VIGOTIP SUBSTITUTION CIPHER

Alwi Alfiansyah Ramdan – 135 08 099

Program Studi Teknik Informatika
Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
e-mail: alfiansyah.ramdan@gmail.com

ABSTRAK

Makalah ini membahas tentang Vigotip Substitution Cipher, sebuah modifikasi Vigenere Cipher yang dikembangkan berdasarkan keuntungan yang ada pada Vigenere Cipher dan One Time Pad Cipher. Pada dasarnya, cipher ini memiliki dua jenis kunci. Kunci pertama adalah sebuah string pendek yang mudah diingat yang akan digunakan berulang sampai mencapai panjang karakter plainteks seperti pada Vigenere Cipher. Kunci kedua adalah sejumlah n bilangan yang mudah diingat, dapat berupa deret maupun barisan aritmatika atau pun yang lainnya, dan n merupakan bilangan yang menyesuaikan dengan panjang plainteks. Kunci kedua ini akan dikalikan dengan kunci pertama dan hasilnya akan ditambahkan pada plainteks dan di-modulus 26 seperti pada Caesar Cipher. Dengan demikian, pergeseran dari tiap karakter pada plainteks yang akan dienkripsi akan berbeda-beda dan sulit untuk dipecahkan.

Kata kunci: *Algoritma kriptografi klasik, Ceasar Cipher, Vigenere Cipher, One Time Pad Cipher, Vigotip Cipher*.

1. PENDAHULUAN

Pada zaman dahulu, untuk mengirimkan pesan kepada kawan dalam perang sangatlah penting. Keamanan pesan yang dikirim harus dapat terjaga dengan baik agar strategi yang akan diterapkan untuk melawan musuh tidak bocor ke tangan lawan.

Banyak sekali peperangan panjang yang selesai karena pesan yang ditujukan kepada kawan dalam perang tersebut bocor ke tangan lawan sehingga lawan mengetahui apa yang akan dilakukan oleh pihak kawan.

Banyak cara yang dapat dilakukan untuk menjaga keamanan dan keutuhan pesan yang dikirim pada pihak yang berhak menerimanya. Salah satunya adalah dengan menggunakan penyandian, dalam hal ini adalah enkripsi dan dekripsi terhadap pesan yang akan dikirimkan.

Proses enkripsi adalah proses yang mengubah pesan asli menjadi pesan yang tak dimengerti pada saat pengiriman dengan menggunakan sebuah kata kunci. Dan proses dekripsi adalah proses yang mengubah pesan yang tak dimengerti menjadi pesan asli yang bermakna dengan menggunakan kata kunci yang sama pada saat proses enkripsi dilakukan. Hal ini dilakukan agar walaupun pesan jatuh ke pihak lawan, pihak lawan tidak mengerti maksud dari pesan tersebut.

Algoritma untuk melakukan penyandian sudah ada sejak dulu. Ada yang menggunakan besar diameter kayu sebagai kunci untuk melakukan enkripsi dan dekripsi pesan. Pesan tersebut ditulis dalam sebuah pita yang digulung pada kayu tersebut. Untuk dapat membacanya kembali digunakan kayu dengan diameter yang sama.

Semakin berkembangnya peradaban, semakin berkembang pula algoritma yang digunakan untuk melakukan enkripsi dan dekripsi pesan. Algoritma yang digunakan untuk melakukan enkripsi dan dekripsi pesan pada masa sebelum enkripsi dan dekripsi dilakukan dengan menggunakan bantuan komputer disebut sebagai Algoritma Kriptografi Klasik.

Pada dasarnya, algoritma kriptografi klasik terdiri dari cipher substitusi dan cipher transposisi.

Salah satu contoh algoritma kriptografi klasik adalah Caesar Cipher. Pada cipher ini, setiap karakter pada pesan yang akan dikirim dengan karakter lain dalam susunan abjad secara berurutan sejauh n kali secara *wrapping* sehingga pesan teracak. Cipher ini digunakan oleh Julius Caesar untuk mengirim pesan kepada para gubernurnya. Cipher ini termasuk ke dalam cipher substitusi.

Contoh lainnya adalah Vigenere Cipher yang dikembangkan oleh Blaise de Vigenere pada abad ke-16. Cara kerja cipher ini adalah mengganti setiap karakter pada pesan yang akan dikirim dengan karakter penggantinya sesuai dengan kata kunci dan tabel bujur sangkar vigenere. Cipher ini juga termasuk ke dalam cipher substitusi.

