KRIPTOGRAFI DENGAN ALGORITMA GRASS CAESAR

Ana Wahyuni

Fakultas Ilmu Komputer, Universitas AKI
e-mail: ana.wahyuni@unaki.ac.id

Abstact

Exchange of information, documents or data packets via the Internet is very widely used. Information that contains important and confidential message intended only for the person entitled to it, can be done in a way to encrypt the message. One simple method to encrypt the message can be developed with the pattern caesar/grass, grass section called algorithms that further improve the security of the message. The use of algorithms grass section on encryption and decryption of a message can also be used to send messages that contain anything that might threaten/harm the sender of a message without being noticed by unauthorized parties, so avoid defamation or insult, and so forth.

Keywords : Caesar Algorithm; Grass Caesar Algorithm; Encryption; Descryption

1. Pendahuluan

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita atau mengamankan data/ pesan. (LSN, 2007). Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu autentikation, data integrity, confidentiality dan non repudiation.(Munir, 2007)

Penggunaan kriptografi pada kehidupan sehari-hari dapat dilakukan dengan metode yang sederhana, salah satunya dengan metode/ algoritma caesar. Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. (Munir, 2007) Misalnya, jika menggunakan geseran 3, w akan menjadi z, i menjadi l, dan k menjadi n sehingga teks terang "wiki" akan menjadi "zlnl" pada teks tersandi.

Nama *Caesar* diambil dari Julius Caesar, jenderal, konsul, dan diktator Romawi yang menggunakan sandi ini untuk berkomunikasi dengan para panglimanya. Pada saat ini, seperti halnya sandi substitusi alfabet tunggal lainnya, sandi Caesar dapat dengan mudah dipecahkan dan praktis tidak memberikan kerahasiaan bagi pemakainya, karena jumlah kunci hanya 26.(Munir, 2007) Kekurangan dari sandi Caesar ini dapat diatasi dengan menambahkan pola grass pada proses enkripsi dan dekripsinya. (Donny, 2012)

2. Metode Penelitian

Metode pengumpulan data dalam penelitian ini adalah sebagai berikut :

1. Observasi

Merupakan metode pengumpulan data dengan cara melakukan pengamatan secara langsung pada obyek yang diteliti yaitu plain teks dan chipper teks.

2. Studi Pustaka

Merupakan metode pengumpulan data dengan cara mengumpulkan data-data dari berbagai sumber yang mendukung penelitian baik itu dari buku, jurnal ilmiah maupun artikel lainnya yang mendukung. Hasil dari studi pustaka berupa teori dan perkembangan terkini mengenai kriptosistem dengan metode Caesar dan teori pendukung lainnya.

Sedangkan alat penelitian yang digunakan dalam proses penelitian ini sebagai berikut :

1. Perangkat Keras berupa seperangkat komputer dengan spesifikasi Pentium (R) Dual Core CPU T4200 @ 2.00 GHz 2.00 GHz, 1.87 GB of RAM.
2. Perangkat Lunak berupa Microsoft Windows XP dan caesarchiper.exe.

3. Tinjauan Pustaka

Beberapa istilah yang umum digunakan dalam pembahasan kriptografi :

1. Plaintext (*message*) merupakan pesan asli yang ingin dikirimkan dan dijaga keamanannya. Pesan ini tidak lain dari informasi tersebut.

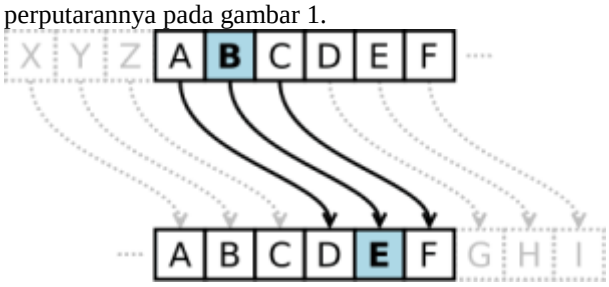
2. Chipertext merupakan pesan yang telah dikodekan (disandikan) sehingga siap untuk dikirimkan.

