JURNAL
TEKNOLOGI INFORMASI
DAN KOMUNIKASI
Vol. 5 No. 1, Juni 2016 : 59 - 70

PENGAMANAN TRANSKRIP NILAI MAHASISWA MENGGUNAKAN KRIPTOGRAFI PLAYFAIR CIPHER DAN STEGANOGRAFI DENGAN TEKNIK LEAST SIGNIFICANT BIT (LSB)

PROTECTING THE STUDENT ACADEMIC TRANSCRIPT USING PLAYFAIR CIPHER CRYPTOGRAPHY AND STEGANOGRAPHY WITH THE LEAST SIGNIFICANT BIT (LSB) TECHNIQUES

Ratna Wati Simbolon
AMIK MBP Medan
Jurusan Manajemen Informatika
e-mail :ratna_sbln@yahoo.com

Diterima : 26 Februari 2016 Direvisi : 14 Maret 2016 Disetuji : 20 Juni 2016

ABSTRAK

Jika kita menyampaikan pesan kepada orang lain, tentu pesan yang dimaksud adalah penting dan diupayakan segera sampai kepada orang yang tepat. Pesan yang dikirim sudah tentu adalah hal yang penting untuk disampaikan. Supaya pesan tersebut aman hingga diterima oleh orang yang tepat, maka perlu dijaga kerahasiaannya dan dihindarkan dari kecurigaan orang lain.Kombinasi antara kriptografi dan steganografi dapat dilakukan untuk lebih meningkatkan keamanan pada pesan yang hendak disembunyikan.Teknik kriptografi yang digunakan dalam penelitian ini adalah playfair cipher. Playfair cipher termasuk dalam Polygram Cipher. Algoritma ini mengenkripsi pasangan alfabet (bigram) pada plaintext. Dalam penelitian ini tabel matriks playfair yang digunakan yaitu matriks 6x6. Steganografi yang digunakan adalah metode spasial domain dengan teknik Least Significant Bit (LSB) yang terdiri dari 2 bagian yaitu LSB Embedding Process dan LSB Extracing Process. Penelitian ini menggunakan metode penelitian kuantitatif yang bersifat pengembangan.Tujuan penelitian ini adalah untuk merahasiakan pesan, dalam hal ini transkrip nilai mahasiswa, yang dilakukan dengan kriptografi, juga supaya menghindarkan pesan tersebut dari kecurigaan, yang kemudian dilakukan dengan proses steganografi.Hasil yang diperoleh adalah berupa file citra bitmap grayscale 8 bit per piksel dengan skala 0 sampai 255, atau dengan format biner. Pesan rahasia berhasil sepenuhnya dikembalikan menjadi pesan asli dengan proses dekripsi.

***Kata Kunci** : Kriptografi, Playfair, Bigram, Steganografi, Least-Significant-Bit*

ABSTRACT

If we convey the message to others, certainly the message in question is important and sought immediately to the right people. Messages sent is of course the important thing to be delivered. In order to secure the message is received by the right person, then it needs to be kept confidential and avoided the suspicion of others. The combination of cryptography and steganography can be done to further improve security in the message that would be hidden. Cryptographic techniques used in this study is the Playfair cipher. Playfair cipher is included in the Cipher Polygram. This algorithm encrypts a couple alphabet (Bigram) in plaintext. In this study Playfair matrix table used is the 6x6 matrix. Steganography is the method of spatial domain by using Least Significant Bit (LSB), which consists of two parts, namely LSB and LSB Embedding Process extracing Process. This study used quantitative research methods development. The purpose of this study was to conceal the message, in this case the transcripts of students, which is done with cryptography, also in order to avoid the message of suspicion, which is then conducted with steganography. The results obtained are in the form of bitmap image files grayscale 8 bits per pixel scale of 0 to 255, or binary format. Secret messages succeed fully restored to the original message with the decryption process.

***Keywords** : Cryptography, Playfair, Bigram, Steganography, Least-Significant-Bit*

PENDAHULUAN

Keamanan data merupakan hal penting dalam menjaga kerahasiaan data-data tertentu yang hanya boleh diketahui oleh pihak yang memiliki hak saja. Seringkali pemindahan data dari suatu tempat ke tempat lain menghadapi ancaman usaha-usaha pihak lain yang ingin mendapatkan data tersebut. Apabila pengiriman data dilakukan melalui jaringan, maka kemungkinan data tersebut diketahui oleh pihak yang tidakberhak menjadi lebih besar.

