ENKRIPSI DAN DEKRIPSI (I)

MATERI

1. Penyadi monoalfabetik
2. Penyandi polialfabetik
3. Penggunaan public key

Setiap orang yang bermaksud menyimpan sesuatu secara pribadi, akan melakukan segala cara untuk menyembunyikannya, sehingga orang lain tidak tahu. Contoh sederhana, ketika kita mengirim surat kepada seseorang, maka kita membungkus surat tersebut dengan amplop agar tidak terbaca oleh orang lain. Untuk menambah kerahasiaan surat tersebut agar tetap tidak dibaca orang dengan mudah apabila amplop dibuka, maka kita mengupayakan untuk membuat mekanisme tertentu agar isi surat tidak secara mudah dipahami.

Salah satu hal yang penting dalam komunikasi menggunakan computer untuk menjamin kerahasiaan data adalah **Enkripsi**. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau *chiper*. Sebuah system pengkodean menggunakan suatu *table* atau kamus yang telah didefinisikan untuk mengganti kata dari informasi atau yang merupakan bagian dari informasi yang dikirim. Sebuah chiper mengunakan suatu algoritma yang dapat mengkodekan semua aliran data (stream) bit dari sebuah pesan menjadi *cryptogram* yang tidak dimengerti (unintelligible). Karena teknik chiper merupakan suatu system yang telah siap untuk di automasi, maka teknik ini digunakan dalam system keamanan computer dan jaringan.

Enkripsi dimaksudkan untuk melindungi informasi agar tidak terlihat oleh orang atau pihak yang tidak berhak. Informasi ini

dapat berupa nomor kartu kredit, catatan penting dalam komputer, maupun password untuk mengakses sesuatu.

Masalah kerahasiaan ini sudah ada jauh sebelum adanya computer. Julius Caesar, yang khawatir jangan sampai pesan untuk para jenderalnya jatuh ke tangan musuh, maka ia menggunakan metode enkripsi sederhana dengan menggeser huruf pada abjad dengan nilai tertentu. Sederhana memang, namun pada waktu itu sudah memadai.

Sepanjang sejarah pembentukan kode dan pemecahannya selalu mendapat perhatian khusus dalam operasi militer. Penggunaan computer untuk pertama kalinya dalam kriptografi merupakan usaha untuk memecahkan kode enigma Nazi sewaktu Perang Dunia II.

Kini, pada zaman modern, adanya computer memungkinkan kita menghasilkan kode yang kompleks, dan sebaliknya pula dapat digunakan untuk memecahkannya.

E-commerce adalah industri lain yang sangat intensif memanfaatkan kriptografi. Dengan meng-enkrip paket data yang lalu lalang di internet, walaupun seseorang dapat menangkap paket-paket data tersebut, tetap saja ia tidak dapat memahami artinya.

Enkripsi juga digunakan untuk verifikasi, maksudnya bila mendownload software, kita akan tahu bahwa software yang kita download adalah yang asli, bukannya yang telah dipasangkan Trojan di dalamnya.

Dalam hal ini terdapat tiga kategori enkripsi, yaitu :

1. Kunci enkripsi rahasia, artinya terdapat sebuah kunci yang digunakan untuk mengenkripsi dan juga sekaligus mendekripsikan informasi

2. Kunci enkripsi public, artinya dua kunci digunakan satu untuk proses enkripsi dan yang lain untuk proses dekripsi.
3. Fungsi one-way, atau fungsi satu arah adalah suatu fungsi dimana informasi dienkripsi untuk menciptakan “signature” dari informasi asli yang bisa digunakan untuk keperluan autentikasi.

Salah satu masalah dalam mengamankan enkripsi secara public adalah bagaimana memastikan bahwa hanya sang penerima yang dapat mengakses data. Jika kita dapat mengunci data dan mengirimkannya bersama kuncinya ke alamat tujuan, tetapi bagaimana memastikan kunci itu tidak dicuri orang di tengah jalan? Salah satu cara untuk memecahkannya adalah bahwa penerima yang mengirimkan kuncinya, tetapi pengirim tidak mengirimkan kuncinya. Si pengirim mengunci data dengan gembok yang dikirim oleh si penerima dan mengirimkannya kembali kepada si penerima. Si penerima kemudian akan membukanya dengan kunci miliknya yang tidak pernah dikirimkannya ke siapa-siapa. Jika data yang digembok itu dicuri orang, maka dengan enkripsi yang kompleks akan sangat sulit bagi orang itu untuk mengakses data yang sudah digembok itu.

