SISTEM PENYANDIAN TEKS MENGGUNAKAN ALGORITMA KRIPTOGRAFI *RAILFENCE* DAN *AUTOKEY*

Dyna Marisa Khairina[1], Anindita Septiarini[2] dan Deni Rahmadi[3]
Jurusan Ilmu Komputer, Fakultas MIPA, Universitas Mulawarman[1,2,3]
Jl. Barong Tongkok No. 4, Gunung Kelua, Samarinda, 75119
E-mail : dyna.ilkom@gmail.com[1] deeta82@yahoo.com[2]

Abstrak

Kerahasiaan data sangat diperlukan dalam hal komunikasi data. Untuk menjamin keamanan dan kerahasiaan data tersebut diperlukan teknik tertentu untuk menyandikan data, pesan maupun informasi yang disebut dengan kriptografi. Kriptografi merupakan seni dan ilmu menyembunyikan data, pesan atau informasi dari pihak yang tidak berhak. Pesan yang belum disandikan disebut dengan plainteks, dan pesan yang telah disandikan disebut dengan cipherteks. Untuk proses menyandikan pesan diperlukan sebuah kunci yang juga digunakan untuk membaca pesan yang telah disandikan. Penelitian ini mengkombinasikan dua bentuk kriptografi sederhana sehingga membuat hasil penyandian menjadi sulit untuk dipecahkan. Dua bentuk kriptografi tersebut adalah kriptografi railfence dan kriptografi autokey. Kriptografi ini merupakan suatu sistem yang menerapkan dua teknik yang berbeda yakni teknik transposisi dan teknik subtitusi. Penelitian ini menghasilkan aplikasi penyandian teks menggunakan algoritma kriptografi railfence dan autokey. Hasil dari penelitian menunjukkan bahwa hasil penyandian yang dilakukan dapat didefinisikan kembali ke bentuk semula sehingga teks dapat terbaca kembali.

***Kata Kunci*: Kriptografi, Railfence, Autokey**

I. PENDAHULUAN

Kemajuan teknologi yang sangat pesat terutama di bidang komputer memungkinkan setiap orang dan komputer di seluruh dunia terhubung melalui dunia maya. Begitu juga organisasi-organisasi diseluruh dunia seperti perusahaan, lembaga negara, lembaga keuangan, militer dan lain sebagainya. Organisasi-organisasi tersebut sangat membutuhkan keamanan bagi aset-asetnya, terutama informasi-informasi dan data-data penting.

Seiring kemajuan teknologi yang sangat membantu kehidupan manusia, diikuti pula dengan sisi buruk dari teknologi itu sendiri. Salah satunya adalah mengenai keamanan data sehingga menimbulkan tuntutan akan tersedianya suatu sistem pengamanan data yang lebih baik agar dapat mengamankan data dari berbagai ancaman yang mungkin timbul. Ini merupakan latar belakang berkembangnya sistem keamanan data yang berfungsi untuk melindungi data yang ditransmisikan atau dikirimkan melalui suatu jaringan komunikasi.

Ada beberapa cara melakukan pengamanan data ataupun pesan yang ditransmisikan melalui suatu jaringan, salah satu diantaranya adalah dengan menggunakan teknik penyandian yang disebut dengan kriptografi. Kriptografi merupakan ilmu sekaligus seni dalam menjaga kerahasiaan data atau pesan. Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa. Sehingga seandainya data tersebut bisa diperoleh dan dibaca oleh orang lain, maka pihak yang tidak berhak tersebut tidak akan bisa mengerti arti dari data tersebut.

Data asli yang akan dikirimkan dan belum mengalami penyandian dikenal dengan istilah plainteks (*plaintext*). Kemudian setelah disamarkan dengan suatu cara penyandian, maka *plaintext* ini disebut sebagai cipherteks (*chipertext*). Proses penyamaran dari plainteks ke cipherteks disebut enkripsi (*encryption*), dan proses pengembalian dari cipherteks menjadi plainteks kembali disebut dekripsi (*decryption*).

Berdasarkan penelitian sebelumnya oleh Purboyono pada tahun 2011 dengan judul "Pemanfaatan *Railfence* Cipher Sebagai Sandi Transposisi Untuk Memperkuat Sandi Subtitusi *Affine* Cipher" dan pada buku yang ditulis oleh Ariyus pada tahun 2008 dengan judul "Pengantar Ilmu Kriptografi : Teori, analisis dan implementasi" yang menjadi sumber referensi pustaka dalam penelitian ini. Penggunaan algoritma kriptografi dan bahasa pemrograman yang berbeda, diharapkan dapat membantu menambah pustaka referensi dan

