\end{bmatrix} = \begin{bmatrix}456\\224\end{bmatrix} mod\ 94 = \begin{bmatrix}80\\36\end{bmatrix}$$

C (rd) :

$$\begin{bmatrix}7 & 3\\3 & 2\end{bmatrix}\begin{bmatrix}43\\29\end{bmatrix} = \begin{bmatrix}388\\187\end{bmatrix} mod\ 94 = \begin{bmatrix}12\\93\end{bmatrix}$$

C (=9) :

$$\begin{bmatrix}7 & 3\\3 & 2\end{bmatrix}\begin{bmatrix}75\\61\end{bmatrix} = \begin{bmatrix}708\\347\end{bmatrix} mod\ 94 = \begin{bmatrix}50\\65\end{bmatrix}$$

C (50) :

$$\begin{bmatrix}7 & 3\\3 & 2\end{bmatrix}\begin{bmatrix}57\\52\end{bmatrix} = \begin{bmatrix}555\\275\end{bmatrix} mod\ 94 = \begin{bmatrix}85\\87\end{bmatrix}$$

Maka didapatkan ciphertext = /D#g<kM|y[“`

-Dekripsi

K = $\begin{bmatrix}7 & 3\\3 & 3\end{bmatrix}$ ⟶ Det K = (7*2)-(3*3) = 5

Invers modulo = 5^{-1} *mod* 94 ⟶ 5x = 1 mod 94 ⟶ 5x = 1+94k, x = (1+94k)/5

Cari k_n sehingga hasil x adalah bilangan bulat.

K = 0, x =(1+94*0)/5, ini bukan bilangan bulat.

K = 1, x =(1+94*1)/5 = 19 adalah bilangan bulat.

Selanjutnya invers modulo determinan digunakan untuk invers matriks :

Misal k = $\begin{bmatrix}a & b\\c & d\end{bmatrix}$ *maka* k^{-1} = *determinan* $\begin{bmatrix}d & -b\\-c & a\end{bmatrix}$

Sehingga $k^{-1} = 19\begin{bmatrix}2 & -3\\-3 & 7\end{bmatrix} = \begin{bmatrix}38 & -57\\-57 & 133\end{bmatrix} mod\ 94 = \begin{bmatrix}38 & 37\\37 & 39\end{bmatrix}$

Untuk modulo bilangan negative, dapat dengan contoh sebagai berikut :

-57 mod 94 = -n mod 94, maka -n mod x = x-(n mod 94) ⟶ *94 = 94-(57mod 94)* ⟶ *94-57 = 37*

Dekripsi = invers k * *ciphertext.*

$$\begin{bmatrix}38 & 37\\37 & 39\end{bmatrix}\begin{bmatrix}89\\3\end{bmatrix} = \begin{bmatrix}3493\\3410\end{bmatrix} mod\ 94 = \begin{bmatrix}15\\26\end{bmatrix}$$

$$\begin{bmatrix}38 & 37\\37 & 39\end{bmatrix}\begin{bmatrix}64\\32\end{bmatrix} = \begin{bmatrix}3616\\3616\end{bmatrix} mod\ 94 = \begin{bmatrix}44\\44\end{bmatrix}$$

$$\begin{bmatrix}38 & 37\\37 & 39\end{bmatrix}\begin{bmatrix}80\\36\end{bmatrix} = \begin{bmatrix}4372\\4364\end{bmatrix} mod\ 94 = \begin{bmatrix}48\\40\end{bmatrix}$$

$$\begin{bmatrix}38 & 37\\37 & 39\end{bmatrix}\begin{bmatrix}12\\93\end{bmatrix} = \begin{bmatrix}3897\\4071\end{bmatrix} mod\ 94 = \begin{bmatrix}43\\29\end{bmatrix}$$

$$\begin{bmatrix}38 & 37\\37 & 39\end{bmatrix}\begin{bmatrix}50\\65\end{bmatrix} = \begin{bmatrix}4305\\4385\end{bmatrix} mod\ 94 = \begin{bmatrix}75\\61\end{bmatrix}$$

$$\begin{bmatrix}38 & 37\\37 & 39\end{bmatrix}\begin{bmatrix}85\\87\end{bmatrix} = \begin{bmatrix}6449\\6538\end{bmatrix} \; mod\ 94 = \begin{bmatrix}57\\52\end{bmatrix}$$

