JURNAL TEKNOLOGI ACADEMIA ISTA ISSN: 1410-5829
Vol. 10. Edisi Khusus 2 September 2005

ANALISIS KRIPTOGRAFI MENGGUNAKAN ALGORITMA *VIGENERE CIPHER* DENGAN MODE OPERASI *CIPHER BLOCK CHAINING* (CBC)

Erna Kumalasari Nurnawati[1]

ABSTRACT

Data security's problem is the important thing in organization or personal area. Moreever, if the data in network and connecting through public network, such as internet. The data have to protected by unregistered user, to protect from either data damaged or lossed. The aim of this research is how to secure the data, and security of sending message from the unregistered user.

Criptography using Vigenere Chipher algorithm were adapted Cipher Block Chaining (CBC) mode operation is the one of security methods. These application though data encription and decription using Borland Delphi 6.0 and the file extention of result is .enc.

Combining Vigenere Cipher and CBC mode operation will produce new methode named Vigenere Cipher+ that repair the disadvanrages of Vigenere Cipher.

Key words : *Cryptography, Encyption, Decription, Vigenere Cipher, CBC.*

INTISARI

Masalah keamanan dan kerahasiaan data merupakan hal yang sangat penting dalam suatu organisasi maupun pribadi. Apalagi kalau data tersebut berada dalam suatu jaringan komputer yang terkoneksi dengan jaringan publik misalnya internet. Tentu saja data yang sangat penting tersebut tidak boleh dilihat atau dibajak oleh orang yang tidak berwenang. Sebab kalau hal ini sampai terjadi kemungkinan data kita akan rusak bahkan bisa hilang yang akan menimbulkan kerugian material yang besar. Pada penelitian ini akan dibahas sistem keamanan pengiriman pesan atau data dengan menggunakan penyandian yang bertujuan untuk menjaga karahasiaan suatu pesan dari akses orang orang yang tidak berhak.

Kriptografi menggunakan Algoritma *Vigenere Cipher* dengan mengadopsi cara kerja mode operasi *Cipher Block Chaining* (CBC) merupakan salah satu metode dari sekian banyak metode pengamanan data. Aplikasi ini meliputi enkripsi dan dekripsi data, yang dibuat dengan menggunakan Borland Delphi 6.0. Data yang telah dienkripsi akan mempunyai ekstensi .enc.

Penggabungan Algoritma *Vigenere Chiper* dan mode operasi CBC ini akan menghasilkan suatu metode baru yang peneliti sebut *Vigenere Chiper* +, pada metode ini kelemahan-kelemahan yang ada pada algoritma *Vigenere Chiper* akan diperbaiki. Seperti memperluas jangkauan 26 huruf alfabeth tersebut menjadi 256 karakter ASCII

Kata kunci : Kriptografi, Enkripsi, Dekripsi, *Vigenere Cipher*, CBC.

PENDAHULUAN

Dengan semakin berkembangnya teknologi komputer, sistem *multiuser* sudah sangat memungkinkan dimana suatu data dapat dibagikan kepada komputer atau user lain dalam suatu jaringan komputer ataupun jaringan yang lebih luas lagi yaitu internet. Tetapi ada data yang memerlukan *privacy* dan harus dijaga kerahasiannya. Data-data penting ini harus dijaga dari pihak-pihak yang tidak bertanggung jawab baik terhadap pemalsuan, pencurian maupun pengubahan data secara illegal.

Untuk mengatasi permasalahan di atas, salah satu solusi yang dapat diambil adalah dengan cara penyandian atau kriptografi. Dengan cara ini sebuah data akan disandikan berdasarkan metode tertentu sehingga orang yang tidak berkepentingan dan tidak memiliki hak akses akan mengalami kesulitan untuk melakukan hal-hal yang tidak diinginkan. Sebaliknya ketika data tersebut akan diakses kembali oleh orang yang berhak maka hasil penyandian tersebut kemudian akan dikembalikan ke bentuk semula. Alasan pemilihan algoritma *Vigenere*

[1] Staf pengajar Jurusan Teknik Informatika IST AKPRIND Yogyakarta

Cipher karena *Vigenere Cipher* mengubah pesan dengan menggunakan kombinasi 26 huruf alfabet dan algoritma ini bertahan cukup lama sampai ditemukannya metode untuk memecahkan algoritma tersebut.

