BAB II

METODE KRIPTOGRAFI SIMETRIK

Seperti telah dijelaskan dalam bab sebelumnya mengenai pengelompokan metode-metode kriptograpfi, bahwa berdasarkan penggunaan kunci-nya metode kriptografi dapat dikategorikan dalam 2 kelompok yaitu : simetrik dan asimetrik. Metode kriptografi simetrik juga sering disebut metode konvensional adalah metode kriptografi yang menggunakan kunci yang sama dalam proses enkripsi dan dekripsinya, dengan kata lain kunci yang digunakan oleh pengrim dalam melakukan enkripsi dan kunci yang digunakan untuk men-dekripsi oleh penerima adalah sama / simetrik.
Tidak semua metode kriptografi semitrik yang ada, akan dibahas / dijelaskan dalam tulisan ini.

A. Caecar Cipher

Diperkenalkan pertama kali 2000 tahun yang lalu oleh Julius Caecar, sehingga dikenal dengan Caecar cipher. Metode ini menggunakan penggeseran sederhana, sehingga metode ini tergolong dalam kelompok metode *stream*.

Algoritma dasar dari metode ini sangat simple, setiap kunci diganti dengan huruf ketiga setelah kunci yang bersangkutan.
misalnya kita miliki *plaintext* seperti berikut :

```
I CAME I SAW I CONQUERED
```

maka kalau kita enkripsikan dengan metode ini, didapatkan cipherteksnya adalah

```
L FDPH L VDZ L FRQTXHUHG
```

atau secara umum substitusi tersebut dapat digambarkan seperti berikut :

Plain : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher : DEFGHIJKLMNOPQRSTUVWXYZABC

Secara Umum Caecar Cipher dapat didefinisikan

Jika A suatu nilai ke 0, B 1, C 2,…Y24 dan Z 25

Maka enkripsi dapat dikodekan dengan

E_k:i → i+k (mod 26)

Dan dekripsi

D_k:i → i-k (mod 26)

Walaupun dalam algoritma ini setiap kunci disubstitusi / digantikan oleh kunci ke-3 setelah kunci yang bersangkutan, namun setiap algoritma enkripsi yang dilakukan dengan mengganti kunci ke-x dengan kunci ke-x+n (baik nilai n positif maupun negatif) termasuk atau dapat digolongkan dalam metode enkripsi Caecar cipher.

Caesar chiper juga tergolong dalam substitution chipers karena setiap huruf digantikan dengan sebuah huruf. Huruf yang sama akan enkripsi memiliki pengganti yang sama. Misalnya huruf “A” digantikan dengan huruf E, maka setiap huruf “A” akab digantikan dengan huruf “E” . Monoalphabetic Chiper ini agak mudah dipecahkan dengan menganalisa chipertext apabila beberapa informasi lain (seperti bahasa yang digunakan) dapat diketahui.

Cara penyerangan Caesar Chiper yang pertama kali mungkin dilakukan adalah dengan cara exhaustive key search yaitu dengan cara menggeser satu persatu dari huruf chipertextnya, misalnya dipunyai chipertext.

Kita ambil sebagian kalimat dari baris pertama :

RIWHQZKHQBRXKDYHDQHQFUBSWHGPH (chipertext asli)

QHVGPYJGPAQ, dengan mencoba menggeser satu huruf, kalimat ini belum bermakna.

PGUFOXIFOZP, dengan menggeser dua huruf kalimat ini juga belum bisa dibaca.

OFTENWHEN, dengan menggeser tiga huruf kalimat ini sudah mempunyai makna.

Bila semua baris kalimat kita geser tiga maka secara lengkap akan didapat :

OFTEN WHEN YOU HAVE AN ENCRYPTED MESSAGE STATISTICAL PROPERTIES CAN BE MEASURED AND UTILIZED TO HELP DECRYPT THE MESSAGE THERE ARE MANY DIFFERENT PROPERTIES WHICH CAN BE USED FOR THIS PURPOSE ONE SUCH STATISTIC IS THE TABLE OF FREQUENCY COUNTS OF THE ENCRYPTED MESSAGE

Dari cara diatas hanya diperlukan 3 kali pergeseran untuk mendapatkan plaintext dari Caesar Chiper, atau secara matematis dapat dituliskan $P = C - 3 \pmod{26}$

