Available *online* at : http://bit.ly/InfoTekJar

InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan

ISSN (Print) 2540-7597 | ISSN (Online) 2540-7600

Decision Support System

Kriptografi Klasik Menggunakan Modifikasi Metode Affine Ciphers

Anggi Syahadat Harahap

Program Studi Administrasi Business Sektor Publik, Politeknik STIA LAN Bandung Bandung Indonesia

KEYWORDS

Affine Ciphers; encryption; decryption; ciphertext; plaintext;

CORRESPONDENCE

Phone: -

E-mail: anggi@poltek.stialanbandung.ac.id

A B S T R A C T

Cryptography is the science or art to maintain the security of messages that include the security aspects such as confidentiality, data integrity and authentication. One method that is able to encrypt messages Affine Ciphers modified. Plaintext encrypted with Affine Cipher using the equation E (P) = (ax + b) mod m, where m is the size of the alphabet, a is an integer relatively prime to m, b is the number of shifts, x is the plaintext is converted to an integer of 0 to m-1 in accordance with the order of the alphabet, E (P) is ciphertext that is converted to an integer of 0 to m-1 in accordance with the order of the alphabet. Affine Ciphers ciphertext is decrypted by using the equation D(E(P))=a-1(E(P)-b) mod m in order to obtain the plaintext.

PENDAHULUAN

Kriptografi saat ini telah menjadi salah satu syarat penting dalam keamanan tehnologi informasi terutama dalam pengiriman pesan rahasia. Pengiriman pesan rahasia sangat rentan terhadap serangan yang dilakukan oleh pihak ketiga, seperti penyadapan, pemutusan komunikasi, pengubahan pesan yang dikirim, dan lain lain. Kriptografi dapat meningkatkan keamanan dalam pengiriman pesan atau komunikasi data. Caranya adalah dengan menyandikan pesan tersebut berdasarkan algoritma dan pesan tertentu yang hanya diketahui oleh pihak pihak yang berhak atas data, informasi dan dokumen tersebut. Semakin rumit metode yang digunakan maka tingkat keamanan yang dihasilkan pun akan semakin baik pula.

Kriptografi dikategorikan dua yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik adalah kriptografi yang berbasis karakter (enkripsi dan dekripsi dilakukan pada setiap karakter). Kriptografi modern adalah kriptografi yang beroperasi pada mode bit (dinyatakan dalam 0 dan 1). Kriptografi klasik dibagi dua yaitu cipher transposisi yang mengubah susunan huruf huruf di dalam pesan. Cipher subsitusi yang mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain. Diantara sekian banyak algoritma kriptografi cipher subsitusi dan cipher transposisi, ada yang disebut affine cipher. Modifikasi affine cipher memberikan penyandian baru sehingga pesan atau informasi lebih sulit untuk dipecahkan oleh kriptanalis dibandingkan dengan hanya affine cipher saja.

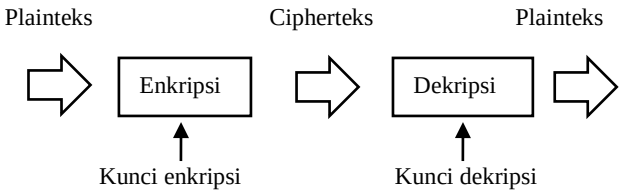
Tujuan pada penelitian ini adalah mempelajari langkah pada modifikasi affine cipher untuk meningkatkan keamanan pesan atau informasi dan mengetahui syarat yang harus dimiliki oleh penerima pesan yang akan dilakukan dekripsi. Pada umumnya affine cipher menggunakan aturan konversi berupa alphabet arab yang berjumlah 26. Sedangkan pada modifikasi affine cipher penulis menambahkan beberapa karakter yaitu angka 0 sampai 9 sehingga ukuran konversi (m) menjadi 36.

TINJAUAN PUSTAKA

Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu Cryptograph dari kata Kryptos (tersembunyi) dan graphein (menulis). Kriptografi dapat diartikan tulisan yang dirahasiakan atau sebagai ilmu ataupun seni yang mempelajari bagaimana sebuah data, informasi dan dokumen dikonversi ke bentuk tertentu yang sulit untuk dimengerti.

