MODIFIKASI KRIPTOGRAFI TEKNIK TRANSPOSISI KOMBINASI DENGAN BILANGAN BINER

Nurhalias Jusman[1](17.83.0079), Rhendy Oentoko[2](17.83.0102), Zainal Ali Ika[3](17.83.0109)

Universias Amikom Yogyakarta, Jalan Ring Road Utara, Condongcatur, (0274) 884201

Program Studi Teknik Komputer, Universitas Amikom Yogyakarta

***e-mail* : [1]Nurhalis.j@gmail.com, [2]rhendy45@gmail.com, [3]zaenal.ali.ika.w@gmail.com**

Abstrak

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain, pengertian ini menurut terminologinya. Kriptografi diperkirakan sudah digunakan sejak 4000 tahun yang lalu di Mesir melalui *hieroglyph*. Kriptografi sangat penting untuk menyampaikan sesuatu yang rahasia agar tidak mudah diketahui secara umum. Dengan adanya kriptografi, rahasia suatu pesan dapat terjamin hingga pesan tersebut sampai kepada penerima. Pada makalah ini akan membahas kriptografi dengan Teknik transposisi dan mengkombinasikannya dengan bilangan biner.

Kata Kunci: *kriptografi, hieroglyph, transposisi, biner*

Abstract

Cryptography is the science and art of maintaining the security of messages when messages are sent from one place to another, this understanding by its terminology. Cryptography is estimated to have been used since 4000 years ago in Egypt through hieroglyph. Cryptography is very important to convey something secret so as not easily known in general. With the existence of cryptography, the secret of a message can be guaranteed until the message reaches the recipient. In this paper we will discuss cryptography with the technique of transposition and combine it with binary numbers.

Keywords*: cryptography, hieroglyph, transposition, binary*

2.PENDAHULUAN

Pada zaman sekarang ini, hampir semua piranti atau gawai terkoneksi dengan jaringan internet, maka dari ini dari sisi keamanan pun harus kita perhatikan. Karena pada saat ini orang lebih suka menggunakan media elektronik seperti *email* dan *instant message* untuk bertukar informasi. Informasi yang dibagikan tidak hanya informasi yang bersifat umum saja, akan tetapi juga informasi yang rahasia. Dalam bertukar informasi yang bersifat rahasia, dibutuhkan keamanan internet agar informasi yang bersifat rahasia tersebut sampai ke penerima yang dituju dan tidak jatuh ke pihak yang tidak berhak.

Salah satu dari algoritma kriptografi yang dapat digunakan untuk mengamankan informasi yaitu Algortima Kriptografi dengan Teknik Transposisi atau bisa disebut dengan Teknik Permutasi, 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. 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.

3. LANDASAN TEORI

Banyak sekali Teknik dalam Kriptografi saat ini. Salah satunya adalah Teknik Transposisi atau juga disebut permutasi, Teknik ini adalah Teknik penyandian dengan cara mengubah letak dari teks pesan yang akan disandikan. Untuk membaca pesan aslinya atau *Plaintext*, cukup dengan mengembalikan letak dan algoritma pergeseran huruf yang telah disepakati. Terdapat beberapa algoritma atau jenis-jenis dalam Teknik Transposisi. Antara lain yaitu, Transposisi Rail Fence, Transposisi Route, Transposisi Kolom, Transposisi Ganda, dan Transposisi Myszkowski.

Rail Fance atau juga bisa disebut alur pagar adalah bentuk penyandian transposisi dengan cara menuliskan huruf-huruf teks asli atau yang disebut dengan *Plaintext* secara turun naik dalam sebuah pagar imajiner. Sedangkan teks sandinya dibaca secara baris perbaris. Teknik ini juga bisa disebut dengan Teknik zig-zag.

Selanjutnya yaitu Transposisi, Teknik ini juga bisa disebut dengan Transposisi spiral. Metode ini hampi sama dengan metode Rail Fance. Penyandian metode Route dilakukan dengan cara menuliskan teks asli atau *Plaintext* secara kolom dari atas kebawah dalam sebuah kisi-kisi imajiner dengan ukuran yanb telah disepakati, misalnya dibaca secara spiral dengan arah jarum jam. Metode ini banyak sekali variasinya namun tidak semua algoritma tersebut memberikan hasil teks sandi yang memenuhi standar yang aman. Beberapa algoritma tidak mengacak teks asli dengan sempurna, sehingga akan memberikan celah yang dapat dengan mudah dipecahkan oleh seorang kriptoanalis.