Enkripsi dibentuk berdasarkan suatu algoritma yang akan mengacak suatu informasi menjadi bentuk yang tidak bisa dibaca atau tidak bisa dilihat. Dekripsi adalah proses dengan algoritma yang sama untuk mengembalikan informasi teracak menjadi bentuk aslinya. Metode enkripsi yang lebih umum adalah menggunakan sebuah algoritma dan sebuah kunci. Kunci harus diletakkan terpisah dari pesan yang terenkripsi dan dikirimkan secara rahasia. Teknik semacam ini disebut sebagai symmetric (single key) atau secret key cryptography. Selanjutnya, akan muncul permasalahan kedua, yaitu bagaimana mengirim kunci tersebut agar kerahasiaannya terjamin. Karena, jika kunci dapat diketahui oleh seseorang maka orang tersebut dapat membongkar pesan yang kita kirim.

MODEL-MODEL ENKRIPSI

Dalam membahas model-model enkripsi beserta algoritma yang akan dipakai untuk setiap enkripsi ada 2 hal yang penting yang akan dijabarkan, yaitu enkripsi dengan kunci pribadi dan enkripsi dengan kunci publik.

ENKRIPSI DENGAN KUNCI PRIBADI

Enkripsi dapat dilakukan jika si pengirim dan si penerima telah sepakat untuk menggunakan metode enkripsi atau kunci enkripsi tertentu. Metode enkripsi atau kuncinya ini harus dijaga ketat supaya tidak ada pihak luar yang mengetahuinya. Masalahnya sekarang adalah bagaimana untuk memberi tahu pihak penerima mengenai metode atau kunci yang akan kita pakai sebelum komunikasi yang aman bisa berlangsung. Kesepakatan cara enkripsi atau kunci dalam enkripsi ini bisa dicapai lewat jalur komunikasi lain yang lebih aman, misalnya dengan bertemu langsung. Tetapi, bagaimana jika jalur komunikasi yang lebh aman ini tidak memungkinkan ? Yang jelas, kunci ini tidak bisa dikirim lewat jalur E-mail biasa karena masalah keamanan.

Cara enkripsi dengan kesepakatan atau kunci enkripsi di atas dikenal dengan istilah enkripsi dengan kunci pribadi, karena cara enkripsi atau kunci yang hanya boleh diketahui oleh dua pribadi yang berkomunikasi tersebut. Cara enkripsi inilah yang umum digunakan pada saat ini baik untuk kalangan pemerintah maupun kalangan bisnis. Cara enkripsi ini juga dikategorikan sebagai kriptografi simetris, karena kedua belah pihak mengetahui kunci yang sama. Selain masalah komunikasi awal untuk penyampaian kunci, cara enkripsi ini juga mempunyai kelemahan yang lain. Kelemahan ini timbul jika terdapat banyak orang yang ingin saling berkomunikasi. Karena setiap pasangan harus sepakat dengan

kunci pribadi tertentu, tiap orang harus menghafal banyak kunci dan harus menggunakannya secara tepat. Sebab, jika tidak maka si penerima tidak bisa mengartikannya.

Jika diformulasikan, jika ada N orang yang ingin saling berkomunikasi dengan cara enkripsi ini, maka total jumlah kunci yang beredar :

$$N * (N - 1) / 2$$

Hal ini akan menimbulkan masalah dalam pengaturan sebuah kunci. Misalnya, kunci yang mana yang akan dipakai untuk mengirim ke A.

Ada beberapa model enkripsi yang termasuk golongan ini :

- Simple Substituton Cipher
- DES
- Triple DES
- Rivest Code (RC2)
- Rivest Code 4 (RC4)
- IDEA
- Skipjack
- Caesar Cipher
- Gost Block Cipher
- Letter Map
- Transposition Cipher
- Blowfish
- Vigenere Cipher
- Enigma Cipher

Simple Substituton Cipher

Adalah sebuah kondisi dimana masing-masing huruf dari sebuah plaintext diganti oleh symbol yang lain. Biasanya yang digunakan daam penggantian symbol ini adalah huruf-huruf dari sederetan alphabet.

