

**Laporan EI 7010
(Keamanan Sistem Lanjut)
Pemecahan Code (Kriptaanalisis)
Algoritma Kriptografi Klasik**

Oleh :

**Nama : Dedi Wahyudi
NIM : 23203102**



**Program Magister Teknik Elektro
Bidang Khusus Teknologi Informasi - Dikmenjur
Institut Teknologi Bandung
2004**

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Kuasa atas segala rahmat dan karunia-Nya, sehingga dalam penyusunan laporan tugas EI 7010 ini dapat penulis selesaikan tepat pada waktunya.

Pada kesempatan yang baik ini penulis ingin menyampaikan ucapan terima kasih yang sebesar - besarnya kepada **Dr. Budi Rahardjo** selaku dosen mata kuliah **Keamanan Sistem Lanjut** yang selama ini telah banyak membimbing dan memberi motivasi. Saya mendoakan semoga amal baik bapak mendapatkan balasan dari Allah S.W.T.

Penulis menyadari bahwa penulisan laporan ini masih jauh dari sempurna, oleh karena itu dengan besar hati penulis menerima saran dan kritik dari para pembaca demi perbaikan laporan ini.

Pada kesempatan ini pula penulis menyampaikan permohonan maaf kepada semua pihak atas segala kesalahan yang penulis sengaja maupun yang tidak disengaja selama penulisan laporan ini.

Penulis berharap semoga karya tulis ini dapat bermanfaat bagi pembaca dan khususnya bagi penulis sendiri.

Terima kasih.

Bandung, Desember 2004

Dedi Wahyudi

DAFTAR ISI

HALAMAN JUDUL	i
KATA PENGANTAR	ii
DAFTAR ISI	iii
DAFTAR TABEL	iv
BAB I PENDAHULUAN	1
BAB II PENGERTIAN MEMECAHKAN KODE RAHASIA	2
BAB III ANALISIS KODE RAHASIA	3
3.1 Analisis Kode Rahasia Substitusi	3
3.2 Analisis Kode Rahasia Transposisi	21
3.3 Mengapa Kode-kode Rahasia Dapat Dipecahkan	23
BAB IV KESIMPULAN DAN SARAN	26
4.1 Kesimpulan	26
4.2 Saran	26
DAFTAR PUSTAKA	27

DAFTAR TABEL

Tabel 3.1 Tabel Frekuensi Distribusi Ciphertext

Tabel 3.2 Tabel Frekuensi Distribusi Standar

Tabel 3.3 Tabel Distribsi Bahasa Indonesia

BAB I

PENDAHULUAN

Untuk membuat sistem enkripsi yang aman, harus dapat menganalisis kelemahan berbagai macam jenis sistem enkripsi. Tanpa mengetahuinya, hampir mustahil dapat membust sistem yang tangguh. Jika pemecahan kode rahasia dapat dilakukan karena banyaknya perulangan dalam kode rahasia yang dipecahkan, maka akan berusaha membuat sistem yang mengurangi perulangan atau bahkan menghilangkannya sama sekali bila dimungkinkan. Untuk melindungi rumah dari pencurian maka harus mengetahui cara-cara pencuri memasuki rumah orang

BAB II

PENGERTIAN MEMECAHKAN KODE RAHASIA

2.1 Apakah yang dimaksud memecahkan kode rahasia?

Sebelum membicarakan langkah-langkah beserta contoh pemecahan kode rahasia atau sandi, akan dibahas terlebih dahulu mengenai definisi *memecahkan kode rahasia*.

Pertanyaan ini mungkin kedengaran sangat aneh. Untuk keperluan praktis jelas, pemecahan kode rahasia berarti berarti dapat membaca *plaintext* yang *dienkrip* menjadi *ciphertext* tanpa harus mendapatkan kuncinya secara sah. Namun, dalam dunia akademik, pemecahan algoritma kriptografi tidaklah harus demikian. Pemecahan diartikan meluas.

Memecahkan sandi berarti mendapatkan kelemahan dalam cipher yang dapat dieksploitasi dengan kompleksitas yang lebih rendah dibanding *brute-force*. Bila *brute-force* membutuhkan 2^{128} dekripsi, maka *attack* yang membutuhkan 2^{115} akan dianggap sebagai *pemecahan*. Pemecahan ini mungkin juga memerlukan jumlah plaintext yang tidak realistis, misalnya 2^{56} blok atau membutuhkan tempat penyimpanan 2^{80} word.

Secara sederhana, pemecahan dapat diartikan sebagai pemberian bukti-bukti kelemahan cipher karena tidak sesuai dengan tingkat keamanan yang dinyatakan sebelumnya.

Keberhasilan analisis sandi juga dapat ditunjukkan dengan memecahkan varian cipher yang disederhanakan. Misalnya keberhasilan memecahkan DES 8 ronde dari 16 ronde yang sesungguhnya. Kebanyakan pemecahan memang bermula dari pemecahan varian cipher dengan kode yang disederhanakan, dan kemudian diperluas menjadi ke seluruh ronde lengkap. Dan bila mendengar bahwa varian DES 8 ronde berhasil *dipecahkan*, bukan berarti tinggal setengah langkah lagi untuk memecahkan DES 16 ronde lengkap, karena kompleksitas 16 ronde bukanlah 2 kali kompleksitas dari 8 ronde melainkan meningkat secara eksponensial.

BAB III

ANALISIS KODE RAHASIA

3.1. Analisis Kode Rahasia Substitusi

Teknik analisis sandi modern mula-mula dipelopori oleh seorang Arab yang bernama Al-Kalka-Shandi pada tahun 1412. Dialah yang mula-mula menyusun secara sistematis cipher substitusi dan transposisi, menggunakan distribusi frekuensi serta teknik cryptanalysis dasar.

3.1.1 Pemecahan kode rahasia (cryptanalysis) algoritma substitusi tunggal

Diberikan karakter CIPHER sebagai berikut :

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

Bila jumlah ciphernya sangat banyak, maka dapat berharap bahwa distribusi frekuensi relatifnya serupa dengan distribusi frekuensi standar. Dari cipher diatas, dihitung jumlah huruf yang muncul, kemudian dihitung prosentasenya. Tabel berikut menunjukkan frekuensi kemunculan huruf-huruf ciphertext di atas.

