PERANGKAT LUNAK KRIPTOGRAFI METODE *MODULAR MULTIPLICATION-BASED BLOCK CHIPER*

Lis Intan Niar Giawa[1], Jeremia Siregar[2], Indra Oloan Nainggoilan[2]

[1)]Mahasiswa Teknik Informatika Fakultas Teknologi Industri, Institut Sains Dan Teknologi TD Pardede
[2), 3)]Dosen Teknik Informatika, Fakultas Teknologi Industri, Institut Sains Dan Teknologi TD Pardede
JL.DR.TD.Pardede No.8 Medan 20153, Sumatera Utara

[1]lisintanniar@gmail.com, jeremiasiregar@istp.ac.id[2] , indraoloan@istp.ac.id

ABSTRAK

Metode MMB ini dirancang agar dapat bekerja pada prosesor 32 bit. Kriptografi metode MMB ini menggunakan plaintext 128 bit dan algoritma iteratif. kriptografi MMB menggunakan 32 bit subblock text (x0, x1, x2, x3) dan 32 bit subblock kunci (k0, k1, k2, k3) serta sebuah fungsi non linier, yang dapat diterapkan enam kali bersama dengan fungsi XOR. Dalam perangkat ini melakukan beberapa proses (tahapan). Proses dimulai dari pembacaan dan pengkonversian data input (berupa plaintext, kunci atau ciphertext) ke Proses dilanjutkan dengan menampilkan tahapan-tahapan proses pembentukan kunci, enkripsi dan dekripsi. Proses diakhiri dengan menampilkan hasil proses yaitu subkey untuk proses pembentukan kunci, ciphertext untuk proses enkripsi dan plaintext untuk proses dekripsi. Perangkat lunak pembelajaran ini akan menampilkan tahapan-tahapan proses pembentukan kunci, enkripsi dan dekripsi. Perangkat lunak pembelajaran juga menyediakan fasilitas 'Simpan' untuk menyimpan proses pembentukan kunci, enkripsi dan dekripsi serta 'Load Data' untuk membuka kembali data yang telah disimpan sebelumnya.

Kata Kunci : ***kriptografi metode modular multiplication based-block chiper***

ABSTRACT

The MMB method is designed to work on 32 bit processors. The MMB cryptography method uses 128 bit plaintext and an iterative algorithm. MMB cryptography uses 32 bit text subblocks (x0, x1, x2, x3) and 32 bit key subblocks (k0, k1, k2, k3) as well as a non-linear function, which can be implemented six times along with the XOR function. In this device perform several processes (stages). The process starts from reading and converting the input data (in the form of plaintext, key or ciphertext) to the Process followed by displaying the stages of the process of forming keys, encryption and decryption. The process ends by displaying the results of the process, namely the subkey for the key formation process, ciphertext for the encryption process and plaintext for the decryption process. This learning software will display the stages of the process of forming keys, encryption and decryption. The learning software also provides a 'Save' facility to save the process of forming keys, encryption and decryption as well as 'Load Data' to reopen previously stored data.

Keywords: *cryptographic method of modular multiplication based-block cipher*

1. PENDAHULUAN

Dalam sebuah Kriptografi MMB ini dapat ditentukan oleh operasi perkalian modulo 2^{32} dengan factor konstan, yang memiliki tingkat sekuritas lebih tinggi bila dibandingkan dengan metode IDEA yang hanya menggunakan operasi perkalian modulo 2^{16} + 1. demikian Hal ini algoritma tersebut sangat cocok diimplementasikan pada prosesor 32 bit. Sebuah fungsi non linier, diterapkan enam kali bersama dengan fungsi XOR.

