Volume 2 No. 2, Desember 2017 MEANS (Media Informasi Analisa dan Sistem)
http://ejournal.ust.ac.id/index.php/Jurnal_Means/ **p-ISSN : 2548-6985, e-ISSN : 2599-3089**

Analisa Pengamanan Data Teks Menggunakan Algoritma ADFGVX

Chandra Purnama
STMIK Budi Darma Medan, Jl. Sisingamangaraja No.338 Simpang Limun Medan
http : //www.stmik-budidarma.ac.id // Email : chandrapurnamagaul@gmail.com

ABSTRACT
This study discusses the implementation of ADFGVX to encode text data. ADFGVX is one of the classic cryptographic methods that uses symmetry keys. this method uses a 6x6 key board for encryption and decryption. The process of encryption and decryption is done by grouping letters in bigram. By using a 6x6 key board, we can encrypt plainteks (original text data to be encrypted) and decrypt ciphertext (encrypted text data) by grouping it. Keyboards are generated randomly by software so that each encryption process (encryption and decryption) can use different keys. This software is also used to verify the results of ADFGVX encryption and decryption with the cube keyboard. ADFGVX software is developed using Visual Basic and graphically based languages in the Windows development environment.

Kata kunci: ADFGVX, papan kunci, enkripsi, dekripsi.

PENDAHULUAN

Dalam komunikasi data, terdapat sebuah metode pengamanan data yang dikenal dengan nama kriptografi. Kriptografi merupakan salah satu metode pengamanan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data, serta keaslian pengiriman. Metode ini bertujuan agar informasi yang bersifat rahasia yang dikirim melalui telekomunikasi umum tidak dapat diketahui atau dimanfaatkan oleh orang yang tidak berkepentingan atau yang tidak berhak menerimanya. Metode kriptografi yang dapat digunakan untuk mengamankan data ada bermacam-macam.

Setiap metode memiliki kelebihan dan kekurangannya masing-masing. Namun, yang menjadi permasalahan dalam memilih metode kriptografi yang cocok adalah bagaimana mengetahui dan memahami cara kerja dari metode kriptografi tersebut. Dalam proses komunikasi data, walaupun data telah dienkripsi kemungkinan data tersebut dapat diketahui oleh orang lain. Salah satu kemungkinan tersebut adalah orang tersebut menyadap media komunikasi yang digunakan oleh kedua orang yang sedang berkomunikasi[1].

Untuk membangun suatu sistem pengamanan data sangat sulit dengan cepat karena membutuhkan pemikiran yang matang dengan mempersiapkan segala sesuatu yang dianggap penting. Maka dari itu diperlukan simulasi agar hasil yang diharapkan sesuai dengan yang diinginkan. Sebab tanpa dilakukan proses simulasi maka resiko dan biaya yang dibutuhkan sangat mahal karena prosesnya langung dilaksanakan tanpa dilakukan proses simulasi terlebih dahulu. Dengan melihat pentingnya keamanan data tersebut akan dikembangkan salah satu teknik pengamanan data atau file dengan menggunakan metode ADFGVX[2]

Berdasarkan latar belakang pemilihan judul, maka yang menjadi permasalahan adalah:

1. Bagaimana merancang aplikasi pengamanan data pesan dengan format teks menggunakan metode ADFGVX ?
2. Bagaimana cara kerja metode ADFGVX untuk proses enkripsi dan dekripsi ?

Untuk menghindari kesalahpahaman dan meluasnya pembahasan, maka penulis membatasi atau memfokuskan masalah yang berkaitan dengan pemecahan masalah yaitu:

1. Data yang akan diterapkan adalah text.
2. Metode yang digunakan adalah ADFGVX.
3. Papan kunci yang digunakan berukuran 6 x 6 dimana setiap bagian dalam papan kunci mewakili huruf dalam alfabet (abjad).
4. Kunci yang digunakan adalah kunci simetris.
5. Bahasa pemrograman yang digunakan adalah Visual Basic.Net 2008

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Membuat simulasi pengamanan data.
2. Mengetahui dan menerapkan metode ADFGVX untuk penyandian data.