P	13,13	H	5,83	F	3,33	B	1,67	C	0
Z	11,67	D	5,00	W	3,33	G	1,67	K	0
S	8,33	E	5,00	Q	2,50	Y	1,67	L	0
U	8,33	V	4,17	T	2,50	I	0,83	N	0
O	7,50	X	4,17	A	1,67	J	0,83	R	0
M	6,67								

Tabel 3.1 Tabel frekuensi distribusi ciphertext

Bandingkan dengan frekuensi relatif standar berikut ini. Hasil ini diperoleh dari pengambilan sampel sejumlah besar kalimat berbahasa inggris secara acak, hasil ini dapat berbeda bila sampelnya berbeda. Jadi misalnya dari 10.000 huruf yang diambil dari sebuah buku diperoleh jumlah huruf E nya sebanyak 1275 buah(12,75%), jumlah huruf T nya sebanyak 925 buah(9,25%), jumlah huruf R nya sebanyak 850 buah(8,5%) dan seterusnya, maka akan diperoleh tabel seperti berikut :

E	12.75	L	3.75	W	1.50
T	9.25	H	3.50	V	1.50
R	8.5	C	3.50	B	1.25
N	7.75	F	3.00	K	0.50
I	7.75	U	3.00	X	0.50
O	7.5	M	2.75	Q	0.50
A	7.25	P	2.75	J	0.50
S	6.00	Y	2.25	Z	0.25
D	4.25	G	2.00		

Tabel 3.2 Tabel frekuensi distribusi standar

Dari perbandingan diatas, nampaknya huruf P dan Z pada cipher adalah E dan T, namun kita **belum** dapat memastikannya.

Huruf S, U, O, M, H dan D nampaknya adalah R, N, I, O, A, dan S. Huruf-huruf berfrekuensi kemunculan terendah A, B, G, Y, I, J nampaknya adalah W, V, B, K, X, Q, J, Z.

3.1.2 Distribusi Frekuensi Kemunculan Huruf Dalam Bahasa Indonesia

Untuk bahasa Indonesia, disini diambil dari teks biasa (plaintext) yang berisi 123174 karakter, dalam tabel 10 huruf yang paling sering muncul dalam teks bahasa Indonesia adalah :

No	Karakter	Frekuensi (%)	Frekuensi
1	A	17.4225	21460
2	N	10.2887	12673
3	I	8.6845	10697
4	E	7.4538	9159
5	K	5.6416	6949
6	T	5.0709	6246
7	R	4.5724	5632
8	D	4.4652	5500
9	S	4.4222	5447
10	M	4.3418	5348

Tabel 3.3 Tabel distribusi bahasa Indonesia

Prosentase frekuensi dihitung dari frekuensi kemunculan huruf dibagi dengan total jumlah huruf, misalnya prosentase kemunculan huruf A adalah $(21460/123174) \times 100\% = 17,4225\%$

3.1.3 Pemecahan kode rahasia digraf

Misalkan diperoleh cipher seperti berikut :

2023 2029 6224 6322 2144 4420 6362 4924 6529 2769
2043 2123 2227 4627 6521 2221 2723 6527 2349 2144
4481 8287 2423 4349 2144 4485 8089 6522 2746 2421
6365 2263 2142 2027 2324 6322 2144 4420 6362 4627
6521 2221 2723 6560 2144 4441 2047 2123 2422 6680

6666 6522 2746 4263 2069 2122 6425 2729 2924 2343
2123 4700

Langkah analisis cipher :

1. Di sini terlihat bahwa jumlah karakter ciphertextnya genap dan setiap pasang angka (2 angka) diawali dengan angka 2,4,6, atau 8 kecuali dua angka terakhir (00). Ini menunjukkan bahwa kelihatannya setiap huruf plaintext dikodekan menjadi 2 huruf ciphertext. Karena angka nol tidak tampak mengawali pasangan angka kecuali di sini, maka anggap saja dulu bahwa ini hanyalah tambahan pelengkap belaka, supaya satu blok tetap 4 angka. Ini menimbulkan kesan bahwa ciphertext ini dibuat dari matrik dengan jumlah baris 4 buah.
2. Memperhatikan digit kedua setiap pasang angka menunjukkan bahwa hanya angka 8 yang tidak digunakan. Nampaknya matrik ini memiliki 9 kolom. Bila kolom untuk angka 8 ada, nampaknya tidak digunakan. Kesimpulan sementara, matrik 4 x 9 digunakan untuk membentuk ciphertext ini.

Perkiraan matrik sementara :

	1	2	3	4	5	6	7	9	0
2									
4									
6									
8									

3. Cek pola yang berulang dan beri garis bawah. Kemudian hitung jumlah pasangan angka yang berulang sebagaimana dalam substitusi tunggal.

2023 2029 6224 6322 2144 4420 6362 4924 6529 2769
 2043 2123 2227 4627 6521 2221 2723 6527 2349 2144
 4481 8287 2423 4349 2144 4485 8089 6522 2746 2421
 6365 2263 2142 2027 2324 6322 2144 4420 6362 4627
6521 2221 2723 6560 2144 4441 2047 2123 2422 6680

6666 6522 2746 4263 2069 2122 6425 2729 2924 2343
 2123 4700

- berikut Pasangan angka 21 muncul 15 x .
- Pasangan angka 23 muncul 10 x dan seterusnya.

Sehingga dapat ditulis dalam matrik sebagai berikut :

	1	2	3	4	5	6	7	9	0
2	15	10	10	7	1		11	4	8
4	1	2	3	10		4	2	3	

Bila dilakukan penyesuaian antara frekuensi relatif standar dengan ciphertext di sini, tidak mendapat kemajuan , karena jumlah plaintextnya terlalu sedikit. Maka melakukan langkah berikutnya.

4. Perhatikan, terlihat deretan bilangan 24 63 22 21 44 44 20 63 62 berulang pada baris pertama dan keempat. Demikian pula 45 27 65 21 22 21 27 23 65 juga berulang pada baris ke-2 dan ke-4 dan ke-5. Dari sini dapat disimpulkan bahwa yang berulang ini mestinya adalah sebuah kata. Dengan pertolongan tabel kata- kata bahasa inggris yang

memiliki 9 huruf , maka dapat memperkirakan kata apa yang dikodekan tersebut. Namun ada cara yang lebih cepat seperti diuraikan sebagai berikut ini.

