Enskripsi Chiperteks Lord Bacon's Biliteral Alphabets Menggunakan Pohon

Krisna Fathurahman/13511006
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13511006@std.stei.itb.ac.id

Lord Bacon's Biliteral Alphabets merupakan salah satu teknik enskripsi plaintext yang terkenal dalam Kriptografi selain Caesar's Chiper dan Skema Shamir's and Blakley's. Dengan menggunakan konsep pohon, chipertext yang menggunakan enskripsi Lord Bacon's Biliteral Alphabet dapat dideskripsikan dengan lebih mudah. Metode-metode yang berkaitan dengan prinsip pohon mampu merepresentasikan proses enskripsi dengan lebih mudah.

Indeks : Lord Bacon's Biliteral Alphabets, kriptografi, pohon, enskripsi.

I. PENDAHULUAN

Kriptografi adalah ilmu yang mempelajari tentang keamanan informasi seperti kerahasiaan, integritas data, mendeteksi kepemilikan dan asal dimana data itu berasal dengan cara menyamarkannya menjadi suatu tampilan yang tak bermakna.

Dalam dunia kriptografi terdapat banyak sekali metode enskripsi yang terkenal, seperti : Caesar's Chiper, Skema Shamir's and Blakley's, Tritheme(Tri-Numeral Alphabets), dan Lord Bacon's Biliteral Alphabets. Beberapa metode di atas termasuk yang mudah untuk dienskripsi plaintext-nya untuk menjadi ciphertext yang tak berarti.

Pada kesempatan kali ini, saya akan memperkenalkan salah satu metode kriptografi tersebut dan mempelajari bagaimana proses enskripsi dipermudah dengan menggunakan prinsip pohon.

II. LANDASAN TEORI

2.1 Kriptografi

Kriptografi adalah ilmu yang mempelajari tentang keamanan informasi seperti kerahasiaan, integritas data, mendeteksi kepemilikan dan asal dimana data itu berasal. Kriptografi tidak hanya bertujuan untuk sekedar keamanan informasi. Tujuan dari kriptografi antara lain adalah sebagai berikut :

- Kerahasiaan, menjaga agar informasi tersebut tetap berada pada pihak yang memiliki dan/atau yang dapat dipercaya
- Integritas Data, membantu mendeteksi kebenaran dari informasi yang didapat begitu saja dari manapun agar tetap memiliki maksud informasi yang sebenarnya(tidak ada manipulasi)
- Kepemilikan, sangat berhubungan dengan identifikasi. Mendeteksi pemilik dari informasi tersebut dan/atau orang yang dituju oleh informasi itu. Menghindari atau membantu mengetahui jika ada pihak ketiga yang akan atau telah merubah isi atau makna dari informasi tersebut
- Non-repudiasi, mencegah penyangkalan dari suatu informasi yang telah diciptakan oleh suatu pihak karena hal ini berhubungan dengan hak cipta dan *signature*(ciri khas)[1]

2.1.1 Sejarah Kriptografi

Kriptografi sudah berkembang sejak 4000 tahun yang lalu, tepatnya di Mesir yaitu berupaHieroglyph. Teknik penyembunyian pesan pada zaman dahulu kebanyakan menggunakan metode enskripsi dengan pensil dan kertas saja, metode sederhana tersebut disebut kriptografi klasik. Sejarah kriptografi zaman dahulu pun menyinggung tentang *Scytale*, merupakan penyandian dengan menggunakan daun papyrus yang dililitkan pada batang pohon yang merpunyai diameter tertentu.

Gambar 2-1 Scytale[7]

Pesan(Plainteks) ditulis secara horisontal pada daun papyrus, selanjutnya setelah daun dilepas, maka yang akan terlihat pada daun papyrus yang panjang itu hanyalah rangkaian huruf yang tak berarti(Chiperteks).

Scytale ini dulu digunakan oleh tentara Sparta di Yunani.[6]

2.2 Lord Bacon's Biliteral Alphabets

Lord Bacon's Biliteral Alphabets ditemukan oleh seorang ilmuwan bernama Francis Bacon pada abad pertengahan. Pada saat itu di Eropa, para sastrawan dan ilmuwan bergerak secara sembunyi-sembunyi dari pihak gereja yang menentang kegiatan para sastrawan dan ilmuwan karena dianggap berlawanan dengan asas dan sudut pandang gereja. Maka banyak sekali metode steganografi yang berkembang pada saat itu untuk berkomunikasi satu sama lain.[4]

Gambar 2-2 Sir Francis Bacon [5]

Lord Bacon's Biliteral Alphabets atau biasa disebut Bacon's Chiper adalah salah satu kriptogram yang terkenal dalam dunia kriptografi. Bacon's Chiper menggunakan alfabet 'a' dan 'b' sebagai pengganti dari alfabet yang kita kenal (26 buah). Tiap 1 alfabet digantikan dengan 5 alfabet yang terdiri dari 'a' dan 'b'.[2]

