APLIKASI TEORI BILANGAN DALAM SANDI VIGENERE DAN CAESAR

Kevin Chandra Irwanto – 13508063

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
E-mail : if18063@students.if.itb.ac.id ; synolyn@yahoo.com

ABSTRAK

Makalah ini membahas tentang aplikasi teori bilangan dalam sandi vigenere. Sandi Vigenere itu sendiri hanyalah salah satu contoh pengaplikasian teori bilangan untuk digunakan dalam suatu sandi. Dalam makalah ini juga akan sedikit dibahas tentang sandi Caesar yang sebelumnya sudah sempat disinggung saat kuliah Struktur Diskrit. Lalu membahas perbedaan dan kelebihan kekurangan antara kedua sandi tersebut.

Kata kunci : Sandi Vigenere, Sandi Caesar, Teori Bilangan, Kriptografi

1. PENDAHULUAN

Teori Bilangan adalah salah satu cabang dari matematika murni yang mempelajari sifat-sifat bilangan bulat yang banyak sekali aplikasi dan contoh penggunaannya.

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan berita. Dalam menjaga kerahasiaan berita tersebut, dipakailah sandi-sandi termasuk Sandi Caesar dan Sandi Vigenere.

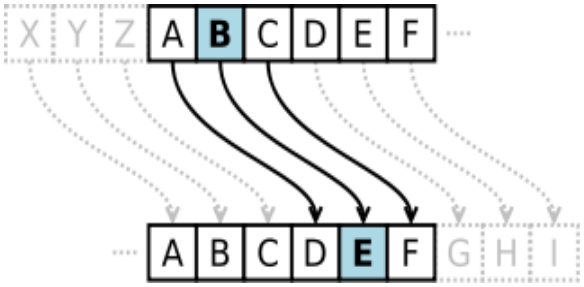
Sandi Caesar ini pertama kali digunakan oleh Julius Caesar, seorang Jendral Romawi, untuk berkomunikasi dengan para panglimanya. Sedangkan Sandi Vigenere pertama kali dijelaskan oleh Giovan Batista Belaso, lalu disempurnakan oleh seorang diplomat Perancis yang bernama Vigenere.

Dalam era yang serba maju ini, kriptografi sudah tidak asing lagi terdengar. Oleh karena itu akan dibahas tentang 2 macam sandi, yakni Sandi Caesar dan Sandi Vigenere.

2. SANDI CAESAR

Sandi Caesar, atau sandi geser, atau Geseran Caesar adalah salah satu teknik enkripsi yang paling dasar, paling sederhana ,dan paling terkenal. Sandi ini hanya cukup menggeser sebanyak n buah. Hasil penggeseran tersebut adalah hasil enkripsi sandi Caesar.

Sebagai contoh, jika n = 3, maka kata ‘Aku ingin mandi’ berubah menjadi ‘Dnx lqjlq pdqgl’.



Gambar 1. Ilustrasi Sandi Caesar.

Sumber : wikipedia.com

2.1.Sejarah Sandi Caesar

Nama Sandi Caesar diambil dari Julius Caesar, seorang Jendral,konsul, dan diktator Romawi. Tertulis dalam buku *Suetonius* “Kehidupan Dua Belas Caesar” bahwa Caesar menggunakan geseran tiga, yang berarti n = 3. Sehingga huruf A berubah menjadi D , dst (*Suetonius – Julius Caesar 56*).

Keponakan Caesar, Augustus juga menggunakan sandi ini, namun dalam penggunaannya ia menggunakan n = 1, sehingga huruf A berubah menjadi B, dst sampai huruf Z berubah menjadi AA (*Suetonius – Augustus 88*).

Lalu Sandi Caesar ini sempat digunakan dalam Perang Dunia I oleh Tentara Kekaisaran Rusia, sehingga mengakibatkan sandi tersebut sangat mudah terbaca oleh kriptoanalis Jerman dan Austria.

Muncul sebutan untuk Sandi Caesar dengan nilai n = 13 yaitu algoritma ROT13. Karena ROT13 ini banyak digunakan untuk spoiler dalam forum-forum internet agar pesan tersebut tidak langsung terbaca.

2.2.Proses Penyandian Sandi Caesar

Proses penyandian(enkripsi) ini dapat ditulis secara matematis dengan operasi modulus (mod) dengan aturan mengubah huruf menjadi angka, yakni A itu 0, B itu 1, C itu 2, dst sampai Z itu 25.

INGAT ! A bukan 1 dan Z bukan 26 karena dalam operasi modulus 26 tidak ada angka 26. 26 (mod 26) ≡ 0.

Secara matematis dapat dituliskan sbb :

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

$E_n(x)$ adalah hasil enkripsi dari suatu huruf. Sandi Caesar tersebut digeser sebanyak n buah.

2.3.Memecahkan Sandi Caesar

Proses memecahkan(deskripsi) Sandi Caesar ini termasuk hal yang mudah karena kita sudah tahu bagaimana mekanisme sandi itu.

