CAESAR CHIPER VS VIGENÈRE

Doni[1], Abu Walad[2]
Manajemen Informatika
PKN & STMIK LPKIA
Jl. Soekarno-hatta No.456 Bandung 40287
E-mail : dhonie_dasta@yahoo.com[1] , max_walad@yahoo.com [2]

Abstrak

Perkembangan teknologi saat ini telah membawa perubahan besar pada dunia komputer, salah satunya pada bidang komunikasi jarak jauh. Sebelum ditemukannya teknologi seperti sekarang ini komunikasi jarak jauh yaitu menggunakan surat yang berisi pesan, sudah pasti pesan yang disampaikan oleh pengirim harus sampai kepada yang menerima dengan keadaan utuh, aman dan terjaga kerahasiaannya. Pada saat ini untuk komunikasi jarak jauh sudah banyak digunakan teknologi yang lebih canggih salah satunya yaitu menggunakan e-mail atau surat elektronik yang berupa data digital.
Untuk menjaga kerahasiaan dan keamanan pesan diperlukan pengkodean atau sering disebut kriptografi (Cryptography). Secara umum kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita. Dalam kriptografi Sandi Caesar (caesar cipher) atau sandi geser adalah salahsatu sandi yang paling populer digunakan, pada zaman yunani kuno sandi caesar digunakan untuk mengirim pesan yang mengandung rahasia atau taktik militer. Selain sandi caesar, sandi yang sering digunakan adalah sandi vigenere (vigenere cipher) merupakan perkembangan dari sandi caesar, sandi ini dikenal luas karena cara kerjanya mudah dimengerti dan dijalankan, dan bagi para pemula sulit dipecahkan. Kelebihan sandi ini dibanding sandi caesar dan sandi lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi.

Kata kunci: e-mail, Cryptography, caesar cipher, vigenere cipher, analisis frekuensi.

1. Pendahuluan

Kemajuan di bidang telekomunikasi dan komputer telah memungkinkan seseorang untuk melakukan transaksi bisnis secara *cashless*, selain itu ia juga dapat mengirimkan informasi kepada temannya secara on-line.Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko bilamana informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak (unauthorized persons). Misalnya, informasi mengenai nomor kartu kredit anda, bila informasi ini jatuh kepada orang-orang yang jahat maka anda harus bersiap-siap terhadap melonjaknya tagihan kartu kredit anda.

Sebelum tahun 1970-an, teknologi kriptografi digunakan terbatas hanya untuk tujuan militer dan diplomatik. Akan tetapi kemudian bidang bisnis dan perorangan mulai menyadari pentingnya melindungi informasi berharga.

Kriptografi adalah ilmu dan seni untuk menjaga keamanan dan kerahasiaan berita,[1] kriptografi juga adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integrasi data dan autentikasi data.[2]

Tidak semua aspek keamanan informasi ditangani oleh kriptografi.

Ada empat tujuan mendasar dari ilmu kriptografi yang juga merupakan aspek keamanan informasi yaitu :

- Kerahasiaan data, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
- Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
- Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.

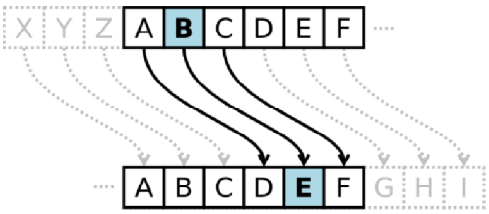
- Non-repuidasi, atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman suatu informasi oleh yang mengirimkan.

1. Bruce Schneier,*Applied Cryptography.*
2. A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography.*

2. Caesar Cipher (Sandi Caesar)

Dalam kriptografi Caesar cipher atau sandi Caesar,kode Caesar atau sandi geser adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi subtitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Misalnya, jika menggunakan geseran 3, B akan menjadi E, U menjadi X, dan K menjadi N sehingga plaintext "buku" akan menjadi "EXNX" pada teks tersandi. Nama *Caesar* diambil dari Julius Caesar, jenderal, konsul, dan diktator Romawi yang menggunakan sandi ini untuk berkomunikasi dengan para panglimanya.

