SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Publikasi Jurnal & Penelitian Teknik Informatika
Volume 2 Nomor 2, April 2018
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Kombinasi Algoritma Playfair Cipher Dengan Metode Zig-zag Dalam Penyandian Teks

Ananda Hariati
STMIK Budi Darma Medan
Jl. SM. Raja No. 338 Sp. Limun Medan
anandahariati1994@gmail.com

Kiki Hardiyanti
STMIK Budi Darma Medan
Jl. SM. Raja No. 338 Sp. Limun Medan
kikihardiyanti83@gmail.com

Widya Eka Putri
STMIK Budi Darma Medan
Jl. SM. Raja No. 338 Sp. Limun Medan
widyaeka015@gmail.com

Abstract — Keamanan teks sebagai salah satu media untuk menyampaikan pesan atau informasi sangat umum digunakan saat ini. Informasi yang disampaikan dalam bentuk teks dapat bersifat penting atau rahasia. Oleh karena itu, perananan teknik pengamanan sangat penting diimplementasikan pada teks yang memiliki sifat seperti itu. Algoritma kriptografi dapat digunakan sebagai salah satu solusi yang dapat digunakan untuk menangkal tindakan-tindakan penyalahgunaan informasi penting dalam bentuk teks. Teknik kriptografi dengan algoritmanya dapat merubah teks informasi asli menjadi sandi-sandi (simbol-simbol) yang sangat sulit ditemukan korelasi dan makanya. Algoritma *playfair cipher* melakukan penyandian teks dengan mensubtitusikan masing-masing karakter teks dengan karakter yang baru sesuai dengan formulasinya, sedangkan metode *zig-zag* akan melakukan transposisi atau pengacakan posisi karakter-karakter yang dihasilkan dari proses enkripsi *playfair cipher*. Tujuan penelitian ini adalah menghasilkan *cipher* dari sebuah teks yang menyulitkan pihak-pihak lain untuk menemukan makna teks yang sebenarnya, sehingga kerahasiaan teks tetap terpelihara dengan baik.

Keywords— *kriptografi, algoritma, playfair, zig-zag, teks.*

I. PENDAHULUAN

Masalah keamanan informasi yang bersifat penting atau rahasia tidak boleh diabaikan. Saat ini penyampaian informasi berbasis teks menjadi elemen yang paling umum digunakan dalam berkomunikasi. Berbagai tindakan penyalahgunaan informasi penting seperti pecurian, penyadapan, pemanfaatan bahakan modifikasi terhadap teks informasi yang didistribusikan masing sering terjadi, sehingga dapat merugikan pemillik informasi sendiri. Tindakan penyalahgunaan sering kali terjadi pada data yang didistribusikan melalui jaringan internet.

Kriptografi sebagai salah satu teknik pengamanan data, dapat diimplementasikan sebagai salah satu solusi untuk meminimalisir tindakan-tindakan kejahatan terhadap informasi penting atau rahasia. Berdasarkan penelitian sebelumnya, mengatakan bahwa media *internet* saat ini menjadi media yang paling banyak digunakan dalam berdistribusi informasi yang bersifat rahasia [1][2]. Setyaningsih dalam penelitiannya mengatakan bahwa teknik kriptografi sangat penting diimplementasikan untuk melindungi data yang ditransmisikan melalui suatu jaringan komunikasi[3].

Playfair Cipher merupakan salah satu metode yang digolongkan dalam kriptogafi klasik yang proses enkripsinya menggunakan pemrosesan dalam bentuk blok-blok yang sangat besar. Metode ini merupakan salah satu cara untuk mengatasi kelemahan metode kriptografi klasik lainnya yang mudah tertebak karena terdapat korespondensi satu-satu antara *plaintext* dengan *ciphertext* [3][4]. Namun algoritma ini masih rentan terhadap serangan karena sandi *playfair cipher* dapat dipecahkan dengan menggunakan teknik analisis frekuensi pasangan huruf [5].

Teknik transposisi *cipher* enkripsi dan dekripsi pesan merupakan teknik yang diterapkan pada metode *zig zag cipher* sehingga mampu mengubah urutan huruf-huruf yang ada di dalam *plaintext* (pesan yang belum dienkripsi) menjadi *ciphertext*[6]. Format *matrix* yang membentuk baris dan kolom dapat diterapkan menjadi pola kerja dari *zig-zag* dalam melakukan transposisi teks asli. Namun

algoritma ini juga memiliki kelemahan, yaitu serumit apapun pola transposisi atau permutasi pada karakter-karakter dalam plainteks, namun yang terjadi bukan merubah karakter yang tekas asli, tetapi hanya mengacak posisi-posisi karakter.