Adapun manfaat dari simulasi yang akan dibangun ini adalah :

1. Dapat digunakan sebagai media pembelajaran kriptografi.

2. Sebagai bahan aplikasi untuk pembuatan aplikasi dari mata kuliah model dan simulasi.

LANDASAN TEORI

2.1. Kriptografi

Kata kriptografi berasal dari bahasa yunani yaitu kripto (*hidden* atau *secret*) dan grafh (*writing*) sehingga berarti *secret writing*. Secara istilah kriptografi didefinisikan sebagai ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) yang mempunyai pengertian, dengan cara menyamarkannya (mengacak) menjadi bentuk yang tidak dapat dimengerti menggunakan suatu algoritma tertentu[3].

2.2 Klasifikasi Kriptografi

Dipandang dari segi era pengembangannya ilmu kriptografi dibagi menjadi dua, yaitu kriptografi klasik dan kriptografi modern.

2.2.1 Kriptografi klasik

Dilihat dari namanya tentu saja kriptografi klasik merupakan awal dari pengembangan ilmu kriptografi. Pada era pengembangan ini kekuatan kriptografi terletak pada kerahasiaan algoritma yang digunakan, jenis algoritma ini dinamakan algoritma *restricted.* Namun ditengah pengembangannya algoritma *restricted* ditemukan banyak kelemahan sehingga tidak relevan lagi untuk keperluan keamanan informasi saat ini[4][5].

2.2.2 Kriptografi Modern

Kriptografi modern dikembangkan untuk membenahi kelemahan-kelamahan yang dimiliki oleh kriptografi sebelumnya yaitu kroptografi klasik[1] . Berlawanan dengan kriptografi klasik, algoritma yang digunakan pada kriptografi modern di buka atau dengan kata lain diketahui oleh umum sehingga tidak bersifat rahasia. Hal ini dilakukan untuk menutupi kelemahan kriptografi klasik, sehingga algoritma dari kriptografi modern bisa di uji ketangguhannya oleh pakar-pakar kriptografi. Lalu dimana letak kekuatan dari kriptografi modern? Kekuatan kriptografi ini bertumpu pada kerahasiaan kunci penyandian. Berdasarkan kunci penyandiannya, kriptografi modern dibagi menjadi dua jenis yaitu kriptografi kunci simetri dan kriptografi kunci asimetri.

2.2.3 Kriptografi Kunci Simetri

Pada kriptografi ini, metode enkripsi dan depenelitian menggunakan kunci yang sama. Misalnya kunci enkripsi adalah K.

2.2.4 Kriptografi Kunci Asimetri

Kriptografi kunci asimetri menggunakan kunci yang berbeda (pasangan kunci) untuk keperluan proses enkripsi dan proses dekripsi. Kunci yang digunakan dalam proses enkripsi biasanya disebut kunci publik atau *public key*, sedangkan kunci yang digunakan dalam proses dekripsi biasanya disebut sebagai kunci privat. Perbedaan yang sangat terlihat antara kriptografi kunci simetri dan kriptografi kunci asimetri terletak pada sifat kunci, pada kriptografi kunci simetri kunci bersifat *private*, sedangkan pada kriptografi kunci asimetri terdapat pasangan kunci yang memiliki dua sifat yang berbeda, yaitu kunci *private* untuk proses dekripsi dan kunci *public* untuk proses enkripsi[2][5].

2.3 Metode ADFGVX

Metode kriptografi ADFGVX yang digunakan oleh tentara Jerman pada Perang Dunia I adalah merupakan salah satu algoritma yang paling dikenal dalam sejarah kriptografi klasik. Algoritma ini ditemukan oleh seorang petugas radio tentara Jerman yang bernama Fritz Nebel (1891 - 1967)[6]. Algoritma ini pertama kali muncul pada tanggal 5 Maret 1918 ketika pihak Jerman menggunakannya dalam sebuah transmisi pesan nirkabel di medan perang di bagian barat Eropa. Dinamakan algoritma ADFGVX karena chiperteks hasil enkripsi pesan tentara Jerman hanya mengandung enam karakter alphabet. Pada awalnya algoritma ini hanya menggunakan 5 karakter saja. Namun pada perkembangannya ditambahkan karakter huruf X agar algoritma ini dapat menangani 26 huruf alphabet dan 10 angka. Huruf-huruf A, D, F, G, V, dan X sendiri dipilih karena representasi huruf-huruf tersebut dalam sandi morse sangatlah berbeda dan oleh karenanya memperkecil kemungkinan terjadinya kesalahan dalam penerimaan pesan. Algoritma ADFGVX *cipher* menggunakan tabel 6 x 6 yang berisi 26 huruf dan 10 angka (0-9). Enkripsinya terdiri dari dua proses, yaitu proses substitusi dan proses transposisi. Selain itu Setiap proses tersebut membutuhkan sebuah kunci.