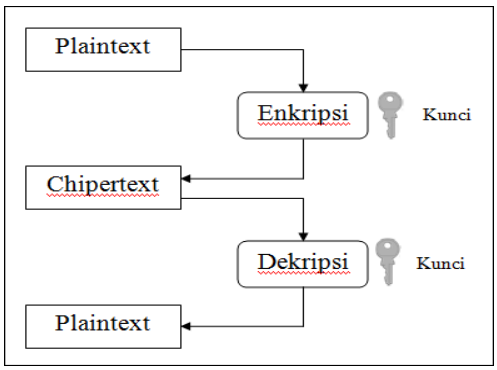
literatur keilmuan pembaca pada umumnya. Dalam membangun aplikasi pada penelitian ini menggunakan algoritma kriptografi *railfence* dan algoritma kriptografi *autokey*. Kedua algoritma ini dikombinasikan untuk menghasilkan cipherteks yang tidak mudah dipecahkan.

II. METODELOGI PENELITIAN

Sistem Penyandian Teks menggunakan Algoritma Kriptografi *Railfence* dan *Autokey* adalah suatu sistem yang dapat digunakan untuk menyandikan dan merahasiakan pesan atau teks sehingga tidak bisa dibaca tanpa menggunakan kunci yang benar. Dalam aplikasi penyandian teks ini, terdapat dua buah proses utama, yaitu proses enkripsi dan proses dekripsi.

1. Kriptografi

Kriptografi berasal dari bahasa Yunani yang terdiri atas dua kata, yaitu *crypto* dan *graphia*. *Crypto* yang mempunyai arti rahasia (*secret*) dan *graphia* yang mempunyai arti menulis (*writing*). Kriptografi adalah ilmu yang berguna untuk mengacak (kata yang lebih tepat adalah *masking*) data sedemikian rupa sehingga tidak bisa dibaca oleh pihak ketiga. Tentu saja data yang diacak harus bisa dikembalikan ke bentuk semula oleh pihak yang berwenang (Fidens, 2006).



Gambar 1. Enkripsi dan Dekripsi Sederhana

Pada dasarnya kriptografi terdiri dari beberapa komponen (Ariyus, 2007) :

1) Enkripsi : merupakan hal yang sangat penting dalam kriptografi sebagai pengamanan atas data yang dikirim agar rahasianya terjaga. Pesan aslinya disebut *plaintext* yang diubah menjadi kode-kode yang tidak dimengerti yang disebut dengan *chipertext*. Untuk mengubah *plaintext* kedalam *chipertext* digunakan algoritma yang bisa mengkodekan data yang diinginkan.
2) Dekripsi : merupakan kebalikan dari enkripsi, pesan yang telah dienkripsi dikembalikan ke bentuk asalnya, yang disebut dengan dekripsi pesan.
3) Kunci : berfungsi untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua, yakni kunci pribadi (*private key*) dan kunci umum (*public key*).
4) *Chipertext* : merupakan suatu pesan yang sudah melalui proses enkripsi. Pesan yang ada pada *chipertext* tidak bisa dibaca karena berisi karakter-karakter yang tidak memiliki makna (arti).
5) *Plaintext* : sering juga disebut sebagai *cleartext*, merupakan suatu pesan bermakna yang ditulis atau diketik (pesan asli) dan *plaintext* itulah yang kemudian akan diproses menggunakan algoritma kriptografi tertentu agar menjadi *chipertext*.
6) Pesan : pesan ini bisa berupa data atau informasi yang dikirim (melalui kurir, saluran komunikasi data, dan sebagainya) atau yang disimpan di dalam media perekaman (kertas, *storage*, dan sebagainya).
7) Kriptanalisis : bisa diartikan sebagai analisis sandi atau suatu ilmu untuk mendapatkan *plaintext* tanpa harus mengetahui kunci secara wajar. Jika suatu *chipertext* berhasil menjadi *plaintext* tanpa menggunakan kunci yang sah, maka proses tersebut dinamakan *breaking code* yang dilakukan oleh para kriptanalis. Analisis sandi juga mampu menemukan kelemahan kunci atau *plaintext* dari *chipertext* yang dienkripsi menggunaan algoritma tertentu.

2. Kriptografi *Railfence*

Railfence merupakan salah satu variasi implementasi cipher transposisi. *Railfence* juga melibatkan penulisan plainteks yang disusun berdasarkan baris. Urutan karakter pada baris pertama akan diikuti oleh karakter berikutnya pada baris dibawahnya pada kolom kedua, dan seterusnya hingga *n-rail*. Apabila penulisan kebawah sudah mencapai *n*, maka penulisan dilakukan ke baris diatasnya dan seterusnya. Bila penulisan keatas juga sudah mencapai *n-rail*, maka penulisan dilakukan seperti awal. Cipherteks dibaca secara horizontal.