Caesar Cipher dan Vigenere Cipher dapat dengan mudah dipecahkan. Begitu pula algoritma kriptografi klasik lainnya, mudah dipecahkan. Namun demikian, algoritma kriptografi klasik ini merupakan sumber pemahaman konsep dasar kriptografi. Dengan mengetahui kelemahan yang dimiliki algoritma kriptografi klasik, kita dapat membuat algoritma yang lebih aman lagi untuk diimplementasikan.

2. TEORI

2.1 Dasar Kriptografi

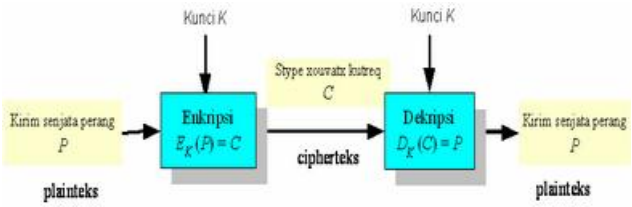
Pada kriptografi, dikenal adanya plainteks, cipherteks, dan kunci. Kunci K adalah parameter yang digunakan untuk transformasi pesan. Sebuah plainteks P akan diubah dengan menggunakan fungsi enkripsi E_k dengan parameter kunci K menghasilkan cipherteks C yang dapat didekripsi dengan menggunakan fungsi dekripsi D_k untuk kembali menjadi plainteks P. Secara umum dapat ditulis

$$E_k(P) = C \quad (1)$$

$$D_k(C) = P \quad (2)$$

Dan kedua fungsi itu memenuhi

$$D_k(E_k(P)) = P \quad (3)$$



Gambar 1. Skema enkripsi dan dekripsi dengan menggunakan parameter kunci

2.1.1 Aspek Keamanan pada Kriptografi

Berikut adalah aspek keamanan kriptografi:

1. Kerahasiaan (confidentiality), adalah layanan yang digunakan untuk menjaga isi pesan dari siapapun yang tidak berhak membacanya. Layanan ini direalisasikan dengan cara menyandikan pesan menjadi bentuk yang tidak dapat dimengerti. Misalnya pesan "Harap datang pukul 8" disandikan menjadi "TrxC#45motypetre!%".

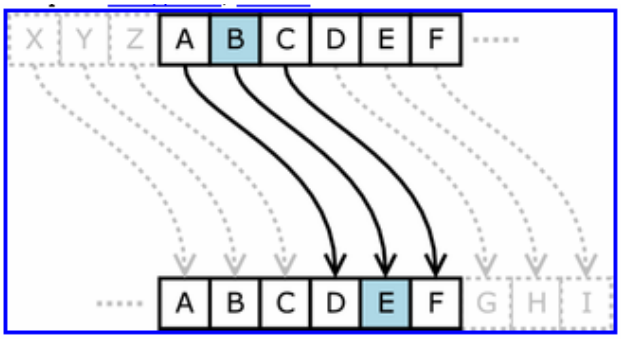
2. Integritas data (data integrity), adalah layanan yang menjamin bahwa pesan masih asli / utuh atau belum pernah dimanipulasi selama pengiriman. Layanan ini direalisasikan dengan menggunakan tanda-tanda digital (digital signature). Pesan yang telah ditandatangani menyiratkan bahwa pesan yang dikirim adalah asli.

3. Otentifikasi (authenification), adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (user authentification atau entity authentification) maupun mengidentifikasi kebenaran sumber pesan (data origin authentification). Layanan ini direalisasikan dengan menggunakan digital signature.

4. Nirpenyangkalan (non-repudiation), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.2 Caesar Cipher

Pada Caesar Cipher, susunan huruf cipherteks diperoleh dengan menggeser huruf-huruf alfabet. Proses enkripsi dan dekripsinya mensubstitusi satu karakter dengan karakter lain pada susunan alfabet secara berurutan dan pergeserannya pun sama untuk semua karakter dalam alfabet. Misalnya suatu string digeser sebanyak 3 karakter. Maka karakter pertama menjadi 3 karakter dibawahnya, karakter kedua juga sama dan seterusnya, sampai semua string terenkripsi semuanya.



Gambar 2. Proses transformasi pada enkripsi Caesar Cipher

Plaintext letter	A	B	C	D	.....	W	X	Y	Z
Ciphertext letter	D	E	F	G	.....	Z	A	B	C

Gambar 3. Tabel substitusi Caesar Cipher

Untuk mempermudah dalam transformasi, tiap karaketer dipasangkan dengan nilai integer 0 sampai 25. Lihat gambar di bawah ini.