PEMBAHASAN

3.1 Analisa

Untuk penggunaan algoritma ADGVX untuk enkripsi dan dekripsi data ini, maka digunakan beberapa syarat yaitu harus memiliki pesan dan kunci Adapun prosesnya dapat dilihat pada proses dibawah ini.

3.1.1 Proses Enkripsi

Enkripsi merupakan sebuah proses dimana data teks asli diubah menjadi data teks

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089

rahasia. Sebelum melakukan enkripsi, pesan yang akan dienkripsi (*plainteks)* diatur terlebih dahulu sebagai berikut :

1. Semua spasi dan karakter yang bukan alphabet dan angka harus dihilangkan dari plainteks
2. Pesan yang akan dienkripsi ditulis dalam pasangan berurut(*bigram*)
3. Kunci dimasukkan dalam tabel ukuran 6 x 6

Contoh Kasus :
Pesan = THIS IS A SECRET
Kunci 1= C3A1LI9F6ORNB2D4E5G7H8J0KMPQSTUVWXYZ
Kunci 2=APOLLO

Berikut ini adalah langkah-langkah dalam mengenkripsi sebuah pesan plainteks dengan menggunakan algoritma ADFGVX *Cipher* :

1. Tentukan kunci pertama yang terdiri dari huruf dan angka, misalkan "C3A1LI9F6ORNB2D4E5G7H8J0KMPQSTUVWXYZ". Jika ada huruf yang berulang, maka cukup satu huruf yang muncul pertama yang dituliskan.
2. Buatlah sebuah tabel 6 x 6 dan isi dengan kunci pertama, kemudian huruf-huruf berurutan yang belum muncul, dan selanjutnya angka-angka berurutan yang belum muncul. Tabel berikut merepresentasikan tabel yang terbentuk dengan kunci "C3A1LI9F6ORNB2D4E5G7H8J0KMPQSTUVWXYZ".

Tabel 1 Tabel Kunci 1

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

3. Selanjutnya, setiap huruf dalam plainteks disubstitusi menjadi dua huruf yang ditentukan oleh posisi baris dan kolom. Sebagai contoh, huruf k menjadi VA, serta huruf g menjadi GA.

Penyelesaian = THIS IS A SECRET
Enkripsikan T menjadi VX ditunjukkan pada papan kunci dibawah ini

Tabel 2 Enkripsi T

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

3.1.2 Proses Dekripsi

Berikut ini adalah langkah-langkah dalam mendekripsi sebuah chipertext menjadi plainteks dengan menggunakan metode ADFGVX *:*

1. Terlebih dahulu kita harus mengetahui kunci 2 dari proses ini. Selanjutnya bagikan jumlah karakter hasil enkripsi dengan panjang kunci ke 2 dimana panjang *chipertext*=36 dan panjang kunci=6 sehingga diperoleh banyak karakter per kolom sebanya 36/6=6 karakter. Gambarkan hasilnya kedalam kotak kunci sebagai berikut :

Tabel 3 Tabel Dekripsi

A	L	L	O	O	P
V	F	A	G	X	X
V	X	V	A	V	V
A	V	F	V	V	F
A	V	F	D	V	A
V	X	X	X	X	X
X	X	X	X	X	X

2. Susun kembali hasil dari langkah 1 sesuai kunci ke 2 yaitu "kunci" . Untuk mendapatkan hasil dari pengurutan ALLOOP menjadi APOLLO maka harus dilakukan proses perulanangan sebanyak n! dimana :
   n = panjang kunci
   sehingga untuk mendapatkan kunci tersebut maka dibutuhkan sebanyak 6! Proses pencarian yaitu sebanyak 720 kali kemungkinan diantaranya :