Pembuktian keberhasilan *kriptoanalisis* akan lebih akurat jika program juga menyediakan fasilitas untuk enkripsi dan dekripsi data. Algoritma *Vigenere Cipher* memiliki beberapa kelemahan, diantaranya hanya menampung 26 huruf alfabet dalam bentuk huruf kecil, sedangkan tanda baca lain tidak dapat terbaca. Untuk itu perlu dilakukan suatu pengevaluasian yaitu dengan memperluas jangkauan 26 huruf alfabet tersebut menjadi 256 karakter ASCII.

Evaluasi dari algoritma *Vigenere Cipher* ini akan mengadopsi cara kerja mode operasi CBC (*Cipher Block Chaining*).

Membuat program yang mampu mengenkripsi dan mengdekripsi data berdasarkan kunci tertentu dengan algoritma *Vigenere Cipher*. Algoritma *Vigenere Cipher* memiliki beberapa kelemahan, untuk itu perlu dilakukan pengevaluasian dengan mengadopsi cara kerja mode operasi CBC (*Cipher Block Chaining*). Untuk mendukung hal tersebut dicoba membuat suatu program dengan bahasa Pemrograman Delphi 6.0, Photoshop 7.0 dan menggunakan Sistem Operasi Windows XP. Diharapkan program mampu melakukan enkripsi teks/*file* teks dengan menggunakan kunci tertentu dan dapat didekripsi ke teks semula dengan menggunakan kunci yang sama pula. Karakter dalam *string input* adalah yang terdapat dalam tabel kode ASCII. Hasil enkripsi / *ciphertext* disimpan sebagai *file* yang baru.

Pembuatan program tersebut bertujuan untuk melakukan pengamanan terhadap suatu file teks sekaligus merancang dan menguji perangkat lunak dengan mengadopsi cara kerja mode operasi CBC (*Cipher Block Chaining*).

Adapun proses yang telah dilakukan meliputi riset pustaka tentang metode Vigenere dengan mode Cipher Block Chaining (CBC) kemudian telah dibuat aplikasi untuk membuktikan hipotesis beserta pengujiannya dengan berbagai data dalam proses enkripsi dan dekripsi

PEMBAHASAN

Algoritma enkripsi dan dekripsi pada *Vigenere Cipher* memiliki beberapa karakteristik, yaitu :

- Hanya menampung 26 huruf alfabeth dalam bentuk huruf kecil, sedangkan tanda baca lain tidak dapat terbaca.
- *Input*an hanya menerima hasil dalam bentuk huruf kecil, apabila terdapat huruf kapital harus dikonversikan terlebih dahulu dalam bentuk huruf besar.
- Panjang kunci yang diterima harus sama dengan panjang *plaintext* (Pi), sehingga membutuhkan memori yang sangat besar yang mengakibatkan proses jadi lama.

Dari karakteristik di atas, maka penulis mengadopsi cara kerja mode operasi CBC (*Cipher Block Chaining*) dengan rumus *Vigenere Cipher* untuk enkripsi dan dekripsi dengan memberikan beberapa solusi:

1. Memperluas jangkauan 26 huruf alfabeth dalam bentuk huruf kecil tersebut menjadi 256 karakter ASCII, sehingga tanda baca lain dan huruf kapital dapat langsung terbaca.
2. Panjang kunci yang dimasukkan dibatasi sampai 10 karakter, sehingga kunci dapat dinotasikan sebagai Ki.

Dengan solusi tersebut maka penulis mengevaluasi metode ini menjadi *Metode Vigenere+*.