Langkah enkripsi oleh sandi Caesar sering dijadikan bagian dari penyandian yang lebih rumit, seperti sandi Vigenère. Pada saat ini, seperti halnya sandi substitusi alfabet tunggal lainnya, sandi Caesar dapat dengan mudah dipecahkan dan praktis tidak memberikan kerahasiaan bagi pemakainya.



Gambar 1 sandi caesar dengan geseran tiga

2.1 Cara kerja Sandi Caesar

Cara kerja sandi Caesar dapat diilustrasikan dengan membariskan dua set alfabet, sandi disusun dengan cara menggeser alfabet biasa ke kanan atau ke kiri dengan angka tertentu (angka ini disebut kunci). Misalnya sandi Caesar dengan kunci 3, adalah sebagai berikut:

Alfabet Biasa:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Alfabet Sandi:
DEFGHIJKLMNOPQRSTUVWXYZABC

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan di alfabet biasa, lalu tuliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut gunakan cara sebaliknya. Contoh penyandian sebuah pesan adalah sebagai berikut:

Alfabet Biasa:
DONI

Alfabet Sandi:
GSQM

Proses penyandian (enkripsi) dapat secara matematis menggunakan operasi modulus dengan mengubah huruf-huruf menjadi angka, A = 0, B = 1,..., Z = 25. Sandi (E_n) dari "huruf" x dengan geseran n secara matematis dituliskan dengan:

$$E_n(x) = (x + n) \mod 26.$$

Sedangkan pada proses pemecahan kode (dekripsi), hasil dekripsi (D_n) adalah:

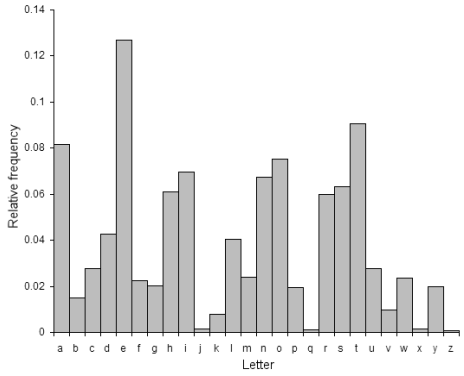
$$D_n(x) = (x - n) \mod 26.$$

Setiap huruf yang sama digantikan oleh huruf yang sama di sepanjang pesan, sehingga sandi Caesar digolongkan kepada *substitusi monoalfabetik* yang berlawanan dengan *substitusi polialfabetik.*

2.2 Deskripsi Sandi Caesar

Proses membaca teks tersandi menjadi plaintextdisebut dekripsi. Sandi Caesar dapat dipecahkan bahkan jika seseorang hanya memiliki teks tersandi tanpa mengetahui nilai geserannya, ataupun bahwa sandi Caesar telah digunakan.

Jika pihak pemecah sandi hanya mengetahui bahwa digunakan substitusi monoalfabetik dalam suatu sandi, sandi tersebut dipecahkan dengan cara analisis frekuensi. Setiap bahasa memiliki huruf yang sering digunakan atau jarang digunakan. Misalnya huruf *a* sering sekali digunakan dalambahasa Indonesia, dan *q* atau *x* jarang sekali muncul. Setiap bahasa memiliki pola frekuensi tertentu, yang menunjukkan frekuensi relatif dari digunakannya huruf-huruf dalam bahasa tersebut. Pola frekuensi huruf dalam bahasa Inggris ditunjukkan dalam gambar sebagai berikut:



Gambar 2 frekuensi kemunculan huruf dalam bahasa inggris

Cara kedua yang lebih mudah, dapat dilakukan jika sang pemecah sandi mengetahui bahwa pengirim sandi menggunakan sandi Caesar. Sandi tersebut akan dipecahkan dengan menggunakan *brute force attack* adalahsebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin, yaitu mencoba ke-26 kemungkinan geseran yang digunakan. Biasanya hanya satu dari ke-26 kemungkinan ini yang dapat dibaca. Misalkan suatu teks tersandi "EXXEGOEXSRGI".

