Studi dan Perbandingan Berbagai Macam Algoritma *Cipher* Transposisi

Reyhan Yuanza Pohan [1)]
1) Jurusan Teknik Informatika ITB, Bandung 40132, email: if14126@students.if.itb.ac.id

Abstract – *Masalah pengiriman data ataupun pesan telah menjadi masalah penting pada era teknologi informasi seperti sekarang ini. Terkadang pesan-pesan ini harus bersifat rahasia agar tidak diketahui secara umum. Apabila pesan tersebut diketahui, maka pesan tersebut dapat disalahgunakan untuk kejahatan oleh orang lain.*

Kriptografi merupakan salah satu alat keamanan yang digunakan untuk menyembunyikan suatu pesan. Kriptografi sudah digunakan di segala bidang keamanan. Salah satu metode algoritma kriptografi klasik yang sudah dikenal sejak lama adalah Transposition Cipher atau Cipher transposisi. Metode ini juga dikenal sebagai permutasi. Algoritma ini memindahkan urutan tiap karakter dalam pesan. Terdapat berbagai macam jenis algoritma cipher transposisi seperti Rail Fence Cipher, Route Cipher, Columnar Transposition, dan Myszkowski transposition.

Pada makalah ini, penulis akan membahas jenis-jenis algoritma di atas. Pembahasan akan meliputi penjelasan, cara kerja masing-masing algoritma, kelebihan dan kekurangannya. Penulis juga akan mencoba memberikan usulan cara untuk meningkatkan tingkat keamanan cipher transposisi.

Kata Kunci*: kriptografi, Transposition Cipher, Rail Fence Cipher, Route Cipher, Columnar Cipher, Myszkowski transposition*

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini sudah berkembang secara pesat. Dengan berkembangnya teknologi informasi ini, pertukaran data dapat menjadi suatu permasalahan. Hampir setiap hari pertukaran data terjadi, data-data ini bervariasi besarnya maupun jenisnya. Adakalanya data-data ini bersifat rahasia seperti data pribadi, data organisasi, ataupun data negara. Kerahasiaan ini perlu dijaga agar tidak orang yang menyalahgunakan data-data tersebut. Untuk itulah, kriptografi dikembangkan.

Kriptografi adalah suatu ilmu menyembunyikan informasi. Sampai dengan saat ini, sudah ada berbagai macam algoritma kriptografi, namun secara keseluruhan algoritma kriptografi dibagi menjadi dua yaitu klasik dan modern. Contoh algoritma klasik adalah *cipher* substitusi dan *cipher* transposisi.

Sedangkan contoh algoritma modern adalah *cipher* blok. Dalam makalah ini, penulis akan melakukan studi dan perbandingan dari berbagai macam algoritma *cipher* transposisi.

Cipher transposisi dapat disebut juga sebagai *cipher* permutasi karena sebenarnya metode *cipher* transposisi ini mempermutasikan karakter-karakter plainteks, yaitu dengan menyusun ulang urutan karakter dalam pesan. Contoh paling sederhana penggunaan *cipher* transposisi adalah dengan membalikkan karakter-karakter dalam suatu kata. Misalkan kata KRIPTOGRAFI dienkripsi menjadi IFARGOTPRIK, ini adalah contoh paling sederhana.
Sedangkan contoh *cipher* transposisi yang lebih rumit sebagai berikut:

Misalkan kita mempunyai plainteks

INI PESAN RAHASIA

Untuk meng-enkripsi pesan, plainteks ditulis secara horizontal dengan lebar kolom tetap, missal selebar 5 karakter (kunci $k = 5$)

```
I N I P E
S A N R A
H A S I A
```

maka cipherteksnya dibaca secara vertikal menjadi

ISHNAAINSPRIEAA

Pada zaman Yunani dahulu, tentara Sparta menggunakan sebuah alat yang dinamakan *scytale*. Alat terdiri dari sebuah silinder dan pita panjang dari daun *papyrus*. Pesan dituliskan horizontal dan bila pita dilepaskan, maka huruf-huruf di dalamnya telah tersusun membentuk pesan rahasia. *Scytale* merupakan suatu penerapan *cipher* transposisi pada zaman dahulu.

