ERWIEN TJIPTA WIJAYA, ST.,M.KOM

KEAMANAN INFORMASI

TEKNIK - TEKNIK PENYANDIAN ENKRIPSI DAN DESKRIPSI DATA
(PART - I)

TERMINOLOGI

- ***Kriptografi*** (***cryptography***) adalah merupakan ilmu dan seni untuk menjaga pesan agar aman. ***Crypto*** berarti ***rahasia*** dan ***graphy*** berarti **tulisan**.
- Pelaku atau praktisi kriptografi disebut ***cryptographer***.
- Algoritma kriptografi (cryptographic algorithm), disebut ***cipher***, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan deskripsi.
- ***Enkripsi*** adalah merupakan proses untuk mengamankan pesan (***plaintext***) menjadi pesan tersembunyi (***ciphertext***).
- ***Ciphertext*** adalah pesan yang sudah tidak dapat dibaca dengan mudah.
- ***Deskripsi*** adalah merupakan proses sebaliknya dari Enkripsi, dimana mengubah ***Ciphertext*** menjadi ***Plaintext***.
- ***Crytanalyst*** adalah seni dan ilmu untuk memecahkan ciphertext tanpa bantuan kunci, sedangkan pelakunya disebut ***Crytanalysis***

TUJUAN KRIPTOGRAFI / PENYANDIAN

- ***Kerahasian*** adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah disandi.

- ***Integritas Data*** adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah, untuk menjaga integritas sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak - pihak yang tidak berhak, antara lain penyisipan, penghapusan dan pensubsitusian data lain kedalam data sebenarnya.

- ***Authentikasi*** adalah 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 diauthentikasi keaslian, isi datanya, waktu pengiriman dan lain - lain

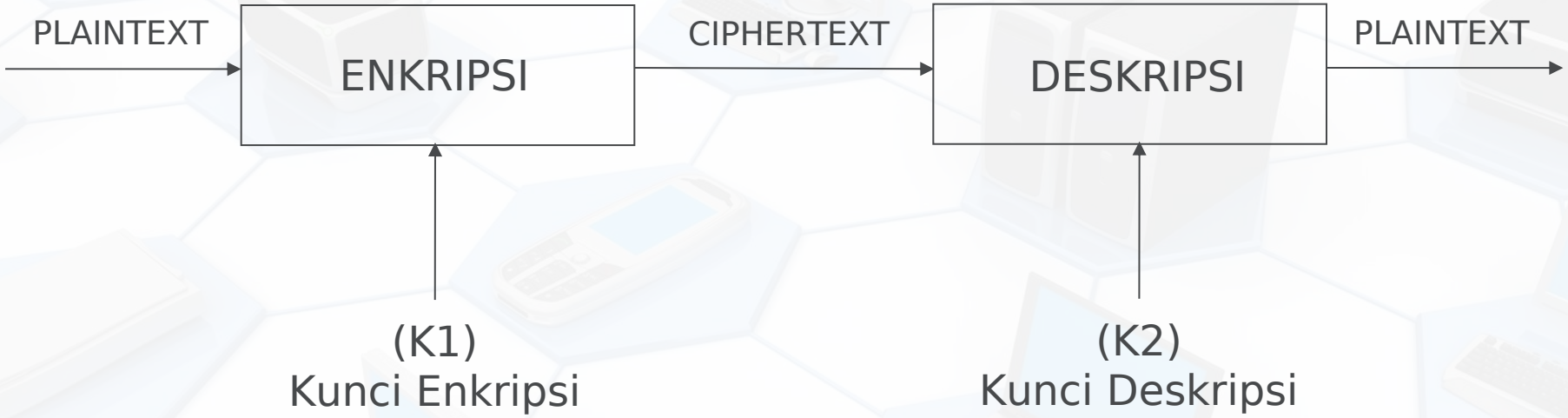
TUJUAN KRIPTOGRAFI / PENYANDIAN

- ***Non-Repudiasi*** atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman / terciptanya suatu informasi oleh yang mengirimkan / membuat.