Sebagai contoh, jika plainteks adalah CT-ONLINE dan ditetapkan $n = 3$. Proses enkripsinya dapat dilihat pada Tabel 1.

Tabel 1. Proses Enkripsi *Railfence*

PLAINTEKS	C	T	-	O	N	L	I	N	E
$n = 3$	C				N				E
		T		O		L		N	
			-				I		
CIPHERTEKS	C	N	E	T	O	L	N	-	I

(Sumber : www.cryptool-online.org, 2012)

3.

Sedangkan untuk proses dekripsi dilakukan dengan menyusun kembali karakter *chipertext* secara zig-zag dengan $n = 3$, dan kemudian dibaca secara horizontal. Proses dekripsinya dapat dilihat pada Tabel 2.

Tabel 2. Proses Dekripsi *Railfence*

PLAINTEKS	C	N	E	T	O	L	N	-	I
n = 3	C				N				E
		T		O		L		N	
			-				I		
CIPHERTEKS	C	T	-	O	N	L	I	N	E

(Sumber : www.cryptool-online.org, 2012)

4. Kriptografi *Autokey*

Autokey merupakan salah satu variasi implementasi cipher subtitusi. *Autokey* adalah pengembangan dari kriprografi Caesar dan Vigenere. Pada kriptografi *autokey,* digunakan sebuah kata sebagai kunci. Kata ini diletakkan di awal kunci kemudian diikuti dengan plaintext sehingga membentuk huruf-huruf yang sama panjangnya dengan plaintext. Urutan huruf-huruf ini yang akan digunakan sebagai kunci pada saat enkripsi. *Autokey* merupakan salah satu jenis kriptografi yang termasuk dalam algoritma kriptografi simetri.

Algoritma enkripsi dan dekripsi *autokey* :

1. Algoritma untuk enkripsi: Ci = (Pi + Ki) mod 26
2. Algoritma untuk dekripsi: Pi = (Ci - Ki) mod 26

Dimana : Ci = Cipherteks ; Pi = Plainteks ; dan Ki = Kunci

Sebagai contoh, jika plainteks adalah THISISASECRET dan kata pada awal kunci adalah KEY, diasumsikan A = 0, B = 1, C = 2, …, Z = 25. Proses enkripsinya dapat dilihat pada Tabel 3.

Tabel 3. Proses Enkripsi *Autokey*

PLAINTEKS	T	H	I	S	I	S	A	S	E	C	R	E	T
	19	7	8	18	8	18	0	18	4	2	17	4	19
KUNCI	K	E	Y	T	H	I	S	I	S	A	S	E	C
	10	4	24	19	7	8	18	8	18	0	18	4	2
(Pi + Ki)	29	11	32	37	15	26	18	26	22	2	35	8	21
mod 26	3	11	6	11	15	0	18	0	22	2	9	8	21
CIPHERTEKS	D	L	G	L	P	A	S	A	W	C	J	I	V

(Sumber : www.cryptool-online.org, 2012)

Sedangkan untuk proses dekripsi dilakukan dengan mengurangkan karakter *chipertext* (diasumsikan A = 0, B = 1, C = 2, …, Z = 25) dengan kunci dan setelah itu di-*mod*-kan 26. Proses dekripsinya dapat dilihat pada Tabel 4.

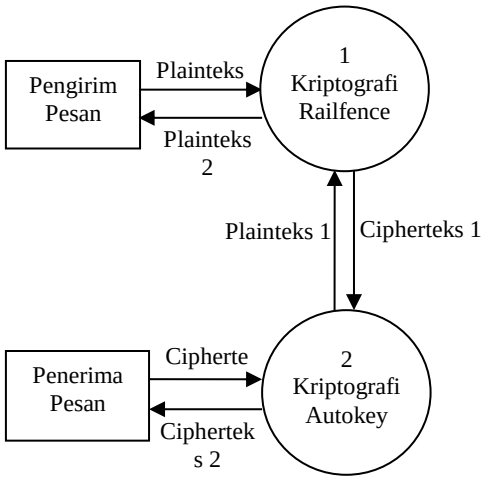
Tabel 4. Proses Dekripsi *Autokey*

CIPHERTEKS	D	L	G	L	P	A	S	A	W	C	J	I	V
	3	11	6	11	15	0	18	0	22	2	9	8	21
KUNCI	K	E	Y	T	H	I	S	I	S	A	S	E	C
	10	4	24	19	7	8	18	8	18	0	18	4	2
(Ci - Ki)	-7	7	-18	-8	8	-8	0	-8	4	2	-9	4	19
mod 26	19	7	8	18	8	18	0	18	4	2	17	4	19
PLAINTEKS	T	H	I	S	I	S	A	S	E	C	R	E	T

