

MANAJEMEN TEKNOLOGI INFORMASI

ENKRIPSI



OLEH :

- 1. Aulya Suryana (040010245)**
- 2. Dewi Santi Santoso (040010255)**
- 3. I Gede Arya Wiryadi (070010434)**
- 4. Fenny Sukanto (070010518)**

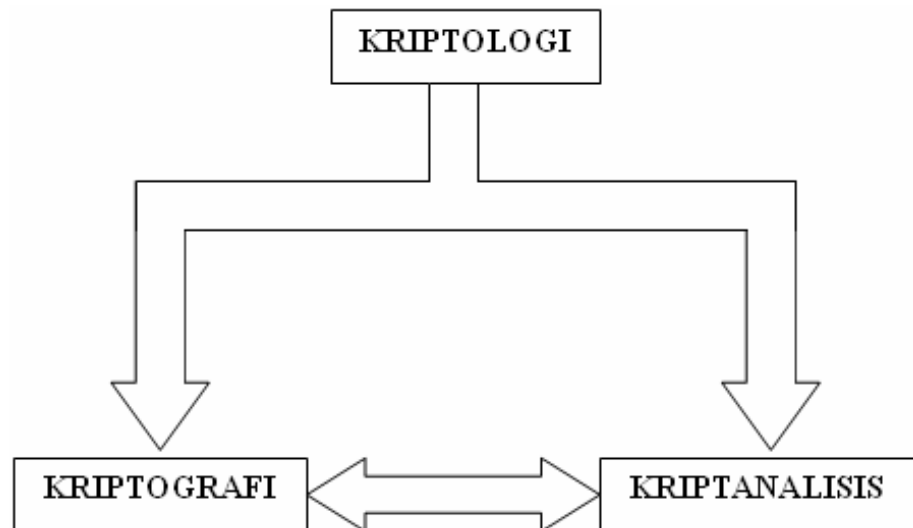
**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN TEKNIK KOMPUTER
(STMIK) – STIKOM BALI**

2007

ENKRIPSI

1. PENGERTIAN

Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Pengetahuan yang mempelajari tentang enkripsi adalah kriptografi. Yang dimaksud dengan kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Namun, tidak semua aspek keamanan informasi ditangani oleh kriptografi. Enkripsi erat kaitannya dengan dekripsi, untuk itulah muncul istilah kriptanalisis. Kriptanalisis adalah ilmu dan seni untuk memecahkan informasi yang telah dienkripsi tanpa mengetahui kunci yang digunakan. Pelaku kriptanalisis disebut dengan kriptanalis.



Gambar 1.1 Pohon kriptologi

2. TUJUAN

Enkripsi merupakan upaya untuk mengamankan data/informasi, meskipun bukan merupakan satu-satunya cara untuk mengamankan data/informasi. Adapun tujuan dari enkripsi adalah sebagai berikut:

a. Kerahasiaan

Yaitu untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah dienkripsi.

b. Integritas data

Untuk menjaga keaslian/keutuhan data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

c. Autentikasi

Ini berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.

d. Non-repudiasi/Nirpenyangkalan

Adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

3. KARAKTERISTIK

Terdapat beberapa cara untuk melakukan enkripsi, yaitu:

a. Symmetric Encryption

Algoritma ini menggunakan sebuah kunci rahasia yang sama (*private key*) untuk melakukan proses enkripsi dan dekripsinya. Algoritma ini memiliki kelemahan dan kelebihan seperti di bawah ini:

Kelemahan :

- Kunci harus dikirim melalui saluran yang aman. Kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci ini.
- Kunci harus sering diubah, mungkin pada setiap sesi komunikasi.

Kelebihan :

- Algoritma ini dirancang sehingga proses enkripsi/dekripsi membutuhkan waktu yang singkat.
- Ukuran kunci relatif lebih pendek.
- Algoritmanya bisa menghasilkan *cipher* yang lebih kuat.
- Autentikasi pengiriman pesan langsung diketahui dari *ciphertext* yang diterima, karena kunci hanya diketahui oleh pengirim dan penerima pesan saja.

Algoritma ini termasuk dalam algoritma kriptografi klasik yang terdiri dari *substitution cipher* dan *transposition cipher*. Berikut adalah penjelasan dari masing – masing *cipher*:

➤ Substitution Cipher

Cara kerja dari algoritma ini adalah dengan menggantikan setiap karakter dari *plaintext* dengan karakter lain.