BACON'S BI-LITERAL ALPHABET

A	aaaaa	IJ	abaaa	R	baaaa
B	aaaab	K	abaab	S	baaab
C	aaaba	L	ababa	T	baaba
D	aaabb	M	ababb	UV	baabb
E	aabaa	N	abbaa	W	babaa
F	aabab	O	abbab	X	babab
G	aabba	P	abbba	Y	babba
H	aabbb	Q	abbbb	Z	babbb

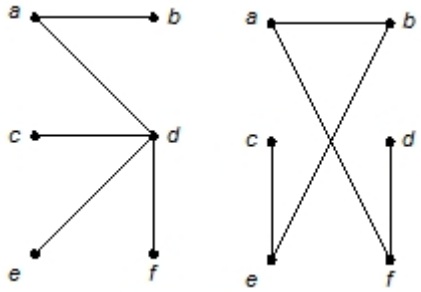
Gambar 2-3 Bacon's Biliteral Alphabets[2]

Hal ini juga telah dikenal lama dalam dunia sastra kuno. Karena Bacon's Chiper dikenal pula bersama dengan karya Shakespeare dalam hal Literal Chiper.[3]

Pada gambar 2-3, huruf I dan J memiliki chiper yang sama karena mengikuti penulisan kuno pada eropa zaman itu. Seperti halnya yang sama pada huruf U dan V. Kemungkinan mengikuti penulisan bahasa Spanyol.

2.3 Pohon

Pohon adalah graf tak berarah terhubung yang tidak mengandung sirkuit.[8]



Gambar 2-4 Pohon[8]

2.3.1 Sifat-sifat Pohon

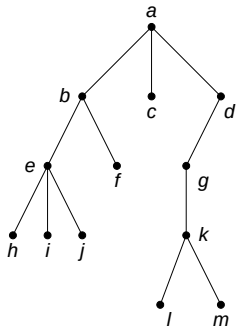
Teorema :

Misalkan G = (V, E) adalah graf tak-berarah sederhana dan jumlah simpulnya *n*. Maka, semua pernyataan di bawah ini adalah ekivalen :

1. G adalah pohon.
2. Setiap pasang simpul di dalam G terhubung dengan lintasan tunggal.
3. G terhubung dan memiliki $m = n - 1$ buah sisi.
4. G tidak mengandung sirkuit dan memiliki $m = n - 1$ buah sisi.
5. G tidak mengandung sirkuit dan penambahan satu sisi pada graf akan membuat hanya satu sirkuit.
6. G terhubung dan semua sisinya adalah jembatan.

Teorema di atas dapat dikatakan sebagai definisi lain dari pohon. [8]

2.3.2 Pohon berakar



Pohon yang satu buah simpulnya diperlakukan sebagai akar dan sisi-sisinya diberi arah sehingga menjadi graf berarah dinamakan pohon berakar (*rooted tree*).[8]

2.3.2.1 Terminologi pada Pohon Berakar

Anak (*child* atau *children*) dan Orangtua (*parent*). *b,c*, dan *d* adalah anak-anak simpul *a*, *a* adalah orangtua dari anak-anak itu. Lintasan dari *a* ke *j* adalah *a,b,e,j*. Panjang lintasan dari *a* ke *j* adalah 3. *f* adalah saudara kandung *e*, tetapi *g* bukan saudara kandung *e*, karena orangtua mereka berbeda. Derajat sebuah simpul adalah jumlah upapohon (atau jumlah anak) pada simpul tersebut. Derajat *a* adalah 3, derajat *b* adalah 2, derajat *d* adalah satu dan derajat *c* adalah 0. Jadi, derajat yang dimaksudkan di sini adalah derajat-keluar. Derajat maksimum dari semua simpul

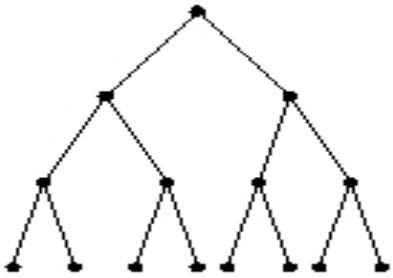
merupakan derajat pohon itu sendiri. Simpul yang berderajat nol (atau tidak mempunyai anak) disebut daun. Simpul *h, i, j, f, c, l,* dan *m* adalah daun. Simpul yang mempunyai anak disebut simpul dalam. Simpul *b, d, e, g,* dan *k* adalah simpul dalam. Pohon di atas memiliki 4 tingkat(*level*) {0,1,2,3,4}. Tingkat meksimum dari suatu pohon disebut tinggi atau kedalaman pohon tersebut. Pohon ini mempunyai tinggi 4.[8]

