SISTEM KEAMANAN INDUSTRI

Dasar-dasar Keamanan Sistem Informasi

Pengamanan Informasi

- David Khan dalam bukunya *"The Code-breakers"*

  membagi masalah pengamanan informasi menjadi dua kelompok; *security* dan *intelligence*.

  1. Security dikaitkan dengan pengamanan data,
  2. Intelligence dikaitkan dengan pencarian (pencurian, penyadapan) data.

- Pengamanan data dapat dilakukan dengan dua cara, yaitu *steganography* dan *cryptography*.

Steganografi

- Pengamanan dengan menggunakan steganografi

  membuat seolah-oleh pesan rahasia tidak ada atau tidak

  nampak. Padahal pesan tersebut ada. Hanya saja kita tidak

  sadar bahwa ada pesan tersebut di sana.

- Pengamanan dengan menggunakan *cryptography* membuat pesan nampak. Hanya bentuknya yang sulit dikenali karena seperti diacak-acak.

  Pada *cryptography* pengamanan dilakukan dengan dua cara, yaitu transposisi dan substitusi.

  a. Pada penggunaan transposisi, posisi dari huruf yang diubah-ubah,

  b. Pada penggunaan substitusi, huruf (atau kata) digantikan dengan huruf atau simbol lain.

Kriptografi

- Cryptography adalah sebuah kumpulan teknik yang digunakan untuk mengubah informasi/pesan (*plaintext*) kedalam sebuah teks rahasia (ciphertext) yang kemudian bisa diubah kembali ke format semula.

- "*Crypto*" berarti "*secret*" (rahasia) dan "*graphy*" berarti "*writing*" (tulisan). Para pelaku atau praktisi kriptografi disebut ***cryptographers***. Sebuah algoritma kriptografik (*cryptographic algorithm*), disebut **cipher**, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi.

- Proses yang dilakukan untuk mengamankan sebuah pesan (*plaintext*) menjadi pesan yang tersembunyi (*ciphertext*) adalah **enkripsi** (*encryption*), terminologi yang lebih tepat digunakan adalah "*encipher*".

- Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut **dekripsi** (*decryption*), terminologi yang lebih tepat untuk proses ini adalah "*decipher*".

- *Cryptanalysis* adalah seni dan ilmu untuk memecahkan *ciphertext* tanpa bantuan kunci. *Cryptanalyst* adalah pelaku atau praktisi yang menjalankan *cryptanalysis*.

- *Cryptology* merupakan gabungan dari *cryptography* dan *cryptanalysis*.

Dasar-dasar Enkripsi

- Enkripsi digunakan untuk menyandikan data-data
- atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Data disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*).
- Untuk membuka (*decrypt*) data tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (*private key cryptography*) atau dengan kunci yang berbeda (*public key cryptography*).
- Secara matematis, proses atau fungsi enkripsi (*E*)
- dapat dituliskan sebagai: $E(M) = C$
- Proses atau fungsi dekripsi (*D*) dapat dituliskan sebagai:
- $D(C) = M$
- dimana: *M* adalah *plaintext* (*message*) dan *C* adalah *ciphertext*.

Elemen dari Enkripsi

1. Algoritma dari Enkripsi dan Dekripsi.
2. Kunci yang digunakan dan panjangnya kunci.
3. Plaintext. adalah pesan atau informasi yang akan dikirimkan dalam format yang mudah dibaca atau dalam bentuk aslinya.
4. Ciphertext. adalah informasi yang sudah dienkripsi.

Dua metode untuk menghasilkan ciphertext adalah:

1. Stream cipher

   setiap bit dari data akan dienkripsi secara berurutan dengan menggunakan 1 bit dari key tersebut (melakukan enkripsi terhadap semua bit). Contoh : Vernam cipher

2. Blok cipher

   Melakukan enkripsi data terhadap kelompok-kelompok data yang berukuran tertentu. Contoh : Data Encyption Standard (DES).

- **Data Encryption Standard (DES)**

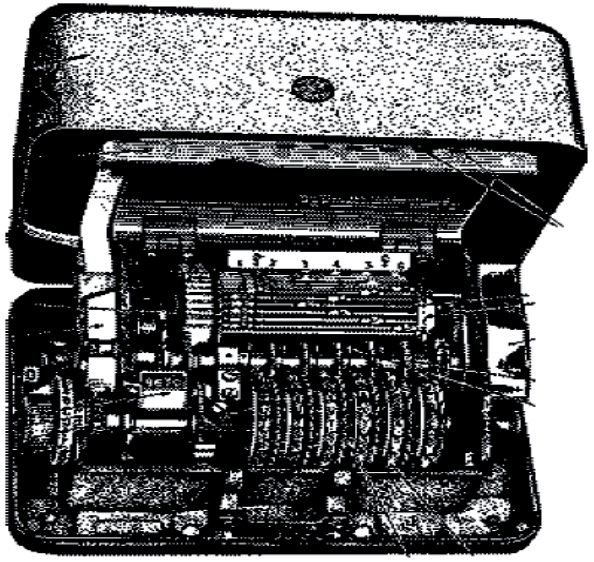
  dikenal sebagai *Data Encryption Algorithm* (DEA) oleh ANSI dan DEA-1 oleh ISO, merupakan algoritma kriptografi simetris yang paling umum digunakan saat ini.