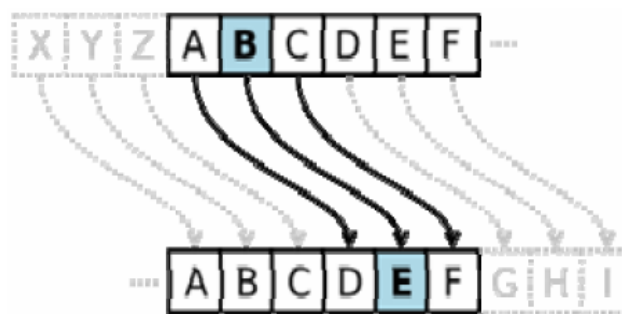
Berikut adalah beberapa contoh penerapan algoritma substitusi:

- **Caesar Cipher**

Algoritma ini pertama kali digunakan oleh *Julius Caesar*, dan disebut juga sebagai *Shift Cipher*, yaitu dengan cara menggeser urutan abjadnya.

→ *Plaintext*: ABCDEFGHIJKLMNOPQRSTUVWXYZ

→ *Cipher*: DEFGHIJKLMNOPQRSTUVWXYZABC



Gambar 3.1 Algoritma Caesar Cipher

Contoh kasus:

Sebuah *cipher* menggunakan algoritma *Caesar Cipher* terdiri dari kata – kata berikut ini :

exxegoexsrgi

Untuk memecahkan kode tersebut, maka kita dapat mencobanya dengan menggesernya sebanyak 25 kali.

Penggeseran	<i>Plaintext</i>
0	exxegoexsrgi
1	dwwdfndwrqfh
2	cvvcemcvqpeg
3	buubdlbupodf
4	attackatonce
5	zsszbjzsnmbd
6	yrryaiyrmlac
...	
23	haahjrhavujl
24	gzzgiqgzutik
25	fyfhpfytshj

Hasil dekripsi

Tabel 3.1 Dekripsi Caesar Cipher

- **Vigenere Cipher**

Vigenere Cipher ditemukan oleh Blaise de Vigenere pada abad ke 16. Untuk menggunakan algoritma ini, maka diperlukan sebuah bujursangkar *vigenere* dimana kolom paling kiri bujursangkar menyatakan huruf-huruf kunci, sedangkan baris paling atas menyatakan huruf-huruf *plaintext* dan setiap baris di dalam bujursangkar menyatakan huruf-huruf *ciphertext*.

	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	S	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

Gambar 3.2 Bujursangkar Vigenere

Contoh:

→ *Plaintext*: ATTACKATDAWN

Maka, kita harus menentukan kata kuncinya. Apabila kata kunci yang digunakan lebih pendek dari panjang *plaintext* maka kata kunci diulang (sistem periodik) seperti berikut:

Panjang *plaintext*: 12 huruf

Kata kunci: LEMON (5 huruf)

Kata kunci: LEMONLEMONLE (12 huruf)

Huruf pertama dari *plaintext* adalah A, dienskripsi dengan menggunakan alfabet pada baris L, yang merupakan huruf pertama pada kata kunci. Ini dilakukan dengan melihat huruf yang terdapat pada baris L dan kolom A pada tabel *vigenere*, yaitu huruf L. Untuk huruf kedua pada *plaintext*, kita menggunakan huruf kedua pada kata kunci, yaitu pada baris E dan kolom T, yaitu huruf X. Lakukan terus hingga huruf terakhir *plaintext* sehingga menghasilkan enkripsi sebagai berikut:

→ *Ciphertext*: LXFOPVEFRNHR

Dekripsi dilakukan dengan cara sebaliknya. Misalkan untuk huruf pertama *ciphertext*, L, kita cari huruf pertama kata kunci pada baris L, dimana huruf pertama kata kunci juga merupakan huruf L. Kemudian kita dapat menemukan pada baris L, huruf L terdapat pada kolom A, yang mengartikan bahwa huruf A merupakan huruf pertama *plaintext*. Lakukan terus hingga jumlah huruf pada kata kunci habis.

➤ **Transposition Cipher**

Algoritma ini diperoleh dengan mengubah posisi *plaintext*nya. Dengan kata lain, algoritma ini melakukan *transpose* terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah **permutasi**, karena *transpose* setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.

Contoh:

<i>Plaintext</i>	:	TECHNOLOGY(10 huruf)
Kunci	:	(10/5=2)
Enkripsi	:	TECHN OLOGY
<i>Ciphertext</i>	:	TOELCOHGNY

Untuk membacanya, maka *ciphertext* dibaca berurutan dengan menggunakan kunci 2, yaitu dengan bergeser sebanyak 2 huruf.

➤ **Block Cipher**

Block Cipher adalah algoritma enkripsi yang akan membagi-bagi *plaintext* yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t , dan setiap blok dienkripsi dengan menggunakan kunci yang sama. Pada umumnya, *block cipher* memproses *plaintext* dengan blok yang relatif panjang lebih dari 64 bit, untuk mempersulit penggunaan pola-pola serangan yang ada untuk membongkar kunci.