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

Gambar 4. Tabel kode alfabet

Sehingga, secara matematis, Caesar Cipher dapat ditulis:

$$c_i = E(p_i) = (p_i + k) \bmod n \quad (4)$$

$$p_i = D(c_i) = (c_i - k) \bmod n \quad (5)$$

dimana,

p_i : plainteks ke-i
c_i : cipherteks ke-i
k : kunci
n : banyaknya range karakter yang digunakan.

Enkripsi dan dekripsi untuk huruf alfabet saja, nilai n adalah 26, sedangkan untuk enkripsi dan dekripsi untuk semua karakter ASCII, nilai n adalah 256.

2.2 Vigenere Cipher

Pada umumnya, dalam Vigenere Cipher plainteks dan cipherteks direpresentasikan dalam bentuk

$$P = p_1p_2p_3....p_{m-1}p_m.....p_N \quad (6)$$
$$C = c_1c_2c_3....c_{m-1}c_m.....c_N \quad (7)$$

Dan K adalah kunci dengan panjang m, yaitu

$$K = k_1k_2...k_m \quad (8)$$

Untuk $1 \leq i \leq N$, $1 \leq j \leq m$ dan panjang n adalah jumlah alfabet yang digunakan, maka berlaku hubungan

$$c_i = (p_i + k_{(i \bmod j)}) \bmod n \quad (9)$$

2.3 One Time Pad Cipher

One Time Pad cipher adalah salah satu algoritma kriptografi yang tidak terpecahkan. One Time Pad (OTP) ditemukan pada tahu 1917 oleh Major Joseph Mauborgone. Cipher ini termasuk algoritma kriptografi kunci simetri.

One Time Pad merupakan algoritma kriptografi yang memiliki kunci berupa deretan-deretan karakter yang dibangkitkan secara acak. Kunci pada OTP hanya digunakan sekali saja untuk mengenkripsi pesan yang kemudian dipakai lagi untuk mendekripsi pesan itu. Setelah selesai maka kunci tersebut dihancurkan.

Aturan enkripsi OTP sama seperti pada cipher substitusi berabjad majemuk, yaitu untuk proses enkripsi :

$$c_i = (p_i + k_i) \bmod 26 \quad (10)$$
$$p_i = (c_i - k_i) \bmod 26 \quad (11)$$

Contoh :
Plainteks : ONETIMEPAD
Kunci : TBFRGFARFM
Nyatakan A = 0 , B = 1, ..., z = 25 maka
Cipherteks : HOJKOREGHP

Sistem OTP tidak dapat dipecahkan karena:

1. Barisan kunci acak yang ditambahkan ke pesan plainteks yang tidak acak menghasilkan cipherteks yang seluruhnya acak.
2. Beberapa barisan kunci yang digunakan untuk mendekripsikan cipherteks mungkin menghasilkan pesan-pesan plainteks yang mempunyai makna, sehingga kriptanalis tidak punya cara untuk menentukan plainteks mana yang benar.

Contoh :

Cipherteks HOJKOREGHP, misal kriptanalis mencoba kunci LMCCAWAAZD maka akan menghasilkan plainteks SALMONEGGS, kemudian kriptanalis juga mencoba kunci ZDVUZOEYEO maka akan menghasilkan plainteks GREENFIELD.

Kedua plainteks itu mempunyai makna, sehingga membingungkan kriptanalis

Meskipun OTP pada teori merupakan cipher yang tidak dapat dipecahkan, tetapi pada prakteknya cipher ini jarang dipakai karena masalah kepraktisan. Kunci OTP sangat panjang sehingga sulit dalam penyampaian, selain itu juga karena panjang kunci tersebut maka pengirim dan penerima tidak mungkin membangkitkan kunci secara simultan sehingga dalam transfer informasinya membutuhkan waktu yang lama.

3. VIGOTIP CIPHER

3.1 Latar Belakang

Algoritma klasik khususnya algoritma substitusi memiliki kekurangan dalam segi keamanan. Algoritma substitusi mudah untuk diserang. Sebagai contoh algoritma substitusi Caesar Cipher yang sangat mudah diserang dengan *ciphertext only attack*, yaitu dengan melihat cipherteksnya kemudian dengan analisis frekuensi sehingga dengan mudah dapat ditemukan kuncinya. Selain itu juga mudah diserang dengan *exhaustive search*, karena hanya memiliki sedikit kemungkinan kunci.