Salah satu cara penyerangan (*attack*) yang lain dapat dilakukan adalah dengan menganalisa statistik dari banyaknya huruf yang sering muncul (frekuensi). Cara ini disebut frequency analysis. Dalam bahasa Inggris menunjukkan bahwa huruf yang sering muncul adalah "E" . Frequency analysis akan banyak bermanfaat bila chipertext yang ada cukup panjang. Chipertext yang pendek mempunyai jumlah huruf yang sedikit sehungga frekuensi kemunculan huruf menjadi makin merata, disini dapat terjadi bias dengan data-data statistik munculnya huruf. Selain itu ada beberapa kasus dimana sengaja dibuat teks yang "merusak" struktur frekuensi tersebut. Jadi misalkan dengan menggunakan caesar chiper jika pesan dalam bahasa Inggris dibuat sebagaimana mungkin menggunakan pesan yang tanpa menggunakan huruf "E". Meskipun banyak usaha dilakukan untuk mempersulit frequency analysis, caesar chiper relatif tetap mudah dipecahkan.

Chipertext

```
RIWHQZKHQBRXKDYHDQHQFUBSWHGPHVVDJHVWDWLVWLFDOSURSHU
WLHVFDQEHPHDVXUHGQGXWLOLCHGWRKHOSGHFUBSWWKHPHVVDJ
HWKHUHDUHPDQBGLIIHUHQWSURSHUWLHVZKLFKFDQEHXVHGIRUWK
LVSXUSRVHRQHVXFKVWDWLVWLFLVWKHWDEOHRIIUHTXHQFBFRXQW
VRIWKHHQFUBSWHGPHVVDJH
```

Dari chipertext dapat dilihat frekuensi kemunculannya yaitu :

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	6	1	15	3	11	8	38	7	3	11	12	0	0	4	5	13	11	10	1	14	19	22	8	1	2

Sehingga dapat dibuat grafik sebagai berikut :

Dari data diatas dapat dilihat bahwa H mempunyai kemunculan dalam chipertext sebanyak 38 kali, sedang data statistik kemunculan karakter dalam bahasa Inggris adalah sebagai berikut :

A	B	C	D	E	F	G	H	I	J	K	L
7.25	1.25	3.5	4.25	12.75	3	2	3.5	7.75	0.25	0.5	3.75

M	N	O	P	Q	R	S	T	U	V	W	X
2.75	7.75	7.50	2.75	0.5	8.5	6.9	9.25	3	1.5	1.50	0.5

Y	Z
2.25	0.25

Atau jika dibawa ke bentuk grafik adalah sebagai berikut :

Dari data diatas dapat dilihat bahwa karakter yang paling sering muncul adalah E = 12,75% kemudian T = 9,25% dan bila dipetakan dengan data statistik dan grafik maka terlihat bahwa dalam chipertext grafik DEF akan terlihat mirip dengan grafik ABC dan grafik GJI mirip dengan grafik DEF. Maka ditambah dengan informasi lain yaitu kecenderungan muncul huruf pasangan dalam bahasa Inggris maka chipertext ini mudah untuk dipecahkan.

Kecenderungan untuk karakter dalam bahasa Inggris yang sering muncul adalah : Untuk dua karakter (diagram) maka probabilitas kemunculan adalah 3 (dalam skala 1 sampai 10).

Digram	TH	HE	I	ER	RE
Frekuensi	10	9.5	7.17	6.65	5.92
Digram	ON	AN	EN	AT	ES
Frekuensi	5.70	5.63	4.76	4.72	4.24
Digram	ED	TE	TI	OR	ST
Frekuensi	4.12	4.04	4.00	3.98	3.81

Digram	AR	ND	TO	NT	IS
Frekuensi	3.54	3.52	3.50	3.44	3.43
Digram	OF	IT	AL	AS	HA
Frekuensi	3.38	3.26	3.15	3.00	3.00
Digram	NG	CO	SE	ME	DE
Frekuensi	2.92	2.80	2.75	2.65	2.65

Sedang untuk trigram pasangan huruf yang sering muncul adalah THE, AND, TIO, ATI, FOR, THA.

Dari tambahan informasi tersebut terlihat bahwa WHK --- THE , maka dapat dicoba-coba untuk kemungkinan-kemungkinan pasangan karakter diatas. Dengan cara ini caesar chiper masih cukup mudah dipecahkan.