Untuk menambah kehandalan algoritma ini, dikembangkan pula beberapa tipe proses enkripsi, yaitu :

- ECB (*Electronic Code Book*)
- CBC (*Cipher Block Chaining*)
- OFB (*Output Feed Back*)
- CFB (*Cipher Feed Back*)

➤ **Stream Cipher**

Stream Cipher adalah algoritma enkripsi yang mengenkripsi data persatuan data, seperti bit, byte, nibble atau per 5 bit. Setiap mengenkripsi satu satuan data digunakan kunci yang merupakan hasil pembangkitan dari kunci sebelumnya.

b. Asymmetric Encryption

Sedangkan pada sistem kunci-asimetris digunakan sepasang kunci yang berbeda, umumnya disebut kunci public (*public key*) dan kunci pribadi (*private key*), digunakan untuk proses enkripsi dan proses dekripsinya. Bila *plaintext* dienkripsi dengan menggunakan kunci pribadi maka *ciphertext* yang dihasilkannya hanya bisa didekripsikan dengan menggunakan pasangan kunci pribadinya. Begitu juga sebaliknya, jika kunci pribadi digunakan untuk proses enkripsi maka proses dekripsi harus menggunakan kunci publik pasangannya. Contohnya adalah Knapsack, RSA (Rivert-Shamir-Adelman), Diffie-Hellman.

Asymmetric Encryption memiliki kelemahan dan kelebihan sebagai berikut:

Kelebihan:

- Hanya *Private key* yang harus benar-benar rahasia/aman.
- Sangat jarang untuk perlu merubah *public key* dan *private key*.

Kelemahan:

- Ukuran kunci lebih besar dari pada *symmetric encryption*.
- Tidak adanya jaminan bahwa *public key* benar-benar aman.

c. Fungsi Hash

Fungsi *hash* ini sering juga disebut sebagai fungsi *hash* kriptografis, yaitu fungsi yang secara efisien mengubah *string input* dengan panjang berhingga menjadi *string output* dengan panjang tetap yang disebut nilai *hash*. Fungsi ini bersifat satu arah sehingga inputan yang telah dienkripsi tidak dapat dibalikkan atau didekripsikan. Contohnya adalah penggunaan MD5 untuk melindungi *password*.

```
$querySimpan = "insert into member values ('$username',md5('$password'),'&status','$nama','$email','$gender',
'$tgl_lahir','$city','$state','$country')";
```

Gambar 3.3 Contoh query SQL untuk mengenkripsi password

	username	password	status	nama	email	gender	tgl_lahir	city	state	country
<input type="checkbox"/>	fenni	b4a7b7defae5c071257ee0c42eaa5ffc	M	Fenni	fenny.s@stikom-bali.ac.id	P	0000-00-00	daohod	oihodhai	oaihoddd
<input type="checkbox"/>	admin	21232f297a57a5a743894a0e4a801fc3	A	Administrator	fenny.s@stikom-bali.ac.id	P	1983-07-23	Denpasar	Bali	Indonesia

Gambar 3.4 Hasil enkripsi yang dapat dilihat pada tabel

4. Kelebihan dan Kelemahan Enkripsi

a. Kelebihan

- Kerahasiaan suatu informasi terjamin
- Menyediakan autentikasi dan perlindungan integritas pada algoritma *checksum/hash*
- Menanggulangi penyadapan telepon dan email
- Untuk *digital signature*

b. Kelemahan

- Penyandian rencana teroris
- Penyembunyian *record* kriminal oleh seorang penjahat
- Pesan tidak bisa dibaca bila penerima pesan lupa atau kehilangan kunci

5. Jenis-jenis serangan

a. Berdasarkan keterlibatan penyerang dalam komunikasi

❖ Serangan pasif

Penyerang tidak terlibat dalam komunikasi antar pengirim dan penerima namun penyerang menyadap semua pertukaran pesan antara kedua entitas tersebut. Tujuannya untuk mendapatkan sebanyak mungkin informasi yang digunakan untuk kriptanalisis. Beberapa metode penyadapan antara lain:

1. *Wiretapping* : Penyadap mencegat data yang ditransmisikan pada saluran kabel komunikasi dengan menggunakan sambungan perangkat keras.

2. *Electromagnetic eavesdropping* :penyadap mencegat data yang ditranmisikan melalui saluran *wireless*, misalnya radio dan *microwave*.
3. *Accoustic eavesdropping* :menangkap gelombang suara yang dihasilkan oleh suara manusia.