Dari sini melihat bahwa jarak perulangannya adalah genap sehingga bertambah yakin bahwa setiap karakter terdiri dari dua bilangan.

Memilih kata yang berisi banyak huruf, karena semakin panjang huruf yang membentuk kata, semakin banyak pula karakter yang berulang. Misalkan pada kode sandi 24 63 22 21 44 44 20 63 62, terlihat bahwa angka 63 , 44 berulang, demikian pula pada kode sandi 45 27 65 21 22 21 27 23 65, terlihat bahwa angka 21, 27, dan 65 berulang. Demikian pula diantara kedua kode tersebut, bilangan 21 dan 22 sama.

Kemudian perhatikan pula bahwa kode rahasia 24 63 22 21 44 44 20 63 62 memiliki pola – A B C D D E A – sedangkan 45 27 65 21 22 21 27 23 65 memiliki pola – A B C D C A E B

Cari pola tersebut dari daftar pola kata bahasa inggris yang memiliki pola semacam itu. Dan akan mendapat bahwa kode rahasia tersebut hanya sesuai bila berasal dari kata “ ARTILLERY “ dan “ POSITIONS “. Dan ini juga sesuai dengan hipotesa sebelumnya bahwa bilangan 21 dan 22 sama diantara kedua deretan bilangan tersebut , yaitu berasal dari “ I “ dan “ T “.

Cipher	24	63	22	21	44	44	20	63	62
Plaintext	A	R	T	I	L	L	E	R	Y
Pola	-	A	B	C	D	D	E	A	-
Cipher	45	27	65	21	22	21	27	23	65
Plaintext	P	O	S	I	T	I	O	N	S
Pola	-	A	B	C	D	C	A	E	B

5. Kemudian masukan plaintext yang sudah berhasil temukan ke dalam ciphertext semula. Disini sudah dapat menemukan bahwa angka 20 berasal dari “e”, angka 63 merupakan huruf “r” dan seterusnya.

e n e y a r t I l l e r y a s o
 2023 2029 6224 6322 2144 4420 6362 4924 6529 2769
 e I n t o p o s I t I o n s o n I l
 2043 2123 2227 4627 6521 2221 2723 6527 2349 2144

I a n I l l s t o p n i
 4481 8287 2423 4349 2144 4485 8089 6522 2746 2421
 r s t r I e o n a r t I l l e r y p o
 6365 2263 2142 2027 2324 6322 2144 4420 6362 4627
 s I t I o n s I l l e n a l
6521 2221 2723 6560 2144 4441 2047 2123 2422 6680
 s t o p r e I t o a n
 6666 6522 2746 4263 2069 2122 6425 2729 2924 2343
 I n
 2123 4700

	1	2	3	4	5	6	7	9	0
2	i	t	n	a			o		E
4				l		p			
6		y	r		s				
8									

Dan karena 21 berasal dari huruf “i”, maka pada baris “2” (bukan baris ke-2 melainkan baris ke-1) dan kolom “1” (juga kolom ke-1) isikan huruf “i”. Demikian juga karena 22 mewakili “t”, maka pada baris ke-2 (baris ke-1) kolom “2” (kolom ke-2) isikan huruf “t”, dan seterusnya. Sehingga diperoleh matrik seperti di atas.

- Kata pertama dari plaintext dapat ditebak sebagai “ *enemy* “. Akhir baris ke-3 dan awal baris ke-4 diperkirakan berupa “ *airstrike*”. Dari sini diperoleh “ 29 “ merupakan “m”. Dan bila letakan ke bagian paling akhir cipher, maka dapat perkiraan pula bahwa plaintext terakhir berbunyi “ *commanding*”.

Dari sini diperoleh susunan plaintext nya berupa :

	1	2	3	4	5	6	7	9	0
2	i	t	n	a	c		o	m	e
4	b	k	d	l		p	g	h	
6		y	r		s			v	w
8									

7. Huruf- huruf di baris ke-3 (b k d l p g h) nampaknya berada pada urutan sebelum baris ke-3. Hanya urutannya tidak jelas. Baris pertama mungkin berisi kata kunci (*key-word*). Sekarang coba atur kembali susunan kolom supaya baris kedua dan ketiga terurut kekanan menurut urutan abjad.

	1	3	5	7	9	0	2	4	6
2	i	n	c	o	m	e	t	a	
4	b	d		g	h		k	l	p
6		r	s		v	w	y		
8									

8. Dari sini dapat ditebak bahwa keywordnya berupa "*income tax*". Selanjutnya sempurnakan urutan abjad yang kurang. Jadi setelah "d" seharusnya "e", namun karena "e" menjadi kata kunci, maka isikan "f", dan seterusnya.

	1	3	5	7	9	0	2	4	6
2	i	n	c	o	m	e	t	a	x
4	b	d	f	g	h		k	l	p
6	q	r	s	u	v	w	y	z	
8									

Plaintextnya : *enemy artillery has moved into positions on hill *** and hill *** stop airstrike on artillery positions will begin at **** stop krev it commanding*

Yang kosong tersebut mungkin berisi jam dan nomor pemetaan perbukitan. Angka 66 nampaknya menyatakan 00 sehingga plaintext menjadi : *enemy artellery has moved*

*into positions on hill *** and hill *** stop airstrike on artellery positions will begin at 00 *0. Stop krev it commanding*

9. Sampai disini tidak dapat memastikan kelanjutan ini matrik tersebut tanpa informasi tambahan.

3.1.4 Sistem Monome-Dinome

Pada contoh sebelumnya, setiap karakter plaintext selalu dikonversi menjadi dua ciphertext. Ini memudahkan analisis sandi membuat matrik pengkodeannya. Dalam contoh berikut, sistem menggunakan monome (pemetaan satu ke satu) dan dinome (pemetaan satu kedua) sehingga satu karakter plaintext kadang dipetakan ke satu karakter ciphertext.

Sebagai contoh, perhatikan kode rahasia berikut ini.