Caranya tinggal digeser kembali sebanyak n buah sampai mendapat suatu teks yang pas untuk dibaca dan dimengerti.

Misal contoh ‘Dnx lqjlq pdqgl’ tadi, dengan cara ‘brutal’, tuliskan saja 26 kemungkinan yang ada (karena nilai n berkisar antara 1 dan 26).

Untuk n = 1, maka teks tersebut menjadi ‘Cmw kphkp ocpfk’. Karena teks masih aneh maka dilanjutkan untuk n = 2.

Ketika n = 2, teks menjadi ‘Blv jogjo nboej’. Jika n = 3, maka teks menjadi ‘Aku ingin mandi’. Karena teks tersebut sudah dapat dibaca dan dimengerti, maka nilai n yang berlaku untuk sandi tersebut adalah 3 atau dengan kata lain digunakan geseran tiga.

Secara matematis, proses deskripsi ini dapat ditulis sbb:

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

$D_n(x)$ adalah hasil deskripsi dari suatu huruf. Sandi Caesar tersebut digeser sebanyak n buah.

Dengan kemajuan teknologi dan computer sekarang ini Sandi Caesar menjadi tidak berguna lagi karena dalam hitungan detik, sandi ini dapat terpecahkan langsung.

Contoh lain, memecahkan kode ‘exxegoexsrgi’ dengan tabel dari n = 1 sampai dengan n = 26.

Decryption shift	Candidate plaintext
exxegoexsrgi	0
dwwdfndwrqfh	1
cvvcemcvqpeg	2
buubdlbupodf	3
attackatonce	4
zsszbjzsnmbd	5
yrryaiyrmlac	6
…	
haahjrhavujl	23
gzzgiqgzutik	24
fyyfhpfytshj	25

Tabel 1. Contoh Deskripsi Sandi Caesar.

Sumber : wikipedia.com

Dengan tabel diatas dapat terlihat bahwa n = 4, pesan tersebut menjadi ‘attack at once’. Maka kesimpulannya Sandi Caesar yang dipake adalah ketika n = 4.

3. SANDI VIGENERE

Sandi Vigenere adalah metode menyandikan teks alfabet dengan menggunakan deretan Sandi Caesar berdasarkan huruf-huruf pada kata kunci. Sandi Vigenere ini merupakan bentuk sederhana dari substitusi polialfabetik.

Sebagai contoh jika kata kunci adalah ‘PIZZA’ dan pesan yang ingin disampaikan adalah ‘Serbu Berlin’ maka pesan tersebut menjadi ‘Hmqau Qmqkic’.

3.1.Sejarah Sandi Vigenere

Sandi ini dijelaskan pertama kali oleh Giovan Batista Belaso dalam bukunya yang berjudul La cifra del. Sig. Giovan Batista Belaso(1553) . Lalu sandi ini disempurnakan oleh seorang diplomat Perancis, yang bernama Blaise de Vigenere(1586).

Pada abad ke-19, karena terlalu banyak orang beranggapan bahwa penemu sandi tersebut adalah Vigenere, maka sandi tesebut dinamakan Sandi Vigenere.

Pernah sandi ini mencapai kejayaan karena sandi ini sulit untuk dipecahkan dan hampir tidak bisa. Sehingga disebut *le chiffre indechiffrable* (Perancis : sandi yang tak terpecahkan).

3.2.Proses Penyandian Sandi Vigenere

Sandi Vigenere ini sebenarnya merupakan pengembangan dari Sandi Caesar. Untuk penyandiannya, digunakan sebuah tabel yang disebut tabel Vigenere. Tabel ini didapatkan dengan cara menuliskan alfabet dalam 26 baris, dengan baris yang satu mengandung geseran satu dari baris sebelumnya.

	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. Vigenere Tabel.

Sumber : wikipedia.com

Contoh tadi menyebutkan pesan ‘Serbu Berlin’ dengan kata kunci ‘PIZZA’ berubah menjadi ‘Hmqau Qmqkic’.

Sama halnya dengan Sandi Caesar, pasangkan huruf S dari serbuberlin dengan huruf P dari pizza sehingga didapat huruf H. Lakukan terus sampai huruf terakhir pada pesan.

Jika kata kuncinya sudah sampai huruf terakhir, maka mulai lagi dari huruf awalnya, begitu seterusnya. Contoh : pizzapizzap.

Secara matematis dapat dituliskan sbb :

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

C_i adalah huruf ke-i pada teks hasil penyandian.
P_i adalah huruf ke-i pada teks aslinya.
K_i adalah huruf ke-i dari kata kunci.

3.3.Memecahkan Sandi Vigenere

Karena sandi ini cukup rumit untuk dipecahkan, maka terdapat beberapa cara untuk memecahkannya.

Secara umum dapat ditulis sbb :

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

C_i adalah huruf ke-i pada teks hasil penyandian.
P_i adalah huruf ke-i pada teks aslinya.
K_i adalah huruf ke-i dari kata kunci.