Dari pengevaluasian algoritma *Vigenere Cipher*, maka secara matematis enkripsi dengan algoritma *Vigenere Cipher* + yang mengadopsi cara kerja mode operasi CBC dapat dipresentasikan sebagai berikut :

$$Enkripsi \rightarrow Ci = (Pi + Ki) \bmod 256$$

Secara matematis *plaintext* dinotasikan dengan Pi, *ciphertext* dinotasikan dengan Ci dan kunci dinotasikan dengan Ki (Ki dibatasi sampai 10 karakter). Maka, algoritma enkripsi dengan *Vigenere Cipher* + adalah :

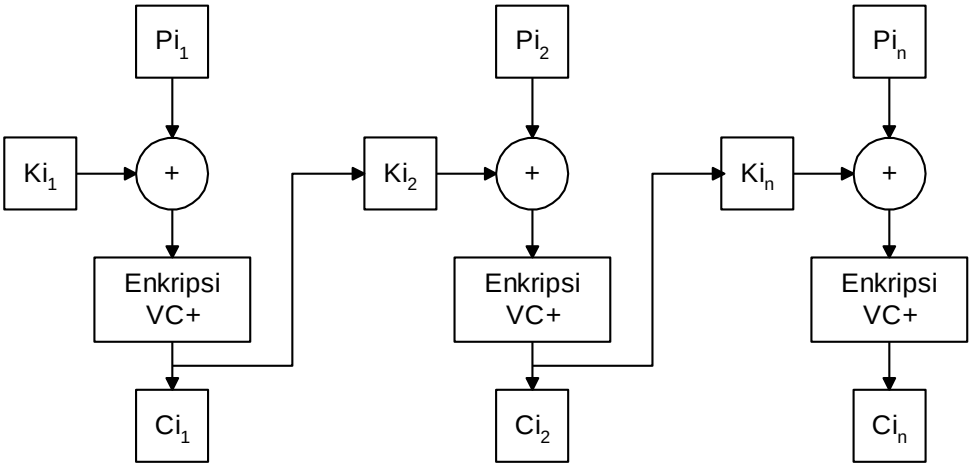
1. *Plaintext* (Pi) dikonversi ke dalam angka yang mewakili huruf, angka dan tanda baca lain yang terdapat

dalam 256 kode ASCII. Lakukan penggabungan penulisan *plaintext* dengan cara blok-blok pengkodean dan menuliskannya sesuai dengan jumlah karakter kunci yang di*input*-kan.

2. Kunci (Ki) dikonversi ke dalam angka yang mewakili huruf, angka dan tanda baca lain yang terdapat dalam 256 kode ASCII. Cek, apakah panjang kunci 0<length(Ki)≤10. Jika ya lanjutkan ke langkah 3, jika tidak maka akan ditampilkan pesan untuk *input* Ki lagi. *Input*an sebelumnya tidak disimpan.
3. Baca karakter Pi satu persatu dan konversi karakter ke dalam kode yang dipresentasikan dalam 256 kode ASCII, kemudian dilanjutkan dengan pembacaan karakter Ki pada posisi yang sama dengan Pi dan lakukan konversi ke dalam kode yang sesuai kemudian dijumlahkan dengan menggunakan rumus enkripsi pada *Vigenere Cipher* yaitu :

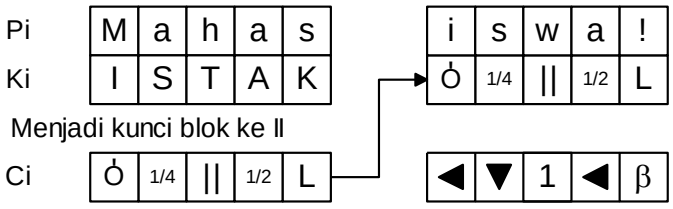
   Ci = (Pi + Ki) mod 256
4. Cek hasil penjumlahan, apabila hasil penjumlahan lebih besar dari 255 maka hasil penjumlahan dikurangi 256. Hasil enkripsi dari plaintext blok I dan kunci blok I menjadi kunci untuk blok II, demikian seterusnya sampai akhir dari panjang blok. Panjang blok ditentukan sesuai dengan jumlah karakter kunci yang dimasukkan.
5. Jika not EOF (End Of File) maka lakukan langkah 4, jika EOF maka cetak variabel yang menampung hasil enkripsi ke layar.