Allop	Aollp
Allpo	Aollp
Alplo	Aopll
Alopl	Aolpl
Allop	Aoplp

Sampai akhirnya diperoleh hasil APOLLO. Adapun proses percobaan tersebut sehingga diperoleh hasil sebagai berikut:

Tabel 4 Tabel Pemasukan Kunci

A	P	O	L	L	O
V	X	G	F	A	X
V	V	A	X	V	V
A	F	V	V	F	V
A	A	D	V	F	V
V	X	X	X	X	X
X	X	X	X	X	X

3. Susun kembali huruf-huruf yang ada di tabel kunci dengan bentuk *bigram* yaitu berpasangan, sehingga menjadi VX GF AX VV AX VV AF VV FV AA DV FV VX XX XX XX XX XX
4. Selanjutnya cari padanan dari abjad berpasangan diatas yang diperoleh dari kunci 1

Tabel 5 Tabel Pencarian Abjad

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

ALGORITMA DAN IMPLEMENTASI

4.1 Algoritma

Algoritma dalam perancangan aplikasi simulasi pengamanan data dibagi dua antara lain :
1. Algoritma proses enkripsi
2. Algoritma proses dekripsi

4.1.1 Algoritma Enkripsi

Algoritma ini digunakan untuk menyandikan teks agar teks tidak dapat dibaca oleh orang yang tidak berhak. Adapun algoritma tersebut adalah sebagai berikut :

```
Deklarasikan i,j,x,y :integer
If PlainIn = "" Then Exit
For i = 1 To Len(PlainIn)
   For j = 1 To 36
      If Mid(PlainIn, i, 1) = Square(j) Then
         'get row and column
         Y = Int((j - 1) / 6)
         X = (j - 1) - (Y * 6)
          EncSquare = EncSquare &
SquareCode(Y) & SquareCode(X)
      End If
   Next
Next
```

4.1.2 Algoritma Dekripsi

Algoritma ini digunakan untuk mengembalikan teks agar teks dapat dibaca oleh orang yang berhak. Adapun algoritma tersebut adalah sebagai berikut :

```
Deklarasikan i,x,y :integer
For i = 1 To Len(CodeIn) Step 2
      Y = GetADFGVXcode(Mid(CodeIn, i, 1))
   X = GetADFGVXcode(Mid(CodeIn, i + 1,
1))
   DecSquare = DecSquare & Square((Y * 6)
+ X + 1)
Next
```

4.2 Implementasi

Implementasi sistem program ini mencakup spesifikasi kebutuhan perangkat keras (*hardware*) dan spesifikasi perangkat lunak (*software*) dan cara mengoperasikan program aplikasi [4].

4.2.1 Cara Menggunakan Perangkat Lunak

Perangkat lunak penyandian data dengan algoritma ADFGVX dapat dijalankan dengan cara sebagai berikut :

4.2.1.1 Form Input Pesan dan Kunci

Form ini digunakan untuk memasukkan pesan yang akan disandikan berserta kunci yang digunakan untuk menyandikan data. Dimana kunci yang digunakan ada 2 yaitu kunci 1 dan kunci 2. Adapun tampilan form tersbut adalah sebagai berikut:

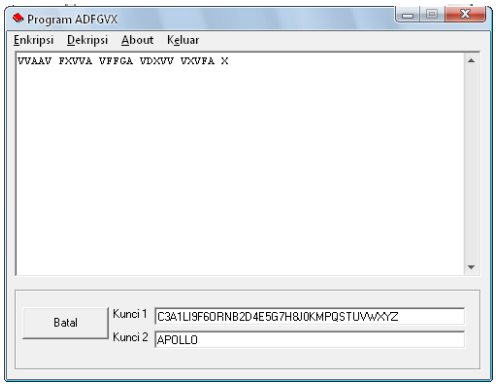
Gambar 1 Form Input Pesan dan Kunci

Keterangan :
1. Enkripsi : Proses menyandikan *plaintext* menjadi *chipertext*
2. Dekripsi : Proses mengembalikan *chipertext* menjadi *plaintext*
3. About : Menampilkan identitas dari pembuat aplikasi
4. Keluar : Keluar dari perancangan aplikasi
5. Masukkan plaintext yang akan di enkripsi/dekripsi
6. Masukkan kunci 1
7. Masukkan kunci 2
8. Untuk membatalkan program