80796	78009	<u>60720</u>	51187	33812
<u>07960</u>	76059	69730	71070	99089
60905	96070	62050	09109	13866
96058	24710	81059	69740	79610
90591	19787	16833	07389	70805
00019	60509	07055	05458	37950
19196	97407	<u>96960</u>	<u>72051</u>	18733
<u>81207</u>	06910	70390	56545	35399
95205	00030	08204		

Number : 1 2 3 4 5 6 7 8 9 0

Frekuensi : 19 8 13 6 22 20 25 16 33 53

1. Hal pertama yang dapat dilakukan adalah menghitung frekuensi kemunculan karakter. Perulangan digaris bawah. Jarak perulangan di sini adalah 153 karakter (dihitung dari awal karakter berikutnya). Karena jaraknya ganjil, maka sistem disini tidak mungkin dinomik. Frekuensi kemunculan yang sangat tinggi bilangan 0 dan 9 dalam hubungan dengan bilangan lain menunjukkan bahwa sistem ini monome-dinome. Sehingga muncul kemungkinan besar bahwa “0” dan “9” dijadikan koordinat baris. Koordinat baris yang juga dimungkinkann namun untuk ini diabaikan dulu.
2. Mulai mengelompokkan bilangan dengan awalan 0 dan 9. Tandai dengan pena, dan harus ingat, bahwa pengelompokan ini dapat berubah. Mulai dengan karakter pertama menuju akhir pesan. Bila karakter tersebut berupa 0 dan 9, anggap sebagai monome (

anggap angka 0 dan 9 sebagai awalan dari dua bilangan), dan bila bukan 0 dan 9 anggap sebagai monome (karakter tunggal satu bilangan).

8/0 7/9 6/ 7/8/0 0/9 6/0 7/2/0 5/1/1/8/7/ 3/3/8/1/2/
0 7/9 6/0 7/6/0 5/9 6/9 7/3/0 7/1/0 7/0 9/9 0/8/9
 6/0 9/0 5/ 9 6/0 7/0 6/2/0 5/0 0/9/ 1/0 9/ 1/3/8/6/6/
 9 6/0 5/8/ 2/4/7/1/0 8/1/0 5/9 6/9 7/4/0 7/9 6/1/0
 9/0 5/9 1/ 1/9 7/8/7/ 1/6/8/3/3/ 0 7/3/8/9 7/0 8/0 5/
 0 0/0 1/9 6/0 5/0 9/ 0 7/0 5/5/ 0 5/4/5/8/ 5/7/9 5/0
 1/9 1/9 6/ 9 7/4/0 7/ 9 6/9 6/0 7/2/0 5/1/ 1/8/7/3/3/
8/1/2/0 7/ 0 6/9 1/0 7/0 3/9 0/ 5/6/3/4/5/ 3/5/3/9 9/
 9 5/2/0 5/ 0 0/0 3/0 0/8/2/0 4

3. Terlihat bahwa bilangan pertama (angka 8) dianggap monome dan 07 dianggap dinome. Demikian juga 96 dianggap dinome karena diawali angka yang termasuk paling sering muncul (9). Kemudian mencoba mengambil “kata” yang berulang dan mencari polanya sebagaimana yang pernah dikerjakan pada contoh sebelumnya.

96 07 2 05 1 1 8 7 3 3 8 1 2 07
- A B C D D E F G G E D B A
R E C O N N A I S S A N C E

4. Isi matrik dan plaintext yang telah ditemukan.

	1	2	3	4	5	6	7	8	9	0
-	n	c	s				i	a		
0					o		e			
9						r				

Baris tidak diisi lengkap (hanya 0 dan 9) karena di ciphertextnya hanya dijumpai satu bilangan.

5. Bagian awal pesan menimbulkan dugaan bahwa plaintextnya berbunyi : *AERIAL RECONNAISSANCE REPORTS ENEMY*. Dan ini akan menambah karakter ciphertext yang dapat diterka.

a e r l a l r e c e n n a l r r a n c
 8/0 7/9 6/ 7/8/0 0/9 6/0 7/2/0 5/1/1/8/7/ 3/3/8/1/2/

e r e p o r r s e n e m y a r
 0 7/9 6/0 7/6/0 5/9 6/9 7/3/0 7/1/0 7/0 9/9 0/8/9
 m o r e o c o l o m n s a r r
 6/0 9/0 5/ 9 6/0 7/0 6/2/0 5/0 0/9/ 1/0 9/ 1/3/8/6/6/
 r o a c h I n n o c t h e r n m
 9 6/0 5/8/ 2/4/7/1/0 8/1/0 5/9 6/9 7/4/0 7/9 6/1/0
 o n n l a I n p a s s e s a t a o
 9/0 5/9 1/ 1/9 7/8/7/ 1/6/8/3/3/ 0 7/3/8/9 7/0 8/0 5/
 I I r o m e o o a I i
 0 0/0 1/9 6/0 5/0 9/ 0 7/0 5/5/ 0 5/4/5/8/ 5/7/9 5/0
 o r t h e r r e c o n n a I s s
 1/9 1/9 6/ 9 7/4/0 7/ 9 6/9 6/0 7/2/0 5/1/ 1/8/7/3/3/
 a n e e d n e b y s s
 8/1/2/0 7/ 0 6/9 1/0 7/0 3/9 0/ 5/6/3/4/5/ 3/5/3/9 9/
 c o I b I a c r
 9 5/2/0 5/ 0 0/0 3/0 0/8/2/0 4

Dan selanjutnya pengisian matrik dapat dilanjutkan menjadi:

	1	2	3	4	5	6	7	8	9	0
-	n	c	s	H		p	i	a		
0	f		b	K	o	d	e	g	m	l
9	u					r	t			y

6. Kolom disusun ulang agar abjad lebih berurutan ke kanan, dan menerka bahwa baris pertama berisi kata kunci. Lengkapi sel kosong dengan urutan huruf yang termasuk ke dalam kata kunci. Misalkan 02 seharusnya diisi “h” karena terletak setelah huruf “g”. Namun karena “h” berada di dalam kata kunci, maka “h” ke kolom 02, demikian pula huruf “i”. Setelah “i” adalah huruf “j”. Dan karena belum masuk pada kata kunci, maka j diletakan setelah “g”. Demikian seterusnya sampai berakhir hingga huruf “z”.