Gambar 1 akan memperlihatkan proses enlripsi dengan menggunakan algoritma *Vigenere Cipher* + (VC+) yang dimodifikasikan dengan mode operasi *chipper block chaining* (CBC).



Gambar 1. Enkripsi Mode CBC dengan Algoritma *Vigenere Cipher* +

Contoh :
Enkripsi :
Plaintext Mahasiswa!
Kunci ISTAK
Ciphertext ó¼‖½└◄▼1◄β
Langkah-langkah :



Setelah mengalami pengevaluasian, maka secara matematis dekripsi dengan algoritma *Vigenere Cipher* + yang mengadopsi cara kerja mode operasi CBC (*Cipher Block Chaining*) dapat dipresentasikan sebagai berikut :

Dekripsi → Pi = (Ci – Ki) mod 256

Secara matematis *ciphertext* dinotasikan dengan Ci, kunci dinotasikan dengan Ki dan *plaintext* dinotasikan dengan Pi. Maka, algoritma dekripsi dengan *Vigenere Cipher* adalah :

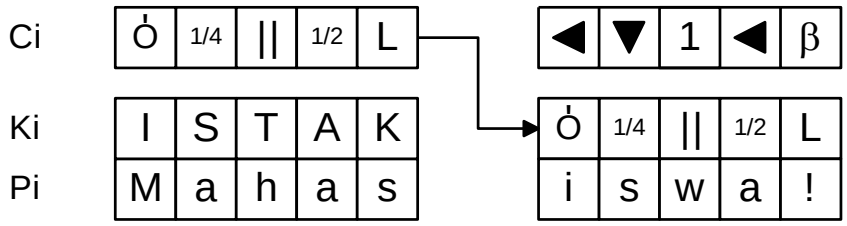
1. *Ciphertext* (Ci) dikonversi ke dalam angka yang mewakili huruf, angka dan tanda baca lain yang terdapat dalam 256 kode ASCII. Lakukan penggabungan penulisan *ciphertext* dengan cara blok-blok pengkodean dan menuliskannya sesuai dengan jumlah karakter kunci yang di*input*-kan.
2. Kunci (Ki) dikonversi ke dalam angka yang mewakili huruf, angka dan tanda baca lain yang terdapat dalam 256 kode ASCII. Cek, apakah panjang kunci 0<length(Ki)≤10. Jika ya lanjutkan ke langkah 3, jika tidak maka akan ditampilkan pesan untuk input Ki lagi. *Input*an sebelumnya tidak disimpan.
3. Baca karakter Ci satu persatu dan konversi karakter ke dalam kode yang dipresentasikan dalam 256 kode ASCII, kemudian dilanjutkan dengan pembacaan karakter Ki pada posisi yang sama dengan Ci dan lakukan konversi ke dalam kode yang sesuai kemudian dikurangkan dengan menggunakan rumus dekripsi pada *Vigenere Cipher* yaitu :

   Pi = (Ci – Ki) mod 256
4. Cek hasil pengurangan, apabila hasil pengurangan lebih kecil dari 0 maka hasil pengurangan ditambahkan 256. Hasil dekripsi dari ciphertext blok I dan kunci blok I menjadi kunci untuk blok II, demikian seterusnya sampai akhir dari panjang blok. Panjang blok ditentukan sesuai dengan jumlah karakter kunci yang dimasukkan.
5. Jika not EOF (End Of File) maka lakukan langkah 4, jika EOF maka cetak variabel yang menampung hasil dekripsi ke layar.