Berikutnya adalah Transposisi metode Kolom. Penyandian metode kolom dituliskan secara baris dengan Panjang yang telah ditentukan sebagai kuncinya. Teks sandinya dibaca secara kolom demi kolom dengan pengacakan melalui permutasi angka kuncinya, panjang baris dan permutasi disebut sebagai kata kunci. Dalam proses metode ini, kata kunci tersebur didefinisikan dahulu dengan angka sesuai urutan abjad. Sedangkan proses untuk mengembalikan ke teks sandi atau *Chipertext* ke *Plaintext* dilakukan langkah kebalikan darinya. Kelebihan - Rail Fence Cipher unggul dalam penulisan plainteks menjadi cipherteks karena penulisan dapat dilakukan dari baris mana saja. - Route Cipher mempunyai rancangan kunci yang paling kuat karena mempunyai kunci paling banyak. - Columnar transposition 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.

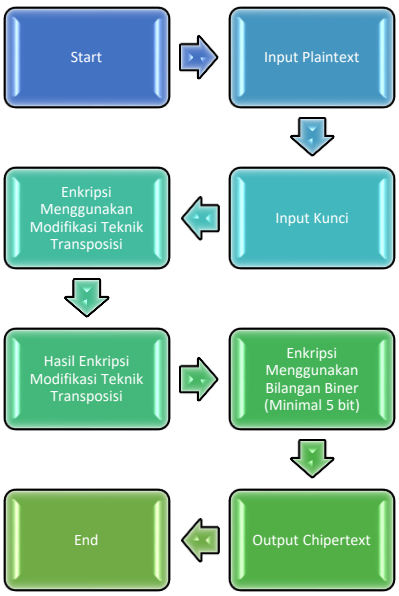
Hipotesis pada jurnal kali ini membahas tentang penguatan peningkatan keamanan pada tekik Transposisi dan Biner sehingga membuat kemanan suatu data meningkat jika menggunakan metone ini.

4. KONSEP DASAR

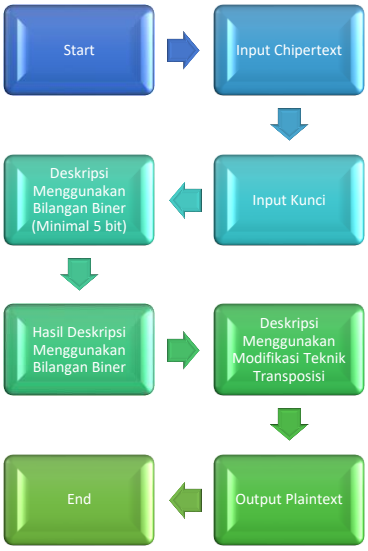
Teknik Transpos-Biner merupakan penggabungan antara Kriptografi Teknik dengan penambahan bilangan biner sesudah proses pengkodean pada tahap permutasi. Pada Teknik ini menggunakan kunci yang berbeda dengan Teknik permutasi yang asli.

Pada Teknik kombinasi ini pada saat proses enskripsi setelah memasukan atau menentukan *Plaintext* yang minimal 8 karakter agar sesuai dengan kunci, lalu masukan kunci 4 6 8 3 7 1 5 2 dan akan mendapatkan *Chipertext* pertama setelah mengenskripsi dengan kunci tersebut kemudian kita mengenskripsi lagi menggunakan Bilangan Biner yang minimal 5 bit.

Selanjutnya akan mendapatkan *output* Chipertext yang merupakan hasil kombinasi antara Teknik Transposisi atau Teknik Permutasi ditambahkan dengan Bilangan Biner minimal 5 bit.



Sedangkan pada saat akan mendeskripsikan suatu *Chipertext*, maka kita memasukan kunci 6 8 4 1 7 2 5 3 pada *Chipertext* lalu pertama mendeskripsikan menggunakan Bilangan Biner 5 bit dan akan menghasilkan hasil deskripsi menggunakan Bilangan Biner. Setelah itu, deskripsikan lagi dengan menggunakan modifikasi Teknik Transposisi dan kita akan mendapatkan sebuah *Plaintext*.