Jadi, hasil dari dekripsi *ciphertext* adalah 15,26,44,44,48,40,43,29,75,61,57,52, yang berarti : Password=9509.

Dan dapat kita lihat hasil diatas, menyatakan bahwa hasil enkripsi plaintext menjadi cipertext dan selanjutnya di dekripsi dari cipertext menjadi plaintext menunjukkan hasil yang signifikan. Ini menandakan bahwa hasil dari pengujian diatas sudah benar dan bisa dibuktikan.

3. Simpulan

Dari uraian diatas, dapat disimpulkan bahwa proses enkripsi dan dekripsi dengan menggunakan algoritma kriptografi hlll cipher ini memiliki kelebihan dalam data enkripsi seperti resitansi terhadap analisis frekuensi. Persamaan aljabar linearnya adalah C = K x P (mod m). Hill Cipher termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas ciphertext saja. Namun, teknik ini dapat dipecahkan dengan cukup mudah apabila kriptanalis memiliki berkas ciphertext dan potongan berkas plaintext.

Ucapan Terima Kasih

Penulis berterima kasih kepada Allah Subhana Wa Ta'ala atas berkah dan rahmat-Nya, Ayah dan Ibu yang selalu mendoakan dan memberikan motivasi, Bapak dan Ibu Dosen, serta rekan-rekan sesama Mahasiswa Teknik Telekomunikasi yang telah membantu memberikan dukungan berupa saran dan kritik sehingga penulis dapat menyelesaikan paper ini.

Daftar Pustaka

[1] Zulham, M., dkk. (2016). *Perancangan Aplikasi Keamanan Data Email Menggunakan Algoritma Enkripsi Rc6. Semin. Nas.*Medan: STMIK Potensi Utama. *Inform.*, pp. 96–101, 2014.

[2] Rachmadi, P. (2017). *Penyandian Teks Dengan Metode Hill Chiper.* Jakarta: Fakultas Teknologi Informasi Perbanas. pp. 1681–1684.

[3] Pattiasina, T.J dan M. Kom. (2014). *Rancang Bangun Aplikasi Enkripsi dan Dekripsi Email Dengan Menggunakan Algoritma Advanced Encryption Standard Dan Knapsack*. Surabaya: Institut Informatika Indonesia. pp. 1–10.

[4] Wandani, H., dkk. (2012). *Implementasi Sistem Keamanan Data dengan Menggunakan Teknik Steganografi End of File (EOF) dan Rabin Public Key Cryptosystem*. Medan: Universitas Sumatera Utara. *Alkhawarizmi*,

[5] PATRICIA, H. (2015). *Teknik Keamanan Data Menggunakan Kriptografi dengan Algoritma Vigenere Cipher dan Steganografi dengan Metode End of File (EoF)*. Semarang: Universitas Dian Nuswantoro. *Progr. Stud. Tek. Inform. Fak. Ilmu Komput. Univ. Dian Nuswantoro*, pp. 1–7, 2015.

[6] Yuniati, V., dkk. (2009). *Enkripsi dan Dekripsi dengan Algoritma AES 256 untuk Semua Jensis File*. *J. Inform.*Yogyakarta: Universitas Kristen Duta Wacana. vol. 5, no. 1, pp. 22–31

[7] Ariyus, Dony. (2008). *Pengantar Ilmu Kriptografi (Teori, Analisis dan Implementasi).* Yogyakarta: ANDI Offset.