Jurnal Pelita Informatika, Volume 7, Nomor 2, Oktober 2018
ISSN 2301-9425 (Media Cetak)
Hal: 193-198

IMPLEMENTASI KEAMANAN DATA MENGGUNAKAN ALGORITMA VERNAM CIPHER DAN PLAYFAIR CIPHER

Pratika Sari Eka

Program Studi Teknik Informatika STMIK Budi Darma, Medan, Indonesia
Jl. Sisingamangaraja No. 338 Simpang Limun, Medan

ABSTRAK

Masalah keamanan akan data dan informasi dan dalam hal ini akan membuka peluang bagi orang-orang yang tidak bertanggung jawab untuk menggunakannya sebagai tindak kejahatan. Dan tentunya akan merugikan pihak tertentu.dalam kesempatan ini penulis akan mencoba menjelaskan berbagai macam ancaman keamanan data dan cara mengatasi ancaman tersebut. Kriptografi dapat menjadi jawaban dari masalah tersebut. Sebagai ilmu yang telah diaplikasikan untuk pengamanan data, kriptografi dapat digunakan untuk mengamankan data-data penting pada sebuah file. Data yang terkandung dalam file disandikan atau dienkripsi untuk diubah menjadi simbol tertentu sehingga hanya orang tertentu saja yang dapat mengetahui isi dari data tersebut, orang – orang yang tidak berkepentingan tidak dapat mengetahui bagaimana bagaimana cara membaca maupun menerjemahkan tulisan tersebut. Pada penelitian ini penulis menggunakan algoritma vernam cipher dan playfair cipher. Kedua algoritma ini dikombinasikan agar cipherteks yang dihasilkan lebih sulit untuk dipecahkan oleh kriptanalis karena cipher teks yang dihasilkan dari algoritma pertama akan diproses kembali menjadi cipherteks kedua sehingga akan lebih memperumit kode yang dihasilkan.

***Kata kunci** : email, keamanan, Kriptografi, Rahasia, dunia maya.*

I. PENDAHULUAN

Perkembangan dunia teknologi informasi semakin pesat sehingga banyak media yang dapat dimanfaatkan. Teknologi informasi telah terbukti merupakan sarana informasi yang mendorong dan meningkatkan kinerja diberbagai salah satunya dibidang keamanan. Karena perkembangan teknologi yang sangat pesat pada masa sekarang membuat manusia dapat dengan mudah bertukar informasi maupun menyimpan data yang bersifat privasi pada suatu individu ataupun institusi sesuai dengan kebutuhan menggunakan media komputer.

Kriptografi dapat menjadi jawaban dari masalah tersebut. Sebagai ilmu yang telah diaplikasikan untuk pengamanan data, kriptografi dapat digunakan untuk mengamankan data-data penting pada sebuah *file*. Data yang terkandung dalam *file* disandikan atau dienkripsi untuk diubah menjadi simbol tertentu sehingga hanya orang tertentu saja yang dapat mengetahui isi dari data tersebut, orang-orang yang tidak berkepentingan tidak dapat mengetahui bagaimana bagaimana cara membaca maupun menerjemahkan tulisan tersebut.
Pada penelitian ini penulis menggunakan algoritma *vernam cipher* dan *playfair cipher*. Kedua algoritma ini dikombinasikan agar *cipher*teks yang dihasilkan lebih sulit untuk dipecahkan oleh kriptanalis karena *cipher* teks yang dihasilkan dari algoritma pertama akan diproses kembali menjadi *cipher*teks kedua sehingga akan lebih memperumit kode yang dihasilkan.

II. TEORITIS

A. Kriptografi

Kriptografi berasal dari Bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim kesuatu tempat ke tempat lain (Dony Ariyus, 2008 : 13). Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data.