3.3.1.Metode Kasiski

Pada tahun 1863, Friedrich Kasiski adalah orang pertama yang mempublikasikan keberhasilannya memecahkan Sandi Vigenere.

Metode ini awalnya menghitung panjang dari kata kunci yang dipakai. Bisa dilihat dalam Sandi *DYDUXRMH*TVDV*NQD*QNW*DYDUXRMH*ARTJGW*NQD*, jarak antara kedua ‘DYDUXRMH’ adalah 18 huruf. Dengan mengasumsikan bahwa kata kunci dan kata yang disandikan itu sama, maka didapat kemungkinan bahwa kata kunci yang digunakan mengandung 18, 9, 6, 3, atau 2

huruf panjangnya. Lalu, jarak antara kedua 'NQD' adalah 20 huruf. Dengan asumsi lagi, maka didapat kemungkinan bahwa kata kunci yang dipakai mengandung 20, 10, 5, 4, 2 huruf panjangnya. Sehingga irisan kedua himpunan tadi didapatkan panjang kata kunci yang dipakai adalah 2 huruf.

Disini kita mengecualikan keadaan bahwa kata kunci yang dipakai hanya mengandung 1 huruf, karena Sandi Vigenere dengan kata kunci hanya 1 huruf sangat mudah untuk dideskripsikan.

3.3.2.Metode Friedman

Metode ini sering disebut sebagai 'kappa test'. Ditemukan oleh William F. Friedman pada tahun 1920.

Metode ini menggunakan suatu indeks yang disebut 'indeks kebenaran'(index of coincidence) yang mencari persentase dari peluang panjangnya kata kunci.dengan indeks kebenaran ini, kita dapat mengetahui berapa panjang kata kuncinya. Setelah itu kita dapat menggunakan rumus

$$\chi = \sum_{i=1}^{c} n_i f_i$$

untuk mencari huruf per huruf dari kata kuncinya.

n_i menunjukkan frekuensi huruf dari suatu kolom huruf. f_i menunjukkan huruf relatif dalam bahasa Inggris(contoh).

Contoh Sandi : QPWKALVRXCQZIKGRBPFAOMFL
JMSDZVDHXCXJYEBIMTRQWNMEAIZRVKCVKVLXNEIC
FZPZCZZHKMLVZVZIZRRQWDKECHOSNYXXLSPMYKVQ
XJTDCIOMEEXDQVSRXLRLKZHOV

Size	Delta I.C.
1	1.12
2	1.19
3	1.05
4	1.17
5	1.82

Size	Delta I.C.
6	0.99
7	1.00
8	1.05
9	1.16
10	2.07

I.C. = Index of Coincidence

Tabel 2. Data Peluang pada Indeks Kebenaran

Sumber : wikipedia.com

Menurut data indeks kebenaran, dapat dilihat bahwa persentase panjangnya 10 paling besar. Tapi size = 5 juga mengandung nilai indeks yang cukup besar.

Lalu dengan rumus di atas, didapat kata kuncinya adalah 'EVERY'. Sehingga pesan tersebut berbunyi 'Must change meeting location from bridge to underpass since enemy agents are believed to have been assigned to watch bridge stop meeting time unchanged'.

Dalam metode ini juga ada peluang pesan tersebut dapat terdeskripsikan sebanyak

$$\frac{\kappa_p - \kappa_r}{\kappa_o - \kappa_r}$$

dengan

$$\kappa_o = \frac{\sum_{i=1}^{c} n_i(n_i - 1)}{N(N-1)}$$

dengan c = 26 yaitu banyaknya alfabet. n = banyaknya huruf.

Cara ini pun mirip dengan Kaskisi, yaitu pertama kali mencari banyaknya huruf pada kata kunci yang digunakan.

Selain kedua metode diatas, dapat dilakukan Analisis Frekuensi dan Eliminasi Kata Kunci. Syarat kedua cara tersebut adalah harus diketahui banyaknya huruf dalam kata kunci yang dipakai.

4. KESIMPULAN

Kesimpulan yang dapat diambil dari makalah ini adalah:

1. Dari salah satu bentuk Teori Bilangan yakni operasi modulo aritmatik, dapat dibuat suatu sandi yang begitu rumit dan sulit untuk di deskripsikan kembali.
2. Sandi Caesar yang sekarang sudah tidak berbobot lagi, dapat dikembangkan hingga menjadi suatu sandi yang lebih rumit
3. Pakailah Sandi Vigenere daripada memakai Sandi Caesar.

DAFTAR REFERENSI

[1] Munir, Rinaldi. "Diktat Kuliah IF2091 Struktur Diskrit", STEI, ITB, 2008.

[2] http://en.wikipedia.org/wiki/Vigenere_cipher#Cryptanalysis Minggu, 20 Desember 2009

[3] http://en.wikipedia.org/wiki/Caesar_cipher Minggu, 20 Desember 2009

[4] http://id.wikipedia.org/wiki/Kriptografi Minggu, 20 Desember 2009

[5] http://en.wikipedia.org/wiki/Index_of_coincidence Minggu, 20 Desember 2009