Cipher transposisi mempunyai berbagai macam algoritma yang berbeda-beda seperti *Rail Fence Cipher, Route Cipher, Columnar Transposition, dan Myszkowski transposition*. Setiap algoritma itu mempunyai kelebihan dan kekurangannya masing-masing. Pada makalah ini, penulis akan mencoba

merumuskan sebuah usulan algoritma baru yang dapat menutupi kekurangan *cipher* transposisi.

2. ALGORITMA *CIPHER* TRANSPOSISI

2.1. *Rail Fence Cipher*

Algoritma ini melibatkan penulisan plainteks sehingga mempunyai baris atas dan baris bawah yang terpisah. Urutan karakter pada baris atas akan diikuti oleh karakter berikutnya pada baris bawahnya, dan seterusnya sehingga *n-rail*. Apabila penulisan ke bawah sudah mencapai *n*, maka penulisan dilakukan ke baris atasnya dan seterusnya. Bila penulisan ke atas juga sudah mencapai *n-rail*, maka penulisan dilakukan seperti awal. Cipherteks dibaca secara horizontal. Untuk lebih jelasnya, berikut adalah contohnya:

Misalkan kita mempunyai plainteks

MEET ME AT NOON

enkripsi dilakukan dengan kunci $k = 3$, *offset* = 0

```
M . . . M . . . N . . .
. E . T   E . T . O . N
. . E . . . A . . . O .
```

maka cipherteksnya menjadi

MMNET ETONE AO

Namun enkripsi juga dapat dilakukan dengan memulainya bukan dari baris paling atas (*offset* = 0), namun bisa juga dari baris lainnya. Dengan menggunakan contoh plainteks di atas:

Enkripsi dilakukan dengan kunci $k = 3$, *offset* = 2

```
. . E. . . . A . . . O .
. E . T   E . T . O . N
M . . . M . . . N . . .
```

maka cipherteksnya menjadi

EAOET ETONM MN

Biasanya penulisan cipherteks dilakukan menjadi blok-blok standar biasanya sepanjang 5 karakter. Bila hasil cipherteks tidak habis dibagi dengan panjang karakter, maka penambahan karakter *dummy* dilakukan pada saat pengenkripsian.

2.2. *Route Cipher*

Dalam algoritma *route cipher*, plainteks dituliskan ke dalam suatu dimensi yang sudah ditentukan, cara ini seperti enkripsi yang dilakukan pada bab pendahuluan. Namun perbedaannya adalah pembacaan cipherteks dilakukan dalam pola yang diberikan dalam kunci. Sebagai contoh:

Misalkan kita mempunyai plainteks

WE ARE DISCOVERED FLEE AT ONCE

enkripsi dilakukan dengan kunci $k = 9$, spiral ke dalam arah jarum jam kanan atas

```
W R I O R F E O E
E E S V E L A N J
A D C E D E T C X
```

maka cipherteksnya menjadi

EJX CTE DEC DAE WRI ORF EON ALE VSE

Pada zaman perang saudara di Amerika (*American Civil War*), sebuah varian dari *route cipher* digunakan yaitu *Union Route Cipher*. Cara kerja algoritma varian ini sama dengan *route cipher* biasa, hanya saja transposisi dilakukan pada keseluruhan kata dibandingkan tiap karakter

2.3. *Columnar Transposition*

Pada *columnar transposition*, pesan ditulis dalam baris dengan panjang tertentu, kemudian dibaca kembali dari kolom ke kolom. Pembacaan per kolomnya berdasarkan urutan yang acak. Panjang baris dan permutasi kolomnya biasanya didefinisikan oleh sebuah kata kunci. Sebagai contoh kata COLUMN mempunyai panjang 6 (sehingga panjang baris adalah 6) dan permutasi didefinisikan dengan urutan alphabet dari kata kunci. Dengan menggunakan kata COLUMN, maka urutannya akan menjadi [1 5 2 6 3 4]. Untuk lebih jelasnya, berikut adalah contohnya:

Misalkan kita mempunyai plainteks

ESCAPE TONIGHT THROUGH TUNNEL

enkripsi umum *columnar transposition* dilakukan dengan kunci PRISON [4 5 1 6 3 2]

4	5	1	6	3	2
E	S	C	A	P	E
T	O	N	I	G	H
T	T	H	R	O	U
G	H	T	U	N	N
E	L	Q	K	J	E

Maka cipherteksnya menjadi

CNHTQ EHUNE PGONJ ETTGE SOTHL AIRUK

Pada *columnar transposition* yang umum, semua area kosong diisi dengan nilai *dummy* seperti contoh di atas, dalam hal ini [Q K J E]. Sedangkan pada beberapa *coloumnar transposition* yang lain, area kosong dibiarkan tetap kosong. Dengan menggunakan contoh plainteks dan kunci seperti di atas:

4	5	1	6	3	2
E	S	C	A	P	E
T	O	N	I	G	H
T	T	H	R	O	U
G	H	T	U	N	N
E	L				

maka cipherteksnya menjadi

CNHTE HUNPG ONETT GESOT HLAIR U

Untuk mendapatkan kembali plainteks, penerima pesan harus mencari jumlah kolom dengan membagi panjang pesan dengan panjang kunci. Kemudian dia akan dapat menulis kembali pesan dalam kolom-kolom. Selanjutnya mengurutkan kembali kolom tersebut dengan melihat kata kunci.

2.4. *Myszkowski Transposition*

Sebenarnya *myszkowski transposition* ini merupakan sebuah variasi dari *columnar transposition* yang diusulkan oleh Émile Victor Théodore Myszkowski pada tahun 1902. Varian ini memerlukan sebuah kata kunci yang mempunyai karakter berulang. Dalam *columnar transposition* biasanya, kemunculan karakter yang sama diperlakukan seperti karakter berikutnya dalam urutan abjad, sebagai contoh kata kunci TOMATO akan mempunyai urutan [5 3 2 1 6 4]. Dalam *myszkowski transposition*, kemunculan karakter yang sama diberi nomor urutan yang sama sehingga kata kunci TOMATO mempunyai urutan [4 3 2 1 4 3]. Kolom plainteks dengan nomor urutan angka yang unik dibaca ke bawah, sedangkan kolom dengan nomor urutan yang sama dibaca dari kiri ke kanan. Untuk lebih jelasnya, diberikan contoh sebagai berikut:

Misalkan kita mempunyai plainteks

THIS IS A VERY SECRET MESSAGE

enkripsi dilakukan dengan kunci TOMATO [4 3 2 1 4 3]

4	3	2	1	4	3
T	H	I	S	I	S
A	V	E	R	Y	S
E	C	R	E	T	M
E	S	S	A	G	E

maka cipherteksnya menjadi

SREA IERS HSVS CMSE TIAY ETEG

3. HASIL PERBANDINGAN DAN USULAN PERBAIKAN

Cara kerja masing-masing algoritma *cipher* transposisi telah dijelaskan di bab sebelumnya, bab ini akan melakukan perbandingan dari masing-masing algoritma dan usulan perbaikan dalam merancang suatu algoritma *cipher* transposisi yang baru

3.1. Hasil Perbandingan

Rail Fence cipher mempunyai kelebihan dibandingkan algoritma lainnya dalam proses penulisan plainteks menjadi cipherteks karena penulisan dapat dilakukan di baris mana saja. Hal ini akan menambah kerumitan dalam proses enkripsi maupun dekripsi.

