Teknik Transposisi / Permutasi

Kriptografi

Kelompok 4

1. Deni Salvana E. (A11.2010.05204)
2. Ghulam Maulana R (A11.2010.05499)
3. Moh. Yusud Bakhtiar (A11.2010.05763)
4. Putranto Adhi N (A11.2010.05741)
5. Mohammad Hindam A.(A11.2010.05726)

Teknik Transposisi

Pada teknik transposisi, plainteks tetap sama tetapi urutannya diubah. 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.

Teknik Transposisi

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

Dengan kata lain, algoritma ini melakukan *transpose* terhadap rangkaian huruf di dalam plainteks.

Algoritma Kriptografi Klasik (SIMETRI)

Misalnya:

Ada 6 kunci untuk melakukan permutasi kode (proses enkripsi):

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

Dan 6 kunci untuk inversi dari permutasi tesebut (proses dekripsi):

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

Untuk melakukan enkripsi terhadap kalimat: “SAYA SEDANG BELAJAR KEAMANAN KOMPUTER”

Maka terlebih dahulu kalimat tersebut dibagi menjadi 6 blok dan apabila terjadi kekurangan tambahkan huruf yang disukai (dalam contoh ini menggunakan huruf “X”)

Setelah dibagi menjadi 6 blok, maka dengan menggunakan kunci diatas, setiap blok menjadi:

YSSEAA NBDEGA JRLKAA MNEAAA OPNUMK RXTXXE

Untuk mendekripsi chipertext diatas, maka dengan menggunakan kunci:

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

Y	S	S	E	A	A	N	B	D	E	G	A	J	R	L	K	A	A	M	N	E	A	A	A	O	P	N	U	M	K	R	X	T	X	X	E
3	6	1	5	2	4	3	6	1	5	2	4	3	6	1	5	2	4	3	6	1	5	4	2	3	6	1	5	2	4	3	6	1	5	2	4
S	A	Y	A	S	E	D	A	N	G	B	E	L	A	J	A	R	K	E	A	M	A	N	A	N	K	O	M	P	U	T	E	R	X	X	X

Teknik Transposisi

Ada beberapa model kriptografi dengan teknik transposisi diantaranya adalah sebagai berikut:

- Segitiga
- Spiral
- Diagonal
- Zigzag

1. Segitiga: memasukan plaintext dengan pola segitiga menjadi 6 baris (K=6) dan dibaca dari baris atas ke baris bawah:

					S					
				A	Y	A				
			S	E	D	A	N			
		G	B	E	L	A	J	A		
	R	K	E	A	M	A	N	A	N	
K	O	M	P	U	T	E	R	X	X	X

Chipertext:

KROGKMSBEPAEEAUSYDLMTAAAAENJNRAAXNXX

Untuk melakukan enkripsi terhadap chipertext diatas,

- Susunlah setinggi 6 baris dimulai dari bawah, dimana setiap perpindahan kolom huruf betambah tinggi satu baris dan setelah mencapai baris ke-6, huruf kembali menurun satu baris.
- Kemudian baca mulai dari pucuk untuk memperoleh kembali plaintext

Dieroleh kembali teks asli:

SAYA SEDANG BELAJAR KEAMANAN KOMPUTERXX

					S					
				A	Y	A				
			S	E	D	A	N			
		G	B	E	L	A	J	A		
	R	K	E	A	M	A	N	A	N	
K	O	M	P	U	T	E	R	X	X	X

2. Spiral: memasukan plaintext menjadi baris dan kolom 6 dengan pola spiral dan dibaca dari baris atas ke baris bawah:

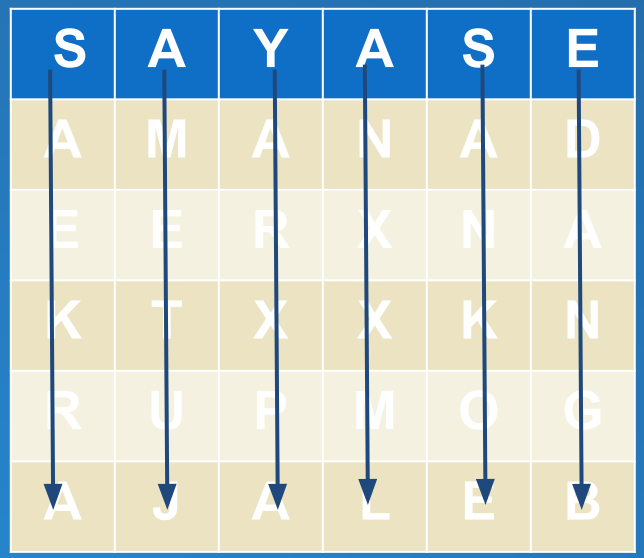
S	A	Y	A	S	E
A	M	A	N	A	D
E	E	R	X	N	A
K	T	X	X	K	N
R	U	P	M	O	G
A	J	A	L	E	B