Penelitian ini menguraikan penyandian teks rahasia atau penting dengan mengkombinasikan algoritma *playfair cipher* dengan metode *zig-zag*. Teks asli akan disandikan terlebih dahulu berdasarkan algoritma *playfair cipher*, kemdudian sandi yang dihasilkan dari proses enkripsi *playfair cipher* akan dienkripsi kembali berdasarkan metode *zig-zag*. Proses penyandian yang dilakukan secara ganda (dua kali) ini bertujuan untuk menghasilkan teks yang benar-benar acak serta tidak memperlihatkan pola-pola keterhubungannya dengan teks asli, sehingga dapat mempersulit pihak-pihak lain yang berusaha untuk mengetahui dan mendapatkan makna asli dari teks yang bersifat rahasia.

II. LANDASAN TEORI

A. *Kriptografi*

Teknik kriptografi merupakan teknik yang dapat digunakan untuk mengenkripsi naskah asli (*plaintext*) yang diacak menggunakan suatu kunci enkripsi menjadi naskah acak yang sulit dibaca atau dimengerti oleh pihak lain [7][8]. Penerapan teknik kriptografi harus dapat menjamin kerahasiaan, integritas, otentikasi dan nir- penyangkalan [9].

Hal-hal yang harus tercapai dalam menggunakan kriptografi untuk mengamankan data adalah aspke kerahasiaan artinya informasi harus benar-benar terjaga aksesnya dari pihak yang tidak berwenang, integritas data adalah aspek yang bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berwenang, autentikasi yang berhubungan dengan pemeriksaan hak akses dan yang terakhir adalah *nir*-penyangkalan yang berfungsi untuk mencegah terjadinya penyangkalan terhadap suatu aksi yang dilakukan oleh pelaku[6][9].

B. *Playfair Cipher*

Playfair cipher merupakan suatu diagram *cipher* substitusi yang ditemukan pada tahun 1854 oleh Charles Wheatstone dan telah digunakan oleh bangsa Inggris. Cipher ini mengenkripsikan pasangan karakter seperti *cipher* klasik lainnya. Kunci yang digunakan ialah 25 buah huruf yang disusun dalam bentuk bujursangkar 5x5 dengan menghilangkan huruf J dalam suatu kalimat dan bukan menjadi kunci. Tujuannya adalah untuk membuat analisa frekuensi menjadi sangat sulit sebab frekuensi kemunculan karakter-karakter di dalam *ciphertext* menjadi datar [5].

Beberapa aturan yang harus diikuti berdasarkan *playfair cipher* dalam proses enkripsi dan dekripsi [10][11] adalah :

1. Bila kedua huruf tidak terletak pada baris dan kolom yang sama, maka huruf pertama menjadi huruf yang sebaris dengan huruf pertama dan sekolom dengan huruf kedua. Huruf kedua menjadi huruf yang sebaris dengan huruf kedua dan yang sekolom dengan huruf pertama. Contohnya, SA menjadi PH, BU menjadi EP.
2. Bila kedua huruf terletak pada baris yang sama maka huruf pertama menjadi huruf setelahnya dalam baris yang sama, demikian juga dengan huruf kedua. Jika terletak pada baris kelima, maka menjadi baris pertama, dan sebaliknya. Arahnya tergantung dari posisi huruf pertama dan kedua, pergeserannya ke arah huruf kedua. Contohnya, AH menjadi TR, LK menjadi KG, BE menjadi CI.
3. Bila kedua huruf terletak pada kolom yang sama maka huruf pertama menjadi huruf setelahnya dalam kolom yang sama, demikian juga dengan huruf kedua. Bila terletak pada kolom kelima, maka menjadi kolom pertama, dan sebaliknya. Arahnya tergantung dari posisi huruf pertama dan kedua, pergeserannya ke arah huruf kedua. Contohnya, DS menjadi LY, PA menjadi GW, DH menjadi HY.
4. Bila kedua huruf sama, maka letakkan sebuah huruf di tengahnya (sesuai kesepakatan).
5. Bila jumlah huruf plainteks ganjil, maka tambahkan satu huruf pada akhirnya, seperti pada aturan ke-4.
6. Sedangkan proses dekripsinya adalah kebalikan dari proses enkripsi.