	3	6	7	1	8	2	4	0	9	5
-	s	p	i	N	a	c	h			
0	b	d	e	F	q	j	k	l	m	o
9	q	r	t	U	v	w	x	y	z	

Dan plaintext sementara menjadi : *AERIAL RECONNAISSANCE REPORTS ENEMY
ERMORED COLUMNS APPROACHING NORTHERN MOUNTAIN PASSES AT
GOLF ROMEO *OH*A*I FURTHER RECONNAISSAINCE DUE BY
*P*H*S*SZ*COL BLACK.*

Disini dijumpai kesulitan untuk melanjutkan, maka bagian yang digaris bawah di atas modifikasi. Kalau perhatikan pada ciphertext, terdapat angka-angka 5 yang sering muncul, maka anggap bahwa 5 ini menjadi bagian dari baris, dan kelihatannya bagian yang bergaris bawah tersebut merupakan angka-angka sehingga kita buat matrik :

	3	6	7	1	8	2	4	0	9	5
-	s	p	i	N	a	c	H			
0	b	d	e	F	G	J	K	l	m	o
9	q	r	t	U	V	W	X	y	z	
5	0	1	2	3	4	5	6	7	8	9

Dan plaintext-plaintext menjadi :

a e r l a l r e c e n n a l r r a n c
8/0 7/9 6/ 7/8/0 0/9 6/0 7/2/0 5/1/1/8/7/ 3/3/8/1/2/
e r e p o r r s e n e m y a r
0 7/9 6/0 7/6/0 5/9 6/9 7/3/0 7/1/0 7/0 9/9 0/8/9
m o r e o c o l o m n s a r r
6/0 9/0 5/ 9 6/0 7/0 6/2/0 5/0 0/9/ 1/0 9/ 1/3/8/6/6/
r o a c h I n n o c t h e r n m
9 6/0 5/8/ 2/4/7/1/0 8/1/0 5/9 6/9 7/4/0 7/9 6/1/0
o n n l a I n p a s s e s a t a o
9/0 5/9 1/ 1/9 7/8/7/ 1/6/8/3/3/ 0 7/3/8/9 7/0 8/0 5/
I I r o m e o o a I i
0 0/0 1/9 6/0 5/0 9/ 0 7/0 5/5/ 0 5/4/5/8/ 5/7/9 5/0
o r t h e r r e c o n n a I s s
1/9 1/9 6/ 9 7/4/0 7/ 9 6/9 6/0 7/2/0 5/1/ 1/8/7/3/3/
a n e e d n e b y s s
8/1/2/0 7/ 0 6/9 1/0 7/0 3/9 0/ 5/6/3/4/5/ 3/5/3/9 9/
c o I b I a c r

9 5/2/0 5/ 0 0/0 3/0 0/8/2/0 4

Sekarang plaintext menjadi :

*AERIAL RECONNAISSANCE REPORTS ENEMY ERMORED COLUMNS
APPROACHING NORTHERN MOUNTAIN PASSES AT GOLF ROMEO 7642. FURTHER
RECONNAISSANCE DUE BY 1600Z. COL BLACK.*

Dan semua plaintext yang dienkrip menggunakan matrik ini dapat buka plaintextnya.

3.1.5 Sistem variant

Misalkan kita peroleh ciphertext sebagai berikut :

IIUC RAPC OIPU IANU NMDR NIRI ISIU AIII PSPR AUUN
AMDG ANPG URDU IMMA PRAU MROU RIIM NAMO ICDN UUUA
UIOM ARAA AIII DSMI RRNO MMPU RGUR UNDS NIIA RMMA
PSUC UONM IOAR RADU PUPG OCIA PUMO ROMM MCDR ROIA
SORI AONM UNRI IMII SMRA ANNA SRNM ROMI NONR RAUC

RIPN SADG AUPR IONA DUUU MRJA OGNR RAIR MAIA RGNI
MOPO RAMM MUI DRPS MIAR MOAC DGUA URAC NISR NOIG
DSSI RORM MINO MORU DOUA PGRR USXX

- Langkah pertama harus menganggap bahwa kode rahasia ini berjenis variant. Tentu saja bila terkaan ini salah, harus mencoba asumsi yang lain. Kemudian karena berjenis varian, maka buat matrik sebagai berikut :

	A	C	G	I	M	N	O	R	S	U
A	1	3		3	1	2		3		3
D			3			1	1	3	3	3
I	6	1	1	5	3		2	1	1	1
M	3	1		4	4		4	2		2
N	3			4	4		4	2		1
O		1	1	1	1					1
P		1	3			1	1	3	3	4
R	6	1	2	5	2		3	2		1
S	1			1	1		1	2		
U	3	3		1		3	1	3	1	2

Untuk sementara anggap setiap karakter ciphertext terdiri atas 2 huruf , sehingga buat pada sisi baris adalah huruf yang muncul pertama kali dari setiap pasang huruf, sedangkan kolom berasal dari huruf kedua dari setiap pasang huruf ciphertext.

Kemudian hitung jumlah frekuensi kemunculan setiap pasang huruf cipher. Misalkan kemunculan Aa dalam ciphertext sebanyak 1 kali, AC 3 kali dan seterusnya.

2. kalau perhatikan jumlah frekuensi kemunculan huruf , melihat pola yang sesuai antara baris dan kolom tertentu. Sebagai contoh, baris I dan R hampir identik. Demikian pula kolom A dan I hampir sama. Baris dan kolom yang hampir identik ini anggap satu kesatuan, sehingga I dipasangkan dengan R, A dengan I. Atau pasangan barisnya : AU, DP, IR, MN dan OS. Sedangkan pasangan kolomnya : AI, CN, GS, MO dan RU.
3. Dari sini dapat menyederhanakan matrik menjadi

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

Disini memang belum tahu sebenarnya isi matrik. Urutan A-Y seperti yang dimasukan ke matrik tersebut barulah terkaan belaka. Yang jelas membuat pasangan AU, DP dan seterusnya dengan asumsi, bahwa frekuensi kemunculan A hampir sama dengan pasangannya U, D sama dengan P dan seterusnya.