Chipertext:

SAEKRAAMETUJYARXPAANXXMLSANKOEEDANGB

Untuk melakukan dekripsi terhadap chipertext diatas, maka susunlah menjadi 6 baris/kolom (K=6), dari atas ke bawah dimulai pada kolom pertama seperti di bawah ini:

S	A	Y	A	S	E
A	M	A	N	A	D
E	E	R	K	N	A
K	T	X	X	K	N
R	U	F	M	C	G
A	J	A	L	E	B

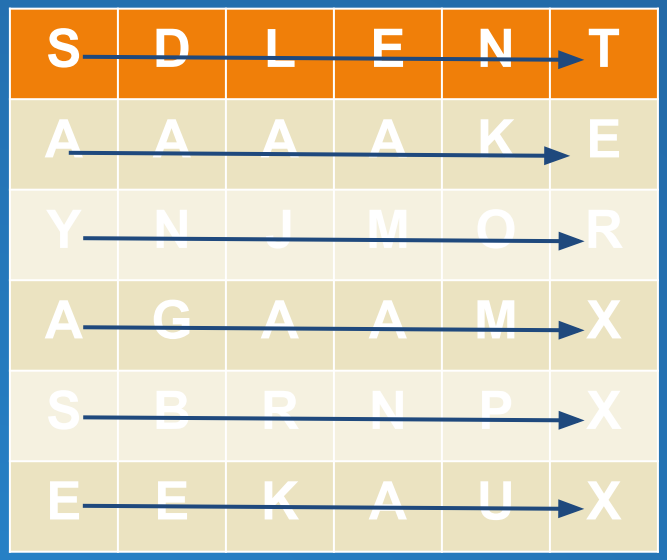


Lalu baca secara spiral untuk mendapatkan plaintext kembali

Chipertext:

SAEKRAAMETUJYARXPAANXXMLSANKOEEDANGB

3. Diagonal: memasukan plaintext menjadi 6 baris/kolom secara diagonal seperti berikut:



Chipertext:

SDLENTAAAAKEYNJMORAGAAMXSBRNPXEEKAUX

4. Zig-zag: memasukan plaintext dengan pola zig-zag dan dibaca dari atas ke bawah, misalnya:

*** Plaintext: SAYA SEDANG BELAJAR KEAMANAN KOMPUTER**

*** Susunlah plaintext secara zig-zag menjadi 4 baris (K=4)**

seperti di bawah ini,

			A					G						A						A					M					X
		Y		S				N		B				J		R				M		N				O		P				R	
	A				E		A				E		A				K		A				A		K				U		E		
S						D						L						E						N						T				

* Chipertext:

AGAAMXYSNBJRMNOPRAEAEAKAAKUESDLENT

Kesimpulan

Cipher transposisi atau cipher permutasi merupakan salah satu algoritma kriptografi klasik yang melakukan pengacakan urutan karakter dalam plainteks. Cipher transposisi mempunyai berbagai macam algoritma. Setiap algoritma mempunyai cara kerja, kelebihan dan kekurangan masing-masing.

Kelebihan

- Rail Fence Cipher (zig-zag) unggul dalam penulisan plainteks menjadi cipherteks karena penulisan dapat dilakukan dari baris mana saja.
- Route Cipher (spiral) mempunyai rancangan kunci yang paling kuat karena mempunyai kunci paling banyak.
- Columnar transposition (kolom) digunakan untuk menambah kekuatan dan kerumitan suatu cipher lain.

Kekurangan

Semua teknik cipher transposisi kelemahannnya adalah frekuensi kemunculan karakter cipherteks sama dengan plainteks sehingga bisa diserang menggunakan analisis frekuesi.

Untuk meningkatkan tingkat keamanan sebuah cipher transposisi adalah dengan menggabungkannya dengan algoritma klasik lain yaitu cipher substitusi.