Suatu data yang tidak disandikan disebut plaintext atau cleartext sedangkan data yang telah disandikan disebut ciphertext. Proses yang dilakukan untuk mengubah plaintext menjadi ciphertext disebut enkripsi (encryption). Untuk mengubah ciphertext kembali ke plaintext disebut dekripsi (decryption).



Gambar 1. Skema Enkripsi dan Dekripsi

Tujuan Kriptografi

Dalam pengamanan pesan, ada 3 bagian tujuan kriptografi :

1. Keabsahan pengiriman (user authentication)
   Yaitu keaslian pengiriman dengan sebuah pertanyaan : "Apakah pesan yang diterima benar benar berasal dari pengirim yang sesungguhnya ?".
2. Keaslian pesan (message authentication)
   Yaitu keutuhan pesan (data integrity) dengan sebuah pertanyaan : "Apakakah sebuah pesan yang diterima tidak mengalami perubahan/modifikasi ?".
3. Anti Penyangkalan (nonrepudation)
   Yaitu pengirim tidak dapat menyangkal (berbohong) bahwa dialah yang mengirim pesan.

METODE PENELITIAN

Penelitian dan pengembangan system kriptografi mengunakan metode affine cipher diharapkan bahwa data atau informasi yang dikirim akan menjadi lebih aman dari pengguna yang tidak bertanggung jawab.

Untuk mendukung dan mempercepat proses penulisan diperlukan sebuah metode. Adapun metode yang digunakan dalam penulisan jurnal ini adalah :

a. Studi pustaka

Studi pustaka dilakukan dengan mencari berbagai referensi seperti buku,beberapa jurnal online maupun informasi dari internet seperti e-book yang berkaitan dengan tema yang dibahas.

HASIL DAN PEMBAHASAN

Algoritma Kriptografi

Kriptografi menggunakan suatu algoritma (cipher) dan kunci (key). Cipher adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi. Kunci adalah sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data. Algoritma kriptografi terdiri dari algoritma simetri dan algoritma asimetri.

Cipher dan Key (Kristanto, A. 2003)

Jika P adalah plaintext dan C adalah ciphertext, maka fungsi enkripsi E yang memetakan P ke cipher C adalah :

$$E(P)=C \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Fungsi dekripsi D yang memetakan cipher C ke plaintext P adalah

$$D(C)=P \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Proses enkripsi menjadi dekripsi yaitu mengebalikan pesan ke pesan asal adalah

$$D(E(P))=P \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

Kunci (key) adalah parameter yang digunakan untuk melakukan transformasi enkripsi dan dekripsi yaitu

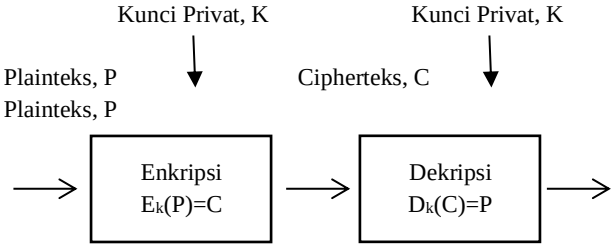
$$E_k(P)=C \text{ dan } D_k(C)=P \quad \ldots\ldots\ldots\ldots\ldots (4)$$

Persamaan (4) dapat memenuhi jika persamaan tersebut dapat diformulasikan yaitu

$$D_k(E_k(P))=P \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

Algoritma Simetris

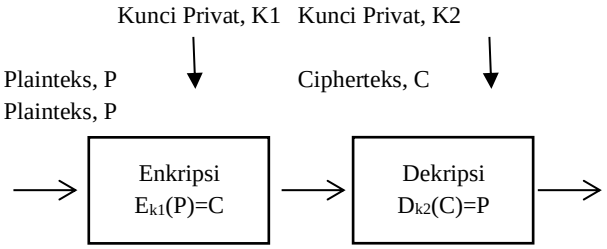
Algoritma Kriptografi Simetri (algoritma kriptografi konvensional) adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Algoritma kriptografi simetris terdiri dari 2 kategori yaitu algoritma aliran (stream ciphers) dan algoritma blok (block ciphers). Algoritma aliran proses penyandiannya berorientasi pada satu bit (satu byte data). Sedangkan algoritma blok, proses penyandiaannya berorientasi pada sekumpulan bit (per blok).