4. Bila matrik di atas anggap benar , maka ciphertext II=k, UC=B, RA=K dan seterusnya. Sehingga dapat tulis sebagai berikut :

KB KG UJ KT SJ PK MO AK HJ EB
 IIUC RAPC OIPU IANU NMDR NIRI ISIU AIII PSPR AUUN
DH BH EJ NP JE TY KN PS LG EA
 AMDG ANPG URDU IMMA PRAU MROU RIIM NAMO ICDN UUUA
 AX EA AK HP OS SJ ME BH PK NP
 UIOM ARAA AIII DSMI RRNO MMPU RGUR UNDS NIIA RMMA
 HB DS NE KJ JH VK JS LS OJ NK
 PSUC UONM IOAR RADU PUPG OCIA PUMO ROMM MCDR ROIA

X K D S B K N K X K P P Y S N P S T K B
 SORI AONM UNRI IMII SMRA ANNA SRNM ROMI NONR RAUC
K G U H E J N P I L I K O T K O P K M P
 RIPN SADG AUPR IONA DUUU MRJA OGNR RAIR MAIA RGNI
 S I K S T K J H P L S B H A E B P Y S M
 MOPO RAMM MUI DRPS MIAR MOAC DGUA URAC NISR NOIG
 H U N N P S T O S A I A H O C
 DSSI RORM MINO MURU UMAI DOUA PGRR USXX

5. Dari terkaan plaintext, terlihat adanya perulangan –perulangan. Misalkan KBKG muncul di baris pertama dan akhir baris kelima serta awal baris keenam. HEJNPJE muncul pada baris kedua dan keenam, dan seterusnya. Tapi perulangan berkurang karena sistemnya varian (satu karakter plaintext dapat memiliki lebih dari satu macam karakter ciphertext). Dengan bantuan tabel dilampiran D dan cara-cara seperti yang pernah lakukan (mencari kata yang mengikuti pola tertentu dari tabel D), diperoleh tabel sebagai berikut:

	A	C	G	M	R
	I	N	S	O	U
AU	l	n	k	g	i
DP	-	m	a	b	r
IR	e	f	d	s	c
MN	t	u	-	o	p
OS	y	z	x	v	w

e n e m y r e p o r t e d c l e a r I n
KB KG U J K T S J P K M O A K H J E B
 IIUC RAPC OIPU IANU NMDR NIRI ISIU AIII PSPR AUUN
 G a n a I r s t r I p w e s t o f m I l
D H B H E J N P J E T Y K N P S L G E A
 AMDG ANPG URDU IMMA PRAU MROU RIIM NAMO ICDN UUAU
 L v I l l e a t c o o r d I n a t e s t
 A X E A A K H P O S S J M E B H P K N P
 UIOM ARAA AIII DSMI RRNO MMPU RGUR UNDS NIIA RMMA
 A n g o s I e r r a z e r o f o u r s e
 H B D S N E K J J H V K J S L S O J N K
 PSUC UONM IOAR RADU PUPG OCIA PUMO ROMM MCDR ROIA
 V e n o n e s e v e n t w o s t o p e n
X K B S B K N K X K P P Y S N P S T K B
 SORI AONM UNRI IMII SMRA ANNA SRNM ROMI NONR RAUC
 E m y a I r s t r I p e x p e c t e d t
K G U H E J N P J K T K O T K O P K M P

RIPN SADG AUPR IONA DUUU MRJA OGNR RAIR MAIA RGNI
 O B e o p e r a t I o n a l I n t w o d
 S I K S T K J H P E S B H A E B P Y S M
 MOPO RAMM MUI DRPS MIAR MOAC DGUA URAC NISR NOIG
 A y s s t o p c o l b l a c k
 H U N N P S T O S A I A H O C
 DSSI RORM MINO MURU UMAI DOUA PGRR USXX

Plaintext : *ENEMY REPORTED CLEARING AN AIRSTRIP WEST OF MILLVILLE AT
 COORDINATE STAN GO SIERRA ZERO FOUR SEVEN TWO STOP ENEMY
 AIRSTRIP EXPECTED TO BE OPERATIONAL IN TWO DAYS STOP COL BLACK*

6. Setelah matrik diplaintext, maka dapat lihat bahwa urutan abjadnya belum terurut, maka dapat mengurutkannya ke arah kanan berdasar baris terbawah.

	M	R	G	A	C
	O	U	S	I	N
AU	g	i	k	i	n
DP	b	r	a	-	m
IR	s	c	d	e	f
MN	o	p	-	t	u
OS	v	w	x	y	z

Agar gikin berurut dengan op-tu, maka AU diturunksn ke baris tiga sehingga menjadi

	M	R	G	A	C
	O	U	S	I	N
DP	b	r	a	-	m
IR	s	c	d	e	f
AU	g	i	k	l	n
MN	o	p	-	t	u
OS	v	w	x	y	z

7. Sekarang tinggal huruf- huruf h, j dan q yang belum dimasukan ke dalam matrik. Biasanya I dan J dijadikan satu sel, demikian pula u dan v pada matrik 5 X 5. Namun u dan v dapat dipisah, maka pisahkan dulu. Sedangkan huruf j masukan ke dalam I. Huruf q masukan antara p dan t, sedangkan h dapat masuk ke tempat kosong antara a dan m. Kata kuncinya menjadi BRAHMS (nama seorang komposer lagu klasik). Dari sini dapat menerka, bahwa susunan kolom dan barisnya membentuk nama-nama musik PIANO, MUSIK, DRUMS dan ORGAN.

	O	R	G	A	N
	M	U	S	I	C
DP	b	r	a	h	m
RI	s	c	d	e	f
UA	g	i/j	k	l	n
MN	o	p	q	t	u
SO	v	w	x	y	z

3.1.6 Sistem persegi-empat standard

Misalkan mendapatkan kode rahasia sebagai berikut :

TATO UTOD HIDM FIPK ROFM HRVH BMAH NHKM UNAN ZMRO
 SKHH RQBX FSYP KQNS QFAT KQUY SMQP SMNT MYRO RYDM
FIPK ROFM IQLT TYSQ RYRF FEDC ATGR RHTO AOTD QP

- Langkah pertama, seperti biasa, mencari karakter yang berulang, kemudian beri garis bawah. Misalkan saja mencurigai bahwa ciphertext ini dibangkitkan dari sistem substitusi digrafik persegi empat standar. Bila terkaan ini salah, maka tidak akan dapat menemukan matrik pembentuknya, dan harus mengulang langkah dari awal dengan terkaan sistem enkripsi yang lain.