B. Algoritma *Vernam Cipher*

Aliran kode (*cipher stream*) mengenkripsi teks asli menjadi teks kode *bit* per *bit* (1*bit* setiap kali transformasi). Pertama kali diperkenalkan oleh Vernam melalui algoritma yang dikenal dengan nama kode *vernam.* Kode *vernam* diadopsi dari *one time pad cipher.* Yang dalam hal ini karakter diganti dengan bit (0 atau 1). Teks kode yang diperoleh dengan melakukan penjumlahan modulo 2 satu bit teks asli dengan satu bit kunci (Doni Ariyus, 2008 : 87).

$$Ci=(Pi+Ki) \bmod 2 \quad \text{.....(2.1)}$$

Yang dalam hal ini
Pi = bit teks asli
Ki = bit kunci
Ci = bit teks kode

1. Teks asli diperoleh dari penjumlahan modulo 2 satu bit teks kode dengan satu bit kunci
$$Pi=(Ci-Ki) \bmod 2 \quad \text{.....(2.2)}$$
2. Dengan kata lain, kode vernam adalah versi lain dari kode *one time pad cipher.*
3. Oleh karena operasi penjumlahan modulo 2 identik dengan operasi bit dengan operator *XOR* maka persamaan poin 1 dapat ditulis sebagai
$$Ci=Pi \oplus Ki \quad \text{.....(2.3)}$$
Dengan proses dekripsi menggunakan persamaan.
$$Pi=Ki \oplus Ki \quad \text{.....(2.4)}$$

Pada aliran kode, bit hanya mempunyai dua buah nilai sehingga proses enkripsi hanya menyebabkan 2 keadaan pada bit tersebut. Berubah atau tidak berubah. Dua buah keadaan ditentukan oleh kunci enkripsi yang disebut aliran bit kunci (*keyStream*) (Doni Ariyus, 2008 : 88).

Aliran bit kunci dibangkitkan oleh sebuah pembangkit yang dinamakan pembangkit aliran bit kunci (*keystream Generator*). Aliran bit kunci sering dinamakan *running key* di-XOR-kan dengan aliran bit-bit teks asli p_1, p_2..... p_i untuk menghasilkan aliran bit teks kode

$Ci=Pi \oplus Ki$

Karena

$C_i \oplus K_i = (P_i \oplus K_i) \oplus K_i = P_i \oplus (K_i \oplus K_i) = P_i \oplus 0 = P_i$

C. Algoritma *flayfair cipher*

Sandi Playfair digunakan oleh Tentara Inggris pada saat Perang Boer II dan Perang Dunia I. Ditemukan pertama kali oleh Sir Charles Wheatstone dan Baron Lyon Playfair pada tanggal 26 Maret 1854. Playfair merupakan *digraphs cipher*, artinya setiap proses enkripsi dilakukan pada setiap dua huruf. Misalkan plainteksnya "KRIPTOLOGI", maka menjadi "KRIPTOLOGI". Playfair menggunakan tabel 5x5. Semua alfabet kecuali J diletakkan ke dalam tabel. Huruf J dianggap sama dengan huruf I, sebab huruf J mempunyai frekuensi kemunculan yang paling kecil. Kunci yang digunakan berupa kata dan tidak ada huruf sama
yang berulang. Apabila kuncinya "MATAHARI", maka kunci yang digunakan
adalah "MATHRI". Selanjutnya, kunci dimasukkan ke dalam tabel 5x5, isian pertama adalah kunci, selanjutnya tulis huruf-huruf berikutnya secara urut dari baris pertama dahulu, bila huruf telah muncul, maka tidak dituliskan kembali.
Algoritma Enkripsi Playfair pada File Teks : 30.
Berikut ini aturan-aturan proses enkripsi pada Playfair yaitu

1. Jika 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. Jika 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. Jika kedua huruf terletak pada kolom yang sama maka huruf pertama menjadi huruf setelahnya dalam kolom yang sama, demikian juga dengan huruf kedua. Jika 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. Jika kedua huruf sama, maka letakkan sebuah huruf di tengahnya (sesuai kesepakatan).

Jika jumlah huruf plainteks ganjil, maka tambahkan satu huruf pada akhirnya, seperti pada aturan ke-4. Sedangkan proses dekripsinya adalah kebalikan dari proses enkripsi. Contohnya, HR didekrip menjadi HT, BS didekrip menjadi DP, ZU didekrip menjadi RZ (Rina Chandra Noer Santi, Implementasi Algoritma Enkripsi Playfair pada File Teks : 30).