ENKRIPSI

- ***Enkripsi*** digunakan untuk menyandikan data - data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak.
- Proses enkripsi adalah data disandikan (***encrypted***) dengan menggunakan sebuah kunci (***key***).
- Proses deskripsi adalah membuka data dengan menggunakan kunci yang sama dengan kunci untuk mengenkripsikan data (***private key***) atau dengan kunci yang berbeda (***public key***).

PROSES ENKRIPSI



Secara matematis :
Fungsi Enkripsi (E) dapat dituliskan E(M) = C

dimana :
M = Plaintext (Message)
C = Ciphertext

Fungsi Deskripsi (D) dapat dituliskan D(C) = M

ALGORITMA PENYANDIAN / KRIPTOGRAFI

- Algoritma yang berfungsi untuk melakukan tujuan kriptografis. Algoritma tersebut harus memiliki kekuatan untuk melakukan (*Shannon*).

- Ada 2 jenis teknik algoritma untuk kriptografi yaitu :

1. Konfusi (pembingunan), dari teks terang sehingga sulit untuk direkonstruksikan secara langsung tanpa menggunakan algoritma deskripsinya.

2. Difusi (peleburan), dari teks terang sehingga karakteristik dari teks terang tersebut hilang.

- Algoritma kriptografi berdasarkan jenis kunci yang digunakan :

1. Algoritma Simetris dimana kunci yang digunakan untuk proses enkripsi dan deskripsi adalah kunci yang sama.

2. Algoritma Asimetris dimana kunci yang digunakan untuk proses enkripsi dan deskripsi menggunakan kunci yang berbeda.

ALGORITMA PENYANDIAN / KRIPTOGRAFI

- Algoritma penyandian berdasarkan besar data yang diolah :

1. Algoritma blok cipher : informasi / data yang hendak dikirim dalam bentuk blok - blok ini dioperasikan dengan fungsi enkripsi yang sama dan akan menghasilkan informasi rahasia dalam blok - blok yang berukuran sama.

2. Algoritma stream cipher : informasi / data yang hendak dikirim dioperasikan dalam bentuk blok - blok yang lebih kecil (byte atau bit), biasanya satu karakter persatuan - persatuan waktu proses, menggunakan transformasi enkripsi yang berubah setiap waktu.

ALGORITMA KRIPTOGRAFI KLASIK

- Cipher Substitusi (***Subsitution Ciphers***)

1. Caesar Cipher
2. ROT13 (Rotate by 13 places)
3. Cipher Alfabet-Tunggal
4. Cipher Alfabet-Majemuk
5. Cipher Substitusi Homofonik
6. Cipher Substitusi Poligram

- Cipher Transposisi (***Transposisi Ciphers***)

CIPHER TRANSPOSISI

- Cipher transposisi, huruf - huruf dalam plaintext tetap sama, hanya saja urutannya diubah.
- Nama lain untuk metode ini adalah ***permutasi*** atau ***pengacakan*** (scrambling) karena transpose setiap karakter didalam teks sama dengan mempermutasikan karakter - karakter tersebut.
- Contoh :

  Misalkan plainteks adalah :

  JURUSAN TEKNIK INFORMATIKA DI MALANG

- untuk mengenkripsi pesan, plainteks ditulis secara horizontal dengan lebar kolom tetap, misalnya selebar 6 karakter (Kunci k = 6)

CIPHER TRANSPOSISI

- Sehingga akan menghasilkan sebagai berikut

J	U	R	U	S	A
N	T	E	K	N	I
K	I	N	F	O	R
M	A	T	I	K	A
D	I	M	A	L	A
N	G				

- Sehingga apabila disusun secara vertikal akan menghasilkan enkripsi sebagai berikut :

JNKMDNUTIAIGRENTM UKFIA SNOKL AIRAA

PENYANDI MONOALFABETIK

- Penyandian monoalfabetik adalah merupakan setiap huruf digantikan dengan sebuah huruf. Huruf yang sama akan memiliki pengganti yang sama. Misalnya huruf "a" diganti dengan "e", maka setiap huruf "a" akan digantikan dengan huruf "e".
- Metode penyandi monoalfabetik :