Substitusi sederhana adalah dimana dalam pesan, symbol plaintext selalu diganti dengan symbol ciphertext yang sama. Dengan kata lain, terjadi hubungan satu persatu di antara huruf-huruf dalam ciphertext maupun plaintext.

Meskipun ada 26 cara alphabet ciphertext yang mungkin, semua pihak tahu bahwa cipher substitusi yang sederhana ini secara relative mudah dapat memecah sandi dengan analisis frekuensi huruf dan menebak kata-kata yang sering dipakai.

Contoh ada pesan dalam bahasa Inggris:
TK IL KQ JKT TK IL TBST CR TBL OULRTCKJ

9 huruf yang paling seriang dipakai dalam bahasa Inggris adalah E, T, N. A, O, R, I, S, dan H. 5 huruf yang kurang sering muncul adalah J, K, Q, X, dan Z.

2 huruf yang paling sering muncul dalam bahasa Inggris adalah :
OF TO IN IS IT BE BY HE AS ON AT OR AN SO IF NO

Krn ada kata-kata dalam 2 huruf dalam pesan tersebut, diasumsikan K=O, sehingga ;
-O - - O- -O- -O - - - - - - - - - - - - - - - - - - O –
T=T, sehingga
TO - - O- -OT TO - - T- - T - - T - - - - - - T - O –

3 huruf dalam alphabet Inggris yang sering diawali dengan T adalah THE, sehingga : B=H , L=E; maka diperoleh :
TO – E O - -OT TO –E TH-T - - THE - - E – T – O –
Terlihat pola TH-T = THAT , pola –OT = NOT, maka J=N, S=A,
TO –E O- NOT TO –E THAT - - THE - - E - T- ON
Pola T-ON=TION, maka C=I
TO –E O- NOT TO –E THAT I- THE - - E – TION

Setelah kita substitusi terakhir, maka diperoleh pesan :
TO BE OR NOT TO BE THAT IS THE QUESTION

Caesar Cipher

Caesar cipher adalah cipher pergeseran karena alphabet ciphertext diambil dari alphabet plaintext dengan menggeser masing-masing huruf dengan jumlah tertentu.

Vigenere Cipher

Merupakan pengembangan dari Caesar cipher dimana dasar dari algoritma ini adalah beberapa huruf dari kata kunci yang diambil dari pergeseran yang dilakukan oleh Caesar cipher.

Metode ini menggunakan polyalphabetic substitution cipher yang melibatkan penggunaan 2 atau lebih cipher alphabet, hal ini untuk membuat cipher lebih aman.

Vigenere cipher pertama kali diusulkan oleh Blaise de Vigenere dari pengadilan Henry III di Perancis pada abad 16, dimana usul tadi berupa polyalphabetic substitution berdasarkan pada table berikut 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
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		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

Tabel Vigenere

Masing-masing baris dalam table berhubungan dengan Caesar cipher.

Contoh : TO BE OR NOT TO BE THAT IS THE QUESTION
Kata kunci:RELAT IONSR ELATI ONSRE LATIONSREL
Plaintext : TOBEO RNOTT OBETH ATIST HEQUESTION
Ciphertext:KSMEH ZBBLK SMEMP OGAJX SEJCSFLZSY

Kekuatan vigenere cipher terhadap analisis frekuensi dapat dilihat dengan menguji ciphertext di atas. Dari analisis di atas, pesan yang telah dienkrip dengan menggunakan vigenere cipher adalah kumpulan banyak cipher yang digunakan untuk mengganti huruf-huruf yang ada dalam kata kunci.

Variasi dari vigenere cipher adalah gronsfeld cipher. Gronsfeld cipher menggunakan digit dari angka yang terdapat pada kata kunci, bukan dari huruf-huruf yang terdapat pada kunci-kunci.