III. ANALISA

A. Analisa Masalah

Kemudahan akses informasi ini memberi pengaruh dengan adanya ancaman-ancaman yang dapat membahayakan informasi tersebut, misalnya berupa interupsi, penyadapan, maupun modifikasi informasi. Hal ini dapat mempengaruhi tingkat keamanan dari dokumen/informasi yang berakibat pada keamanan data dan memunculkan kekhawatiran dalam menyimpan dokumen-dokumen penting maupun dalam pengiriman dan penerimaan informasi apakah pesan/informasi yang dikirimkan masih aman atau sudah mengalami perubahan. Sebagai contoh sebuah perusahaan ingin mengirimkan sebuah dokumen penting ataupun pesan kepada mitra bisnisnya tetapi perusahaan ingin agar dokumen/pesan tersebut aman dari ancaman penyadapan yang dapat dilakukan oleh pihak lain.

Dalam melakukan enkripsi ada beberapa langkah yang dilakukan yaitu:

1. Inputkan file berekstensi txt/doc yang berisi pesan/informasi (*plaintext*) yang akan dienkripsi.
2. Proses enkripsi *file* dengan menambahkan kunci.
3. Hasil akhir adalah file yang telah dikodekan dengan algoritma *Vernam Cipher* dan *Playfair Cipher*.

Dalam melakukan dekripsi ada beberapa langkah yang dilakukan yaitu:

1. Inputkan file berekstensi txt/doc yang berisi pesan/informasi (*ciphertext*) yang akan didekripsi.
2. Proses dekripsi *file* dengan menambahkan kunci.

Hasil akhir adalah file yang telah didekripsi dengan algoritma *Vernam Cipher* dan *Playfair Cipher*.

B. Penerapan Algoritma *Playfair Cipher* dan *Vernam Cipher*

1. Enkripsi Algoritma *Playfair Cipher*

Sebelum melakukan enkripsi algoritma *playfair cipher*, plainteks yang akan dienkripsi diatur terlebih dahulu sebagai berikut:

1. Semua spasi dan karakter yang bukan alfabet harus dihilangkan dari plainteks (jika ada).
2. Jika ada huruf J pada palinteks 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*..
5. Jika jumlah huruf pada plainteks adalah ganjil maka pilih sebuah huruf tambahan yang dipilih oleh orang yang mengenkripsi dan tambahkan di akhir plainteks. Huruf tambahan dapat dipilih sembarang misalnya huruf Z atau X.

Plainteks =P R A T I K A S A R I E K A
Hilangkan semua karakter yang bukan alfabet.

1. Tidak ada huruf J, maka langsung tulis pesan dalam pasangan huruf.
2. Jika ada huruf yang sama pasangan huruf (*bigram*), maka tambahkan huruf X ditengahnya.
   Plainteks yang telah dilakukan pengaturan:
   PR AT IK AS AR IE KA

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 (pada kunci yang telah diperluas).
2. Jika ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf di bawahnya (pada kunci yang telah diperluas).
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 3 huruf yang digunakan sampai sejauh ini

Kunci = S T M I K B U D I D A R M A

Tabel 1. Kunci

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

Berikut ini aturan-aturan proses enkripsi pada Playfair yaitu

1. Jika 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
2. Jika 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.

Plainteks = PR AT IK AS AR IE KA
Cipher teks = QA UI KS BI RB TG IR

2. Enkripsi Algoritma *Vernam Cipher*

Setelah didapat cipherteks dari algoritma playfair cipher, maka cipher tersebut menjadi plainteks dalam proses selanjutnya yaitu enkripsi algoritma *vernam cipher*. Cara kerja dari algoritma vernam cipher Setiap blok plainteks P_i dienkripsi secara individual dan independen menjadi blok cipherteks C_i.
Plainteks = QA UI KS BI RB TG IR
Kunci = s t m i k b u d i d a r m a

Tabel 2. konversi plainteks kenilai biner

Karakter plainteks	Nilai desimal	Nilai biner
Q	81	01010001
A	65	01000001
U	85	01010101
I	73	01001001
K	75	01001011
S	83	01010011
B	66	01000010
I	73	01001001
R	82	01010010
B	66	01000010
T	84	01010100
G	71	01000111
I	73	01001001
R	82	01010010

Tabel 3. Konversi Kunci Kenilai Biner

Karakter kunci	Nilai desimal	Nilai biner
s	115	1110011
i	105	1101001
r	114	1110010
e	101	1100101
g	103	1100111
a	97	1100001
r	114	1110010
s	115	1110011
i	105	1101001
r	114	1110010