C. *Metode Zig-zag Cipher*

Metode *zig zag cipher* merupakan salah satu algoritma kriptografi klasik dengan teknik transposisi. Teknik transposisi menggunakan permutasi karakter, yang mana dengan menggunakan teknik ini pesan yang asli tidak dapat dibaca kecuali orang yang memiliki kunci untuk menggembalikan pesan tersebut ke bentuk semula [7].

Algoritma *zig-zag* ini merupakan pembentukan dari algoritma transposisi kolom (*Columnar Transposition Cipher*) dan Transposisi *Rail Fance Cipher*. Teknik transposisi menggunakan permutasi karakter, sehingga pesan yang asli tidak dapat dibaca kecuali orang yang memiliki kunci untuk menggembalikan pesan tersebut ke bentuk semula [6][7]. Metode *zig-zag* memiliki kelebihan dibandingkan dengan algoritma lainnya (dalam *cipher* transposisi), dalam proses penulisan plainteks menjadi chiperteks karena penulisan dapat dilakukan dari baris mana saja. Hal ini akan menambah kerumitan dalam proses enkripsi maupun dekripsi.

Publikasi Jurnal & Penelitian Teknik Informatika
Volume 2 Nomor 2, April 2018
e-ISSN : 2541-2019
p-ISSN : 2541-044X

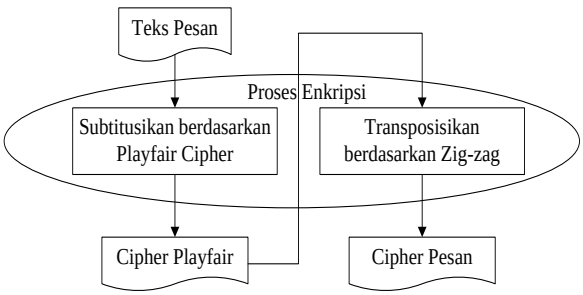
III. PEMBAHASAN

Berdasarkan uraian latar belakang di atas bahwa sangat penting diimplementasikan teknik kriptografi dalam menngamankan data, terutama data-data yang bersifat rahasia atau penting. Secara umum data teks masing sering digunakan dalam mendistribusikan informasi atau pesan kepada orang lain. Oleh karena itu, sangat diperlukan sebuah teknik pengamanan agar informasi tersebut tidak dapat dimanfaatkan atau dimanipulasi oleh pihak lain selain penerima yang sah.

Playfair cipher dengan keterbatasannya terhadap karakter-karakter *cipher* yang dihasilkan menyebab-kan terdapatnya celah bagi pihak lain untuk dapat menerjemahkan kembali sandi yang dihasilkan. Demikian halnya dengan metode *zig-zag* yang hanya melakukan transformasi posisi karakter-karakter dari sebuah teks. Oleh karena itu, pengkombinasian dua algoritma ini sangat efektif dalam mengoptimalkan ketahanan sebuah teks pesan atau informasi untuk menyembunyikan atau mengaburkan makana aslinya terhadap orang-orang yang tidak bertanggungjawab.

Penerapan kombinasi dua algoritma ini pada teks dilakukan dengan dua cara, yaitu mensubtitusikan karakter-karakter dari sebuah informasi atau pesan rahasia, kemudian mengacak kebali posisi-posisi pesan yang telah disubtitusikan sebelumnya. Subtitusi dilakukan berdasarkan *playfair cipher*, sedangkan transposisi dilakukan berdasarkan metode *zig-zag*.

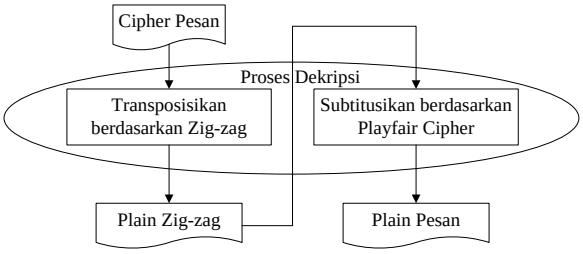
Skema proses enkripsi berdasarkan kombinasi *playfair cipher* dengan metode *zig-zag* dapat dilihat pada gambar di bawah ini.