  Aplikasi yang menggunakan DES antara lain:

  - enkripsi dari password di sistem UNIX,
  - berbagai aplikasi di bidang perbankan

Enigma Rotor Machine

Enigma rotor machine merupakan sebuah alat enkripsi dan dekripsi mekanik yang digunakan dalam perang dunia ke dua oleh Jerman.



Enigma Rotor Machine

Aplikasi dari Enkripsi

- Contoh penggunaan enkripsi adalah program *Pretty Good Privacy* (PGP), dan *secure shell* (SSH).
  - Program PGP digunakan untuk mengenkripsi dan menambahkan *digital signature* dalam e-mail yang dikirim.
  - Program SSH digunakan untuk mengenkripsi sesion *telnet* ke sebuah host.

Kelemahan Enkripsi

1. Penanganan yang salah atau kesalahan manusia
   Kurangnya manajemen data enkripsi
2. Kekurangan dalam cipher itu sendiri
3. Serangan brute force

Algoritma Kriptografi Klasik

Pendahuluan

- Algoritma kriptografi klasik berbasis karakter
- Menggunakan pena dan kertas saja, belum ada komputer
- Termasuk ke dalam kriptografi kunci-simetri
- Algoritma kriptografi klasik:
  - *Cipher* Substitusi (*Substitution Ciphers*)
  - *Cipher* Transposisi (*Transposition Ciphers*)

1. Cipher Substitusi

- Monoalfabet : setiap karakter chipertext menggantikan satu macam karakter plaintext
- Polyalfabet : setiap karakter chipertext menggantikan lebih dari satu macam karakter plaintext
- Monograf /unilateral: satu enkripsi dilakukan terhadap satu karakter plaintext
- Polygraf /multilateral: satu enkripsi dilakukan terhadap lebih dari satu karakter plaintext

1. Cipher Substitusi - Caesar Cipher

- Tiap huruf alfabet digeser 3 huruf ke kanan

p_i : 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
c_i : **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**

- Contoh:

  Plainteks: AWASI ASTERIX DAN TEMANNYA OBELIX

  Cipherteks: **DZDVL DVWHULA GDQ WHPDQQBA REHOLA**

1. Cipher Substitusi - Caesar Cipher

- Dalam praktek, cipherteks dikelompokkan ke dalam kelompok n-huruf, misalnya kelompok 4-huruf:

  DZDV LDVW HULA GDQW HPDQ QBAR EHOL A

- Atau membuang semua spasi:

  DZDVLDVWHULAGDQWHPDQQBAREHOLA

- Tujuannya agar kriptanalisis menjadi lebih sulit

1. Cipher Substitusi - *Vigènere Cipher*

- Termasuk ke dalam cipher abjad-majemuk (polyalpabetic substitution cipher).
- Algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya cipher tersebut kemudian dinamakan Vigènere Cipher.
- Vigènere Cipher menggunakan Bujursangkar Vigènere untuk melakukan enkripsi.
- Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar Cipher.

1. Cipher Substitusi - *Vigènere Cipher*

Kunci	Plainteks																								
	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 4.2 Bujursangkar *Vigènere*

1. Cipher Substitusi - *Vigènere Cipher*

- Contoh penerapan Vigènere Cipher :

  Plainteks : THIS PLAINTEXT

  Kunci : sony sonysonys

  Cipherteks : **LVVQ HZNGFHRVL**

- Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik. Dalam hal ini Kunci “sony” diulang sebanyak panjang plaintext-nya

2. Cipher Transposisi

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

2. Cipher Transposisi (Contoh)

Contoh: Misalkan plainteks adalah

```
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
```

Enkripsi:

```
POLITEK
NIKELEK
TRONIKA
NEGERIS
URABAYA
```

Cipherteks: (baca secara vertikal)

PNTNUOIRERLKOGAIENEBTLIRAEEKIYKKASA

PNTN UOIR ERLK OGAI ENEB TLIR AEEK IYKK ASA

Tugas :

1. Buatlah enkripsi cipher substitusi pada kalimat berikut ini :
   Aku adalah mahasiswa udinus semarang

2. Buatlah enkripsi cipher substitusi dengan huruf pada kalimat berikut ini :
   > Udinus terletak jalan Imam Bonjol 207 Semarang

3. Buatlah enkripsi cipher transposisi dengan vertikal
   > Udinus menerima mahasiswa baru tahun ajaran 2020

4. Buatlah enkripsi transposisi dengan Horisontal
   > Udinus menerima mahasiswa baru tahun ajaran 2020

5. Buatlah enkripsi substitusi (Vigenere chiper) dengan kalimat berikut ini :
   > Mahasiswa Udinus menggikuti pelatihan CCNA dengan gratis

Referensi

- Diktat materi keamanan sistem Informasi Bina Sarana Informatika