IMPLEMENTASI KOMBINASI ALGORITMA TRANSPOSISI RAIL FENCE CHIPPER DAN AFFINE CHIPPER PADA KEAMANAN UNTUK APLIKASI PEYANDIAN PESAN

Kristin Lorensi Sitompul[1] , Jefri Sirait[2]
[1] Prodi Sistem Informasi Program Sarjana Universitas Audi Indonesia
[2] Mahasiswa Prodi Sistem Informasi Program Sarjana Universitas Audi Indonesia
sriwijaya11121987@gmail.com

ABSTRAK

Dalam permasalahan pengiriman pesan atau data telah menjadi permasalah yang besar atau penting pada zaman era teknologi yang semakin canggih sekarang ini. Ada kala pengiriman pesan harus bersistem rahasia agar tidak diketahui oleh orang lain dalam arti tidak diketahui secara umum. Apabila pesan tersebut diketahui orang lain atau dapat dikomsumsi orang lain secara umum maka dapat disalahgunakan untuk melakukan kejahatan. Kriptografi adalah seni teknik untuk pengamanan pesanan yang dianggap rahasia. Metode klasik adalah salah satu cara untuk menyembunyikan pesan rahasia dari para kriptanalis. Dalam paper ini penulis memaparkan sebuah pengembangan dari algoritma klasik untuk mempersulit kriptanalis mencuri pesan yang dirahasiakan. Untuk itu penulis mencoba mengkombinasi algoritma transposisi Rail Fence Chipper dengan Affine Chipper. Dengan adanya kombinasi algoritma ini, maka kriptanalis akan sulit dan membutuhkan waktu lama untuk mencuri pesan yang sudah dirahasiakan

Kata Kunci: Transposisi Rail Fence Chipper, Affine Chipper, Kriptografi Kalsik

IMPLEMENTATION OF THE COMBINATION OF THE RAIL FENCE CIPHER AND AFFINE CIPHER TRANSPOSITION ALGORITHM ON SECURITY FOR MESSAGE ENCORDING APPLICATIONS

ABSTRACT

The problem of sending messages or data has become a big or important problem in the era of increasingly sophisticated technology today. There are times when sending messages must be confidential so as not to be known by others in the sense of not being known in general. If the message is known to others or can be consumed by others in general, it can be misused to commit crimes. Cryptography is the art of engineering for securing orders that are considered secret. The classic method is one way to hide secret messages from cryptanalysts. In this paper, the author describes a development of a classical algorithm to make it difficult for cryptanalysts to steal confidential messages. For this reason, the author tries to combine the Rail Fence Chipper transposition algorithm with the Affine Chipper. With this combination of algorithms, cryptanalysts will find it difficult and take a long time to steal messages that have been kept secret.

Keywords: *Rail Fence Chipper Transposition, Affine Chipper, Kalsik Cryptography*

PENDAHULUAN

Kemajuan teknologi di bidang komputer memungkinkan ribuan orang dan komputer di seluruh dunia terhubung dalam satu dunia maya yang dikenal sebagai *cyberspace* atau Internet. Begitu juga ratusan organisasi seperti perusahaan, lembaga negara, lembaga keuangan, militer dan sebagainya.Tetapi sayangnya, kemajuan teknologi selalu diikuti dengan sisi buruk dari teknologi itu sendiri. Salah satunya adalah rawannya keamanan data sehingga menimbulkan tantangan dan tuntutan akan tersedianya suatu sistem pengamanan data yang sama canggihnya dengan kemajuan teknologi komputer itu sendiri. Ini adalah latar belakang berkembangnya sistem keamanan data untuk melindungi data yang ditransmisikan melalui suatu jaringan komunikasi. Ada beberapa cara melakukan pengamanan data yang melalui suatu saluran, salah satu diantaranya adalah kriptografi. Dalam kriptografi, data yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa sehingga kalaupun data itu bisa dibaca maka tidak bisa dimengerti oleh pihak yang tidak berhak. Data yang akan dikirimkan dan belum mengalami penyandian dikenal dengan isitilah plaintext, dan setelah disamarkan dengan suatu cara penyandian, maka plaintext ini akan berubah menjadi ciphertext. Pembakuan penulisan pada kriptografi dapat ditulis dalam bahasa matematika. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi.