3. Cipher merupakan algoritma matematis yang digunakan untuk proses Enkripsi *plaintext* menjadi ciphertext.

4. Enkripsi (*encryption*) merupakan proses yang dilakukan untuk menyandikan *plaintext* sehingga menjadi *chipertext*

5. Dekripsi (*decryption*) merupakan proses yangdilakukan untuk memperoleh kembali *plaintext* dari *chipertext.*

6. Kriptosistem merupakan sistem yang dirancang untuk mengamankan suatu sistem informasi dengan memanfaatkan kriptografi. (Munir, 2007)
mmmm
Algoritma Caesar merupakan metode enkripsi yang dilakukan pada zaman Julius Caesar. Hanya dipergunakan pada alfabet baik huruf kapital maupun huruf kecil, tidak case sensitive artinya tidak ada perbedaan penggunaan huruf kapital ataupun kecil. Algoritma ini tidak dapat dilakukan pada plain text selain huruf, misalnya angka, simbol dan lain-lain. (LSN.2007) Banyak perputaran karakter dinyatakan dengan n. Misal n = 3 diberikan ilustrasi perputarannya pada gambar 1.



Gambar 1. Perputaran karakter pada algoritma caesar dengan n = 3
Cara enkripsi dari metode ini yaitu dengan memutar sejauh n langkah. Jika n negatif berarti memutar kearah kiri, sebaliknya jika n positif kearah kanan. Jika n>26 berarti n = sisa pembagian dengan 26 = n mod 26. Contoh jika n = 3, bentuk dari enkripsi ini adalah sebagai berikut:
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
D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C
Contoh Caesar Cipher 1 :
Misalnya menggunakan caesar cipher dengan pergeseran 3 huruf:
Plaintext: KOPLER akan dienkripsi menjadi Ciphertext : NRSOHU
ROT 13
Yaitu suatu metode enkripsi sebagai penerapan algoritma Caesar dengan cara menukarkan huruf sejauh 13 huruf. Bentuk dari metode enkripsi ini adalah sebagai berikut:
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
Contoh menggunakan ROT 13:
Plaintext : KOPLER akan dienkripsi menjadi Ciphertext : XBCYRE
contoh algoritma Caesar Cipher 2 :

THE COLOURS AND DESIGNS ARE OFTEN VERY BEAUTIFUL
Hasil enkripsi kalimat diatas menggunakan algoritma Caesar Cipher sesuai perputaran karakter pada gambar 1 adalah sebagai berikut :
wkh frorxuv dqg ghvljqv duh riwhq yhub ehdxwlixo. Skema atau pola yang digunakan untuk mengenkrip :

1. Kata “wkh” , “dqg”, dan “duh” dapat berarti 3 kata yang sering digunakan dalam bahasa inggris seperti : the, are, was, car, you.
2. Pola spasi yang digunakan jelas.
3. Kata “wkh” dan “duh” mempunyai akhiran yang sama sehingga mempermudah dalam pencarian kata.
4. Jika diperhatikan setiap huruf yang digunakan selalu dikurangi 3 huruf dari huruf sebelumnya yang dapat mempunyai arti dan polanya teratur disetiap huruf.

Dari contoh ini terlihat relatif mudahnya algoritma caesar dipecahkan. Hal ini dapat diminimalkan dengan mengkombinasikan Algoritma Caesar yang dengan menggunakan Keyword. Berikut ini diberikan beberapa contohnya,
1. Keyword : authorize
Berikut cara untuk enkripsi dengan algoritma menggunakan keyword :
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
a u t h o r i z e b c d f g j k l m n p q s v w x y
2. Keyword : background
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
b a c k g r o u n d c e f h I j l m p q s t v w x y z
3. Keyword : category
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
c a t e g o r y b d f h I j k l m n p q s u v w x z
4. Keyword : rezqy
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
r e z q y a b c d f g h I j k l m n o p s t u v w x
5. Keyword : widgets
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
w i d g e t s a b c f h i j k l m n o p q r u v x y z

Caesar cipher mudah dipecahkan dengan metode exhaustive key search karena jumlah kuncinya sangat sedikit (hanya ada 26 kunci). (http://informatika.stei.itb.ac.id).
Dengan menggunakan pemrograman, tentulah sangat mudah untuk memecahkan maupun membentuk ciphertext dengan pola enkripsi seperti ini. Tidak masalah mau menggunakan pergeseran huruf sejauh berapapun. Criptanalist dapat dengan mudah mendapatkan informasi dari hasil enkripsi ataupun dekripsinya. Hal ini merupakan kekurangan algoritma Caesar. Kekurangan ini dapat diatasi dengan menambahkan pola *grass* pada algoritmanya sehingga disebut algoritma grass caesar.