Tabel 1 contoh Metode Brute force attack

Deskripsi pergeseran	**Kandidat plaintext**
0	exxegoexsrgi
1	dwwdfndwrqfh
2	cvvcemcvqpeg
3	buubdlbupodf
4	attackatonce
5	zsszbjzsnmbd
6	yrryaiyrmlac
.....	
23	haahjrhavujl
24	gzzgiqgzutik
25	fyyfhpfytshj

Pada tabel diatas ditunjukkan hasil percobaan yang dilakukan, dan hanya satu hasil yang dapat dibaca, yaitu *attackatonce*. Hal ini berarti pesan yang disandikan adalah pesan berbahasa Inggris "attack at once", yang berarti "serang sekarang juga".

Dengan kemajuan komputer dan teknologi informasi, kedua cara diatas dapat dijalankan dengan mudah dan cepat, sehingga saat ini sandi Caesar sama sekali tidak berguna untuk menyembunyikan atau menyandikan dokumen-dokumen atau perintah-perintah penting dan rahasia.

3. Vigenère Cipher (Sandi Vigenère)

Sandi Vigenère adalah metode penyadian teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Sandi Vigenère merupakan bentuk sederhana dari sandi substitusi polialfabetik. Kelebihan sandi ini dibanding sandi Caesar dan sandi monoalfabetik lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi.

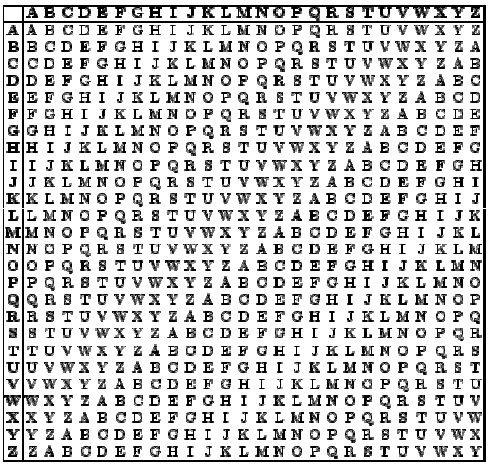
Giovan Batista Belaso menjelaskan metode ini dalam buku *La cifra del Sig. Giovan Batista Belaso* (1553) dan disempurnakan oleh diplomat Perancis Blaise de Vigenère pada 1586. Pada abad ke-19, banyak orang yang mengira Vigenère adalah penemu sandi ini sehingga sandi ini dikenal luas sebagai "sandi Vigenère".

Metode pemecahan sandi Vigenère baru ditemukan pada abad ke-19. Pada tahun 1854 Charles Babbage menemukan cara untuk memecahkan sandi Vigenère. Metode ini dinamakan tes *Klasiki* karena Friedrich klasiki yang pertama mempublikasikannya.

3.1 Cara kerja Sandi Vigenère

Sandi Vigenère sebenarnya merupakan pengembangan dari sandi Caesar. Pada sandi Caesar, setiap huruf plaintext digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalkan pada sandi Caesar dengan geseran 3, maka A menjadi D, B menjadi E dan seterusnya. Sandi Vigenère terdiri dari beberapa sandi Caesar dengan nilai geseran yang berbeda.

Untuk menyandikan suatu pesan, digunakan sebuah tabel alfabet yang disebut tabel Vigenère. Tabel Vigenère berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, membentuk ke-26 kemungkinan sandi Caesar. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang.



	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	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	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
C	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	B
D	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
E	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	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Gambar 2 Tabel Vigenère

Contoh plaintext yang akan disandikan adalah "JAM SEPULUH" sedangkan kata kuncinya adalah "TIBA". Kata "rumah" diulang sehingga jumlah hurufnya sama dengan plaintext, yaitu "TIBATIBATI".