Selain Caesar Cipher algoritma substitusi abjad tunggal pun dapat diserang dengan teknik analisis frekuensi. Untuk cipher substitusi lainnya seperti cipher substitusi homofonik memang lebih baik dari pada cipher substitusi abjad tunggal, karena teknik analisis frekuensi tidak dapat lagi digunakan, hal itu disebabkan tidak ada lagi keterkaitan antara frekuensi pada plainteks dan cipherteks. Namun cipher substitusi homofonik ini juga dapat dipecahkan dengan serangan *known-plainteks attack*, yaitu dengan menerka pada kata-kata yang umum dipakai. Misal string ”dengan hormat” pada awal kalimat surat resmi.

Untuk algoritma cipher abjad majemuk yang merupakan sejumlah substitusi abjad tunggal yang dibuat dengan kunci yang berbeda memang lebih aman. Tetapi keberadaan kunci yang berulang-ulang menyebabkan cipherteks hasil enkripsinya juga terdapat pengulangan-pengulangan karakter. Contoh terkenal dari substitusi abjad majemuk adalah Vigenere Cipher. Vigenere Cipher memang mengatasi serangan dengan teknik analisis frekuensi dan *known-plainteks* karena setiap huruf yang sama dapat dienkripsikan menjadi huruf yang berbeda. Tetapi jika panjang kunci sudah diketahui dan tidak terlalu

panjang maka dengan *exhaustive search* pencarian kunci dapat dilakukan.

One Time Pad merupakan algoritma klasik yang tidak dapat dipecahkan. Hal itu dikarenakan panjang kunci enkripsi memiliki panjang sama dengan jumlah karakter yang akan dienkripsikan. One Time Pad memiliki kelemahan panjang kunci yang terlalu panjang, tetapi selain kelemahan hal itu juga merupakan kelebihannya. Kelemahan dari One Time Pad ini menyebabkan One Time Pad sulit untuk didistribusikan.

Dengan melihat keterangan-keterangan di atas, maka perlu adanya pengembangan algoritma kriptografi klasik baru yang merupakan hasil modifikasi algoritma klasik yang sudah ada yang memiliki kunci enkripsi yang panjangnya sama dengan jumlah karakter pada plain teks, tetapi mudah diingat dan didistribusikan.

Vigotip Cipher lahir dari latar belakang tersebut. Nama Vigotip diambil dari kata Vigenere-One Time Pad sebab cipher ini adalah modifikasi Vigenere Cipher dan One Time Pad Cipher.

3.2 Algoritma Vigotip Cipher

Algoritma Vigotip Cipher merupakan algoritma yang dibuat dengan tujuan mengurangi kelemahan yang dimiliki oleh algoritma kriptografi klasik. Algotirma ini dikembangkan dengan Vigenere Cipher sebagai dasarnya. Ide awal pembuatan cipher ini adalah kehebatan One Time Pad Cipher yang tak bisa dipecahkan.

Mirip seperti pada One Time Pad Cipher,yang kuncinya dibangkitkan secara random dan panjang kunci sama dengan panjang plainteks yang akan dienkripsi, kunci pada Vigotip Cipher juga memiliki panjang yang sama dengan panjang plain teks namun tidak dibangkitkan secara random tetapi secara otomatis dan cipherteks yang satu saling berhubungan dengan proses yang dialami cipherteks yang lainnya.

Algoritma Vigotip Cipher ini menggunakan cara yang sama dengan Vigenere Cipher dalam hal substitusi abjad antara plainteks dan cipherteks. Persamaan cara ini terletak pada adanya kunci pendek yang mudah diingat dan dalam penggunaannya akan diulang sampai mencapai panjang plainteks. Algoritma ini lebih baik daripada Vigenere Cipher karena selain menggunakan kunci berupa string untuk melakukan substitusi, akan ada kunci lain berupa n buah bilangan yang akan dikalikan dengan kunci pertama yang berupa string, dan n adalah panjang plainteks. Sebanyak n buah bilangan ini, dapat berupa n buah angka yang sama, deret bilangan aritmatika, barisan bilangan aritmatika, deret bilangan ganjil ataupun genap, deret bilangan fibbonaci, maupun deret bilangan yang dibuat senfiri dengan suatu aturan tertentu.

Pada Algoritma Vigotip Cipher, kunci pertama yang berupa string dapat diasosiasikan dengan angka dari 1 sampai 26 untuk tiap karakternya (dari A sampai Z), seperti pada Caesar Cipher.