METODE PENELITIAN

Rail Fence Cipher merupakan salah satu variasi implementasi *cipher* transposisi. Pada *Rail Fence Cipher*, plainteks dituliskan secara vertikal ke bawah sepanjang n-*rails*, dan menulis lagi ke kolom baru ketika telah mencapai karakter ke-n. Cipherteks yang dihasilkan adalah urutan karakter yang dibaca secara horizontal. Sebagai contoh, kita mempunyai n=3 dan sebuah pesan WE ARE DISCOVERED FLEE AT ONCE , maka ditulis

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

Karakter tambahan di akhir cipherteks sengaja dibubuhkan diantaranya untuk melengkapi cipherteks sehingga melengkapi blok dan atau untuk mengelabui kriptanalis. Pesan tersebut kemudian dibaca. WRIOR FEOEX EESVE LANXX ADCED ETCXX.

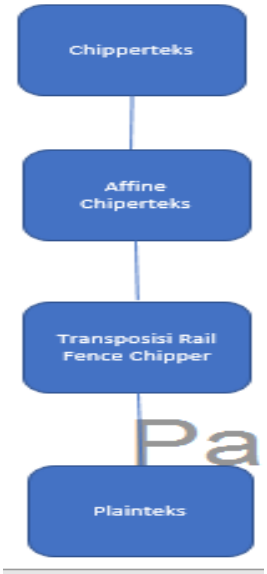
Penulisan pesan menjadi blok-blok standar, biasanya sepanjang 5 karakter, dilakukan untuk memudahkan pentransmisian pesan pada telegraf. Algoritma *Rail Fence Cipher* ini tidak terlalu kuat, kemungkinan kunci-kunci yang dipakai terlalu kecil sehingga kriptanalis dapat mencobanya semua dengan manual. Algoritma Affine Chiper Affine cipher pada metode affine adalah perluasan dari metode Caesar Cipher, yang mengalihkan plainteks dengan sebuah nilai dan menambahkannya dengan sebuah pergeseran P menghasilkan cipherteks C dinyatakan dengan fungsi kongruen:

$C \equiv m P + b \pmod n$

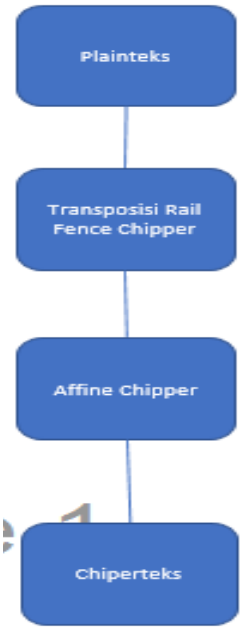
Yang mana n adalah ukuran alphabet, m adalah bilangan bulat yang harus relatif prima dengan n (jika tidak relatif prima, maka dekripsi tidak bisa dilakukan) dan b adalah jumlah pergeseran (Caesar cipher adalah khusus dari affine cipher dengan m=1). Untuk melakukan deskripsi, persamaan (4) herus dipecahkan untuk memperoleh P. Solusi kekongruenan tersebut hanya ada jika inver m (mod n), dinyatakan dengan m^{-1}. Jika m^{-1} ada maka dekripsi dilakukan dengan persamaan sebagai berikut: $P \equiv m^{-1}(C - b) \pmod n$.

HASIL PENELITIAN DAN PEMBAHASAN

Yang dilakukan penulis dalam makalah ini adalah dengan menggunakan *Rail Fence Cipher* yang telah dimodifikasi oleh penulis dan selanjutnya menggunakan *Affine Cipher*. Sebagai penjelasan , proses enkripsi dan dekripsi pada dapat dilihat pada bagan pada gambar berikut:



Gambar 1. Bagan enkripsi hasil modifikasi



Gambar 2. Bagan dekripsi hasil modifikasi

Penggunaan modifikasi *Rail Fence Cipher* dan *Affine Cipher* dalam melakukan proses enkripsi plainteks dapat dilihat pada contoh berikut: Penggunaan modifikasi *Rail Fence Cipher* dan *Affine Cipher* dalam melakukan proses enkripsi plainteks dapat dilihat pada contoh berikut:

Kita mempunyai pesan " INDAH PELANGI" dengan kunci "IBU" maka dilakukan proses sebagai berikut :

41.Melakukan enkripsi dengan *Rail Fence Cipher* yang telah dimodifikasi, ditulis

Y	I	A	E	N

E	N	H	H	G
S	D	P	A	I

Karakter tambahan di akhir cipherteks sengaja dibubuhkan diantaranya untuk melengkapi cipherteks sehingga melengkapi blok dan atau untuk mengelabui kriptanalis. Pesan tersebut kemudia dibaca berdasarkan keterurutan abjad, dalam contoh di atas kunci YES berarti dibaca sesuai urutan abjad yaitu ESY sehingga pesan menjadi NHHG DPAI IAEN Penulisan pesan menjadi blok-blok standar, biasanya sepanjang 4 karakter.

Melakukan enkripsi dengan Affine Chiper

C = 7.P + 3 Mod 26

Untuk melakukan enkripsi gunakan rumus diatas
Plainteks : NHHG DPAI IAEN

M = 7
K = 3
Enkripsi :

"N" = C1 = 7 (13) + 3 MOD 26 = 16 (Q)
"H" = C2 = 7 (7) + 3 MOD 26 = 0 (A)
"H" = C2 = 7 (7) + 3 MOD 26 = 0 (A)
"G" = C4 = 7 (6) + 3 MOD 26 = 19 (T)
"D" = C1 = 7 (3) + 3 MOD 26 = 24 (Y)
"P" = C1 = 7 (15) + 3 MOD 26 = 4 (E)
"A" = C1 = 7 (0) + 3 MOD 26 = 3 (D)
"I" = C1 = 7 (8) + 3 MOD 26 = 7 (H)
"I" = C1 = 7 (8) + 3 MOD 26 = 7 (H)
"A" = C1 = 7 (0) + 3 MOD 26 = 3 (D)
"E" = C1 = 7 (4) + 3 MOD 26 = 5 (F)
"N" = C1 = 7 (13) + 3 MOD 26 = 16 (Q)

Maka diperoleh cipherteks hasil enkripsi sebagai berikut:

" QAAT YEDH HDFQ"

3. Melakukan Deskripsi Affine chiper
   m^{-1}(c-k)mod n
   $kunci = 3$
   $m^{-1} = 15$
   Sehingga dapat menggunakan contoh diatas
   Chiperteks : QAAT YEDH HDFQ
   Kunci : 3
   Plainteksnya : NHHG DPAI IAEN
4. Melakukan Deskripsi dengan Rail Fence Cipher
   Dengan menggunakan kata kunci YES
   a. Langkah selanjutnya adalah mengurutkan kunci sesuai dengan abjad. Dalam kasus ini kunci adalah YES

Y=	I	A	E	N
E=	N	H	H	G
S=	D	P	A	I

b. Dan jika diurutkan sesuai abjad menjadi EYS

E=	N	H	H	G
S=	D	P	A	I
Y=	I	A	E	N

KESIMPULAN

Kombinasi beberapa metode pada kriptografi klasik seperti Transposisi Rail Fence Chipper dengan Affine Chipper output enkripsi dapat menambah tingkat kesulitan bagi kriptanalis yang berusaha meretas pesan yang dirahasiakan. Waktu yang disedot untuk memecahkan modifikasi algoritma kriptografi klasik ini dipastikan lebih lama dari pada memakai satu lapis algoritma saja.Maka pemakaian enkripsi berlapis dengan algoritma yang berbeda sangat baik untuk digunakan.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. 2004. Diktat Kuliah IF2153 Matematika Diskrit – Edisi Keempat. Bandung: Program Studi Tenik Informatika, STEI ITB. 2004. Sistem Chiper Klasik.http://kur2003.if.itb.ac.id/file/Sistem%20Chiper%20Klasik.doc.

[2] 23 Desember 2006. Pengamanan Informasi dan Kriptografi - Menambah khasanah bacaan kriptologi dan pengamanan informasi bagi masyarakat

[3] http://www.geeksforgeeks.org/implementation-affine-cipher/

[4] http://www.sanfoundry.com/cpp-program-implement-affine-cipher/

[5] Ariyus, Dony, *Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi,* Andi, 2008