Kriptografi merupakan salah satu cara untuk mengamankan data, yaitu dengan menyandikan pesan asli (*plaintext*) ke dalam bentuk pesan rahasia (*ciphertext*)[1]. Proses pengamanan ini melibatkan algoritma dan kunci. Kunci enkripsi dapat dengan mudah mengembalikan *plaintext*dari *ciphertext*.Oleh karena itu diperlukan algoritma kriptografi yang kuat. Dengan berkembangnya ilmu penyandian, orang dapat dengan mudah memperoleh kunci penyandian lewat berbagai macam cara.

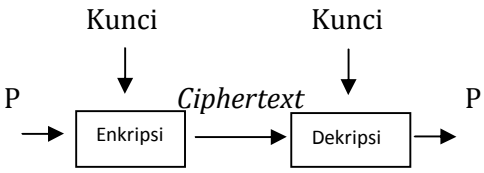
Perumusan masalah dalam penelitian ini meliputi pada :

1. Bagaimana menyisipkan kunci pada tabel *playfair* dengan matriks 6 x 6
2. Bagaimana melakukan enkripsi dengan *playfair cipher* terhadap pesan asli yaitu transkrip nilai mahasiswa menggunakan kode *AmericanStandard Code for Information Interchange* (ASCII)
3. Bagaimana menerapkan steganografi dengan LSB *Embedding Process* dan LSB *Extracting Process* terhadap pesan rahasia (*ciphertext*) yang dihasilkan dan kemudian mengembalikan pesan rahasia tersebut menjadi pesan asli dengan proses dekripsi.

Penelitian ini bertujuan merahasiakan data transkrip nilai mahasiswa, dengan proses kriptografi, serta sekaligus menghindarkan pesan tersebut dari kecurigaan, yang dapat dilakukan dengan proses steganografi. Keamanan data (kriptografi) akan lebih baik menggunakan kode ASCII dengan 256 karakter.

Kriptografi

Kriptografi (*cryptography*) sendiri berasal dari bahasa Yunani yakni "*cryptós*" artinya rahasia, sedangkan "*gráphein*" artinya tulisan, digabungkan menjadi "tulisan rahasia"[2]. Saat ini kriptografi digunakan pada banyak hal terutama untuk keamanan informasi seperti kerahasiaan/privasi (*confidentiality/privacy*), integritas data (*data integrity*), otentikasi (*authentication*),dan tanpa penyangkalan (*non-repudiation*)yang digunakan untuk pembuktian[3].Kriptografi bertujuan untuk menjaga kerahasiaan data, informasi, dan dokumen supaya tidak dapat diketahui oleh pihak yang tidak berhak mengetahuinya (*unauthorized person*)[4].



Gambar 1. Skema Enkripsi dan Dekripsi[2]

Terminologi tentang kriptografi adalahsebagai berikut[2]:

a. Pesan, *plaintext*, dan *ciphertext*. Pesanatau nama lainnya *plaintext* merupakan data atau informasi yang dapat dibaca dan dimengerti maknanya, oleh karena itu siapapun dapat mengetahuinya. Pesan baik data maupun informasi yang disimpan dalam media perekam baik berupa teks, citra, suara,video ataupun berkas biner dapat dikirimkan melalui kurir/saluran komunikasi. Pesan yang dikirim dapat saja dicuri kemudian dipergunakan oleh yang tidak berhak, dengan demikian perlu disandikan agar aman. Bentuk pesan yang disandikan disebut *ciphertext* atau kriptogram (*cryptogram*). *Ciphertext* harus dapat diubah kembali ke dalam *plaintext* sehingga pesan mudah di baca dan dimengerti kembali.

b. Pengirim dan penerima. Pesan baik sebagai data ataupun informasi akan melibatkan dua entitas yaitu pengirim (*sender*) dan penerima (*receiver*) sehingga komunikasi data dapat terjadi.
c. Enkripsi dan dekripsi. Enkripsi (*encryption*) merupakan proses penyandian pada *plaintext*, atau disebut sebagai *enciphering* jika mengacu penamaan menurut standar ISO 7498-2. Dekripsi (*decryption*) merupakan proses mengembalikan *ciphertext* menjadi *plaintext*, dan disebut sebagai *deciphering* jika mengacu penamaan menurut standar ISO 7498-2.
d. *Cipher* dan kunci. Pada algoritma kriptografi sering disebut juga sebagai *cipher*, merupakan aturan untuk *enciphering* dan *deciphering* yang menggunakan fungsi matematika untuk enkripsi dan dekripsi. Kunci (*key*) merupakan parameter yang digunakan untuk transformasi *enciphering* dan *deciphering*.
e. Sistem kriptografi (*cryptosystem*).
f. Kumpulan yang terdiri atas algoritma kriptografi, semua *plaintext* dan*ciphertext* yang mungkin dan kunci.
g. Penyadap (*eavesdropper*). Orang yang mencoba menangkap pesan selama ditransmisikan dan bertujuan mendapatkan informasi sebanyak-banyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi kemudian digunakan dalam memecahkan ciphertext.
h. Kriptanalisis dan kriptologi. Kriptanalisis (*cryptanalysis*) merupakan ilmu dan seni untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kuncinya. Pelakunya disebut kriptanalis. Kriptologi (*cryptology*) adalah studi tentang kriptografi dan kriptanalisis.