Karakter kunci	Nilai desimal	Nilai biner
e	101	1100101
g	103	1100111
a	97	1100001
r	114	1110010

Proses enkripsi algoritma *Vernam Cipher* menggunakan formula $C_i = P_i \oplus K_i$

P=0 1 0 1 0 0 1 1 0 1 0 0 0 0 1 0 0 1 0 0 1 0 0 1 0
1 0 1 0 0 1 0 0 1 0 0 0 0 1 0
K=0 1 1 0 0 0 0 1 0 1 1 1 0 0 1 0 0 1 1 1 0 0 1 1 0
1 1 0 1 0 0 1 0 1 1 1 0 0 1 0 ⊕
C=0 0 1 1 0 0 1 0 0 0 1 1 0 0 0 0 0 0 1 1 1 0 1 0 0
0 1 1 1 0 1 1 0 0 1 1 0 0 0 0

P=0 1 0 1 0 0 1 1 0 1 0 0 0 0 1 0 0 1 0 0 1 0 0 1 0
1 0 1 0 0 1 0 0 1 0 0 0 0 1 0
K=0 1 1 0 0 0 0 1 0 1 1 1 0 0 1 0 0 1 1 1 0 0 1 1 0
1 1 0 1 0 0 1 0 1 1 1 0 0 1 0 ⊕
C=0 0 1 1 0 0 1 0 0 0 1 1 0 0 0 0 0 0 1 1 1 0 1 0 0
0 1 1 1 0 1 1 0 0 1 1 0 0 0 0

P=0 1 0 1 0 1 0 0 0 1 0 0 0 1 1 1 0 1 0 0 1 0 0 1 0
1 0 1 0 0 1 0
K=0 1 1 0 0 1 0 1 0 1 1 0 0 1 1 1 0 1 1 0 0 0 0 1 0
1 1 1 0 0 1 0 ⊕
C=0 0 1 1 0 0 0 1 0 0 1 0 0 0 0 0 0 0 1 0 1 0 0 0 0
0 1 0 0 0 0 0

Kelompokkan bit menjadi 8 bit per kelompok
00100010 => 34 =>"
00101000 =>40 =>(
00100111=>39 =>'
00101100 =>44 =>,
00101100 =>44 =>,
00110010 =>50 =>2
00110000 =>48 =>0
00111010 =>58 =>:
00111011 =>59 =>;
00110000 =>48 =>0
00110001 =>49 =>1
00100000 =>32 =>
00101000 =>40 =>(
00100000 =>32 =>
Cipher teks adalah " (' , , 2 0 : ; 0 1 (

3. Dekripsi Algoritma *Vernam Cipher*

Cipherteks = " (' , , 2 0 : ; 0 1 (

Tabel 4. Konversi *Cipher*teks Kenilai Biner

Karakter cipher	Nilai desimal	Nilai biner
"	34	00100010
(	40	00101000
'	39	00100111
,	44	00101100
,	44	00101100
2	50	00110010
0	48	00110000
:	58	00111010
;	59	00111011
0	48	00110000
1	49	00110001
	32	00100000
(	40	00101000
	32	00100000

Tabel 5. konversi kunci2 kenilai biner

Karakter kunci	Nilai desimal	Nilai biner
S	115	1110011
I	105	1101001
r	114	1110010
e	101	1100101
g	103	1100111
a	97	1100001
r	114	1110010
s	115	1110011
i	105	1101001
r	114	1110010
e	101	1100101
g	103	1100111
a	97	1100001
r	114	1110010

Proses Dekripsi algoritma *Vernam Cipher* menggunakan formula $P_i = C_i \oplus K_i$

C=0 0 1 0 0 0 1 0 0 0 1 0 1 0 0 0 0 0 1 0 0 1 1 1 0
0 1 0 1 1 0 0 0 0 1 0 1 1 0 0
K=0 1 1 1 0 0 1 1 0 1 1 0 1 0 0 1 0 1 1 1 0 0 1 0 0
1 1 0 0 1 0 1 0 1 1 0 0 1 1 1 ⊕
P=0 1 0 1 0 0 0 1 0 1 0 0 0 0 0 1 0 1 0 1 0 1 0 1 0
1 0 0 1 0 0 1 0 1 0 0 1 0 1 1