Kemudian dalam hal ini keamanann data salah satu hal penting dalam pertukaran data, khususnya pertukaran data didunia maya yang didalamnya terdapat banyak ancaman untuk proses itu sendiri. Bagi suatu organisasi keamanan data nilai sangat rahasia. Suatu hal yang dirasa perlu dan penting bagi pengguna adalah teknik dalam keamanan data, hal ini menunjukkan bahwa tingkat keamanan data harus ditingkatkan. Salah satu teknik dalam yang akan melindungi data ialah dengan menggunakan algoritma metode MMB yang merupakan metode sederhanatidak terlalu kompleks namun pesan yang disembunyikan cukup aman.

1.1 Batasan masalah

Perangkat lunak ini adalah Metode MMB yang dapat mengoperasikan modulo 2^{32}, namun bahasa pemrograman *Microsoft Visual Basic* hanya mendukung bilangan numerik maksimal 32 bit, sehingga diperlukan pembuatan fungsi-fungsi khusus untuk melakukan operasi perkalian modulo 2^{32} tersebut, Bagaimana menampilkan animasi prosedur kerja dari proses enkripsi, dekripsi dan fungsi f pada metode MMB.

1.2. Rumusan masalahnya

Perangkat lunak juga menyediakan fitur untuk pengaturan kecepatan proses, *Input* data berupa karakter (*string*) dengan panjang *plaintext*, *ciphertext* dan *key* adalah 16 karakter. Perangkat lunak tidak menampilkan tahap – tahap konversi *string* ke dalam biner.

1.3 Tujuan penelitian.

1. Untuk membuat suatu perangkat lunak yang dapat menyembunyikan dan melindungi keamanan data pada pesan teks.
2. Untuk mengamankam data pada pesan teks yang bersifat rahasia.

1.4. Manfaat penelitian.

untuk melindungi kerahasiaan data pada pesan teks.

1. Untuk menambah fasilitas pada keamanan data yang berupa rahasia.

2. LANDASAN TEORI

Dalam perkembangannya, kriptografi ini juga dapat mengindentifikasi dalam mengirim sebuah pesan dengan keaslian pesan pada sidik jari digital. Kriptografi disumbangkan pemikirannya oleh empat kelompok, yakni militer, korps diplomatik, *diarist*, dan orang yang sedang jatuh cintai. Di dalam organisasi militer, pesan-pesan yang telah di-*encode* secara tradisional diberikan kepada pekerja kode berupah rendah untuk selanjutnya dienkrip dan ditransmisikan. kemudian Tugas ini diusahakan agar tidak dapat melakukan spesialis yang elit, dan setelahnya Kendala tambahan telah menjadi kesulitan dalam peralihan yang cepat dari satu algoritma kriptografi ke algoritma lainnya

2.1. METODE MMB

Proses Pembentukkan Kunci.

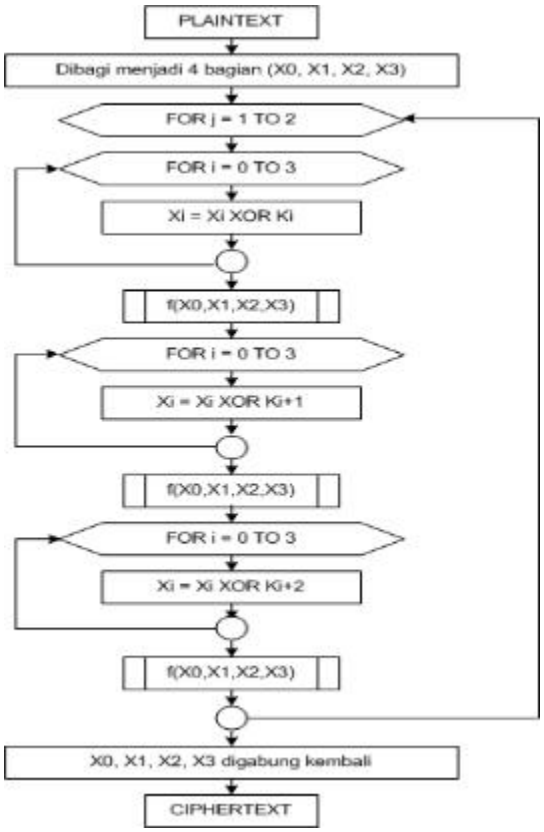
Metode MMB ini akan dipecah menjadi 4 buah sub kunci (subkey) dengan panjang masing-masing sub kunci adalah sebesar 32 bit.