Playfair Cipher

Sandi Playfair digunakan oleh Tentara Inggris pada saat Perang Boer II dan Perang Dunia I. Playfair ditemukan pertama kali oleh Sir Charles Wheatstone dan Baron Lyon Playfair pada 26 Maret 1854.

Menurut Aftab[5], Chaoudhary[6], Vatsa[7]*ciphertext* hasil enkripsi relatif mudah dipecahkan ketika kriptanalisis mengetahui *ciphertext* dan tabel *cipher*-nya, walaupun kriptanalis hanya mengetahui *ciphertext* tanpa mengetahui tabel *cipher* kriptanalis dapat menebak bigram berdasarkan huruf yang bermakna dari sebuah kata.

Menurut Harris dan Attia[8], Kumar[9], Nidhal dan Wasfi[10], Shakti dan Gupta[11], tabel bawaan yang ada pada *playfair cipher* tidak dapat mengenkripsi *plaintext* yang berisi huruf kecil (a-z), angka (0-9) dan simbol-simbol. Kelemahan yang lain pada *playfair* adalah terjadinya ambigu pada hasil dekripsi karena pada persiapan enkripsi *playfaircipher* memiliki mekanisme mengganti J dengan I. Perlunya modifikasi tabel *playfair cipher* yang dapat digunakan untuk melakukan enkripsi huruf kapital, huruf kecil, angka dan simbol.

Menurut Stallings[12], *playfair cipher* menggunakan papan kunci yang berbentuk bujursangkar dalam melakukan penyandian. Papan kunci ini berukuran 5x5, dimana setiap bagian dalam papan kunci mewakili huruf-huruf dalam alfabet (abjad) dengan menghilangkan huruf J dari abjad.

Playfair merupakan digraphs cipher, artinya setiap proses enkripsi dilakukan pada setiap dua huruf[13].Sandi *Playfair* hanya dapat digunakan untuk proses enkripsi dan dekripsi data yang berupa teks alfabet, karakter yang tidak berupa teks alfabet dapat dihindari dengan menuliskannya dalam bentuk teks alfabet.

Matriks kunci akan diisi sesuai dengan urutan kemunculan huruf pada kunci. Huruf yang digunakan tidak boleh digunakan lagi, sedangkan huruf yang tidak digunakan kunci akan disusun setelahnya sesuai dengan urutan alphabet[14].

Khumar (2013) memodifikasi tabel *cipher* menjadi 6x6 yang berisi (A-Z) dan (0-9). *Playfair* dengan tabel *cipher*5x5 tanpa

modifikasi akan membuat *cipher* mudah dipecahkan.

Algoritma *Playfair Cipher*

Algoritma *playfair* merupakan bagian dari algoritma kriptografi klasik yang menggunakan teknik subtitusi. Subtitusi adalah penggantian setiap karakter plainteks dengan karakter lain. Berdasarkan jenis kuncinya algoritma *playfair* merupakan algoritma simetri. Kunci yang digunakan untuk enkripsi sama dengan dekripsinya[15].

Playfair Cipher mengenkripsi pasangan huruf (digram atau digraf), bukan huruf tunggal seperti pada *cipher* klasik/tradisional lainnya. Tujuannya untuk membuat analisis frekuensi menjadi sulit sebab frekuensi kemunculan huruf di dalam *ciphertext*akan menjadi datar.

Menurut Stallings[12] Sebelum melakukan enkripsi, pesan yang akan dienkripsi (*plaintext*) diatur terlebih dahulu sebagai berikut :

1. Semua spasi dan karakter yang bukan alfabet harus dihilangkan dari *plaintext* (jika ada).
2. Jika ada huruf J pada *plaintext*, maka ganti huruf tersebut dengan huruf I.
3. Pesan yang akan dienkripsi ditulis dalam pasangan huruf (bigram).
4. Jika ada huruf yang sama dalam pasangan huruf, maka sisipkan huruf X atau Z di tengahnya. Huruf yang disisipkan sebaiknya huruf X karena sangat kecil kemungkinan terdapat huruf X yang sama dalam bigram, tidak seperti huruf Z
5. Jika jumlah huruf pada *plaintext* adalah ganjil maka pilih sebuah huruf tambahan yang dipilih oleh orang yang mengenkripsi dan tambahkan di akhir *plaintext*. Huruf tambahan dapat dipilih sembarang misalnya huruf Z atau X.