MEMECAHKAN VIGENERE CHIPER : METODE KASISKI / KERCHOFF

Vigenere yang seperti substitution cipher dianggap oleh banyak orang secara praktis tidak apat dipecahkan selama 300 tahun. Pada tahun 1863 Mayor Prussian bernama Kasiski mengusulkan metode untuk memecahkan vigenere cipher, yang terdiri dari penemuan tentang panjang kata kunci dan kemudian membagi pesan tersebut dalam banyak cryptogram substitusi yang baru.

Analisis frekuensi ini kemudian dapat digunakan untuk memecahkan hasil substitusi yang sederhana.

Teknik Kasiski dipakai untuk menemukan panjang kata kunci berdasarkan pengukuran jarak diantara bigrams yang diulang dengan ciphertext

Contoh:

Posisi	:	01234	56789	01234	56789	01234	56789
Key	:	RELAT	IONSR	ELATI	ONSRE	LATIO	NSREL
Plaintext	:	TOBEO	RNOTT	OBETH	ATIST	HEQUE	STION
Cipher	:	KSMEH	ZBBLK	SMEMP	OGAJX	SEJCS	FLZSY

Dengan metode Kasiski akan tercipta sesuatu seperti berikut :

Repeated Bigram	Location	Distance	Factors
KS	9	9	3, 9
SM	10	9	3, 9
ME	11	9	3, 9

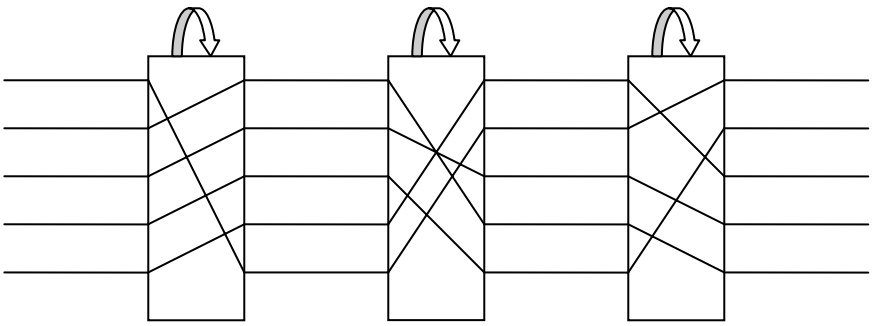
Memfaktorkan jarak di antara bigram terulang adalah cara mengidentifikasikan panjang ikatan kunci yang mungkin dengan factor-faktor tersebut yang terjadi paling sering akan menjadi kandidat yang paling bagus untuk panjang ikatan kunci.

Dalam contoh di atas, 3 adalah factor dari 9 dan angka 3 dan 9 ini akan menjadi kandidat ang layak untuk panjang kata kunci.

Enigma Cipher

Adalah suatu metode yang terkenal untuk kontribusinya pada waktu Perang Dunia II bagi pihak Jerman.

Waktu itu dikembangkan sesuatu model yang disebut dengan mesin Enigma. Mesin ini didasarkan pada system 3 rotor yang menggantikan huruf dalam ciphertext dengan huruf dalam plaintext. Rotor itu akan berputar dan menghasilkan hubungan antara huruf yang satu dengan huruf yang lain, sehingga menampilkan berbagai substitusi seperti pergeseran Caesar.



Enigma Machine

Letter Map

Standar Letter Map menggunakan table korespodensi yang dipilih secara sembarang.

Contoh :

Huruf asli : a b c d e f g h i j …..

Huruf sandi : q w e r t y u i o p ….

Transposition Cipher

Standar transposition cipher menggunakan huruf kunci yang diberi nama dan nomor kolom sesuai dengan urutan huruf pada huruf kunci tersebut.

Contoh :

Kata Kunci : WAHANA

No.kolom : 163425

Plaintext : naskah buku segera dikirimkan sebelum deadline

W	A	H	A	N	A
1	6	3	4	2	5
n	a	s	k	a	h
b	u	k	u	s	e
g	e	r	a	d	I
k	i	r	i	m	k
a	n	s	e	b	e
l	u	m	d	e	a
d	l	i	n	e	

Ciphertext : nbgkald asdmbee skrrsmi kuaiedn heiakea aueinul