(Sumber : www.cryptool-online.org, 2012)

5. Data Flow Diagram (DFD)

Data Flow Diagram (DFD) adalah suatu diagram yang menggunakan notasi-notasi untuk menggambarkan arus dari data sistem. *Data Flow Diagram* (DFD) adalah gambaran sistem secara logika, gambaran ini tidak tergantung pada perangkat keras, perangkat lunak, struktur data dan organisasi file. Keuntungan menggunakan DFD adalah memudahkan pemakai (*user*) yang kurang menguasai bidang komputer untuk mengerti dan memahami sistem. Penggunaannya sangat membantu untuk memahami sistem secara logika, terstruktur dan jelas.

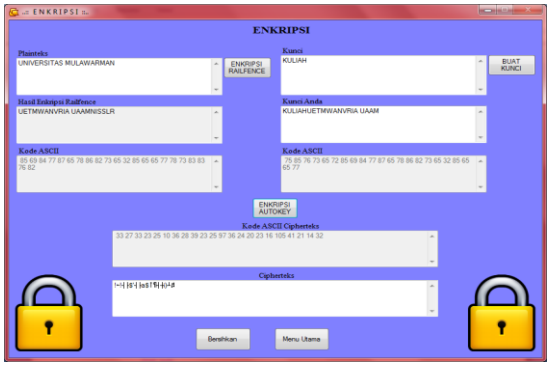


Gambar 2. Data Flow Diagram Penyandian Pesan

III. HASIL DAN PEMBAHASAN

1. Form Proses Enkripsi

Form proses enkripsi merupakan *form* yang dibuat untuk proses penyandian pesan dari pesan asli menjadi pesan yang tidak bisa dibaca tanpa menggunakan kunci yang benar. Proses enkripsi pesan terdiri dari dua tahap utama. Yang pertama adalah proses enkripsi menggunakan algoritma kriptografi *railfence* dan yang kedua adalah proses enkripsi menggunakan algoritma kriptografi *autokey*. Adapun implementasi *form* proses enkripsi dengan menggunakan plainteks UNIVERSITAS MULAWARMAN dan kata kunci KULIAH (karakter diasumsikan dengan menggunakan nilai ASCII dan penggunaan *modulo* 127) ditunjukkan pada Gambar 3.



Gambar 3. Implementasi *Form* Proses Enkripsi

2. Form Proses Dekripsi

Form proses dekripsi merupakan *form* yang dibuat untuk proses penerjemahan pesan dari cipherteks menjadi pesan asli atau plainteks, dengan menggunakan kunci yang digunakan dalam proses enkripsinya. Proses dekripsi pesan terdiri dari dua tahap utama. Yang pertama adalah proses dekripsi menggunakan algoritma kriptografi *autokey* dan yang kedua adalah proses dekripsi menggunakan algoritma kriptografi *railfence*. Adapun hasil implementasi *form* proses dekripsi ditunjukkan pada Gambar 4.

Gambar 4. Implementasi *Form* Proses Dekripsi

IV. KESIMPULAN

Berdasarkan hasil penelitian dan implementasi sistem penyandian teks dapat diambil kesimpulan bahwa sistem ini mampu melakukan penyandian pesan dan penerjemahan kembali pesan yang telah disandikan dengan menggunakan algoritma kriptografi *railfence* dan *autokey*. Untuk memperoleh cipherteks yang kuat, kelemahan dari algoritma *railfence* mampu diatasi dengan penggunaan algoritma *autokey*. Namun, penggunaan algoritma *autokey* membuat kunci menjadi sama panjang dengan plainteks.

Berdasarkan hasil uji coba pada plainteks, dapat disimpulkan bahwa pesan dapat dienkripsi dan didekripsikan kembali dengan tepat, kecuali penggunaan tombol *Enter* pada plainteks yang tidak dapat didekripsikan.

V. DAFTAR PUSTAKA

[1] Ariyus, D. *Kriptografi : Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu. 2006.

[2] Ariyus, D. *Pengantar Ilmu Kriptografi : Teori, analisis dan implementasi*. Yogyakarta: Andi. 2008.

[3] Kusumo, A. S. *Kriptografi Menggunakan VB.NET*. 2003.

[4] Munir, R. *Algoritma dan Pemrograman : Dalam Bahasa Pascal dan C*. Bandung: Informatika. 2004.

[5] Munir, R. *Kriptografi*. Bandung: Informatika. 2006.

[6] Purboyono, A. *Pemanfaatan Railfence Cipher Sebagai Sandi Transposisi Untuk Memperkuat Sandi Subtitusi Affine Cipher*. Skripsi Sarjana Jurusan Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta. 2011.