Algoritma enkripsi untuk setiap bigram adalah sebagai berikut:

1. Jika ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya
2. Jika ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf di bawahnya
3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua.
4. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf yang digunakan

a. Algoritma dekripsi merupakan kebalikan dari algoritma enkripsi untuk setiap bigram adalah sebagai berikut:

1. Jika ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kirinya
2. Jika ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf di atasnya.
3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua.
4. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari huruf yang digunakan

Steganografi

Steganografi adalah seni menyembunyikan pesan atau informasi dalam suatu obyek, seperti teks atau *image*.Tujuannya untuk menghindari kecurigaan.

Teknik yang digunakan adalah sebagai berikut.

- *Spasial Domain*

Memodifikasi langsung nilai byte dari *cover object* (nilai byte dapat merepresentasikan intensitas/warna pixel atau amplitudo). Metode spasial domain ada 2, yaitu *Least Significant Bit* (LSB) dan *Most Significant Bit* (MSB).[9]

- *Transform Domain*

Memodifikasi hasil transformasi sinyal dalam ranah frekuensi.

Dalam penelitian ini teknik steganografi menggunakan spasial domain.

LSB *Embedding Process*

LSB adalah salah satu metode untuk menyembunyikan pesan dalam media digital dengan cara menyisipkan pesan tersebut pada satu bit paling kanan ke piksel file obyek. Berikut ini penyisipan data pada file citra *bitmap grayscale* 8 bit per *pixel* dengan skala 0 sampai 255, atau dengan format biner 00000000 sampai 11111111. Misalnya piksel-piksel citra yang akan digunakan sebagai wadah (*cover image*) adalah :

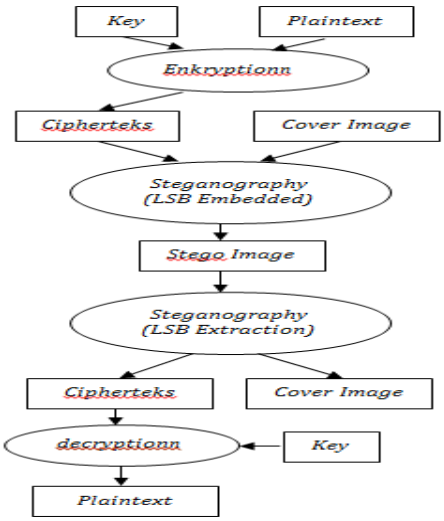
(010011010010111010101110 10001010 10101111 10100010 00101011 10101011)

LSB *Extracing Process*

Proses ekstraksi dilakukan dengan dua tahap. Pertama untuk memperoleh *ciphertext* diambil bit-bit paling belakang dari *stegoimage*. Kedua, untuk memperoleh *cover image*, tambahkan satu bit paling belakang pada piksel-piksel sisa tahap pertama dengan bit yang sama dengan bit paling belakang *cover image*.

Kombinasi Kriptografi dan Steganografi

Kombinasi kriptografi dengan metode *playfaircipher* dan steganografi dengan metode LSB dapat digambarkan dalam skema Gambar 2.



Gambar 2. Proses Kriptografi-Steganografi

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kuantitatif yang bersifat pengembangan. Dilengkapi dengan pengembangan studi literatur, dilakukan penerapan teknik-teknik dari metode *playfair cipher*dengan memanfaatkan kode ASCII dan dikombinasi dengan steganografi menggunakan LSB.

Tahapanyang dilakukan dalam penelitian ini adalah :

a. Tentukan kunci yang akan digunakan, kemudian kunci tersebut letakkan pada tabel *playfair* dengan matriks 6x6
b. Tentukan *plaintext* yang akan di enkripsi menggunakan *key* yang telah disediakan.
c. Lakukan proses enkripsi sehingga menghasilkan *ciphertext*.
d. Hasil *ciphertext* diubah kebentuk kode ASCII agar bisa disesuaikan dengan*cover image*dengan menentukan piksel citra yang akan digunakan sebagai wadah.
e. Kemudian lakukan proses steganografi dengan LSB *embedding process* untuk menghasilkan *stego image*.
f. Dari *stego image* yang diperoleh, lakukan steganografi LSB*extracting process*. Hasil yang didapat masih dalam bentuk *ciphertext*, kemudian ubah ke bentuk kode ASCII dan lakukan dekripsi (menggunakan tabel *playfair* dengan matriks 6x6) untuk mengembalikan ke pesan asli (*plaintext*).