Gambar 1. Skema Enkripsi

Berdasarkan gabar 1 di atas, diketahui bahwa proses enkripsi (penyandian) diawali dengan menggunakan *playfair cipher* dengan tujuan mensubtitusikan setiap karakter teks pesan dengan karakter-karakter baru. *Cipher* yang dihasilkan akan dienkripsi kembali melalui proses transposisi berdasarkan metode *zig-zag* sehingga dihasilkan *cipher* pesan akhir yang akan didistribusikan atau dikirimkan kepada penerima pesan.

Proses dekripsi merupakan kebalikan dari skema proses enkripsi. Proses yang dilakukan dapat diilustrasikan pada gambar di bawah ini :



Gambar 2. Skema Dekripsi

Berdasarkan gambar 2 di atas, terlihat bahwa proses dekripsi diawali dengan dekripsi *cipher* pesan berdasarkan transposisi *zig-zag*. *Plaintext* yang dihasilkan akan disubtitusikan kembali berdasarkan metode dekripsi *playfair cipher*, sehingga diperoleh teks asli (*plaintext*) dari pesan asli.

Berikut ini akan diuraikan contoh penyandian teks berdasarkan kombinasi dua algoritma ini.
Plaintext = KIKI WIDIA NANDA
Kunci Playfair = HARIATI
Kunci Zig-zag = 3 dan offset = 0

1. Proses enkripsi berdasarkan *playfair cipher*
   Sebelum proses enkripsi dimulai, terlebih dahulu dilakukan pemetaan kunci ke dalam bentuk matriks yang dijadikan sebagai tabel acuan.

   Kunci : HARIATI

H	A	R	I	T
B	C	D	E	F
G	K	L	M	N
O	P	Q	S	U
V	W	X	Y	Z

   Setelah tabel acuan kunci terbentuk, berikutnya dilakukan operasi terhadap pesan yang akan dienkripsi, yaitu:
   a. Ganti seluruf huruf “j” dengan huruf “i”
   b. Tulis kembali pesan dalam bentuk pasangan huruf
   c. Setiap pasangan huruf yang sama harus dipisah dan disisipkan huruf “z” di tengahnya
   d. jumlah huruf ganjil, maka ditambahkan huruf “z” di akhir

   Pesan setelah diolah berdasarkan tabel *matrix* kunci adalah KI KI WI DY AN AN DA
   Misalnya untuk mencari cipher K pada blok KI, maka yang dilakukan adalah temukan huruf K pada baris *matrix*, kemudian temukan huruf I pada posisi kolom. Karakter yang ada pada *cell* pertamuan antara baris K dan kolom I merupakan *cipher* dari huruf K. Hasil proses ini adalah M.

Lakukan hal yang sama untuk mencari karakter teks blok yang lain, sehingga *cipher* akhir adalah **MA MA YA XE KT KT CR.** *Cipher* inilah yang kemudian dienkripsi kembali berdasarkan metode *zig-zag*.

2. Proses enkripsi berdasarkan *zig-zag*
Input yang dijadikan sebagai *plaintext* pada proses enkripsi berdasarkan *zig-zag* adalah *cipher* yang dihasilkan dari proses *playfair cipher*.

Plaintext = **MAMAYAXEKTKTCR**
Kunci = 3 dan *offset* = 0

M				Y				K				C	
	A		A		A		E		T		T		R
		M				X				K			

Proses penulisan *cipher* dimulai dari baris pertama, kemudian disusul oleh baris berikutnya. Karakter-karakter yang ada pada setiap baris dijadikan sebagai *cipher*. Berasarkan tabel transposisi di atas, maka ditemukan *ciphertext* adalah **MYKC AAAETTR MXK**.

3. Proses Dekripsi
Seperti Berdasarkan penjelasan di atas bahwa proses dekripsi diawali oleh dekripsi berdasarkan metode *zig-zag*, kemudian disusul oleh dekripsi *playfair cipher*.
Ciphertext = **MYKC AAAETTR MXK**
Kunci = 3; offset = 0 dan jumlah cipher = 14

Dekripsi berdasarkan metode *zig-zag* :
Hal pertama yang perlu dilakukan untuk mendekripsi *cipher* berdasarkan metode *zig-zag* adalah membentuk tabel acuan dekripsi *zig-zag*, kemudian diisi sembarang karakter untuk menemukan pola *zig-zag* enkripsi. Pada proses ini, nilai kunci dan *offset* serta jumlah karakter *ciphertext* sangat menentukan.