Huruf pertama pada plaintext adalah J disandikan dengan menggunakan baris berjudul T huruf pertama pada kata kunci. Pada baris J dan kolom T di tabel Vigenère, terdapat huruf C. Demikian pula untuk huruf kedua, digunakan huruf yang terletak pada baris I (huruf kedua kata kunci) dan kolom A (huruf kedua plaintext), yaitu huruf I. Maka penyandiannya adalah:

Plaintext : JAMSEPULUH

Kata kunci : TIBATIBATI

Ciphertext : CINSXXVLNP

Proses dekripsi dilakukan dengan mencari huruf Ciphertext pada baris berjudul huruf dari kata kunci. Misalnya, pada contoh diatas, untuk huruf pertama, kita mencari huruf C (huruf pertama Ciphertext) pada baris T (huruf pertama pada kata kunci), yang terdapat pada kolom J, sehingga huruf pertama adalah J. Lalu I terdapat pada baris I di kolom A, sehingga diketahui huruf kedua plaintext adalah A, dan seterusnya hingga didapat perintah "JAMSEPULUH".

Enkripsi atau penyandian dengan sandi Vigenère juga dapat dituliskan secara matematis, C_i adalah huruf ke-i pada teks tersandi, P_i adalah huruf ke-i pada plaintext, K_i adalah huruf ke-i pada kata kunci, dan *mod* adalah operasi modulus (sisa pembagian). Enkripsi dengan menggunakan penjumlahan dan operasi modulus, yaitu:

$$C_i \equiv (P_i + K_i) \mod 26$$

Sedangkan deskripsi dengan menggunakan penjumlahan dan operasi modulus, yaitu:

$$P_i \equiv (C_i - K_i) \mod 26$$

3.2 Algoritma Sandi Vigenere

Dalam pemrograman untuk keamanan komputer, algoritma sandi Vigenere seringkali digunakan untuk dasar pengembangan pemrograman, adapun ketentuan yang digunakan dalam algoritma sandi vigenere adalah:

- Strings dan array menggunakan 0-indikasi dasar.
- Huruf diwakili oleh integer 0 sampai 25.
- Dalam analisis kompleksitas C adalah panjang Ciphertext dan K adalah panjang kunci.

Algoritma enkripsi:

```
Vigenere-encrypt(S, key)
    for i = 0 to length(S)-1
        T[i] = (S[i] + key[i mod length(key)]) mod 26
    return T
```

Algoritma deskripsi:

```
Vigenere-decrypt(S, key)
    for i = 0 to length(S)-1
        T[i] = (S[i] - key[i mod length(key)]) mod 26
    return T
```

4. Kesimpulan

Dari pembuatan makalah ini dapat ditarik beberapa kesimpulan yang berkaitan tentang sandi Caesar, sandi Vigenere dan kriptografi:

1. Belum adanya formula yang pasti untuk menghitung panjang kunci yang sebenarnya, membuat algoritma kunci bergeser ini semakin kuat.
2. Penggunaan sandi dalam mengirim pesan atau kriptografi sangat perlu digunakan untuk mengirim pesan rahasia.
3. Sandi Caesar merupakan sandi yang populer digunakan dan pemecahan sandi caesar sudah banyak diketahui dengan menggunakan analisis frekuensi.
4. Sandi Vigenere merupakan pengembangan dari sandi Caesar dan pemecahannya lebih rumit dari sandi Caesar.
5. Algoritma sandi vigenere dapat dikembangkan lagi untuk aplikasi keamanan komputer.

5. Daftar pustaka

[1] Ariyus, Doni, 2008, *Pengantar Ilmu Kriptografi*,Andi: Yogyakarta
[2] http://en.wikipedia.org/wiki/Caesar_cipher
[3] http://id.wikipedia.org/wiki/Kriptografi
[4] http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
[5] http://egiewendra.blog.upi.edu/2010/01/19/algoritma-kriptografi-klasik/