4. Hasil dan Pembahasan

Algoritma ini dinamakan algoritma grass caesar, karena menggunakan perpaduan algoritma yang sudah ada sebelumnya, yaitu algoritma caesar, dan

istilah grass diambil karena dalam proses enkripsinya ada susunan huruf yang berbentuk rumput. (Donny, 2012)

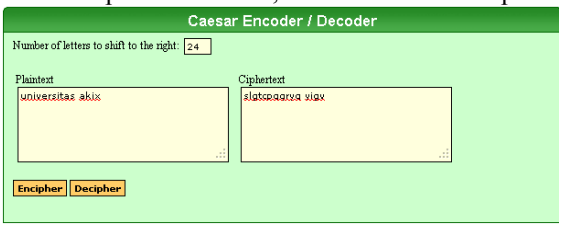
Pada algoritama ini, banyak kunci dan besar rotasi (panjang kunci) yang akan digunakan bebas. Semakin banyak dan panjang kunci yang dipakai semakin meningkatkan keamanan data yang dirahasiakan. Sebagai contoh jika menggunakan 4 kunci yaitu :
Kunci 1 : 24
Kunci 2 : 06
Kunci 3 : 01
Kunci 4 : 31
Contoh :
Plaintext: Universitas Aki
Langkah enkripsi di pihak pengirim pesan (sender) yaitu :
1) Menyusun plaintex hingga menjadi seperti gambar rumput, dengan ketentuan di awali dengan rumput kecil, kemudian rumput besar dan penambahan huruf X jika rumput belum sempurna. Contoh dengan plaintex Universitas Aki maka ada penambahan huruf X sebanyak 1.

			E				S			
	N		V		R		I		A	
U		I				S		T		

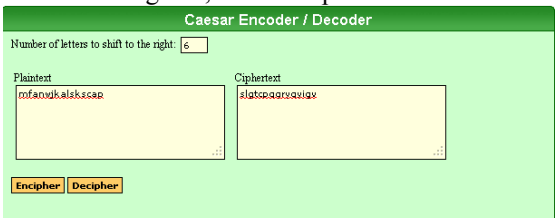
			A				I			
		K		X						

Kemudian kita enkripsikan plaintex tersebut dengan 4 kunci yang sudah di tentukan, maka akan di dapat hasil seperti di bawah ini:
Catatan : Program aplikasi .exe dapat di download di **CaesarChiper.exe**
(www.4share.com/file/caesarchiper.html)

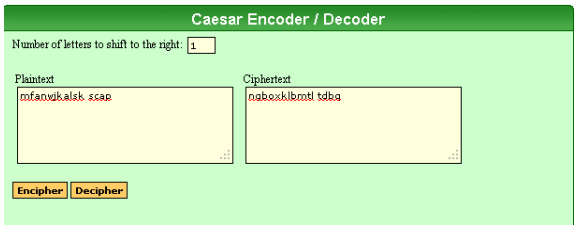
KUNCI 1 : 24 (ambil dari atas/ enkripsi).
Masukkan angka 24 dan plainteks : Universitas Aki, catatan : tidak case sensitive/ huruf kapital atau kecil tidak ada perbedaan hasil, kemudian klik ”encipher”.



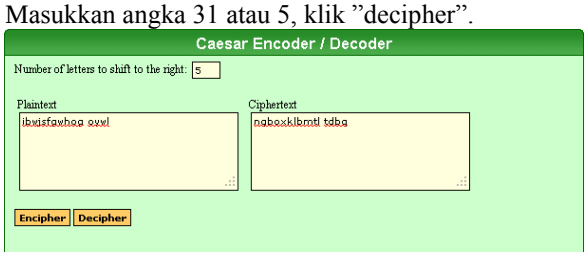
Hasil : Cypertext : slgtcpqgryq yigv
KUNCI 2 : 6 (ambil dari bawah/ dekripsi).
Masukkan angka 6, klik ”decipher”.



Hasil : Plaintext : mfanwjkalsk scap
KUNCI 3 : 1 (ambil dari atas/ enkripsi).
Masukkan angka 1, kemudian klik ”encipher”.



Hasil : cypertext : ngboxklbmti tdbq
KUNCI 4 : 31 atau 5 = 31 mod 26 (ambil dari bawah/ dekripsi).
Masukkan angka 31 atau 5, klik ”decipher”.