Misalkan diketahui input kunci = ‘CRYPTOGRAPHY MMB’,

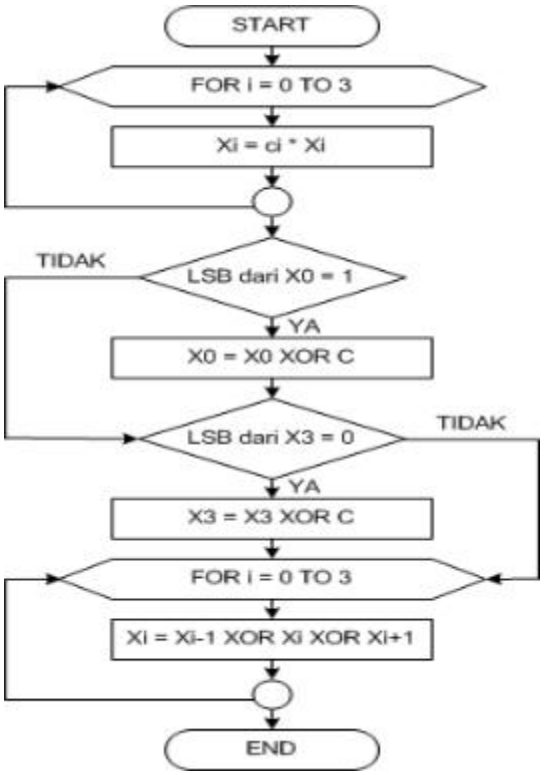
```
Kunci = CRYPTOGRAPHY MMB
Ubah ke bentuk biner =
01000011010100100101100101010000010
10100010011110100011101010010010000
01010100000100100001011001001000000
10011010100110101000010
Dipecah menjadi 4 buah sub kunci :
K(0)=0100001101010010010110010101000
00
K(1)=0101010001001111010001110101001
10
K(2)=0100000101010000010010000101101
01
K(3)=0010000001001101010011010100001
10
```

Enkripsi metode MMB

Proses enkripsi dari metode MMB ini memiliki *input* data *plaintext* 128 bit yang identik dengan 32 digit heksadesimal atau 16 karakter.



Gambar 2.6 flowchart Proses Enkripsi pada Metode MMB



(*Least Significant Bit*) dari $x_0 = 1$, maka

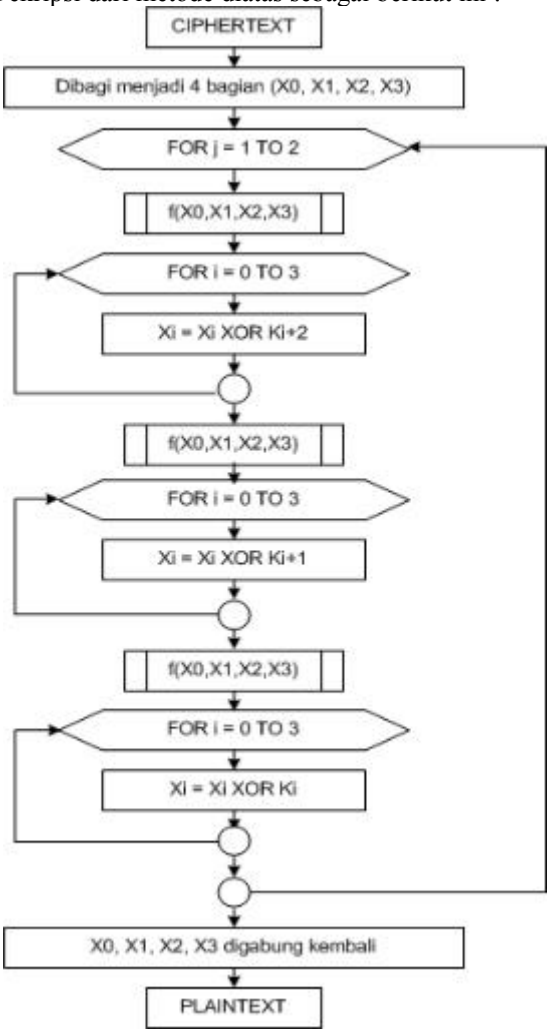
Gambar 2.7 Fungsi pada Proses Enkripsi Metode MMB