2.3.3 Pohon *n-ary*

Pohon berakar yang setiap simpul cabangnya mempunyai paling banyak *n* buah anak disebut pohon *n-ary*. Pohon *n-ary* dikatakan teratur atau penuh jika setiap simpul cabangnya mempunyai tepat *n* anak.[8]

2.3.4 Pohon Biner (*binary tree*)

Pohon Biner adalah pohon n-ary dengan n = 2. Setiap simpul di dalam pohon biner mempunyai paling banyak 2 buah anak. Pohon biner dibedakan antara anak kiri (*left child*) dan anak kanan (*right child*). Karena ada perbedaan urutan anak, maka pohon biner adalah pohon terurut.[8]



Gambar 2-5 Pohon Biner

2.3.5 Penelurusan (Traversal) Pohon Biner

- *Preorder* : R, T_1, T_2
  - Kunjungi R
  - Kunjungi T_1 secara *preorder*
  - Kunjungi T_2 secara *preorder*

- *Inorder* : T_1, R, T_2
  - Kunjungi T_1 secara *inorder*
  - Kunjungi R
  - Kunjungi T_2 secara *inorder*

- *Postorder* : T_1, T_2, R
  - Kunjungi T_1 secara *postorder*
  - Kunjungi T_2 secara *postorder*
  - Kunjungi R

Dimana R adalah *parent*(orang tua), T_1 adalah anak kiri, dan T_2 adalah anak kanan.[8]

III. PEMBAHASAN

Steganografi menggunakan Bacon's Chiper memiliki banyak sekali dalam penerapannya. Contoh penulisan chiperteks menggunakan Bacon's Chiper adalah sebagai berikut :

"KRIPTOGRAFI" = abaab baaaa abaaa abbba baaba abbab aabba baaaa aaaaa aabab abaaa

Dipilih kalimat "nanti malam setelah kuliah kita ada latihan marching band, krisna" yang memiliki jumlah karakter 55 buah (dari 11 dikali 5, 11 karakter untuk "KRIPTOGRAFI", 5 untuk tiap karakter Bacon's Chiper yang memang mengandung 5 karakter 'a' dan/atau 'b') diubah menjadi memiliki sandi Bacon's Chiper dengan mengubah tiap karakter menjadi kapital untuk karakter yang memiliki alfabet 'b' menjadi seperti berikut : "nAntI Malam sEtelaH KUlIah KitA AdA laTIhAn marching baNd, KrIsna" yang memiliki arti yang berbeda dari informasi sebenarnya.

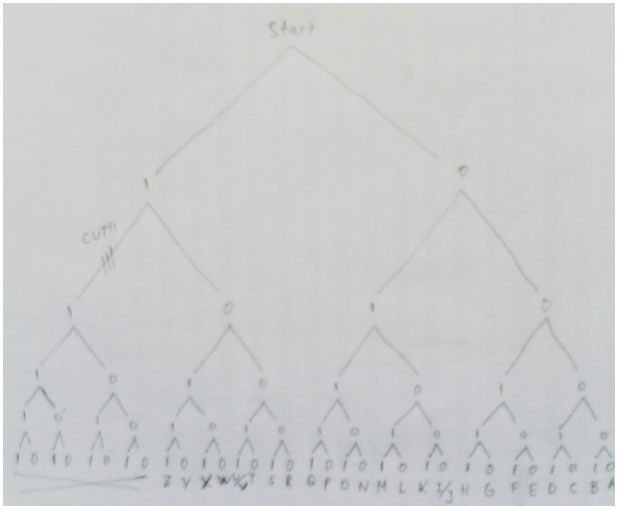
Contoh lainnya untuk menuliskan kata "STRUKTUR DISKRIT" dapat dienskrip menjadi chiperteks bilangan biner sebagai berikut :

D = aaabb → 00011
I/J = abaaa → 01000
K = abaab → 01001
R = baaaa → 10000
S = baaab → 10001
T = baaba → 10010
U/V = baabb → 10011

STRUKTUR DISKRIT = 10001100101000010011010011001010011100000001101000100010100110000010001001010

Enskripsi di atas memanfaatkan karakter 'a' dan 'b' yang digunakan sebagai Bacon's Chiper menjadi angka 0 dan 1 (bilangan biner) dengan perubahan a → 0 dan b → 1. Dengan menggunakan enskripsi seperti ini dapat membuat pihak ketiga yang ingin "*menyerang*" informasi yang dikirimkan oleh pemilik kode kepada pemilik kode yang lain dan dianggap sebagai bilangan biner yang hanya merepresentasikan sebuah bilangan dalam beberapa bit tertentu.