HASIL DAN PEMBAHASAN

Pada penelitian ini akan dibahasproses enkripsi dan dekripsi menggunakan *playfair* dengan tabel matriks 6x6.

Diberikan kunci “KOMINFO”, maka matriks akan menjadi seperti pada Gambar 3.

K	O	M	I	N	F
A	B	C	D	E	G
H	J	L	P	Q	R
S	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Gambar3. Matriks hasil kunci “KOMINFO”

Gambar 3 menunjukkan penempatan kunci "KOMINFO" pada tabel matriks 6 x 6. Penulisan huruf yang samadilakukan hanya satu kali saja dan dilanjutkan dengan urutan abjad. Huruf yang sudah terdapat pada kunci tidak akan diulang lagi pada susunan alfabet.Kemudian disisipkan urutan angka 0-9.

Salinan transkrip nilai mahasiswa dapat dilihat pada Lampiran 1.Lampiran 1 menunjukkan Salinan transkrip nilai seorang mahasiswa dengan menampilkan atribut Semester, Kode, Mata_Kuliah, SKS dan Nilai.

Dari salinan transkrip nilai yang tertera pada Lampiran 1, maka yang menjadi *plaintext* adalah 8 karakter dari NPM mahasiswa, dan gabungan semester mata kuliah, kode mata kuliah, dan nilai seperti dituliskan sebagai berikut.

37038019	32KP503B
31KW504A	41KW510A
31KW502B	41KP508A
31KW503A	41KW509A
31KW501A	41KW507A
32KP510A	42KW512A
32KW505B	42KW513A
32KW506B	42KW511B

Baris pertama dari *plaintext* diatas adalah NPM mahasiswa dan baris berikutnya gabungan semester, kode mata kuliah dan nilai. Untuk semester, misal 2013 ganjil dinyatakan dengan kode 131 dan cukup hanya dituliskan 31 karena hanya menampung 8 karakter saja.

Plaintext diatas kemudian dienkripsi menggunakan *playfair cipher* dengan matriks hasil kunci KOMINFO seperti pada Gambar 4.

K	O	M	I	N	F
A	B	C	D	E	G
H	J	L	P	Q	R
S	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Gambar4. Matriks Enkripsi '37'

Gambar 4 menunjukkan proses enkripsi dari plainteks '37' dan menghasilkan cipherteks '19'.

K	O	M	I	N	F
A	B	C	D	E	G
H	J	L	P	Q	R
S	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Gambar5. Matriks Enkripsi '03'

Gambar 5 menunjukkan proses enkripsi dari plainteks '03' dan menghasilkan *ciphertext*'1Y'.Setelah dilakukan enkripsi terhadap seluruh*plaintext*, maka diperoleh *ciphertext* seperti pada Tabel 1.

Tabel 1. Hasil Enkripsi

No	Plainteks	Cipherteks
1	37038019	191Y6237
2	31KW504A	Y2NS6ZKH
3	31KW502B	Y2NS6ZZE
4	31KW503A	Y2NS6ZYG
5	31KW501A	Y2NS6ZYD
6	32KP510A	Y3IH7ZYC
7	32KW505B	Y3NS6ZOJ
8	32KW506B	Y3NS6Z5C
9	32KP503B	Y3IH6ZZG
10	41KW510A	7YNS7ZYC
11	41KP508A	7YIH6Z4E
12	41KW509A	7YNS6Z4G
13	41KW507A	7YNS6Z4D
14	42KW512A	8YNS7ZYE
15	42KW513A	8YNS7ZYG
16	42KW511B	8YNS7ZZD

Tabel 1 menampilkan hasil keseluruhan *ciphertext* setelah dilakukan enkripsi. Setelah diperoleh hasil *ciphertext*, maka setiap karakter diubah ke bentuk kode ASCII supaya dapat diimplementasikan ke *cover image* yang digunakan. Piksel-piksel citra yang akan digunakan sebagai wadah (*cover image*) adalah :
(01001101 0010111010101110 10001010 10101111 10100010 00101011 10101011)