Hasil : plaintext : ibwjsfgwhog oywl

2) Kemudian hasil enkripsi, pada contoh di atas yaitu dengan kunci terakhir (kunci 4), hasil tersebut disusun dengan pola rumput seperti di bawah ini.

			s				g			
	B		j		f		w		o	
I		w				g		h		

	o		o		w					
		y		l						

Kemudian diambil dari baris paling bawah secara horisontal dari kiri kekanan, kemudian baris atasnya horisontal dari kanan ke kiri, dan baris yang paling atas horisontal dari kiri ke kanan. Dari algoritma rumput tersebut dihasilkan: iwghylwoowfjbsg

3) Setelah dienkripsikan dengan algoritma Grass Caesar, kemudian dimasukkan dalam nilai desimal ASCII dari suatu huruf, kemudian menjumlahkannya dengan kunci-kunci yang dipakai. Kemudian di mod 128. Banyak kode ASCII adalah 128. Kemudian hasil (yaitu angka desimal) yang sudah di mod, direstrukturisasi pada karakter pada kode ASCII. Catatan : kode ASCII bersifat case sensitive artinya menghasilkan nilai yang berbeda untuk huruf kapital dan huruf kecil. Perhitungan dan hasilnya diberikan di tabel 1.

Tabel 1. Hasil karakter ASCII dari contoh enkrips

HURUF	NILAI	KUNCI 1	KUNCI 2	KUNCI 3	KUNCI 4	JUMLAH	Jumlah MOD 128	KARAKTER ASCII
I	105	24	6	1	31	167	39	‘
W	119	24	6	1	31	181	53	**5**
G	103	24	6	1	31	165	37	**%**
H	104	24	6	1	31	166	38	**&**
Y	121	24	6	1	31	183	55	**7**
L	108	24	6	1	31	170	42	*****
W	119	24	6	1	31	181	53	**5**
O	111	24	6	1	31	173	45	**-**
O	111	24	6	1	31	173	45	**-**
W	119	24	6	1	31	181	53	**5**
F	102	24	6	1	31	164	36	**$**
J	106	24	6	1	31	168	40	**(**
B	98	24	6	1	31	160	32	**SP**
S	115	24	6	1	31	171	49	**1**
G	103	24	6	1	31	165	37	**%**

4) Selanjutnya pesan yang dikirim adalah ’5%7*5—5$(SP1% dengan kunci 1,2,3,dan 4. Diasumsikan pihak penerima pesan sudah tahu algoritma yang digunakan. Kunci yang digunakan juga bisa dienkripsi dengan algoritma pertukaran kunci atau dikirim terpisah dari pesan, atau dikirim lewat jaringan lain, misal pesan dikirim lewat email dan kunci dikirim lewat SMS.

Langkah dekripsi di pihak penerima pesan (receiver) yaitu :
Karena menggunakan algoritma Caesar yang merupakan algoritma simetris, maka untuk langkah deskripsi sama dengan dekripsi hanya dengan urutan

Tabel 2. Hasil karakter ASCII dari contoh dekrip

KARAKTER ASCII	Nilai Desimal	Invers MOD 128 =inv	KUNCI 1	KUNCI 2	KUNCI 3	KUNCI 4	Inv-(kunci1 sd 4)	Karakter ASCII
‘	39	167	24	6	1	31	105	i
5	53	181	24	6	1	31	119	w
%	37	165	24	6	1	31	103	g
&	38	166	24	6	1	31	104	h
7	55	183	24	6	1	31	121	y
*****	42	170	24	6	1	31	108	l
5	53	181	24	6	1	31	119	w
-	45	173	24	6	1	31	111	o
-	45	173	24	6	1	31	111	o
5	53	181	24	6	1	31	119	w
$	36	164	24	6	1	31	102	f
(	40	168	24	6	1	31	106	j
SP	32	160	24	6	1	31	98	b
1	49	171	24	6	1	31	115	s
%	37	165	24	6	1	31	103	g

terbalik, yaitu untuk langkah pertama kita kembalikan dari karakter ASCII ke huruf. Pada contoh diatas yaitu pesan ’5%7*5--5$(SP1% sebagai berikut :

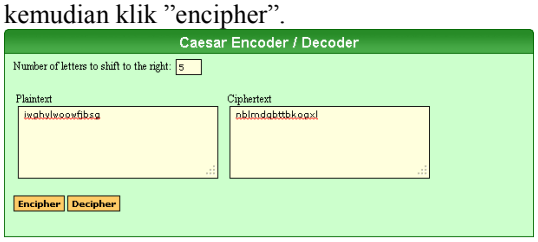
Dilihat dari isi pesan pada contoh diatas hanya SP yang bisa bernilai desimal berbeda. Ada dua kemungkinan :

1. masing-masing karakter direstrukturisasi ke nilai desimalnya atau
2. SP dihitung sebagai satu karakter untuk direstrukturisasi ke nilai desimalnya.