- Buat pola ciphertext yang berulang

Ciphertext DM FI PK RO FM
 Pola -B A- - - AB

- Diperoleh bahwa plaintext yang memenuhi pola -B A- - - AB hanyalah kata "INFORMATION".

I n f o r m a t I o n

TATO UTOD HIDM FIPK ROFM HRVH BMAH NHKM UNAN ZMRO
 SKHH RQBX FSYP KQNS QFAT KQUY SMQP SMNT MYRO RYDM
 Form a t I o n
FIPK ROFM IQLT TYSQ RYRF FEDC ATGR RHTO AOTD QP

	a	b	c	d	e				R	
	f	g	h	i/j	k			d	F	
p1	l	m	n	o	p					H1 c1
	q	r	s	t	u		P			
	v	w	x	y	z					
					a	b	c	d	e	
					f	g	h	i/j	k	
c2	I	K		M		l	m	n	o	p
	O					q	r	s	t	u
						v	w	x	y	z

R
Q

4. Karena menganggap pengkodenya sistem persegi empat, maka pola p1 dan p2 anggap seperti matrik di atas. Kemudian dari pasangan ciphertext- plaintext “DM FI PK RO FM – in fo rm at io n’ yang telah ditemukan, bisa mengisi matrik c1 dan c2. Misalkan dari p1=I dan p2=n, buat segiempat dengan I dan n sebagai sudut segiempat, maka beri sudut lainnya dengan D (=c1) dan M (=c2). Demikian pula selanjutnya.

Pada akhir plaintext “information”, huruf “n” dikodekan menjadi H dan I. Perhatikan ciphertext-nya! Dan karena posisi H dan I berada pada posisi c1, dan harus berada pada baris n (dalam kelompok p1). Karena itulah tuliskan H dan I sebaris dengan n (p1), namun di luar matrik, karena belum tahu secara persis kolomnya. Demikian pula perlakukan R dan Q yang harus sekolom dengan “n” dengan alasan yang sama.

Perhatikan lagi ciphertext yang terletak setelah plaintext “information”, yaitu HRVH dan IQLT. Artinya plaintext “n”, “?” (plaintext yang belum diketahui) dan ciphertext “H”, “R” membentuk segiempat.

5. Pada baris ketiga c2, bisa sisipi L dan N sehingga menjadi IKLMN. Kemudian H dan I nampaknya berada pada dua kolom pertama, baris ketiga c2. Dan G dapat masukan setelah F pada baris kedua c1. Sehingga diperoleh matrik sebagai berikut.

Phi digrafik lebih rendah karena pasangan dua huruf dapat terpecah pada metode transposisi. Sedangkan Phi monografiknya sama dengan Phi monografik plaintext, karena huruf yang muncul pada ciphertext sama persisi dengan yang muncul pada plaintext, demikian pula halnya dengan frekuensi kemunculannya. Bila ciphertext yang kita peroleh hanya sedikit jumlahnya, perkiraan di sini dapat keliru. Bila tidak dapat dipecahkan dengan asumsi ini, maka harus digunakan asumsi lain.

2. Bila hitung, terdapat 45 huruf ciphertext, namun karena di akhir terdapat XXX, maka anggap bahwa XXX hanyalah tambahan yang dapat diabaikan (karena sepertinya hanyalah pelengkap), sehingga jumlah huruf plaintext-nya menjadi 42 buah.
3. Karena 42 dapat berasal dari 6×7 atau 7×6 maka mencoba menyusun matrik 6×7 , dan masukan ciphertext di atas, terurut dari atas ke bawah, dari kolom paling kiri ke kanan. Bila terkaan salah, dapat mencoba membuat matrik berukuran lain dan memasukan ciphertext ke dalamnya.

1	2	3	4	5	6	7
E	R	E	N	E	F	R
R	U	O	M	E	Y	C
E	G	A	N	S	S	C
S	R	E	I	M	B	U
O	F	O	U	T	W	X
R	P	O	E	S	T	R
I	T	S	S	U	E	Q
E	T	N	D	R	A	G

7	5			
R	E			
C	E			
E	S			
U	M			
X	T			
R	S			
Q	U			
G	R			

4. Dari matrik di atas, nampaknya sudah mulai bisa menerka sebagian plaintext. Baris 1 nampaknya akan membentuk kata REFERENCE. Terkaan ini juga dapat dilakukan dari awal. Namun belum tahu penempatan huruf E setelah "REF" apakah berasal dari kolom 1 atau 3.

7	5	6
R	E	F
C	E	Y
E	S	S
U	M	B
X	T	W
R	S	T
Q	U	E
G	R	A

5. Bila anggap E berikutnya dari kolom 1 (dengan kunci 7561234 supaya baris pertama membentuk kata *REFERENCE*, maka baris pertama dan baris kedua akan membentuk tulisan *REFEREN CEYRUOM*, dan bila anggap urutan kuncinya 7563214(dengan mengambil huruf E setelah “REF” dari kolom ke-3), maka akan diperoleh matrik sebagai berikut :

7	5	6	3	2	1	4
R	E	F	E	R	E	N
C	E	Y	O	U	R	M
E	S	S	A	G	E	N
U	M	B	E	R	S	I
X	T	W	O	F	O	U
R	S	T	O	P	R	E
Q	U	E	S	T	I	S
G	R	A	N	T	E	D

6. Dan peroleh plaintext : *REFEREBCE YOUR MESSAGE NUMBER SIX TWO FOUR STOP REQUEST IS GRANTED.*

3.3 Mengapa kode-kode rahasia di atas dapat dipecahkan ?

1. Karena terdapat bagian pesan atau kata-kata yang berulang pada ciphertext-nya. Tanpa perulangan, akan sangat kesulitan untuk memperkirakan plaintext suatu kata. Bila diffusion berjalan baik. Maka akan sangat sulit untuk melihat perulangan-perulangan ini.