Penerjemahan chiperteks biner yang salah adalah sebagai berikut menganggap itu bilangan 4 bit dan 5 bit : 10001100101000010011010011001010011100000001101000100010100110000010001001010 → 1000 1100 1010 0001 0011 0100 1100 1010 0111 0000 00011 01000 10001 01001 10000 01000 10010 → 8 12 10 1 3 4 12 10 7 0 3 8 17 9 16 8 18. Angka tersebut menjadi tak berarti apa-apa, tidak mungkin melambangkan urutan dalam sistem alfabet (1 sampai dengan 26) karena mengandung angka 0 yang sangat tidak mungkin. Maka dari itu penerapan steganografi ini saya rasa cukup efektif untuk menyembunyikan informasi yang dikirim. Maka dari itu saya rancang sebuah pohon biner yang dapat digunakan untuk menenskripsi sebuah karakter menjadi Bacon's Chiper.



Gambar 3-1 Pohon Bacon's Chiper rancangan saya

Pada pohon itu upapohon/subpohon dibawah *parent* '1' pada tingkat pertama tidak memiliki karakter satu pun pada daun terakhir. Karakter terakhir ('Z') berkode 10111 atau 'babbb'

Jika direpresentasikan menggunakan tabel, maka didapat hasil sebagai berikut :

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

Tabel 3-1 Tabel yang merepresentasikan Bacon's Chiper

Dengan dokumentasi struktur di atas alfabet yang berjumlah 26 buah dikelompokan menjadi 2 kelompok alfabet besar yaitu kelompok alfabet 'a' dan kelompok alfabet 'b' yang dibedakan dari karakter awal tiap alfabet dalam bentuk Bacon's Chiper.

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

Tabel 3-2 Tabel kelompok besar alfabet

Telah berkembang pula gaya penulisan chiperteks Bacon's Chiper menggunakan sifat kelompok besar alfabet seperti pada tabel di atas. Contohnya pada kata "DEKAN SITH-R" memiliki Bacon's Chiper "aaaaa babab" yang didekode menjadi "AX" sama halnya dengan kata "NICE ABALON" menjadi "AA" atau "KOTA PADANG" menjadi "EA".

Proses traversal untuk pohon Bacon's Chiper sama halnya dengan proses pencarian pada tabel Bacon's Chiper di atas. Jika ditinjau berdasarkan prinsip Kompleksitas Algoritma, kompleksitas waktu yang dilakukan untuk menenskripsi plainteks adalah $T_{(Ens)} = 5$ baik di kasus terbaik ataupun di kasus terburuk. Karena kompleksitas waktu proses traversal selalu sedalam pohon Bacon's Chiper yaitu 5. Gaya penulisan chiperteks pun tidak akan mempengaruhi kompleksitas waktu dari algoritma enskripsi Bacon's Chiper menggunakan representasi prinsip pohon karena tetap saja harus mentraversal pohon seperti cara yang semestinya.

Sedangkan jika ditinjau berdasarkan kompleksitas ruang $S_{(Ens)}$ memang lebih memakan memori lebih karena memang struktur pohon lebih memakan memori akan sel/ruang yang berbentuk sebagai *array* multidimensi dan belum ada lagi struktur data yang dapat memperkecil kompleksitas ruang dari Bacon's Chiper.

IV. KESIMPULAN

Representasi Bacon's Chiper menggunakan struktur pohon memang cara yang terbaik (mangkus/efisien) menurut saya untuk saat ini. Selain mempermudah dalam hal pembendaharaan Chiper yang cukup membingungkan untuk hanya sekedar dihafal tetapi juga dapat mempermudah proses enskripsi yang hanya membutuhkan proses traversal pohon Bacon's Chiper. Dari segi kompleksitas algoritma memang struktur pohon memang yang paling mangkus/efisien jika ditinjau dari kompleksitas waktu walau sedikit kontroversial pada kompleksitas ruang/memori. Diharapkan dengan analisis ini kita dapat lebih mudah dalam mengenal dan mempergunakan Bacon's Chiper untuk hal kriptografi.

REFERENCES

Menezes. A. “Handbook of Applied Cryptography” CRC Press Inc. 1996 ch. 1

Gaines. Helen Fouche. “Cryptanalisis : A Study of Chipers And Their Solutions”. 2th Ed. Dover Publication Inc. 1956.

http://www.sacred-texts.com/eso/sta/sta42.htm diakses pada tanggal 17 Desember 2012

http://www.math.cornell.edu/~morris/135/Bacon.pdf diakses pada tanggal 17 Desember 2012

biography.com/ diakses pada tanggal 17 Desember 2012

http://ae89crypt5.wordpress.com/2008/05/12/sejarah-kriptografi/ diakses pada tanggal 17 Desember 2012

geocaching.com/ diakses pada tanggal 17 Desember 2012

Munir. Rinaldi. “Presentasi IF2091 Struktur Diskrit” Kurikulum 2008-2013

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, 17 Desember 2012

Krisna Fathurahman/13511006