Route cipher bisa dikatakan mempunyai proses enkripsi dan dekripsi yang sangat rumit. Hal ini didukung oleh kunci yang digunakan dapat membuat proses enkripsi dan dekripsi yang fleksibel. *Route cipher* mempunyai kunci yang paling banyak dibandingkan algoritma lainnya. Untuk sebuah pesan dengan panjang yang masuk akal, jumlah kemungkinan kunci potensial akan terlalu besar sekalipun untuk komputasi modern. Akan tetapi, justru kunci dari *route cipher* ini yang membuat algoritma ini mempunyai kekurangan. Pemilihan rute kunci yang buruk dapat meninggalkan kelebihan potongan plainteks, sehingga dapar memberikan seorang kriptanalis sebuah petunjuk.

Algoritma *columnar transposition* sebenarnya adalah contoh algoritma *cipher* transposisi yang paling standar. Algoritma ini bersifat sangat matematis sehingga proses enkripsi dan dekripsi tidak begitu rumit untuk komputasi modern. Algoritma ini lebih digunakan sebagai suatu komponen dalam *cipher* yang lebih kompleks.

Dari semua algoritma *cipher* transposisi, algoritma *myszkowski transposition* merupakan algoritma yang memiliki tingkat kerumitan tinggi dengan kunci yang sederhana. *Myszkowski transposition* mempunyai kerumitan yang lebih tinggi dibandingkan *columnar transposition* karena pembacaan cipherteks tidak hanya satu arah namun bisa dua arah.

Namun secara keseluruhan, semua algoritma *cipher* transposisi mempunyai kelemahan yaitu serumit apapun kita melakukan transposisi atau permutasi pada karakter-karakter dalam plainteks, kita hanya melakukan mengacak urutan dari plainteks tidak mengubahnya. Kemunculan karakter cipherteks akan sama dengan plainteks, hal ini dapat memberikan pertunjuk bahwa proses enkripsi menggunakan salah satu algoritma *cipher* transposisi. Sehingga, usaha untuk memecahkan suatu *cipher transposisi* tidaklah sulit bila kita mencoba semua algoritma *cipher* transposisi. Pada subbab berikutnya, penulis akan mencoba memberikan usulan algoritma *cipher* transposisi yang baru.

3.2 Usulan Perbaikan

Setelah membandingkan kelebihan dan kekurangan

dari masing-masing algoritma *cipher* transposisi, penulis memberikan sebuah usulan perbaikan dengan merancang sebuah algoritma *cipher* transposisi yang menggabungkan kelebihan dari semua algoritma lama.

Algoritma baru ini melakukan urutan penulisan plainteks menjadi cipherteks menggunakan *rail fence cipher* dalam bentuk kolom-kolom seperti pada *columnar transposition* dengan tambahan kunci seperti pada *route cipher*. Jadi bisa dikatakan algoritma baru ini merupakan sebuah *cipher* transposisi ganda. Untuk lebih jelasnya, contoh dari algoritma baru adalah sebagai berikut:

Misalkan kita mempunyai plainteks

HERE IS A SECRET MESSAGE THAT WILL BE ENCRYPTED BY A NEW ALGORITHM

enkripsi dilakukan dengan kunci KRIPTOGRAFI [6 9 4 8 11 7 3 10 1 2 5], *offset* = 1, ganjil atas-bawah, genap kiri-kanan

6	9	4	8	11	7	3	10	1	2	5
	H	E	R	E	I	S	A	S	E	C
T	E	G	A	S	S	E	M	T	E	R
H	A	T	W	I	L	L	B	E	E	N
N	A	Y	B	D	E	T	P	Y	R	C
E	W	A	L	G	O	R	I	T	H	M

maka cipherteksnya menjadi

STEYT SELTR CRNCM ISLEO HEAAW ESIDG ERAET GAMEH TWBEN YBPRE ALIH

Proses enkripsi dimulai dengan menghitung jumlah karakter dalam kata kunci, dalam hal ini KRIPTOGRAFI yaitu 11. Nilai ini menjadi nilai *k* seperti pada *rail fence cipher*, berarti kita akan membuat 11 kolom. Kesebelas kolom tersebut diberi nomor urutan sesuai abjad seperti pada *columnar transposition*. Urutan penulisan dilakukan sepert *rail fence cipher* secara horizontal, dan karena itu nilai *offset* perlu diperjhatikan, dalam hal ini bernilai 1, sehingga penulisan dilmulai dari dari kolom ke-2.