Tabel 2. Pesan Cipherteks dalam Kode ASCII

Ci	1	9	1	7	6	2	3	7
ASCII	49	57	49	89	54	50	51	55
Ci	Y	2	N	S	6	Z	K	H
ASCII	89	50	78	83	54	90	75	72
Ci	Y	2	N	S	6	Z	Z	E
ASCII	89	50	78	83	54	90	90	69
Ci	Y	2	N	S	6	Z	Y	G
ASCII	89	50	78	83	54	90	89	71
Ci	Y	2	N	S	6	Z	Y	D
ASCII	89	50	78	83	54	90	89	68
Ci	Y	3	I	H	7	Z	Y	C
ASCII	89	51	73	72	55	90	89	67
Ci	Y	3	N	S	6	Z	O	J
ASCII	89	51	78	83	54	90	79	74
Ci	Y	3	N	S	6	Z	5	C
ASCII	89	51	78	83	54	90	53	67
Ci	Y	3	I	H	6	Z	Z	G
ASCII	89	51	73	72	54	90	90	71
Ci	7	Y	N	S	7	Z	Y	C
ASCII	55	89	78	83	55	90	89	67
Ci	7	Y	I	H	6	Z	4	E
ASCII	55	89	73	72	54	90	52	69
Ci	7	Y	N	S	6	Z	4	G
ASCII	55	89	78	83	54	90	52	71
Ci	7	Y	N	S	6	Z	4	D
ASCII	55	89	78	83	54	90	52	68
Ci	8	Y	N	S	7	Z	Y	E
ASCII	56	89	78	83	55	90	89	69
Ci	8	Y	N	S	7	Z	Y	G
ASCII	56	89	78	83	55	90	89	71
Ci	8	Y	N	S	7	Z	Z	D
ASCII	56	89	78	83	55	90	90	68

Tabel 2menampilkan perubahan *ciphertext* ke kode ASCII untuk dapat diimplementasikan ke wadah (*cover image)* yang digunakan.Dari wadah yang digunakan, maka piksel-piksel *cover image*tersebut akan berubah.

49 = 00110001

0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**0**	1010000**1**	0010101**0**	1010101**1**

57= 00111001

0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**1**	1010000**1**	0010101**0**	1010101**1**

49 = 00110001

0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**0**	1010000**1**	0010101**0**	1010101**1**

89 = 01011001

0100110**0**	0010111**1**	1010111**0**	1000101**1**
1010111**1**	1010000**1**	0010101**0**	1010101**1**

54 = 00110110

0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**0**	1010000**1**	0010101**1**	1010101**0**

50 = 00110010

0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**0**	1010000**1**	0010101**1**	1010101**0**

51 = 00110011

0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**0**	1010000**1**	0010101**1**	1010101**1**

55 = 00110111

0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**0**	1010000**1**	0010101**1**	1010101**1**

Perubahan piksel-piksel*cover image* diatas, hanya menampilkan satu baris kode ASCII yang dihasilkan dari *ciphertext* seperti yang terdapat padaTabel 2.

Dengan perubahan yang tidak signifikan ini tidak akan terdeteksi oleh mata manusia sehingga tidak akan mengandung kecurigaan.

Dari proses penyisipan karakter *ciphertext* diperoleh *stegoimage* seperti pada Tabel 3.

Tabel 3.*Stego Image*

(0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**0**	1010000**1**	0010101**0**	1010101**1**)
(0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**1**	1010000**1**	0010101**0**	1010101**1**)
(0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**0**	1010000**1**	0010101**0**	1010101**1**)
(0100110**0**	0010111**1**	1010111**0**	1000101**1**
1010111**1**	1010000**1**	0010101**0**	1010101**1**)
(0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**0**	1010000**1**	0010101**1**	1010101**0**)
(0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**0**	1010000**1**	0010101**0**	1010101**0**)
(0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**0**	1010000**1**	0010101**1**	1010101**1**)
(0100110**0**	0010111**0**	1010111**1**	1000101**1**
1010111**0**	1010000**1**	0010101**1**	1010101**1**)

Tabel 3 menampilkan perubahan piksel-piksel*cover image* sehingga membentuk *stego image*.Hasil yang diperoleh dengan mengambil bit-bit paling belakang dari *stegoimage* tersebut dapat ditampilkan pada Tabel 4.

Tabel 4. Bit paling belakang *stego image*

ASCII dari Cipherteks	Bit belakang
49	00110001
57	00111001
49	00110001
89	01011001
54	00110110
50	00110010
51	00110011
55	00110111

Tabel 4 menunjukkan hasil pemilihan bit-bit paling belakang dari *stego image* pada Tabel 3.Untuk mengembalikan teks yang telah dienkripsi menjadi pesan asli dapat dilakukan pendekripsian.Lampiran 2 menampilkan kode ASCII dalam pesan *ciphertext* yang digunakan untuk mengembalikan pesan yang telah dienkripsi menjadi pesan asli.

Tahapan proses dekripsi *ciphertext* menjadi *plaintext* ditunjukkan pada Gambar 6, Gambar 7, Gambar 8 dan Gambar 9. Sementara hasil akhir dekripsi ditunjukkan pada Tabel 5.