Secara garis besar, fungsi proses enkripsi pada Vigotip Cipher ini untuk 26 karakter adalah sebagai berikut:

$$C_i = E_i(P_i) = \begin{cases} (E_{i-1}(P_i) + R_i * K_{i \bmod j}) \bmod 26, & i > 0, \\ (P_i + R_0 * K_0) \bmod 26, & i = 0 \end{cases} \quad (12)$$

dan fungsi proses dekripsinya adalah sebagai berikut:

$$P_i = D_i(C_i) = \begin{cases} D_{i-1}(C_i - R_i * K_{i \bmod j}) \bmod 26, & i > 0 \\ (C_i - R_0 * K_0) \bmod 26, & i = 0 \end{cases} \quad (13)$$

dimana

P_a : karakter plainteks ke-a
C_a : karakter cipherteks ke-a
E_a : fungsi enkripsi ke-a
D_a : fungsi dekripsi ke-a
R_a : bilangan kunci pengali ke-a
K_a : karakter kunci string ke-a
i : indeks yang menyatakan posisi ke-i pada plainteks maupun cipherteks
j : indeks yang menyatakan posisi ke-j pada kunci string

Misal sebuah plainteks berisi VIGOTIP, dan kunci yang digunakan adalah string "kunci" dan deret bilangan asli.

Maka cipherteks didapat dari:

$C_0 = E_0(P_0) = (22 + 1 * 11) \bmod 26 = 7$ (G)

$E_0(P_1) = (9 + 1 * 11) \bmod 26 = 20$ (T)
$C_1 = E_1(P_1) = (20 + 2 * 21) \bmod 26 = 10$ (J)

$E_0(P_2) = (7 + 1 * 11) \bmod 26 = 18$ (R)
$E_1(P_2) = (18 + 2 * 21) \bmod 26 = 8$ (H)
$C_2 = E_2(P_2) = (8 + 3 * 14) \bmod 26 = 24$ (X)

dan seterusnya sampai ditemukan cipherteks GJXRPSQ, dimana

R = {1,2,3,4,5,6.....};
K = {'K','U','N','C','I'} ≡ {11,21,14,3,9 };
j = |K| = 5;

i	Key		Pi						
	Ri	K(i mod j)	V	I	G	O	T	I	P
			Ei(P0)	Ei(P1)	Ei(P2)	Ei(P3)	Ei(P4)	Ei(P5)	Ei(P6)
0	1	K	G	T	R	Z	E	T	A
1	2	U	-	J	H	P	U	J	Q
2	3	N	-	-	X	F	K	Z	G
3	4	C	-	-	-	R	W	L	S
4	5	I	-	-	-	-	P	E	L
5	6	K	-	-	-	-	-	S	Z
6	7	U	-	-	-	-	-	-	Q
Ci			G	J	X	R	P	S	Q

Gambar 5. Contoh tabel proses enkripsi

Dengan demikian, cipherteks untuk VIGOTIP adalah GJXRPSQ.

Mari kita coba dengan plainteks yang lebih sederhana, yaitu ABCD dengan kunci yang sama.

$C_0 = E_0(P_0) = (1 + 1 * 11) \bmod 26 = 12$ (L)

$E_0(P_1) = (2 + 1 * 11) \bmod 26 = 13$ (M)
$C_1 = E_1(P_1) = (13 + 2 * 21) \bmod 26 = 3$ (C)

$E_0(P_2) = (3 + 1 * 11) \bmod 26 = 14$ (N)
$E_1(P_2) = (14 + 2 * 21) \bmod 26 = 4$ (D)
$C_2 = E_2(P_2) = (4 + 3 * 14) \bmod 26 = 20$ (T)

$E_0(P_3) = (4 + 1 * 11) \bmod 26 = 15$ (O)
$E_1(P_3) = (15 + 2 * 21) \bmod 26 = 5$ (E)
$E_2(P_3) = (5 + 3 * 14) \bmod 26 = 21$ (U)
$C_3 = E_3(P_3) = (21 + 4 * 3) \bmod 26 = 7$ (G)

Sehingga cipherteks yang dihasilkan dari plainteks ABCD adalah LCTG. Dari sini, kriptanalis tidak bisa menentukan hubungan antara plainteks dengan cipherteks.

Kita coba lagi dengan plainteks yang lebih mudah, yaitu AAAA dengan kunci yang sama.