Setelah penulisan plainteks menjadi bentuk kolom-kolom, pembacaan cipherteks dilakukan sesuai dengan kunci pembacaan seperti pada *route cipher*, dalam hal ini “ganjil atas-bawah, genap kiri-kanan”. Hal ini berarti untuk semua nomor urutan ganjil pembacaan dilakukan dari atas ke bawah dan semua nomor urutan genap dibaca dari kiri ke kanan. Urutan kunci menentukan urutan pembacaan sehingga penulisan cipherteks yang dilakukan terlebih dahulu adalah nomor ganjil karena dalam kunci ganjil disebutkan terlebih dahulu.

Area-area kosong dapat diisikan dengan nilai *dummy* seperti pada *columnar transposition* ataupun tidak.

Penulis juga mempunyai sebuah usulan perbaikan lain dalam merancang sebuah *columnar transposition*. Perbaikan ini mengganti cara penempatan penulisan plainteks menjadi kolom-kolom. Apabila pada biasanya dalam *columnar transposition*, penulisan plainteks dalam satu baris dari kolom pertama sampai kolom terakhir terisi, dalam perbaikan ini.tidak semua kolom tersebut terisi. Setiap baris hanya memenuhi kolom sampai dengan nomor urutannya. Sebagai contoh:

Misalkan contoh plainteksnya adalah seperti sebelumnya, dengan menggunakan kunci KRIPTOGRAFI juga

6	9	4	8	11	7	3	10	1	2	5
H	E	R	E	I	S	A	S	E		
C	R	E	T	M	E	S	S	A	G	
E	T	H	A	T	W	I				
L	L	B								
E	E	N	C	R	Y	P	T	E	D	B
Y										
A	N	E	W	A	L					
G	O	R	I							
T	H									
M										

maka cipherteksnya menjadi

EAEGD ASIPR EHBNE RBHCE LEYAG TMSEW YLETA CWIER TLENO HSSTI MTRA

4. 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* adalah penulisan plainteksnya menjadi cipherteks. *Route Cipher* mempunyai rancangan kunci yang paling kuat. *Columnar transposition* digunakan untuk menambah kekuatan dan kerumitan suatu *cipher* lain. *Myszkowski transposition* adalah algoritma *cipher* transpose yang terbaik di antara algoritma lainnya.

Semua algoritma *cipher* transposisi mempunyai kelemahan 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. Atau dengan merancang sebuah algoritma baru sehingga menambah kemungkinan proses enkripsi yang digunakan.

Penulis merancang dua algoritma *cipher* transposisi baru. Algoritma pertama menggunakan kelebihan penulisan plainteks *rail fence cipher*, kunci *route cipher*, dan kolom-kolom *columnar transposition*. Algoritma kedua adalah sebuah variasi pengembangan dari *columnar transposition*. Algoritma ini menuliskan plainteks dalam kolom-kolom di mana setiap barisnya diisi sampai dengan nomor urutan kunci.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Sekolah Teknik Elektro dan Informatika ITB, 2007.

[2] http://en.wikipedia.org/wiki/Transposition_cipher, Akses: Oktober 2007

[3] http://www.purplehell.com/riddletools, Akses: Oktober 2007

[4] http://www.math.temple.edu/~renault/cryptology, Akses: Oktober 2007

[5] http://www.antilles.k12.vi.us/math/cryptotut, Akses: Oktober 2007