K	O	M	I	N	F
A	B	C	D	E	G
H	J	L	P	Q	R
S	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Gambar6. Matriks dekripsi huruf '19'

K	O	M	I	N	F
A	B	C	D	E	G
H	J	L	P	Q	R
S	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Gambar7. Matriks dekripsi huruf '1Y'

K	O	M	I	N	F
A	B	C	D	E	G
H	J	L	P	Q	R
S	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Gambar8. Matriks dekripsi huruf '62'

K	O	M	I	N	F
A	B	C	D	E	G
H	J	L	P	Q	R
S	T	U	V	W	X
Y	Z	0	1	2	3
4	5	6	7	8	9

Gambar9. Matriks dekripsi huruf '37'

Tabel 5. Hasil Dekripsi

No	Cipherteks	Plainteks
1	191Y6237	37038019
2	Y2NS6ZKH	31KW504A
3	Y2NS6ZZE	31KW502B
4	Y2NS6ZYG	31KW503A
5	Y2NS6ZYD	31KW501A
6	Y3IH7ZYC	32KP510A
7	Y3NS6ZOJ	32KW505B
8	Y3NS6Z5C	32KW506B
9	Y3IH6ZZG	32KP503B
10	7YNS7ZYC	41KW510A
11	7YIH6Z4E	41KP508A
12	7YNS6Z4G	41KW509A
13	7YNS6Z4D	41KW507A
14	8YNS7ZYE	42KW512A
15	8YNS7ZYG	42KW513A
16	8YNS7ZZD	42KW511B

Gambar 6 menunjukkan proses dekripsi terhadap cipherteks ‘19’ dan kembali menjadi pesan asli (*plaintext*) yaitu ‘37’.Gambar 7 menunjukkan proses dekripsi terhadap *ciphertext* ‘1Y’ dan kembali menjadi pesan asli (*plaintext*) yaitu ‘03’.Gambar 8 menunjukkan proses dekripsi terhadap *ciphertext* ‘62’ dan kembali menjadi pesan asli (*plaintext*) yaitu ‘80’.Gambar 9 menunjukkan proses dekripsi terhadap *ciphertext* ‘37’ dan kembali menjadi pesan asli (*plaintext*) yaitu ‘19’. Tabel 5 menampilkan hasil keseluruhan *plaintext* (pesan asli) yang telah dikembalikan dari pesan rahasia (*ciphertext*) setelah dilakukan dekripsi.

Proses dekripsi berhasil dilakukan dengan mengembalikan pesan rahasia menjadi pesan asli. Dengan demikian penelitian kriptografi pada kode ASCII menggunakan metode *playfair cipher* dan dikombinasikan dengan steganografi menggunakan LSB, dapat diterapkan.

SIMPULAN

Kriptografi *playfair cipher* mengenkripsi pasangan huruf dengan tujuanmembuat analisis frekuensi menjadi sulit sebab frekuensi kemunculan huruf di dalam *ciphertext*akan menjadi datar. Penerapan kode ASCII juga akan membuat hasil enkripsi semakin sulit untuk dimengerti oleh pihak ketiga. Kombinasi steganografi menggunakan LSB dengan hasil file citra *bitmap grayscale* 8 bit per piksel dengan format biner akanmenghindari kecurigaan. Dengan adanya penerapan kombinasi kriptografi dan steganografi dalam pengamanan data transkrip nilai mahasiswa, dipastikan tidak akandiketahui oleh orang lain karena tidak akan mengandung kecurigaan.

Kontribusi dari penelitian ini pada ilmu pengetahuan khususnya untuk Kominfo adalah supaya dalam penyampaian komunikasi dan informasi yang sifatnya rahasia sehingga tidak menimbulkan kecurigaan bagi pihak ketiga, dapat dilakukan penerapan kriptografi dan dikombinasi dengan steganografi.

Daftar Pustaka

[1]Schneier, Bruce 1996, Aplied Cryptography 2nd, John Wiley & Sons, New York

[2]Munir, R. 2006. *Kriptografi*, Cetakan Pertama, Penerbit Informatika, Bandung.

[3]Menezes, Alfred., Paul C van Oorschot, and Scott A. 1996. Vanstone, Handbook of Applied Cryptography, CRC Press.

[4]Septiarini, A dan Hamdani. 2011. *Sistem Kriptografi untuk Text Message Menggunakan Metode Affine*, Jurnal Informatika Mulawarman, Vol 6 No. 1.

[5]Aftab, A. A., Shah, B. K., dan Muhammad, C. S., 2013.A Modified Version of Playfair Cipher Using 7×4 Matrix., International Journal of Computer Theory and Engineering., Volume 5., No. 4.

[6]Choudhary, J., Kumar, R. G dan Singh, S., 2013. A Generalized Version of Play Fair Cipher., international journal of advanced computer technology., Volume 2., PP 2-6.

of Information and Network Security., Volume 1., No.4., PP 313-320.