$C_0 = E_0(P_0) = (1 + 1 * 11) \bmod 26 = 12$ (L)

$E_0(P_1) = (1 + 1 * 11) \bmod 26 = 12$ (L)
$C_1 = E_1(P_1) = (12 + 2 * 21) \bmod 26 = 2$ (B)

$E_0(P_2) = (1 + 1 * 11) \bmod 26 = 12$ (L)
$E_1(P_2) = (12 + 2 * 21) \bmod 26 = 2$ (B)
$C_2 = E_2(P_2) = (2 + 3 * 14) \bmod 26 = 18$ (R)

$E_0(P_3) = (1 + 1 * 11) \bmod 26 = 12$ (L)
$E_1(P_3) = (12 + 2 * 21) \bmod 26 = 2$ (B)
$E_2(P_3) = (2 + 3 * 14) \bmod 26 = 18$ (R)
$C_3 = E_3(P_3) = (18 + 4 * 3) \bmod 26 = 4$ (D)

Sehingga cipherteks yang dihasilkan dari plainteks AAAA adalah LBRD. Dari sini, kriptanalis mulai mendapatkan petunjuk. Keita lihat

E0(A) = L E0(A) = L
memiliki selisih 0 karakter
(perbedaan karakter A dan A)

E1(A) = B E1(B) = C
memiliki selisih 1 karakter
(perbedaan karakter A dan B)

E2(A) = R E2(C) = T
memiliki selisih 2 karakter
(perbedaan karakter A dan C)

E3(A) = D E3(D) = G
memiliki selisih 3 karakter
(perbedaan karakter A dan D)

Jika demikian, algoritma ini dapat diserang dengan menggunakan teknik *Chosen Plaintext Attack*. Hal ini dapat dicegah dengan jalan mengganti kunci setiap selesai melakukan enkripsi dan dekripsi, sehingga setiap proses enkripsi dan dekripsi pada kesempatan berbeda memiliki kunci yang berbeda-beda pula. Hal ini diadopsi dari karakteristik One Time Pad Cipher.

3.3 Kekuatan Algoritma Vigotip Cipher

Algoritma Vigotip Cipher adalah algoritma kunci simetri dan termasuk ke dalam algoritma substitusi abjad majemuk. Algoritma ini memperhatikan prinsip *confusion* dan *diffusion*, pemilihan kunci yang acak yang menyebabkan cipherleks juga acak, panjang kunci yang sama dengan panjang plainteks seperti pada One Time Pad. Secara garis besar, proses yang terjadi pada saat enkripsi dan dekripsi dalam algoritma ini sama dengan proses enkripsi dan dekripsi pada Vigenere Cipher, namun ditambah sedikit modifikasi.

Secara lebih dalam, poin-poin berikut akan menguraikan kekuatan Algoritma Vigotip Cipher.

1. Menggunakan prinsip *confusion* dan *diffusion*.
   Prinsip *confusion* menyatakan bahwa kriptanalis akan kebingungan dalam melakukan serangan terhadap suatu algoritma kriptografi jika antara plainteks dan cipherteks tidak memiliki hubungan yang jelas. Algoritma Vigotip Cipher ini sudah jelas memperhatikan prinsip *confusion* ini karena cipherteks "terlihat" tidak ada kaitan dengan plainteks. Pada contoh di atas, plainteks VIGOTIP di enkripsi menjadi cipherteks GJXRPSQ. Dapat dilihat, bahwa antara plainteks dan cipherteks tidak terlihat adanya suatu hubungan, termasuk tidak terlihatnya adanya kesempatan dalam menggunakan frekuensi kemunculan huruf untuk menebak pemetaan plainteks terhadap cipherteks. Prinsip *diffusion* menyatakan bahwa proses enkripsi dan dekripsi yangsaling berhubungan tiap tahapnya dan dilakukan secara berulang akan sangat menyulitkan kriptanalis dalam melakukan serangan. Pada Algoritma Vigotip Cipher, proses enkripsi pada tahap ke-i bergantung pada porses enkripsi tahap ke-(i-1), begitu juga dalam proses dekripsi dimana proses dekripsi pada tahap ke-i bergantung pada proses dekripsi pada tahap ke-(i-1). Hal inilah yang menyebabkan jika terjadi kesalahan pada cipherteks atau ada cipherteks yang

diganti, maka proses dekripsi selanjutnya akan tidak beres dan mengalami gangguan/kekacauan.