Contoh :
Dekripsi:

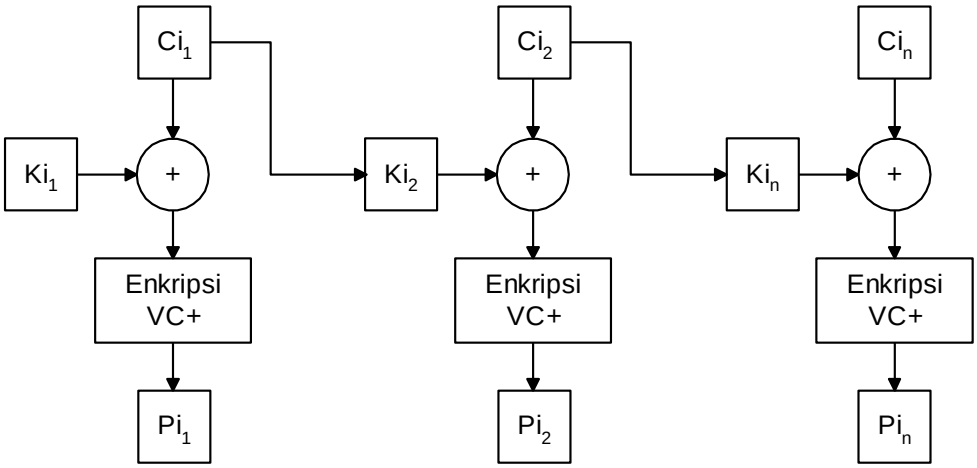
Ciphertext	ó¼‖½└◄▼1◄β
Kunci	ISTAK
Plaintext	Mahasiswa!

Langkah-langkah :



Gambar 2 akan memperlihatkan proses dekripsi dengan menggunakan algoritma *Vigenere Cipher* + (VC+) yang dimodifikasikan dengan mode operasi CBC.

Dengan mengadopsi cara kerja mode operasi CBC (*Cipher Block Chaining*), maka terdapat beberapa perbedaan cara kerja algoritma enkripsi-dekripsi *Vigenere Cipher* dengan algoritma enkripsi-dekripsi *Vigenere Cipher*+. Beberapa perbedaan tersebut tertuang dalam tabel 1 berikut.