[8]Harris, J., dan Attia, A., 2013. Modified Version of Cryptography Playfair Cipher with 8x8 Linear Feedback Shift Register., European Journal of Industrial and System Engineering., Volume 11.

[9]Kumar, D. M., dan Jain, D., 2013.The Problem Analysis on Encryption Technique in Cryptography., International Journal of Societal Applications of Computer Science., Volume 2.

[10]Nidhal, O. A. H., dan Wasfi, B. A., 2013.11 × 11 Playfair Cipher based on a Cascade of LFSRs., IOSR Journal of Computer Engineering., Volume 12., PP 29-35.

[7]Vatsa, S., Mohan, T., dan Vatsa, A. K., 2012. Novel Cipher Technique Using Subtitution Method., International Journal

[11]Shakti, S. S., dan Gupta, N.2011.A Novel Approach to Security using Extended Playfair Cipher., International Journal of Computer Applications.

[12]Stallings, W. 2010.Cryptography and Network Security: Principles and Practice., 5thedition, Prentice Hall.

[13]Santi, R.C.N. 2010.Implementasi Algoritma Enkripsi Playfair pada File Teks. Jurnal Teknologi Informasi DINAMIK. XV, 22-37.

[14]Yonathan, F. 2012.Modifikasi Playfair Cipher dengan Teknik Pemutaran Kunci Dua Arah. Makalah IF3058 Kriptografi Sem. II Tahun 2011/2012

[15]Kurniawan, Y. 2004.Kriptografi keamanan Internet dan Jaringan Komputer. Bandung: Informatika Bandung.

LAMPIRAN

Lampiran 1.Salinan Transkrip Nilai Mahasiswa

Nama Mahasiswa		**Ratna Wati Simbolon**		
NPM		**137038019**		
Sem	**Kode**	**Mata Kuliah**	**SKS**	**Nilai**
Ganjil 2013	KW504	Data Mining	3	A
Ganjil 2013	KW502	Kecerdasan Buatan	3	B
Ganjil 2013	KW503	Keamanan Komputer	3	A
Ganjil 2013	KW501	Algoritma	3	A
Genap 2013	KP510	Kriptografi	3	A
Genap 2013	KW505	Kecerdasan Komputasional	3	B
Genap 2013	KW506	Desain Kompiler	3	B
Genap 2013	KP503	Neural Networks	3	B
Ganjil 2014	KW510	Bahasa Inggris (TOEFL & Writing)	2	A
Ganjil 2014	KP508	Machine Learning	3	A
Ganjil 2014	KW509	Metodologi Penelitian	3	A
Ganjil 2014	KW507	Desain dan Praktik Sistem Operasi	3	A
Genap 2014	KW512	Seminar	2	A
Genap 2014	KW513	Tesis	6	A
Genap 2014	KW511	Kolokium	1	B

Lampiran 2. Kode ASCII dalam pesan *ciphertext*

ASCII	49	57	49	89	54	50	51	55
Ci	1	9	1	7	6	2	3	7
ASCII	89	50	78	83	54	90	75	72
Ci	Y	2	N	S	6	Z	K	H
ASCII	89	50	78	83	54	90	90	69
Ci	Y	2	N	S	6	Z	Z	E
ASCII	89	50	78	83	54	90	89	71
Ci	Y	2	N	S	6	Z	Y	G
ASCII	89	50	78	83	54	90	89	68
Ci	Y	2	N	S	6	Z	Y	D
ASCII	89	51	73	72	55	90	89	67
Ci	Y	3	I	H	7	Z	Y	C
ASCII	89	51	78	83	54	90	79	74
Ci	Y	3	N	S	6	Z	O	J
ASCII	89	51	78	83	54	90	53	67
Ci	Y	3	N	S	6	Z	5	C
ASCII	89	51	73	72	54	90	90	71
Ci	Y	3	I	H	6	Z	Z	G
ASCII	55	89	78	83	55	90	89	67
Ci	7	Y	N	S	7	Z	Y	C
ASCII	55	89	73	72	54	90	52	69
Ci	7	Y	I	H	6	Z	4	E
ASCII	55	89	78	83	54	90	52	71
Ci	7	Y	N	S	6	Z	4	G
ASCII	55	89	78	83	54	90	52	68
Ci	7	Y	N	S	6	Z	4	D
ASCII	56	89	78	83	55	90	89	69
Ci	8	Y	N	S	7	Z	Y	E
ASCII	56	89	78	83	55	90	89	71
Ci	8	Y	N	S	7	Z	Y	G
ASCII	56	89	78	83	55	90	90	68
Ci	8	Y	N	S	7	Z	Z	D