Operasi perkalian yang digunakan merupakan operasi perkalian modulo $2^{32} - 1$.

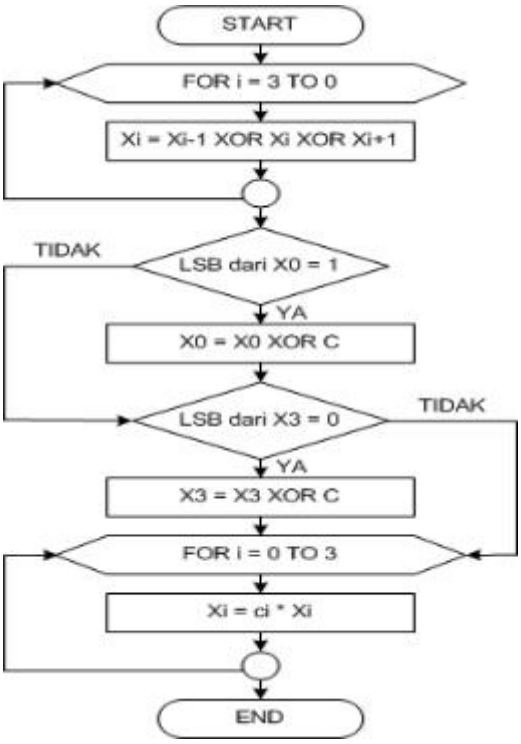
- $C = (2AAAAAAA)_{16}$
- $c_0 = (025F1CDB)_{16}$
- $c_1 = 2 * c_0$
- $c_2 = 2^3 * c_0$
- $c_3 = 2^7 * c_0$

1.2 dekripsi metode MMB.

Dekripsi dari metode diatas sebagai berikut ini :



Gambar 2.8 flowchart Proses Dekripsi pada Metode MMB



Gambar 2.9 fungsi f Proses Dekripsi Metode MMB

Sedangkan konstanta yang digunakan dapat dirincikan sebagai berikut :

- $C = (2AAAAAAA)_{16}$
- $c_0^{-1} = (0DAD4694)_{16}$
- $c_1^{-1} = 2^{-1} * c_0^{-1}$
- $c_2^{-1} = 2^{-3} * c_0^{-1}$
- $c_3^{-1} = 2^{-7} * c_0^{-1}$

1.3 Perbandingan Antara MMB dan IDEA

Beberapa perbedaan mendasar antara MMB dan IDEA dapat dijabarkan sebagai berikut :

MMB	IDEA
Panjang *plaintext* dan *ciphertext* adalah 128 bit.	Panjang *plaintext* dan *ciphertext* adalah 64 bit.
Kunci berjumlah 4 buah sub kunci	Kunci berjumlah 52 buah sub kunci.
Panjang setiap sub kunci adalah 32 bit.	Panjang setiap sub kunci adalah 16 bit.
Kunci yang digunakan sama.	Kunci pada dekripsi merupakan operasi kebalikan dari kunci enkripsi.
Proses enkripsi dan dekripsi memiliki o tingkat sekuritas lebih tinggi.	menggunakan operasi perkalian modulo $2^{16} + 1$.
Algoritma pada proses enkripsi berbeda dengan algoritma pada proses dekripsi. Algoritma proses dekripsi merupakan proses kebalikan dari proses enkripsi.	Algoritma pada proses enkripsi sama dengan algoritma pada proses dekripsi.
Proses enkripsi dan dekripsi menggunakan sebuah fungsi nonlinier f.	Tidak menggunakan fungsi nonlinier

Gambar tabel 3.1 perbandingan MMB dan IDEA

Sedangkan, beberapa kesamaan antara MMB dan IDEA adalah : terlalu sederhana, Menggunakan operasi perkalian modulo.