Latihan :

1. Tentukan cipher text dari plain text berikut :

   FAKULTAS TEKNOLOGI INDUTRI

   dengan : kunci ke-x disubstitusi oleh kunci ke-x+5

2. Tentukan plaintext dari ciphertext berikut :

   Cipher: NQTAJDTZAJWDRZHM

B. Fixed Monoalphabethic cipher

Monoalphbetic diperkenalkan oleh ilmuwan Arab, Abu Alkindi dalam bukunya ‘A Manuscript on Deciphering Cryptographic Messages’ yang dipublikasikan pada abad ke-9. Monoalphabetic cipher telah dipergunakan dalam bidang pemerintahan dan militer dalam beberapa abad silam.

Metode ini juga sering dikenal dengan mixed Monoalphabethic cipher. Metode ini lebih dari sekedar penggeseran dalam alphabetic. Dalam metode ini setiap kunci dapat disubstitusi dengan sembarang kunci secara acak dalam batasan 26 huruf dalam alphabet.

Monoalphabetic chiper merupakan algoritma yang menggantikan huruf yang digunakan untuk mengirim pesan dengan huruf lain dengan korespodensi satu-satu atau satu huruf tepat digantikan dengan satu huruf lain.

contoh :

Plain : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher : DKVQFIBJWPESCXHTMYAUOLRGZN

maka jika dilakukan enkripsi dengan metode tersebut

Plainteks : IF WE WISH TO REPLACE LETTERS
cipherteks : WI RF RWAJ UH FYTSDVF SFUUFYA

C. Easier Monoalphabethic cipher

Metode ini sesuai dengan namanya tentu saja tidak jauh berbeda dengan metode sebelumnya, mixed monoalphabetic. Dalam mixed monoalphabetic kata kunci ditentukan sebanyak 26 huruf yang acak, tentu saja sederet kata kunci 26 huruf tersebut sulit untuk dihafal urutannya, maka dalam easier ini kata kunci (*keyword*) hanya menggunakan suatu kata atau sekelompok kata, kemudian dihilangkan / dihapus huruf yang sama dalam kata kunci tersebut dan kemudian untuk huruf berikutnya

diteruskan dengan huruf terakhir dalam kata kunci tersebut dan seterusnya secara urut dalam 26 alphabet.

Contoh

1. Diberikan kata kunci : SISTEM BERKAS

Plain : ABCDEFGHIJKLMNOPQRSTUVWXYZ
cipher : SITEMBRKACDFGHJLNOPQUVWXYZ

maka jika dengan metode tersebut dilakukan enkripsi

Plainteks : TEKNOLOGI INDUSTRI
cipherteks : QMDHJFJRA AHEUPQOA

2. kata kunci : CHIPER TEXT

Plain : ABCDEFGHIJKLMNOPQRSTUVWXYZ
cipher : CHIPERTXYZABDFGJKLMNOQSUVW

maka hasil enkripsi dari : TEKNOLOGI INDUSTRI

Plainteks : TEKNOLOGI INDUSTRI
cipherteks : NEAFGBGTY YFPOMNLY

D. General Monoalphabetic

Metode ini masih setipe dengan 2 metode monoalphabetic sebelumnya. Perbedaan dengan *mixed monoalphabetic*, dalam *mixed* kata kunci menggunakan rangkaian 26 alphatic secara acak yang sulit dihafal. Perbedaan dengan *easier,* pada *general*

spesifikasi enkripsi ditentukan oleh perulangan pada posisi kolom yang bersesuain dengan jumlah alphabet yang berbeda dalam kata kunci.

Contoh

Diberikan suatu kata kunci : STARWARS

Maka alphabet yang sama dihapus : STARW

Lakukan dengan pengulangan kolom untuk huruf lain dalam 26 alphabet :

```
STARW
BCDEF
GHIJK
LMNOP
QUVXY
Z
```

Kemudian dibaca secara kolom, maka didapatkan translasi seperti berikut

```
Plain   : ABCDEFGHIJKLMNOPQRSTUVWXYZ
cipher  : SBGLQZTCHMUADINVREJOXWFKPY
```

maka jika digunakan untuk melakukan enkripsi / dekripsi :

```
Plain   : I KNOW ONLY THAT I KNOW NOTHING
cipher  : H UINF NIAP OCSO H UINF INOCHIT
```

Latihan

1. dekripsikan cipherteks berikut : DQITSVSUNDQIGHIOSHUXLHU
   menggunakan kata kunci STARWARS

2. enkrispsikan plainteks berikut, dengan kata kunci ‘ENTROPY’
   TAK ADA PROBLEM YANG TAK BISA DISELESAIKAN