C=0 0 1 1 0 0 1 0 0 0 1 1 0 0 0 0 0 0 1 1 1 0 1 0 0
0 1 1 1 0 1 1 0 0 1 1 0 0 0 0
K=0 1 1 0 0 0 0 1 0 1 1 1 0 0 1 0 0 1 1 1 0 0 1 1 0
1 1 0 1 0 0 1 0 1 1 1 0 0 1 0 ⊕
P=0 1 0 1 0 0 1 1 0 1 0 0 0 0 1 0 0 1 0 0 1 0 0 1 0
1 0 1 0 0 1 0 0 1 0 0 0 0 1 0

C=0 0 1 1 0 0 0 1 0 0 1 0 0 0 0 0 0 0 1 0 1 0 0 0 0
0 1 0 0 0 0 0
K=0 1 1 0 0 1 0 1 0 1 1 0 0 1 1 1 0 1 1 0 0 0 0 1 0
1 1 1 0 0 1 0 ⊕
P=0 1 0 1 0 1 0 0 0 1 0 0 0 1 1 1 0 1 0 0 1 0 0 1 0
1 0 1 0 0 1 0

Kelompokkan bit menjadi 8 bit per kelompok
01010001= 81 => Q
01000001= 65 => A
01010101= 85 => U

01001001= 73 => I
01001011= 75 => K
01010011= 83 => S
01000010= 66 => B
01001001= 73 => I
01010010= 82 => R
01000010= 66 => B
01010100= 84 => T
01000111= 71 => G
01001001= 73 => I
01010010= 82 => R
maka plainteks dari algoritma vernam cipher adalah QA UI KS BI RB TG IR

4. Dekripsi Algoritma *Playfair Cipher*

Setelah didapat *plain*teks dari algoritma *vernam cipher*, maka *plain*teks tersebut menjadi *cipher*teks dalam proses selanjutnya yaitu dekripsi algoritma *playfair cipher*. Berikut ini merupakan langkah-langkah proses dekripsi algoritma *playfair cipher*.

Cipher teks = QA UI KS BI RB TG IR
Algoritma Dekripsi 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 (pada kunci yang telah diperluas).
2. Jika ada dua huruf terdapat pada kolom yang sama maka tiap huruf diganti dengan huruf di bawahnya (pada kunci yang telah diperluas).
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 3 huruf yang digunakan sampai sejauh ini.
   Kunci = S T M I K B U D I D A R M A

Tabel 6. Kunci2

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

Berikut ini aturan-aturan proses Dekripsi pada algoritma *Playfair cipher* yaitu :

1. Jika 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
2. Jika 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.

Cipher teks = QA UI KS BI RB TG IR
Plain teks = PR AT IK AS AR IE KA

IV. IMPLEMENTASI

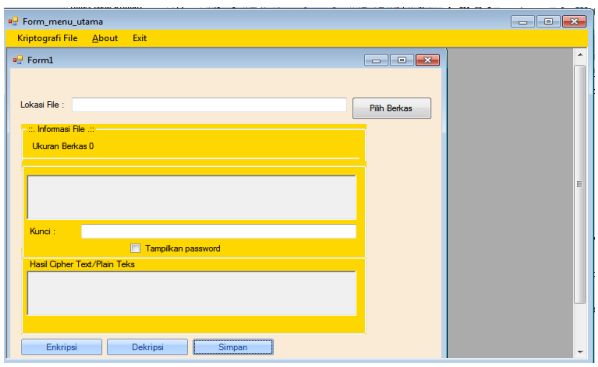
A. Implementasi Sistem

Perancangan aplikasi kriptografi algoritma playfair cipher dan vernam cipher telah selesai dirancang dan dibuat dengan menggunakan aplikasi Microsoft Visual Studio 8 dan bahasa pemograman Visual Basic. Adapun tampilan *form* aplikasi kriptografi file yang dirancang penulis adalah sebagai berikut :

1. *Form* Menu utama
   Pada tampilan menu utama merupakan tampilan yang akan tampil setelah menjalankan program utama. Tampilan ini berisi judul penelitian, gambar latar serta tampilan menu. Tampilan menu terdiri dari kriptografi file, about dan keluar. Tampilan untuk menu utama dapat dilihat pada gambar 1.