2. Karena terdapat hubungan yang jelas antara plaintext dengan ciphertex-nya. Artinya, confusion tidak berlangsung dengan baik. Plaintext yang sering muncul akan tercermin pada sering munculnya ciphertext.
3. Terdapat keteraturan pada susunan plaintext, ciphertext ataupun kuncinya. Dalam setiap contoh pemecahan kode rahasia di atas, selalu menganggap terdapat keteraturan plaintext, misalnya susunan plaintext-nya beraturan dari “a” lalu “b” disusul “c” dan seterusnya. Keteraturan ciphertext yang juga mencerminkan keteraturan plaintext juga sangat membantu pemecahan kode rahasia ini.
4. Jumlah ciphertext-nya terlalu banyak. Yang dimaksud terlalu banyak di sini karena sampai menimbulkan perulangan, baik perulangan kunci, perulangan plaintext, maupun perulangan ciphertext. Bila jumlah ciphertext-nya sedikit sehingga tidak menimbulkan perulangan baik plaintext, ciphertext, kunci, maupun pola-pola keteraturannya, maka pemecahan kode tentu akan sangat sulit sekali. Namun apakah setiap pesan akan enkrip dengan sistem yang berbeda? Bagaimana bila memiliki 1000 pesan perbulan? Haruskah menciptakan puluhan macam sistem enkripsi baru setiap bulannya? Sebagai contoh, dalam perang dunia kedua, sebelum pasukan sekutu mendaratkan pasukan di Normandia Prancis pada tahun 1944, sebanyak 10 juta karakter cipher setiap hari dikirimkan sekutu bagi tentaranya. Namun cipher sekutu tidak berhasil dipecahkan Nazi Jerman.
5. Bila mengetahui bahasa penyusun plaintext-nya. Dalam perang dunia kedua, Amerika tidak menggunakan bahasa Inggris, melainkan menggunakan bahasa Navajo (bahasa Indian) untuk keperluan militernya, sehingga Jerman dan Jepang yang menjadi lawannya tidak mempunyai petunjuk apapun mengenai kode rahasia Amerika Serikat. Memang sejak lama, puluhan ribu bangsa Indian telah banyak ikut serta dalam tentara Amerika selama ratusan tahun. Mungkin juga bisa menggunakan bahasa penduduk pedalaman Irian Jaya atau dapat membuat bahasa baru khusus untuk kasus tertentusupaya komunikasi tidak dapat disadap orang lain. Atau siapa tahu Amerika telah memiliki daftar kata untuk seluruh macam sistem kriptografi yang pernah di kenal manusia dan untuk semua bahasa? Contoh bahasa navajo dapat dilihat pada lampiran E. Sebenarnya, penggunaan bahasa Navajo semacam ini serupa dengan penggunaan

enkripsi berlapis ganda. Hanya saja, sistem enkripsi dua lapis dianggap tidak meningkatkan keamanan, sehingga yang biasa digunakan adalah lapis tiga.

6. Kita mengetahui sistem enkripsi yang digunakan. Dalam kasus tertentu, penyembunyian algoritma enkripsi memang dapat meningkatkan keamanan sistem, namun itu bukan hal yang mutlak! Sebab dari ciphertext-nya analis sandi dapat memperkirakan sistem enkripsi yang digunakan. Demikian juga, analis kode rahasia tidak akan segan-segan membongkar algoritma enkripsi dari file exe-nya (file biner). Agar algoritma tidak dapat dilihat lawan, jangan sekali-kali mengimplementasikannya dengan perangkat lunak. Implementasikan ke dalam chip yang dibuat otomatis akan rusak bila ada yang membukanya. Dan jangan pernah membuat ciph tersebut dapat dibaca dari luar seperti data yang terdapat pada kartu SIM Gsm. Dan jangan percayakan pembuatan ciphnya kepada orang lain.
7. Jumlah kemungkinan terkaan yang mungkin terjadi, terbatas. Dalam artian, semua kemungkinan sistem enkripsi yang digunakan dapat dicoba. Apalagi dengan penggunaan komputer, hampir semua kemungkinan sistem yang dijelaskan pada bab sebelum ini, dapat dicoba oleh komputer dalam waktu singkat. Harus diingat, bahwa bila salah menerka sistem enkripsi yang digunakan, harus menggunakan perkiraan sistem yang lain. Dan ini tentunya mudah bila dilakukan dengan komputer. Bila dengan komputer pun diperlukan waktu satu tahun untuk memecahkan sandinya, sementara informasi hanya perlu diamankan selama 6 bulan, maka sistem aman. Dan bila sebaliknya, maka sistem tidak aman.

BAB IV

KESIMPULAN DAN SARAN

4.1 Kesimpulan

1. Membuat penyandi rahasia yang mampu mengatasi masalah-masalah di atas, maka kode akan lebih aman, namun ternyata dalam sistem yang sangat maju dan menggunakan komputer sekalipun, sangat sulit untuk mengatasi kelemahan-kelemahan tersebut.
2. Dalam sistem modern berbasis komputer, yang pengkodeannya berbasis bilangan biner, para ahli kriptografi mengikuti cara-cara klasik seperti di atas untuk memecahkan kode-kode rahasia. Misalnya mereka mencari hubungan antar kunci-kunci yang memberi efek keteraturan pada ciphertext-nya. Teknik ini disebut key-relation-attack. Teknik ini dapat dimanfaatkan untuk memecahkan kode rahasia meskipun kunci dibangkitkan dari sumber yang acak sekalipun! Mereka juga menggunakan perubahan plaintext untuk mencari keteraturan perubahan plaintext untuk menemukan kunci enkripsinya. Teknik ini disebut sebagai differential dan linear attack.

4.2 Saran

1. Patut dicontoh negara RRC yang tidak mau menggunakan windows 2000 untuk keperluan jaringan computer di tingkat pemerintahan, karena dengan mudah dapat disadap Amerika. Mereka menggunakan Linux yang open source, meskipun ini tidak otomatis menyelesaikan masalah. Sebab agar yakin akan keamanannya harus memeriksa jutaan baris kode program Linux sebelum menyatakan aman dari cacat keamanan yang disengaja maupun yang tidak disengaja.

DAFTAR PUSTAKA

- [1] Abdul Kadir, *Pengenalan Sistem Informasi*, Penerbit Andi Yogyakarta, 2002.
- [2] James E. Goldman, Cs., *Applied Data Communication*, John Willey & Son, INC., New York, 2001.
- [3] Tabratas Tharom, Dkk, *Mengenal Teknologi Informasi*, Elex Media Komputindo, Jakarta, 2002.
- [4] Suhono, *Pengantar Sistem Komunikasi Nirkabel*, Direktorat Jenderal Perguruan Tinggi, Jakarta, Oktober 2002.