4. HASIL DAN PEMBAHASAN

Pada metode MMB, operasi aritmatika modular yang dipakai adalah operasi perkalian modulo $2^{32} –$ Contoh :

$(12457865 * 12456) \bmod (2^{32} – 1) = 155175166440 \bmod 4294967295 = 556343820$ perkalian ini menggunakan algoritma yang hampir sama dengan *inverse* perkalian pada metode IDEA. Perbedaannya nilai modulonya saja. Pada metode IDEA, digunakan aritmatika modulo $2^{16} + 1$ sedangkan pada metode MMB digunakan aritmatika modulo $2^{32} – 1$.

```
Inverse(A)
    n = 4294967295
    G0 ← n
    G1 ← A
    V0 ← 0
    V1 ← 1
    Ketika (G1 <> 0)
       Y ← Int(G0 / G1)
       G2 ← G0 - Y * G1
       G0 ← G1
       G1 ← G2
       V2 ← V0 - Y * V1
       V0 ← V1
       V1 ← V2
    End Ketika
    Jika (V0 >= 0) Maka
       Inverse ← V0
    Jika tidak,
       Inverse ← V0 + n
    End Jika
End Fungsi
```

Algoritma ini hanya diimplementasikan pada waktu mencari besar konstanta c_0 untuk proses dekripsi. Pada proses enkripsi c_0 yang digunakan bernilai sebesar $(025F1CDB)_{16}$, maka nilai c_0 yang digunakan pada proses dekripsi adalah sebesar $(0DAD4694)_{16}$.

2.9.1 Operasi XOR

Tabel 2.1 Aturan Operasi XOR

A	B	A ⊕ B
0	0	0

0	1	1
1	0	1
1	1	0

Nilai A jika di-XOR-kan dengan nilai B sebanyak dua kali maka akan didapatkan nilai A kembali.

$P \oplus K = C$; $C \oplus K = P$

Keterangan,

P = *Plaintext*

K = *Key*

C = *Ciphertext*

Berikut ini adalah contoh operasi XOR :

```
1101 0110 0001 0100
1000 0001 1110 0000 ⊕
                    0101
0111 1111 0100
```

Kemudian Perangkat lunak bantu pemahaman ini dirancang dengan menggunakan bahasa pemrograman *Microsoft Visual Basic 6.0* dan menggunakan *MDI Form* (*Multiple Document Interface Form*) sebagai *form* induk (*main form*) dan fasilitas *menu editor* untuk membuat dan mengatur tampilan menu *pull down*. Perangkat lunak bantu pemahaman ini dirancang dengan menggunakan beberapa *form*, antara lain :

1. *Form* '*Main*', yang dirancang dengan menggunakan *MDI Form* dan berfungsi sebagai *form induk* untuk menggabungkan semua *form* yang ada.
2. *Form* 'Teori'.
3. *Form* 'Proses Pembentukan Kunci', merupakan *child form* dari *form* '*Main*'.
4. *Form* 'Proses Enkripsi', merupakan *child form* dari *form* '*Main*'.
5. *Form* 'Proses Dekripsi', merupakan *child form* dari *form* '*Main*'.
6. *Form* 'Kecepatan Animasi'.