4.2.1.2 Form Enkripsi

Form ini digunakan untuk menyandikan data yang telah diinput oleh user dimana syaratnya harus memiliki kunci. Adapun

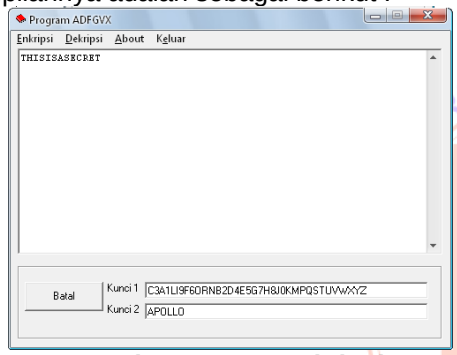
tampilan form tersebut adalah sebagai berikut:



Gambar 2 Form Enkripsi

4.2.1.3 Form Dekripsi

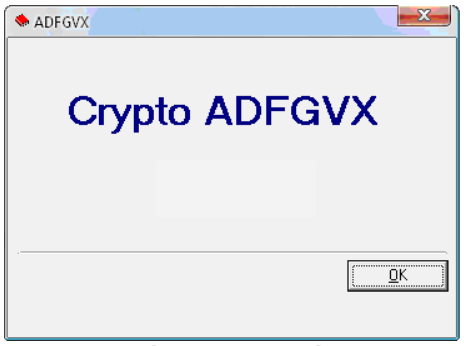
Form ini digunakan untuk mengembalikan pesan yang telah dienkripsi. Adapun tampilannya adalah sebagai berikut :



Gambar 3 Form Dekripsi

4.2.1.4 Form About

Form ini digunakan hanya untuk menampilkan identitas dari pembuat program aplikasi. Adapun tampilan dari form about adalah sebagai berikut :



Gambar 4 Form About

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil pengujian dan analisis terhadap Algoritma *ADFGVX*, dapat diambil beberapa kesimpulan sebagai berikut:

1. *ADFGVX* dengan papan kunci berbentuk bujursangkar dapat menyandikan pesan sehingga hanya pihak yang berhak saja yang dapat melihat isi pesan.
2. *ADFGVX* dengan menggunakan papan kunci adalah solusi yang lebih baik dalam mengatasi masalah keamanan dan kerahasian data teks.
3. Proses enkripsi dan dekripsi harus dilakukan dengan menggunakan papan kunci yang sama untuk mendapatkan isi arsip yang asal.

5.2 Saran

Berdasarkan hasil pengujian dan analisis terhadap Algortima *ADFGVX*, dapat diambil beberapa kesimpulan sebagai berikut:

1. Sebuah papan kunci yang digunakan dalam proses penyandian sebaiknya tidak digunakan lebih dari sekali. Hal ini untuk mengurangi kemungkinan papan kunci telah dipecahkan oleh orang yang tidak berkepentingan.
2. *ADFGVX* dapat dikembangkan lebih lanjut dengan tidak menggunakan pengelompokan huruf secara *bigram* melainkan *trigram* atau yang lain.

DAFTAR PUSTAKA

[1] J. Simarmata, “Pengamanan Sistem Komputer,” *Andi, Yogyakarta*, 2006.

[2] D. Ariyus, *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*. Penerbit Andi.

[3] R. Sadikin, “Kriptografi untuk keamanan jaringan,” *Penerbit Andi, Yogyakarta*, 2012.

[4] T. Limbong and P. D. P. Silitonga, “Testing the Classic Caesar Cipher Cryptography using of Matlab,” *Int. J. Eng. Res. Technol.*, vol. 6, no. 2, pp. 175–178, 2017.

[5] R. Munir, “Kriptografi,” *Inform. Bandung*, 2006.

[6] T. Limbong *et al.*, “The implementation of computer based instruction model on Gost Algorithm Cryptography Learning,” in *IOP Conference Series: Materials Science and Engineering*, 2018, vol. 420, no. 1, p. 12094.