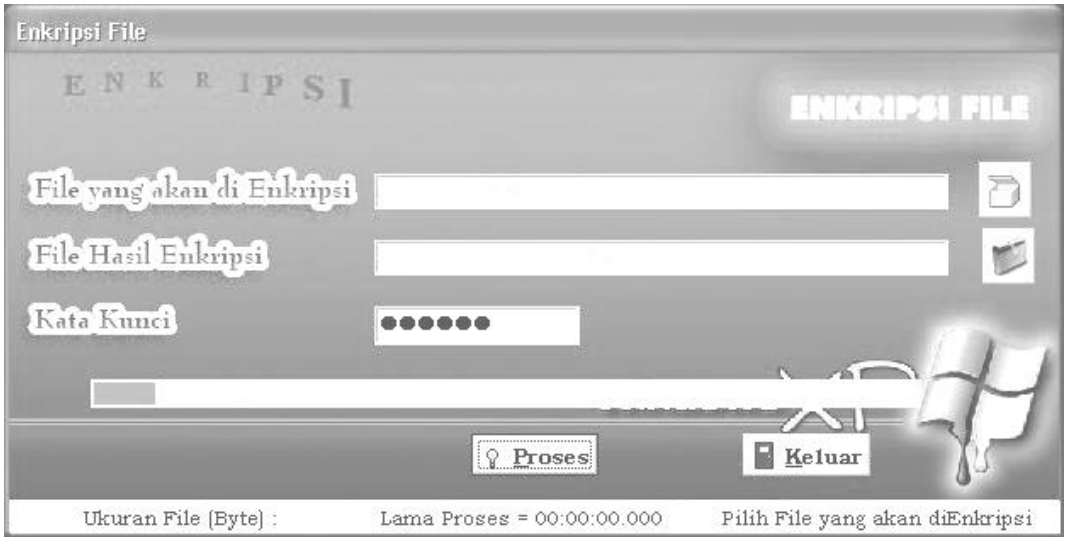


Gambar 2. Dekripsi Mode CBC dengan Algoritma *Vigenere Cipher* +

Tabel 1. Perbedaan Vigenere Cipher dengan Vigenere Cipher +

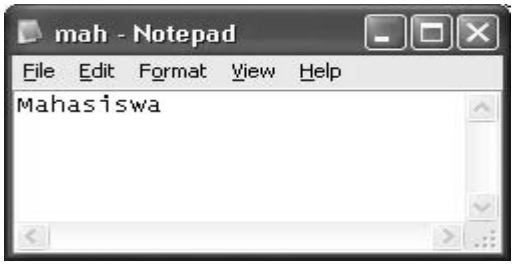
Vigenere Cipher	*Vigenere Cipher + / CBC*
1. Menggunakan 26 huruf alfabeth dalam bentuk huruf kecil.	Menggunakan 256 karakter ASCII.
2. Panjang kunci harus sama dengan panjang *plaintext* dan *ciphertext*.	Kunci dibatasi sampai 10 karakter.
3. Tidak menggunakan blok-blok pengkodean sehingga setiap satu huruf dalam *plaintext* dan *ciphertext* mendapat satu huruf kunci sampai akhir dari panjang *plaintext* dan *ciphertext*.	Menggunakan blok-blok pengkodean. Hasil dari enkripsi blok I menjadi kunci untuk blok II, demikian seterusnya sampai akhir dari panjang blok.

Berikut adalah dialog untuk proses enkripsi dengan memasukkan nama file yang akan dienkripsi beserta hasilnya dan kata kunci yang dimasukkan:



Gambar.3. Dialog proses Enkripsi

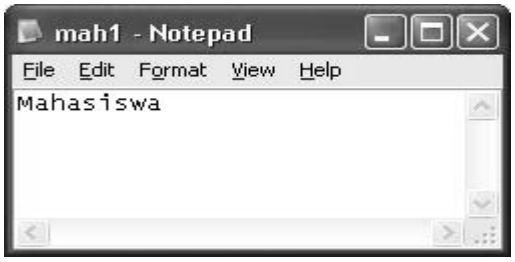
Berikut contoh file dengan kapasitas kecil (1 Kb) yang akan dienkripsi dengan kata kunci akprind, di buka dalam *Notepad* dengan nama mah.txt.



Gambar 4. Form Teks Mah.Txt

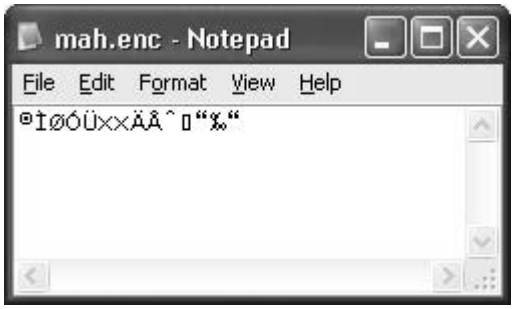
File teks dengan kapasitas yang kecil tersebut akan dienkripsi sebanyak dua kali dengan nama *File* yang berbeda. Kemudian dicek, apakah hasil dari kedua enkripsi tersebut sama atau tidak. Apabila sama, maka proses enkripsi sudah sempurna.

Di bawah ini adalah contoh teks dengan kapasitas kecil yang sama (1 KB) dengan teks diatas tetapi dengan nama *File* yang berbeda, di buka dalam *Notepad* dengan nama mah1.txt. Yang kemudian akan di-enkripsi dengan kata kunci yang sama.