❖ Serangan aktif

Penyerang mengintervensi komunikasi dan ikut mempengaruhi sistem untuk keuntungan dirinya, misalnya penyerang mengubah aliran pesan seperti menghapus sebagian *ciphertext*, mengubah *ciphertext*, mereply pesan lama, mengubah informasi yang tersimpan, dan sebagainya.

Yang termasuk jenis serangan aktif adalah *man-in-the-middle*, dimana penyerang mengintersepsi komunikasi antara dua pihak yang berkomunikasi, kemudian ”menyerupai” pihak yang berkomunikasi (pihak lainnya tidak menyadari kalau dia berkomunikasi dengan pihak yang salah). Tujuannya untuk memperoleh informasi berharga seperti kunci.

b. Berdasarkan banyaknya informasi yang diketahui kriptanalis

1. *Ciphertext-only attack*

Jenis serangan ini umum dan paling sulit karena informasi yang tersedia hanyalah *ciphertext* saja. Kriptanalis memiliki beberapa *ciphertext* dari beberapa pesan, semuanya dienkripsi dengan algoritma yang sama. Kriptanalis harus menemukan *plaintext* sebanyak mungkin

dari *ciphertext* tersebut atau menemukan kunci yang digunakan untuk mendekripsi.

2. *Known-plaintext attack*

Ini adalah jenis serangan dimana kriptanalis memiliki pasangan *plaintext* dan *ciphertext* yang berhubungan.

3. *Chosen-plaintext attack*

Salah satu serangan dimana penyerang dapat memilih kuantitas *plaintext* dan kemudian mendapatkan *ciphertext* terenkripsi yang berhubungan.

4. *Chosen-ciphertext attack*

Salah satu serangan dimana penyerang dapat memilih sebuah *ciphertext* dan mencoba mendapatkan *plaintext* yang terdekripsi yang berhubungan dan memiliki akses ke *plaintext* hasil dekripsi (misalnya terhadap mesin elektronik yang melakukan dekripsi).

5. *Chosen-text attack*

Ini merupakan jenis serangan kombinasi *chosen-plaintext attack* dan *chosen-ciphertext attack*.

c. Berdasarkan teknik yang digunakan dalam menemukan kunci

1. *Exhaustive attack* atau *brute force attack*

Serangan ini untuk mengungkap *plaintext* atau kunci dengan mencoba semua kemungkinan kunci.

2. *Analytical attack*

Kriptanalis menganalisis kelemahan algoritma kriptografi untuk mengurangi kemungkinan kunci yang tidak ada

DAFTAR PUSTAKA

- Aji, 2006. **Otentifikasi dan Tanda Tangan Digital**,
http://203.130.205.68/dosen/aji/computer_security/bab_4.pdf. Terakhir diakses pada tanggal 2 November 2007 pada pukul 16.50 WITA
- Anton, 2006. **VPN: Komunikasi Data Pribadi Tanpa Batas**,
<http://antzon.wordpress.com/2006/02/28/vpn-komunikasi-data-pribadi-tanpa-batas/>. Terakhir diakses pada tanggal 2 November pada pukul 16.35 WITA.
- Chieko, 2007. **Enkripsi**, <http://chieko21x.blogspot.com/>. Terakhir diakses pada tanggal 2 November 2007 pada pukul 20.26 WITA
- Ibiblio, 2006. **Keamanan Password dan Enkripsi**,
<http://www.ibiblio.org/pub/Linux/docs/HOWTO/translations/id/other-formats/html/ID-Security-HOWTO-6.html>. Terakhir diakses pada tanggal 2 November 2007 pada pukul 16.37 WITA
- Kelompok 124 IKI-83408 MTI UI, 2005. **Cryptography**,
<http://bebas.vlsm.org/v06/Kuliah/MTI-Keamanan-Sistem-Informasi/2005/124/124P-04-draft-Cryptography.pdf>. Terakhir diakses pada tanggal 15 September 2007 pada pukul 15.12 WITA
- Rinaldi Munir, 2006. Kriptografi, Penerbit Informatika, Bandung.
- Supono, 2007. Algoritma MD5, <http://supono.wordpress.com/2007/06/04/algoritma-md5/>. Terakhir diakses pada tanggal 2 November 2007 pada pukul 16.45 WITA
- Tamatjita, 2006. **Kriptografi Untuk Perlindungan Data**, <http://www.smeapgri-tng.sch.id/sekolah/html/?tab=amik§ion=artikel&num=001&PHPSESSID=90305d3781d3f6b0>. Terakhir diakses pada tanggal 2 November 2007 pada pukul 16.43 WITA
- Yogie, 2007. **Salah Satu Cara Untuk Cracking MD5**, <http://ple-q.com/2007/07/27/salah-satu-cara-untuk-cracking-md5/>. Terakhir diakses pada tanggal 2 November 2007 pada pukul 20.44 WITA