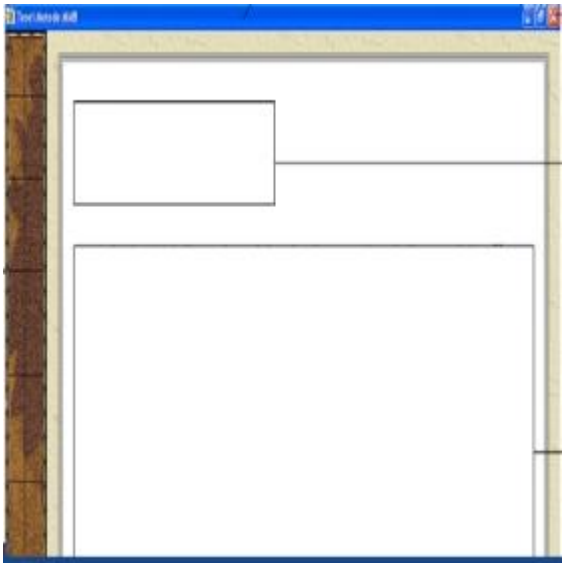
1.3.1 form main

Form ini merupakan *form* induk yang berfungsi untuk menggabungkan semua *form* yang ada pada perangkat lunak. Rancangan *form* '*Main*' ini dapat dilihat pada gambar 3.1 berikut ini :

Gambar 3.1 Rancangan Form 'Main'

1.3.2 Form Teori

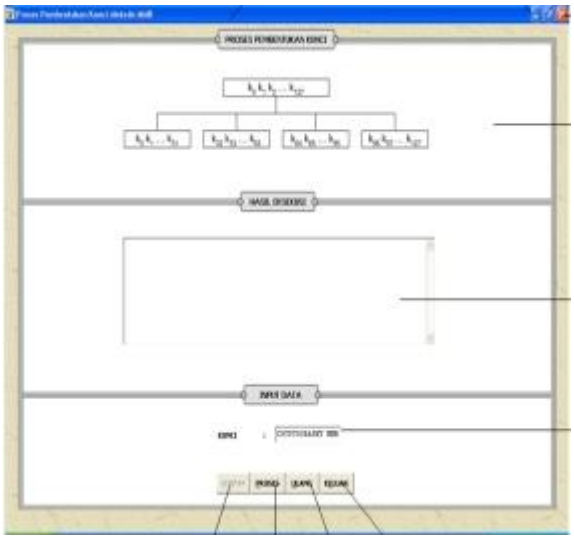
Form ini berfungsi untuk menampilkan teori-teori yang berhubungan dengan perangkat lunak. Rancangan *form* ini dapat dilihat pada gambar 3.3 berikut ini :



Gambar 3.2 Rancangan Form 'Teori'

1.4.3 Form Proses Pembentukan Kunci

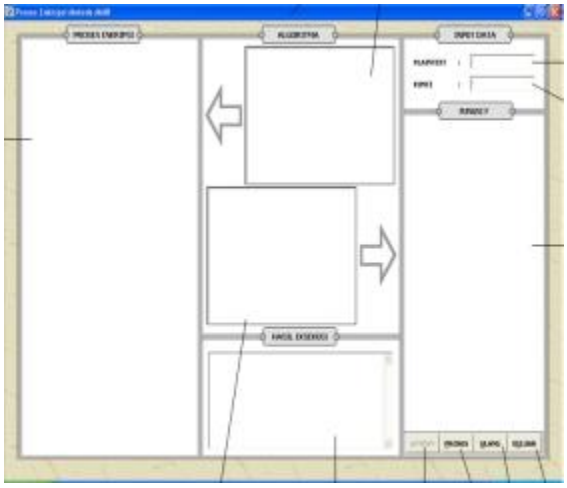
Form ini berfungsi untuk menampilkan proses pembentukan kunci dari metode MMB secara tahap demi tahap. Rancangan *form* ini dapat dilihat pada gambar 3.4 berikut ini :



Gambar 3.3 Rancangan Form 'Proses Pembentukan Kunci'