Jumlah karakter cipher menjadi jumlah kolom tabel acuan, sehingga :

x				x				x				x	
	x		x		x		x		x		x		x
		x				x				x			

Berdasarkan pola tabel acuan, maka didapatkan untuk baris pertama diisi oleh 4 karakter cipher, baris kedua diisi oleh 7 karakter cipher (karakter ke-5 sampai dengan 11) dan baris ketiga terdiri dari tiga karakter (karakter 12 sampai 14).

M				Y				K				C	
	A		A		A		E		T		T		R
		M				X				K			

Proses pembentukan plaintext dilakukan per kolom untuk masing-masing baris. Sehingga didapatkan *plaintext* hasil dekripsi *zig-zag* adalah **MAMAYAXEKTKTCR**

Berkutnya adalah mendekripsi plaintext hasil dekripsi *zig-zag* berdasarkan dekripsi *playfair cipher* dimana prosesnya tidak berbeda seperti proses enkripsi. Hasil akhir dari proses dekripsi playfair adalah plaintext yaitu **KIKI WIDIA NANDA.**

IV. KESIMPULAN

Berdasarkan uraian pembahasan penelitian ini, maka disimpulkan beberapa hal sebagai berikut :

1. *Ciphertext* yang dihasilkan berdasarkan pengkombinasian *playfair cipher* dengan metode *zig-zag* cukup acak dan mampu mengaburkan pola relasinya dengan *plaintext* (teks asli)
2. Kombinasi yang diimplementasikan pada penyandian teks ini merupakan perpaduan antara teknik subtitusi yang dilakukan berdasarkkan *playfair cipher* dan teknik transposisi yang dilakukan berdasarkan transposisi *zig-zag*.
3. Kombinasi dua teknik ini dapat diterapkan pada pengamanan data yang sifatnya rahasia dan penting karena tingkat optimalisasinya yang dapat disebut dengan super enkripsi.

REFERENSI

[1] S.H. Suryawan, Hamdani, "Pengamanan Data File Dengan Menggunakan Algoritma Enkripsi Rivest Code 5 ," *Jurnal Informatika Mulawarman* , vol.8, no. 2, pp. 44-49, Juli 2013.
[2] T. Zebua, "Penerapan Metode LSB-2 untuk Menyembunyikan Ciphertext Pada Citra Digital," *Pelita Inform. Budi Darma*, vol. 10, no. 3, pp. 135–140, 2015.
[3] E. Setyaningsih, "Penyandian Citra Menggunakan Metode Playfair Cipher", J. Teknol., vol. 2, no. 2, pp. 213–219, Desember 2009.
[4] J. Sasongko, "Pengamanan Data Informasi Menggunakan Kriptografi Klasik", Jurnal Teknologi Informasi DINAMIKA, vol.10, no.3, pp.160-167, September 2005.
[5] E. Setyaningsih E, *Kriptografi & Implementasinya Menggunakan MATLAB*, Yogyakarta: Andi Offset, 2015.
[6] R.K.Hondro "Aplikasi Enkripsi dan Dekripsi Dengan Algoritma Zig-Zag Cipher Pada Mobile Phone Berbasis Android", Pelita Informatika Budi Darma,vol.10, no.3, Juli 2015.
[7] D. Ariyus, *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*, Yogyakarta:Andi, 2008.
[8] I. Wibowo, B. Susanto, and J. Karel T, "Penerapan Algoritma Kriptografi Asimetris RSA Untuk Keamanan Data Di Oracle," *J. Inform.*, vol. 5, no. 1, pp. 1–7, 2016.

[9] T. Zebua and E. Ndruru, "Pengamanan Citra Digital Berdasarkan Modifikasi Algoritma RC4," *J. Teknol. Infomasi dan Ilmu Komput.*, vol. 4, no. 4, pp. 275–282, Desember 2017.
[10] R. C. N. Santi, "Implementasi Algoritma Enkripsi Playfair pada File Teks," *J. Teknol. Inf. Din.*, vol. 15, no. 1, pp. 27–33, Januari 2010.
[11] F. Azmi, R. Anugrahwaty, and A. Kriptografi, "Analisis Matriks 5x7 Pada Kriptografi Playfair Cipher," *J. Penelit. Tek. Inform. (Sinkron)*, vol. 1, no. 2, pp. 27–30, 2017.