BAB VI
TEKNIK TRANSPOSISI DAN ONE TIME PAD

6.1 Teknik Kriptografi Transposisi dan One Time Pad

Kriptografi adalah ilmu mengenai teknik enkripsi dimana “naskah asli” (plaintext) diacak menggunakan suatu kunci enkripsi menjadi “naskah acak yang sulit dibaca” (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama adalah sangat kecil.

Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk public key cryptography, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan – bilangan yang sangat besar. (Kromodimoeljo, 2010).

6.1.1 Teknik Transposisi

Metode penyandian transposisi adalah metode penyandian dengan cara mengubah letak dari teks pesan yang akan disandikan. Untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati.

Sebelumnya sudah dijelaskan bahwa metode kuno/ klasik terdiri dari 2 teknik yaitu:

1. Teknik Subtitusi, contoh: kode kaisar (geser, monoalphabet, polyalphabet, playfair, dan lainnya)
2. Teknik Permutasi, contoh: kode transposisi.

Teknik ini menggunakan permutasi karakter, yang mana dengan menggunakan teknik ini pesan asli tidak dapat dibaca kecuali oleh orang yang memiliki kunci untuk mengembalikan pesan tersebut ke bentuk semula.

Sebagai contoh, ada 6 kunci untuk melakukan permutasi kode:

1	2	3	4	5	6
3	5	1	6	4	2

Gambar 6.1 Kunci Permutasian Kode

Dan 6 kunci untuk inversi dari permutasi tersebut:

1	2	3	4	5	6
3	6	1	5	2	4

Gambar 6.2 Kunci Inversi dari Permutasian Kode

Terlebih dahulu plaintext dibagi menjadi beberapa blok dan tiap blok nya terdiri dari 6 karakter, jika terjadi kekurang pada setiap blok maka disisipkan karakter yang disepakati sebelumnya.

Perhatikan contoh dibawah ini:
Plaintext : **PERHATIKAN RAKYAT KECIL**
Cara memutasi plaintext, yaitu :

1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L	X	X	X
3	5	1	6	4	2	3	5	1	6	4	2	3	5	1	6	4	2	3	5	1	6	4	2
R	A	P	T	H	E	A	R	I	A	N	K	A	K	K	E	T	Y	L	X	C	X	X	I

Gambar 6.3 Hasil Teknik Transposisi permutasian kode

Ciphertext : **RAPTHEARIANKAKKETYLXCXXI**

Sedangkan kunci inverse berfungsi untuk mengubah ciphertext menjadi plaintext.

Perhatikan contoh dibawah ini:

1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6
R	A	P	T	H	E	A	R	I	A	N	K	A	K	K	E	T	Y	L	X	C	X	X	I
3	6	1	5	2	4	3	6	1	5	2	4	3	6	1	5	2	4	3	6	1	5	2	4
P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L	X	X	X

Gambar 6.4 Hasil Plaintext Transposisi Permutasian

Selain teknik mutasi-inversi ada beberapa teknik permutasi lainnya yaitu dengan menggunakan permutasi zigzag, segitiga, spiral, dan diagonal.

1. Zig-zag Dengan memasukan plaintext seperti pola zig-zag.
   Plaintext: **PERHATIKAN RAKYAT KECIL**

			H						N						T						X		
		R		A				A		R					A		K				L		
	E				T		K				A		Y				E		I				
P						I						K						C					

Gambar 6.5 Contoh Teknik Permutasian Pola Zigzag

Ciphertext : **HNTXRAARAKLETKAYEIPIKC**

2. Segitiga Dengan memasukan plaintext sepeti pola segitiga.
   Plaintext: **PERHATIKAN RAKYAT KECIL**

				P				
			E	R	H			
		A	T	I	K	A		
	N	R	A	K	Y	A	T	
K	E	C	I	L	X	X	X	X

Gambar 6.6. Contoh Teknik Permutasian Pola Segitiga

Ciphertext : **KNEARCETAIPRIKLHKYXAAXTXX**

3. Spiral Dengan memasukan plaintext disusun seperti pola spiral.
   Plaintext: **PERHATIKAN RAKYAT KECIL**

P	E	R	H	A
T	K	E	C	T
A	X	X	I	I
Y	X	X	L	K
K	A	R	N	A

Gambar 6.7 Contoh Teknik Permutasian Pola Sprial 1

Ciphertextnya : **PTAYKEKXXAREXXRHCILNATIKA**

4. Diagonal Dengan memasukan plaintext disusun seperti pola dibawah ini.
   Plaintext: **PERHARTIKAN RAKYAT KECIL**

P	T	R	T	L
E	I	A	K	X
R	K	K	E	X
H	A	Y	C	X
A	N	A	I	X

Gambar 6.8 Contoh Teknik Permutasian Pola Spiral 2

Ciphertextnya : **PTRTLEIAKXRKKEXHAYCXANAIX**

6.1.2 One Time Pad

Pada umumnya algoritma kriptografi tidaklah sempurna, tetapi untuk mendapatkan algoritma yang lebih baik dan mempunyai sedikit kemunngkinan untuk dipecahkan adalah one time pad (OTP). Salah satu konsep OTP adalah dengan menggunakan enkripsi super. Contoh pada metode ini yaitu :

Plaintext : **PERHATIKAN RAKYAT KECIL**

1. Menggunakan teknik subtitusi dengan algoritma kode geser sebanyak 7.

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
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
P	E	R	H	A	T	I	K	A	N	R	A	K	Y	A	T	K	E	C	I	L					
V	K	X	N	G	Z	O	Q	G	T	X	G	Q	E	G	Z	Q	K	I	O	R					

Gambar 6.9 Teknik One Time Pad geser 7

Ciphertext dari hasil teknik subtitusi di ubah menjadi ciphertext dengan teknik transposisi.

2. Menggunakan teknik transposisi dengan teknik diagonal dengan kunci 5 x 5.

V	Z	X	Z	R
K	O	G	Q	X
X	Q	Q	K	X
N	G	E	I	X
G	T	G	O	X

Gambar 6.10 Teknik One Time Pad diagonal 5x5

Ciphertext : **VZXZRKOGQXXQQKXNGEIXGTGOX.**

Teknik dari enkripsi super sangat penting dan banyak dari algoritma enkripsi modern yang menggunakan teknik ini sebagai dasar pembuatan suatu algoritma modern.

Soal

1. Buatlah ciphertext dari plaintext **INTERNET** dengan menggunakan transposisi!
2. Buatlah ciphertext dari kata **KULIAH ONLINE** dengan menggunakan permutasi zigzag!