Gambar 1. Tampilan *Form Home*

2. *Form* kriptografi file
   Form menu kriptografi file, merupakan *form* inti dari aplikasi yang dirancang penulis. Tampilan form kriptografi file menggunakan algoritma kriptografi *playfair cipher* dan *vernam cipher* untuk melakukan proses enkripsi dan dekripsi. Tampilannya dapat dilihat pada gambar 2. sebagai berikut:



Gambar 2. Tampilan *form* kriptogradi file

Adapun langka dalam melakukan enkripsi dan dekripsi dengan algoritma playfair cipher dan vernam cipher antara lain :

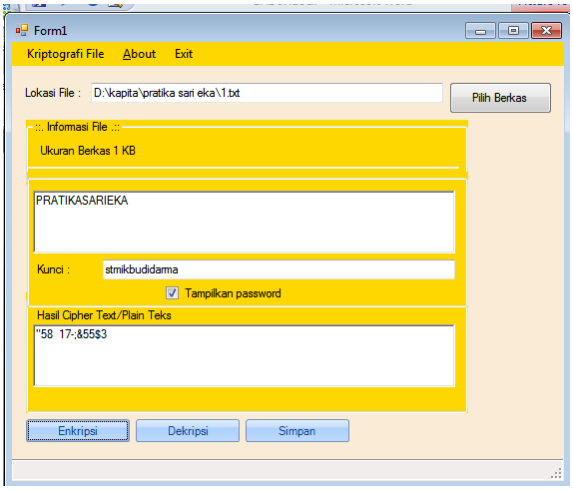
a. Pilih tombol buka terlebih dahulu, kemudian akan tampil *form open* lalu pilih file audio yang akan di proses.
b. Input kunci sebelum melakukan proses enkripsi dan dekripsi.
c. Kemudian tahap akhir tombol enkripsi dan dekripsi untuk melakukan proses pengkodean plainteks ataupun sebaliknya.
d. tombol *Save* berguna untuk menyimpan data yang telah terproses didalam *disk* atau direktori.

3. Hamalam *About*
   Form about merupakan *form* biodata penulis. Tampilan *form about* dapat dilihat pada gambar 3.

Gambar 3. Tampilan *Form About*

4.4 Hasil Pengujian Program

Adapun hasil dari pengujian program yang telah dibuat adalah sebagai berikut. Pada gambar 4. dapat dilihat hasil pengujian program. Plainteks yang diinputkan akan menjadi diacak sehingga tidak dapat dimengerti.



Gambar 4. Tampilan hasil pengujian program

REFERENCES

[1] Abdul Kadir. (2013). "Pengertian Algoritma, Pendekatan Secara Visual dan Interaktif Menggunakan Raptor". Yogyakarta : ANDI.
[2] Adi nugroho. (2010). "Rekayasa Perangkat Lunak Berorientasi Objek Dengan Metode USDP (unified Software Development Process)". Yogyakarta : ANDI.
[3] Dony Ariyus. (2006). "Keamanan Data dan Komunikasi". Yogyakarta : Graha Ilmu.
[4] Dony Ariyus. (2008). "pengantar ilmu kriptografi: teori analisis dan implementasi". Yogyakarta : ANDI.
[5] Edy Irwansyah dan Jurike V. Moniaga. (2014). "Pengantar Teknologi Informasi". Yogyakarta : Deepublish.
[6] Edy winarno ST, M.Eng – Ali Zaki SmitDev Community, (2013). "Step by Step Visual Basic .NET". Jakarta : PT. Alex Media Komputindo.
[7] Rinaldi Munir. (2007). "Algoritma dan Pemograman Dalam Bahasa Pascal dan C". Bandung : INFORMATIKA.
[8] Rina Chandra Noer Santi, (2010) "Implementasi Algoritma Enkripsi Playfair pada File Teks" *Jurnal Teknologi Informasi DINAMIK Volume XV, No.1.*
[9] Tara Baskara. "Modifikasi Rail Fence Cipher Menggunakan Vigenere Cipher".
[10] Windu Gata, Grace Gata. (2013). "Sukses Membangun Aplikasi Penjualan Dengan Java". Jakarta : PT. Alex Media Komputindo.