5. HASIL DAN PEMBAHASAN

Berikut ini adalah contoh untuk proses enskripsi dan diskripsi menggunakan Modifikasi Teknik Transposis di kombinasi dengan Bilangan Biner. Diketahui sebuah *Plaintext* “Saya Anak Teknik Komputer” lalu di urutkan setiap huruf dengan kunci ennskripsi modifikasi teknik transposisi per huruf,

S	A	Y	A	A	N	A	K
4	6	8	3	7	1	5	2
T	E	K	N	I	K	K	O
4	6	8	3	7	1	5	2
M	P	U	T	E	R	X	X
4	6	8	3	7	1	5	2

Karena pada akhir kata kekurangan karakter, maka harus di tambahi dengan

huruf “X” supaya pas dengan kunci dan memudahkan saat proses deskripsi.

Dan pada proses enskripsi tersebut menghasilkan *Chipertext* “ANKYASAA NKOKKTIE TRXUXMEP”.

Selanjutnya masuk ke proses enskirpsi lagi dengan Bilangan Biner. Bilangan biner yang digunakan minimal 5 bit dan maksimal 15 bit, karena jika kurang dari 5 bit akan ada kendala dalam proses enskripsi. Dan akan menghasilkan *Chipertext* yang berupa bilanga biner menurut nilai dari satu huruf pada *Chipertext* sebelumnya.

00000 01101 01010 11000 00000 10010 00000 00000 01101 01010 01110 01010 01010 10011 01000 00100 10011 10001 10111 10100 10111 01100 00100 01111

Dan pada proses deskripsi, diketahui sebuah *Chipertext* yang berupa Bilangan Biner yaitu

00000 01101 01010 11000 00000 10010 00000 00000 01101 01010 01110 01010 01010 10011 01000 00100 10011 10001 10111 10100 10111 01100 00100 01111. Kunci untuk mengubah Bilangan Biner tersebut yaitu dengan 5 Bit. Dan akan menjadi

00000 = A

01101 = N

01010 = K

11000 = Y

00000 = A

10010 = S

00000 = A

00000 = A

01101 = N

01010 = K

01110 = O

01010 = K

01010 = K

10011 = T

01000 = I

00100 = E

10011 = T

10001 = R

10111 = X

10100 = U

10111 = X

01100 = M

00100 = E

01111 = P

Dan akan menghasilkan *chipertext* berupa huruf “ANKYASAANKOKKTIETRXUXMEP”. Selanjutnya *input* kunci untuk deskripsi

A	N	K	Y	A	S	A	A
6	8	4	1	7	2	5	3
N	K	O	K	K	T	I	E
6	8	4	1	7	2	5	3
T	R	X	U	X	M	E	P
6	8	4	1	7	2	5	3

Dengan kunci 68417253, akan didapatkan sebuah *Plaintext* yang terakhir. *Plaintext* atau teks asli dari *Chipertext* tersebut yaitu “ Saya Anak Teknik Komputer xx”.

Kompleksitas Algoritma

- Algoritma yang sudah ada (Teknik Transposisi)
  - Time :
  - Step :
  - Kesulitan :
- Algoritma Yang digunakan (Teknik Kombinasi Transposisi)
  - Time :
  - Step :
  - Kesulitan :

6.KESIMPULAN

Dari keseluruhan makalah ini, dapat diambil kesimpulan sebagai berikut:

1. Algoritma Teknik Transposisi bisa disebut juga dengan algoritma Teknik Permutasi
2. Algortima Teknik Transposisi mempunyai berbagai jenis metode
3. Pada Modifikasi Teknik Transposisi pada saat proses enskripsi menggunakan Kunci 4 6 8 3 7 1 5 2
4. Sedangkan pada saat proses deskripsi menggunakan 6 8 4 1 7 2 5 3
5. Teknik kombinasi ini memerlukan bilangan biner minimal 5 bit dan maksimal 15 bit.

DAFTAR PUSTAKA

Ariyus, Donny. 2008. *Pengantar Kriptografi Teori, Analisis dan Implementasi*. Penerbit Andi.

http://www.antilles.k12.vi.us/math/cryptotut/transposition.htm diakses pada April 2018