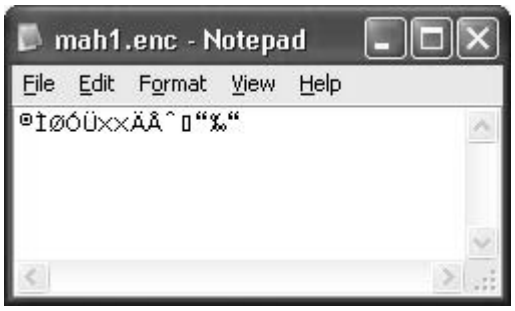
Gambar 5. Form Teks Mah1.Txt

Di bawah ini akan diperlihatkan hasil dari kedua proses enkripsi tersebut. *File* Mah.Enc adalah hasil Enkripsi dari *File* Mah.Txt, dimana besar file hasil enkripsi ini tetap 1 KB sama besar dengan file aslinya. Waktu yang digunakan untuk mengenkripsi file tersebut adalah 060 milidetik.



Gambar 6. Form Hasil Enkripsi Mah.Txt

Di bawah ini adalah File hasil Enkripsi dari *File* mah1.Txt dengan nama mah1.Enc dengan besar file 1 KB dan waktu pengenkripsian sama dengan file diatas.



Gambar 7. Form Hasil Enkripsi Mah1.Txt

Setelah mengalami pengujian, maka hasil enkripsi dari *File* teks sederhana tersebut sama. Sehingga dapat dikatakan bahwa proses enkripsi telah sempurna.

KESIMPULAN

Program Aplikasi ini dapat mengenkripsi jenis file gambar, audio dan video, serta teks.

File hasil enkripsi disimpan menggunakan nama yang sama dengan file asli tetapi ekstensinya menggunakan enc.

Pada saat proses enkripsi dan dekripsi dibutuhkan memori yang sangat besar yang mengakibatkan proses menjadi lama. Untuk itu penulis membatasi panjang kunci sampai dengan 10 karakter.

Algoritma *Vigenere Cipher* asli hanya menampung 26 huruf alfabeth dalam bentuk huruf kecil sedangkan tanda baca lain tidak dapat terbaca.

Sehingga perlu dilakukan suatu pengevaluasian yaitu dengan memperluas jangkauan 26 huruf alfabeth tersebut menjadi 256 karakter ASCII. Dari pengevaluasian tersebut maka algoritma *Vigenere Cipher* asli tersebut disebut dengan algoritma *Vigenere Cipher* +.

Panjang kunci mempengaruhi waktu untuk pengenkripsian dan pendekripsian *file*. Semakin panjang kata kunci yang digunakan maka semakin cepat waktu yang dibutuhkan.

DAFTAR PUSTAKA

Alfred J. Menezes, Paul C. van Oorschot, dan Scott A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, Oktober 1996.

Bruce Schneier, *Applied Cryptography*, Second Edition-Protocols, *Algorithms and Source Code in CI*. USA: John Wiley and Sons, Inc,1996, p. 3-4.

Bruce Schneier, "Crypto-Gram Newsletter", Counterpane Internet Security, Inc., September 30, 2001.

M. Agus J. Alam, *Belajar Sendiri Borland Delphi 6.0*, PT Elex Media Komputindo, Jakarta, 2001.

Corner:*Introduction to Cryptography*. Http://www.ssh.fi/tech/crypto/intro.html-SSH-Tech

What is Cryptography. http://www.hack.gr/users/dij/crypto/overview/whatis.html

Cryptography - Vigenere Cipher. http://Lor.Trincoll.Edu/~cpsc/cryptography/vigenere.html

The Vigenere Cipher http://www.math.ohiou.edu/~qvu/crypto/5.html -.

ECS 253 Winter 1999: Breaking a Vigenere Cipher http://www.csif.cs.ucdavis.edu/~cs253/Vigenere.html -

Terminology, http://www.hack.gr/users/dij/crypto/overview/terminology.htm

Metoda Enkripsi GOST http://bdg.centrin.net.id/~budskman/gost.htm -.

Block Chiper Modes , http://home.ecn.ab.ca/~jsavard/crypto/co0409.htm - .

What s Cipher Block Chaining Mode? Http://www.rsasecurity.com/rsalabs/fag/2-1-4-3.html