2. Kunci dapat dibangkitkan secara acak menyebabkan cipherteks yang juga acak.
   Pada Algoritma Vigotip Cipher, terdapat sebuah kunci yang merupakan deret bilangan yang dapat berupa deret bilangan asli, bilangan bulat, deret bilangan prima, deret bilangan fibbonaci, deret biangan yang dibangkitkan dengan pola tertentu dan lainnya sesuai keinginan. Namun, deret bilangan ini tidak bisa bekerja sendiri. Ada sebuah kunci yang bertipe string pendek yang mudah diingat yang setiap karakterny akan menjadi faktor pengali untuk kunci bertipe deret bilangan sesuai dengan posisinya.
   Perkalina antara kunci deret bilangan dengan kunci string akan menghasilkan kunci utama yang nilainya acak, sehingga akan menghasilkan cipherteks yang acak pula.
3. Panjang kunci utama sama dengan panjang plainteks yang akan dienkripsi.
   Pada Algoritma Vigotip Cipher, terdapat dua buah kunci yang akan diproses untuk melakukan enkripsi dan dekripsi. Yang pertama dan yang akan kita soroti adalah kunci deret bilangan yang panjangnya dapat menyesuaikan dengan panjang palinteksnya. Yang kedua adalah kunci string yang akan digunakan secara berulang seperti pada Vigenere Cipher. Karena kunci utama adalah hasil kali antara kedua kunci tersebut, maka sudah dapat dipastikan bahwa panjang kunci utama yang merupakan hasil perkaliannya akan memiliki panjang yang sama dengan panjang plainteks.

Poin-poin tersebut di atas akan berpengaruh terhadap serangan yang mungkin dapat dilakukan kriptanalis untuk memecahkan cipher. Berikut penjelasannya.

1. *Ciphertext-only attack* dengan menggunakan analisis frekuensi tidak berlaku terhadap Algoritma Vigotip Cipher.
   Hasil dari Algoritma Vigotip Cipher tidak memiliki hubungan yang terlihat dan tidak memiliki frekuensi huruf yang bersesuaian seperti pada plainteks. Sehingga analisis frekuensi hanya akan membuang-buang waktu saja.
2. *Known-plaintext attack* tidak berguna.
   Hal ini terjadi karena keterkaitan antara karakter-karakter yang ada pada plainteks dengan karakter-karakter pada cipherteks yang bersesuaian sama sekali tidak terlihat.
3. Segala bentuk serangan *chosen-plaintext* dan *chosen-ciphertext attack* tidak dapat digunakan.
   Hal ini dapat dipastikan karena penggunaan kunci string dan kunci deret bilangan yang acak dan hanya digunakan sekali untuk masing-masing proses enkripsi dan dekripsi seperti pada One Time Pad Cipher. Ketika proses enkripsi dan dekripsi selsai dilakukan, maka kunci akan diganti lagi sesuai keinginan pengguna.

Selain itu, poin-poin sebelumnya juga berpengaruh terhada beberapa hal lain. Beikut penjelasannya.

1. Kunci utama hasil perkalian antara kunci string dengan kunci deret bilangan memiliki panjang yang sama dengan panjang plainteks.
   Karakteristik ini memang sengaja diambil dari One Time Pad Cipher dengan tujuan dengan panjang kunci yang sama dengan panjang plainteksnya, Vigotip Cipher menjadi salah satu cipher yang *unbreakable* seperti One time Pad Cipher.
2. Distribusi kunci lebih mudah dilakukan.
   Dibangingkan dengan One Time Pad Cipher, pendistribusian kunci akan lebih mudah dilakukan dengan Vigotip Cipher. Alasannya, untuk mendistribusikan kunci yang panjangnya sama dengan panjang plainteks dan memiliki pola yang dibangkitkan secara acak seperti pada One Time Pad Cipher pada kenyataannya sangat sulit dan membutuhkan biaya yang sangat mahal. Dengan Algoritma Vigotip Cipher, pendistribusian kunci akan sama dengan pendistribusian kunci pada Vigenere Cipher maupun cipher substitusi sederhana lainnya karena hanya terdiri dari kunci string pendek yang mudah diingat dan deretan bilangan. Untuk pendistribusian kunci deret bilangan, yang perlu didistribusikan hanyalah pola atau kata kunci yang menggambarkan kunci deret bilangan tersebut tanpa harus mengirim keseluruhan kunci deret bilangan.