3.1.1.1 Form Proses Enkripsi

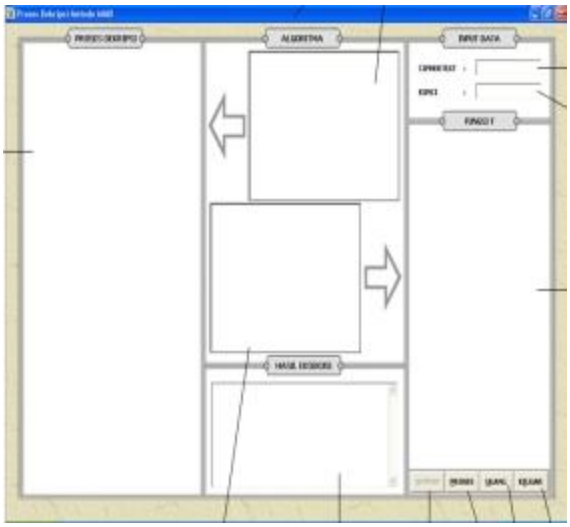
Form ini berfungsi untuk menampilkan proses enkripsi dari metode MMB secara tahap demi tahap. Rancangan *form* ini dapat dilihat pada gambar 3.5 berikut ini :



Gambar 3.5Rancangan Form 'Proses Enkripsi'

3.1.1.2 Form Proses Dekripsi

Form ini berfungsi untuk menampilkan proses dekripsi dari metode MMB secara tahap demi tahap. Rancangan *form* ini dapat dilihat pada gambar 3.6 berikut ini :



Gambar 3.4 Rancangan Form 'Proses Dekripsi'

1. Form Kecepatan Animasi

Form ini berfungsi untuk mengatur kecepatan animasi dari proses pembentukan kunci, enkripsi dan dekripsi. Rancangan *form* ini dapat dilihat pada gambar 3.7 berikut ini :

Gambar 3.6 Rancangan Form 'Kecepatan Animasi

5. KESIMPULAN

Setelah menyelesaikan tugas akhir (skripsi) yang berjudul 'Perancangan Perangkat Lunak Bantu Pemahaman Kriptografi dengan Metode MMB (*Modular Multiplication based Block cipher*' ini, penulis menarik beberapa kesimpulan sebagai berikut :

1. Dengan menggunakan perangkat lunak bantu pemahaman ini, maka *user* dapat menghemat waktu, dimana hasil eksekusi yang pernah diproses sebelumnya dapat disimpan ke dalam bentuk *text file,* sehingga dapat dibuka dan dipergunakan kembali apabila diperlukan.
2. Dengan adanya perangkat lunak bantu pemahaman ini, maka *user* dapat mempelajari metode kriptografi MMB secara tahap demi tahap. Hal ini didukung dengan adanya menu untuk mengatur kecepatan proses (animasi).

1. SARAN

Penulis ingin memberikan beberapa saran yang mungkin berguna untuk pengembangan lebih lanjut pada perancangan perangkat lunak bantu pemahaman kriptografi dengan metode MMB yaitu :

1. Perangkat lunak dapat dikembangkan agar dapat digabungkan dengan pembelajaran terhadap metode kriptografi yang lain.
2. Perangkat lunak dapat ditambahkan soal-soal latihan untuk mendukung proses pemahaman.
3. Perangkat lunak dapat ditambahkan fasilitas multimedia agar lebih menarik.

DAFTAR PUSTAKA

Ario Suryokusumo, ***Microsoft Visual Basic*** , Jakarata, PT. Elex Media Komputindo. 2001.

Bruce Schneier, ***Applied Crytography***, *Second Edition*, John Willey and Sons Inc, 6 Oktober 2005.

Djoko Pramono, **Mudah menguasai *Visual Basic*** , PT. Elex Media Komputindo. 2000.

Jennifer Seberpy, Jojef Pieprzyk, ***Cryptography : An Introduction to Computer Security***.Prentice Hall 1 September 1989.

Jusuf Kurniawan, Kriptografi, **Keamanan Internet dan Jaringan Komunikasi**, Penerbit Informatika Bandung: Informatika, 2004.