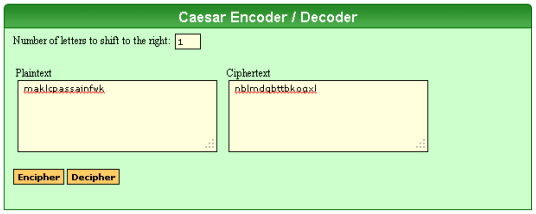
Dua kemungkinan tersebut perlu didekrip oleh pihak receiver, dan diambil hasil dekrip plainteks yang bermakna. Misal receiver mengambil kemungkinan kedua dan melakukan proses dekrip yang diberikan pada tabel 2.

Kemudian akan di dapatkan hasil dekripsi : iwghylwoowfjbsg

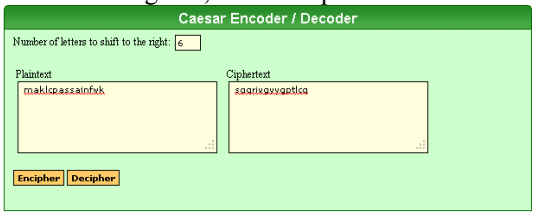
Proses selanjutnya masukkan hasil dekripsi tersebut kedalam kunci yang dipakai dalam langkah enkripsi dengan urutan terbalik.
Kunci 4 : 31 atau 5 (ambil dari atas/ enkripsi).
Masukkan angka 31 atau 5 dan plainteks : iwghylwoowfjbsg, catatan : tidak case sensitive/ huruf kapital atau kecil tidak ada perbedaan hasil, kemudian klik ”encipher”.



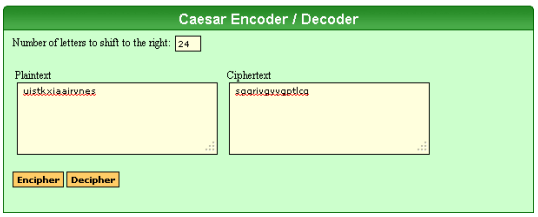
Hasil : nblmdqbttbkogx
Kunci 3 : 1 (ambil dari bawah/ dekripsi).
Masukkan angka 1, klik ”decipher”.



Hasil : maklcpassainfwk
KUNCI 2 : 6 (ambil dari atas/ enkripsi).
Masukkan angka 6, klik ”encipher”.



Hasil : soqrivgyvgptlcq
KUNCI 1 : 24 (ambil dari bawah/ dekripsi).
Masukkan angka 24, klik ”decipher”.



Hasil : uistkxiaairvnes

Hasil akhir adalah uistkxiaairvnes. Selanjutnya menentukan ada berapa rumput dengan cara banyak huruf diibagi 3. Jika sisa bagi sama dengan 0 makan rumput terakhir yaitu rumput kecil, sedangkan jika sisa baginya 1 maka rumput terakhir rumput besar. Pada contoh diatas yaitu uistkxiaairvnes ada 15 huruf, 15/3 = 5 sisa 0 maka ada 5 rumput dengan rumput terakhir, rumput kecil. Jadi hasil uistkxiaairvnes disusun pada 5 rumput dengan rumput terakhir, rumput kecil seperti berikut :

			e						s					
	n		v		r		i		a		a		I	
U		i				s		t				k		x

Hasil Dekripsi: Universitas Akix = Universitas Aki (Catatan : karakter x diakhir pesan adalah karakter tambahan, sehingga diabaikan)

Kesimpulan

Algoritma Grass Caesar dapat digunakan untuk mengirim pesan atau data rahasia via Internet. Penambahan pola grass meningkatkan keamanan transmisi data/ pesan tersebut. Pada algoritama ini, banyak kunci dan besar rotasi (panjang kunci) yang akan digunakan bebas. Semakin banyak dan panjang kunci yang dipakai semakin meningkatkan keamanan data yang dirahasiakan.

Daftar Pustaka

LSN.2007. Jelajah Kriptologi, LSN Jakarta

Munir, Rinaldi. 2007. Kriptografi.Bandung : Informatika.

Donny Seftyanto.2012. Peran Algoritma Caesar Cipher Dalam Membangun Karakter Akan Kesadaran Keamanan Informasi , Prosiding Seminar Nasional Matematika dan Pendidikan Matematika FMIPA UNY Yogyakarta,

http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Algoritma%20klasik.pdf