Gambar 2. Skema algoritma simetri (Munir, 2006)

Algoritma Asimetris

Algoritma kriptografi asimetrik adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma ini disebut juga algoritma umum (public key algorithm) atau dapat diketahui oleh setiap orang. Untuk dekripsi hanya diketahui oleh yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi (private key). Contoh algoritma asimetris adalah RSA dan ECC.



Gambar 3. Skema algoritma Asimetri (Munir, 2006)

Affine Cipher

Affine chipper adalah perluasan dari Caesar cipher yang mengalikan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran. Enkripsi plainteks P menghasilkan cipherteks C dapat dinyatakan dengan fungsi kongruen sebagai berikut :

$$E(P)=(ax+b) \bmod m \quad \ldots\ldots\ldots\ldots\ldots\ldots (6)$$

Dimana :

m = ukuran alphabet
a = bilangan bulat yang harus relatif prima dengan m
(bila tidak relatif prima maka dekripsi tidak bias)
b = Jumlah pergeseran
(Caesar cipher adalah khusus dari affine cipher dengan m=1)
x = Plainteks yang dikonversi menjadi bilangan bulat dari 0 sampai m-1 sesuai dengan urutan dalam alphabet.
E(P) = Cipherteks yang dikonversi menjadi bilangan bulat dari 0 sampai m-1 sesuai dengan urutan dalam alphabet.

Sedangkan fungsi dekripsinya dapat dituliskan dengan menggunakan persamaan sebagai berikut :

$$D(x)=a^{-1}(x-b) \bmod m \quad \text{……..…….. (7)}$$

Dimana a^{-1} adalah invers perkalian a modulus m yang dapat memenuhi persamaan berikut :

$$1=a^{-1} \bmod m \quad \text{…….. (8)}$$

Invers perkalian a hanya ada jika a dan m adalah coprime. Jika tidak maka proses algoritma akan terhenti. Fungsi dekripsi merupakan kebalikan dari fungsi enkripsi yang dapat dituliskan sebagai berikut :

$$D(E(P)) = a^{-1}(E(P)-b) \bmod m$$
$$= a^{-1}(((ax+b) \bmod m)-b) \bmod m$$
$$= a^{-1}(ax+b-b) \bmod m$$
$$= a^{-1} ax \bmod m$$
$$D(E(x))= x \bmod m \quad \text{…….…….. (9)}$$

Contoh konkrit dari kegiatan satu mengenkripsi dan satu menderipsikan dimana alfabet akan menjadi huruf A sampai huruf Z dan akan memiliki nilai sesuai dengan Tabel I.

Tabel I. Enkripsi dan Dekripsi

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Enkrip

Contoh enkripsi adalah SENOPATI dengan menggunakan tabel 1 untuk nilai numeric dari setiap huruf. Misal a adalah 7, b adalah 10 dan m adalah 26 karena ada 26 karakter dalam alfabet yang digunakan. Nilai a yang terbatas karena coprime dengan 26. Nilai a yang mungkin adalah 1, 3, 5, 7, 11, 15, 17, 19, 21, 23, 25. Nilai b bisa sembarang sepanjang a ≠ 1 karena terjadi pergeseran cipher. Dengan demikian, fungsi enkripsi untuk contoh diatas adalah menjadi y=E(P)=(7x+10)(mod 26). Hasil enkripsi pesan dalam SENOPATI seperti Tabel II.

Tabel II. Ekripsi pesan SENOPATI

Plainteks	S	E	N	O	P	A	T	I
X	18	4	13	14	15	0	19	8
7x + 10	136	38	101	108	115	10	143	66
(7x+10) mod 26	6	12	23	4	11	10	13	14
Cipherteks	T	B	U	Z	E	H	Y	V

Dekripsi

Contoh dekripsi dimana cipherteks yang akan didekripsikan adalah cipherteks dari contoh enkripsi. Fungsi dekripsi secara matematis dapat dituliskan sebagai berikut :

$$D(y)=15(y-10) \bmod 26$$

Dimana a^{-1} adalah hasil perhitungan yaitu 15, b adalah 10, m adalah 26.
Hasil proses dekripsi terhadap cipherteks seperti pada tabel 3 Plainteks dekripsi adalah SENOPATI.