3.4 Kekurangan Algoritma Vigotip Cipher

Walaupun secara teori dikatakan Algoritma Vigotip Cipher lebih bagus daripada OTP Cipher dan Vigenere Cipher, kekurangan selalu ada. Beberapa kekurangan diantaranya dijelaskan di bawah ini.

1. Proses enkripsi pada Algoritma Vigotip Vipher dilakukan secara berantai, sehingga cipherteks harus dijaga keasliannya, karena ketia ada cipherteks yang berubah, hasil dekripsi akan menjadikan plainteksnya tidak bermakna.
2. Kompleksitas waktu lebih besar daripada One Time Pad Cipher dan Vigenere Cipher.
   Untuk dapat mengetahui kompleksitas waktu asimptotiknya, perhatikan perhutngan berikut ini.

   Untuk setiap karakter ke-i pada plainteks, jumlah operasinya adalah:

untuk i = 0, 2 operasi (operasi perkalian dan penjumlahan)
untuk i = 1, 2 + 1 operasi
untuk i = 2, 2 + 1 + 1 operasi
untuk i = 3, 2 + 1 + 1 + 1 operasi
.
.
.

Jadi untuk n buah arakter pada plainteks, kompleksitas waktu algoritma ini adalah

$$T(n) = \begin{cases} T(n-1) + n + a, & n > 0 \\ a, & n = 0 \end{cases}$$

Maka kompleksitas waktu asimptotiknya adalah

$T(n) = T(n - 1) + n + a$
$= T(n - 2) + n + a + n + a$
$= T(n - 2) + 2n + 2a$
$= T(n - 3) + n + a + 2n + 2a$
$= T(n - 3) + 3n + 3a$
.
.
.
$= T(n – (n – 1)) + n + a + (n - 2)n + (n - 2)a$
$= T(n – (n – 1)) + (n – 1)\, n + (n – 1)a$
$= T(n - n) + n + a + (n – 1)n + (n – 1)a$
$= T(0) + n^2 + an$
$= a + n^2 + an$
$T(n) = n^2 + an + a$

Sehingga didapat $T(n) = O(n^2)$

Terlihat bahwa kompleksitas waktu asimptotiknya lebih besar dari pada kompleksitas waktu asimptotik Vigenere Cipher dan One Time Pad Cipher yang *O(n)*. Namun demikian, kompleksitas waktu asimptotiknya masih dalam orde linear.

4. KESIMPULAN

Kesimpulan yang dapat diambil antara lain:

1. Vigotip Cipher adalah algoritma kriptografi substitusi yang pada dasarnya memiliki cara kerja yang sama dengan Vigenere Cipher dalam melakukan proses substitusi dan mengambil karakteristik panjang kunci sama dengan panjang plainteks pada One Time Pad Cipher.
2. Vigotip Cipher memiliki tingkat keamanan yang lebih baik daripada Vigenere Cipher. Vigotip Cipher tahan dengan serangan *Ciphertext-Only Attack*, *Known-Plaintext Attack*, dan segala bentuk *Chosen-Plaintext Attack* dan *Chosen-Ciphertext Attack*.
3. Vigotip Cipher memiliki panjang kunci yang sama dengan panjang plainteks yang diambil dari karakteristik pada One Time Pad Cipher namun lebih praktis karena meskipun kunci utama dibangkitkan secara acak, kunci string dan kunci deret bilangan yang merupakan asal kunci utama mudah diingat oleh pengguna.
4. Vigotip Cipher memiliki kompleksitas waktu asimptotik lebih besar dari pada Vigenere Cipher maupun One Time Pad Cipher karena proses substitusi dilakukan berulang dan mempengaruhi proses substitusi yang lainnya.

REFERENSI

[1] Rinaldi Munir, "Diktat Kuliah IF3058, Kriptografi", Program Studi Teknik Informatika, STEI ITB, 2006.
[2] Substitutuin Cipher, Wikipedia – The Free Encyclopedia, http://en.wikipedia.org/wiki/Substitution_cipher, 2011. Tanggal akses: 12 Maret 2011, pukul 20.00 WIB.
[3] Vigenere Cipher, Wikipedia – The Free Encyclopedia, http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher, 2011. Tanggal akses: 12 Maret 2011, pukul 20.00 WIB.
[4] One-Time Pad Cipher, Wikipedia – The Free Encyclopedia, http://en.wikipedia.org/wiki/One-time_pad, 2011. Tanggal akses: 12 Maret 2011, pukul 20.00 WIB.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 13 Maret 2011

Alwi Alfiansyah Ramdan
135 08 099