1. Caesar
2. ROT13

CAESAR CIPHER

- Metode caesar cipher yang digunakan Julius Caesar, pada prinsipnya setiap huruf digantikan dengan huruf yang berada 3 posisi dalam urutan alfabet.
- Sebagai contoh huruf "a" digantikan dengan huruf "D" dan seterusnya.
- Transformasi yang digunakan sebagai berikut :

(P = Plaintext; C = Ciphertext)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
P	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	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

ROT13

- Pada sistem ini sebuah huruf digantikan dengan huruf yang letaknya 13 posisi darinya.
- Sebagai contoh huruf "A" digantikan dengan huruf "N", huruf "B" digantikan dengan huruf "O" dan seterusnya.
- Secara matematis proses ***Enkripsi*** dapat dituliskan :

  C **ROT13** = (M)

- Proses ***Deskripsi*** dilakukan dengan cara proses Enkripsi ROT13 sebanyak 2x.

  M **= *ROT13(ROT13(***M***))***

PENYANDI POLIALFABETIK

- Enkripsi dapat dilakukan dengan mengelompokkan beberapa huruf menjadi sebuah kesatuan (unit) yang kemudian dienkripsi.
- Metode penyandi polialfabetik adalah ***Playfair***
- Playfair : Merupakan salah satu metode yang digolongkan dalam kriptografi klasik yang proses enkripsinya menggunakan pemrosesan dalam bentuk blok - blok yang sangat besar.
- Metode ini merupakan salah satu cara untuk mengatasi kelemahan metode kriptografi klasik lainnya yang mudah tertebak karena terdapat korespondensi satu - satu antara plainteks dengan cipherteks.

PLAYFAIR

- Membuat kunci dari ***Kata*** atau ***Kalimat***, misal : **KOMPUTERCERDAS**
- Membuang huruf yang ***berulang*** dan huruf (J) jika ada, sehingga menjadi : **KOMPUTERCDAS**
- Menambahkan huruf - huruf yang belum ada. (kecuali J), sehingga menjadi : KOMPUTERCDASBFGHILNQVWXYZ
- Memasukan kunci tersebut didalam matrik 5x5

K	**O**	**M**	**P**	**U**
T	**E**	**R**	**C**	**D**
A	**S**	**B**	**F**	**G**
H	**I**	**L**	**N**	**Q**
V	**W**	**X**	**Y**	**Z**

PLAYFAIR

- Jumlah kemungkinan kuncinya adalah

  25! = 15.511.210.043.330.985.984.000.000

- Memperluas susunan kunci didalam matrik dengan nambahkan kolom ke-6 dan baris ke-6

- Tabel kunci akan menjadi :

K	O	M	P	U	K
T	E	R	C	D	T
A	S	B	F	G	A
H	I	L	N	Q	H
V	W	X	Y	Z	V
K	O	M	P	U	

PLAYFAIR

- Plaintext : **TEKNIK INFORMATIKA**

  ENKRIPSI

- Mengganti huruf J (Bila ada) dengan huruf (I).
- Menulis pesan dalam pasangan huruf.
- Jika terdapat pasangan huruf yang sama, maka harus disisipkan huruf X ditengahnya,
- Jika jumlah huruf ***ganjil***, maka harus ditambahkan huruf X diakhir kunci
- Pesan di enkripsi menjadi : **TE KN IK IN FO RM AT IK AX**

ALGORITMA PLAYFAIR

- Jika terdapat 2 huruf pada ***baris*** kunci yang sama maka masing - masing huruf diganti dengan huruf di***kanan***nya (pada kunci yang sudah diperluas).
- Jika terdapat 2 huruf pada kolom kunci yang sama maka masing - masing huruf diganti dengan huruf di***bawah***nya
- Jika 2 huruf tidak tidak terdapat pada ***baris*** dan ***kolom*** yang sama, maka huruf pertama digantikan dengan huruf pada perpotongan ***baris*** huruf ***pertama*** dengan ***kolom*** huruf yang **kedua**. Huruf yang ke-2 diganti dengan huruf pada titik sudut ke empat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan.

Enkripsi :

- Plaintext : **TE KN IK IN FO RM AT IK AX**
- Ciphertext : **ER PH HO LQ SP RM AT HO BV**

Terima Kasih