Tabel III. Dekripsi pesan TBVZEHYV

Cipherteks	T	B	V	Z	E	H	Y	V
Y	6	12	23	4	11	10	13	14
15(y-10)	-60	30	195	-90	15	0	45	60
(15(y-10) mod 26)	18	4	13	14	15	0	19	8
Plainteks	S	E	N	O	P	A	T	I

Modifikasi Affine Ciphers

Modifikasi affine ciphers (Munir, 2006) yang akan dikembangkan merupakan kebalikan dari affine chippers dimana huruf dan angka sebagai plainteks akhir dalam password akan menjadi ciphers awal. Biasanya password dapat terdiri dari alfabet dan angka maka pendekripsian alfabet A sampai Z dan angka 0 sampai 9 dengan nilai sesuai seperti tabel 4. Nilai a yang terbatas karena coprime dengan 36 sehingga nilai a mungkin salah satu dari 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35.

Tabel IV. Enkripsi dan Dekripsi Modifikasi Affine Ciphers

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

Contoh :
Password : TIC2014 dengan kunci a=7 dan b=10 dan m=36

Enkripsi

Enkripsi untuk password : TIC2014 dengan menggunakan modifikasi metode affine cipher menghasilkan ETM0Y49, seperti Tabel V. berikut :

Tabel V. Enkripsi TIC2014 dengan modifikasi affine cipher

Plainteks	T	I	C	2	0	1	4
Mod. Plainteks	4	1	0	2	C	I	T
X	30	27	26	28	2	8	19
7x+10	220	199	192	206	24	66	143
(7x+10) mod 36	4	19	12	26	24	30	35
Ciphertek s	E	T	M	0	Y	4	9

Dekripsi

Fungsi dekripsi dituliskan sebagai berikut :
D(y)=31(y-10) mod 36 dimana a^{-1} adalah hasil perhitungan yaitu 31, b adalah 10, m adalah 36. Dekripsi untuk cipherteks UL0YJK menghasilkan password asal AFC25W seperti Table VI berikut :

Tabel VI. Dekripsi ETM0Y49 dengan modifikasi affine cipher

Cipherteks	E	T	M	0	Y	4	9
Mod. Cipherteks	9	4	Y	0	M	T	E
y	35	30	24	26	12	19	4
31(y-10)	775	620	434	496	62	279	-186
31(y-10) mod 36	19	8	2	28	26	27	30
Plainteks	T	I	C	2	0	1	4

KESIMPULAN

Beberapa kesimpulan yang dapat diambil antara lain :

1. Kriptografi klasik di enkripsi dan di dekripsi menggunakan modifikasi metode affine cipher. Karakter yang dapat di enkripsi dan di dekripsi yaitu alfabet dan bilangan asli.
2. Kriptografi klasik menggunakan metode affine cipher agar tidak dapat dibaca oleh orang yang tidak berhak walaupun dengan melihat kode sumber programnya.
3. Perhitungan pada modifikasi affine cipher menghasilkan cipherteks yang memiliki karakter tidak mudah didekripsi oleh kpritanalis.
4. Apabila pesan rahasia (cipherteks) ingin di dekripsikan maka penerima pesan (receiver) harus mengetahui kunci dan aturan konversi yang telah disepakati oleh kedua belah pihak, karena jika terjadi perbedaan pemilihan kunci maupun aturan konversi oleh penerima pesan maka cipherteks tidak dapat didekripsikan.

REFERENSI

[1] Abraham, O. dan Shefiu, G.O. 2012. *An Improved Caesar Cipher (ICC) Algorithm, International Journal of Engineering Science & Advanced Tehnology, Volume 2, Issue-5.:1199-2012*

[2] Ariwibowo, E. 2008. *Aplikasi Pengamanan Dokumen Office dengan Algoritma Kriptografi Kunci Asimetri Elgamal, Jurnal Informatika Vol 2 No. 2*

[3] Forouza, Behrouz, Cryptography and Network Security, McGraw-Hill, 2008

[4] Munir, Rinaldi, Diktat KuliahIF5054 Kriptografi, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, 2006

[5] Ariyus, Dony, Kriptografi : Keamanan Data dan Komunikasi, Graha Ilmu, Yogyakarta, 2006

[6] Munir, R. 2006. Kriptografi, Cetakan Pertama, Penerbit Informatika, Bandung

[7] Kristanto, A. 2003. Keamanan Data pada Jaringan Komputer, Edisi Pertama, Penerbit Grava Media, Yogyakarta