P-ISSN: 2548-9704
E-ISSN: 2686-0880

IMPLEMENTASI ALGORITMA KRIPTOGRAFI *MODULAR MULTIPLICATION – BASED BLOCK CIPHER* (MMB) PADA KEAMANAN DATA

Rio Wiranata[1)], Husnul Khair[2)], Suci Ramadani[3)]

[123]STMIK Kaputama
Jl. Veteran No. 4A-9A, Binjai, 20714, Sumatera Utara
Telp. 061-8828840, Fax. 88228845
E-mail : riowiranata8@gmail.com[1], husnul.khair@gmail.com[2], suci.ramdani23@gmail.com[3]

ABSTRACT

In everyday life, humans depend a lot on information technology. Then a variety of media began to emerge to access information and manage information so that many conveniences were then obtained to access information. Information security issues are very important in an information system for mutual security or personal security. For this reason, a security system is needed that can protect information for data security to anticipate such threats as cryptographic techniques. Cryptography Modular Multiplication Based Block Cipher (MMB) method can be used to maintain message security when messages are sent from one place to another. The application program that has been built only encrypts plaintext with the format doc, txt, xls, ppt. This research resulted in a program to secure secret messages in the form of files. The encrypted file can be re-expressed exactly the same as the original file and has not changed the contents of the file in the slightest.

Keywords:* *Cryptography, Modular Multiplication Based Block Cipher.

ABSTRAK

Dalam kehidupan sehari – hari manusia banyak bergantung pada teknologi informasi. Maka mulai bermunculan berbagai media untuk mengakses informasi dan mengelola informasi sehingga banyak kemudahan-kemudahan yang kemudian didapat untuk mengakses suatu informasi. masalah keamanan informasi menjadi hal yang sangat penting dalam suatu sistem informasi untuk keamanan bersama maupun keamanan pribadi. Untuk itu diperlukan suatu sistem keamanan yang dapat melindungi suatu informasi untuk pengamanan data untuk mengantisipasi ancaman tersebut seperti teknik kriptografi. Kriptografi metode *Modular Multiplication Based Block Cipher* (MMB) dapat digunakan untuk menjaga keamanan pesan saat pesan dikirim dari suatu tempat ke tempat yang lain. Program aplikasi yang telah dibangun hanya mengenkripsi *plaintext* dengan format doc, txt, xls, ppt. Penelitian ini menghasilkan suatu program untuk mengamankan pesan rahasia berbentuk file. File yang dienkrip dapat diungkapkan kembali sama persis dengan file aslinya dan tidak mengalami perubahan isi file sedikit pun.

Kata Kunci : Kriptografi, *Modular Multiplication Based Block Cipher*

P-ISSN: 2548-9704
E-ISSN: 2686-0880

1. PENDAHULUAN

Perkembangan teknologi dan informasi seperti sekarang ini kecepatan dalam memperoleh atau mengakses informasi sangatlah penting. Seiring dengan berkembangnya teknologi informasi akan mempermudah manusia dalam berkirim pesan maupun menerima pesan. Pesan yang disampaikan ada kalanya berupa pesan yang bersifat rahasia sehingga tidak semua pihak dapat melihat pesan tersebut. Namun, seiring dengan berkembangnya hal tersebut berkembang pula pelanggaran atau penyalah gunaan dalam keamanan data yang dikirim seperti dengan cara merusak, menyadap, merubah pesan tersebut untuk kepentingan pribadi. Kegiatan tersebut membuat informasi atau pesan yang bersifat rahasia dapat dilihat oleh orang yang tidak bertanggung jawab. Oleh karena itu, masalah keamanan informasi menjadi hal yang sangat penting dalam suatu sistem informasi untuk keamanan bersama maupun keamanan pribadi. Untuk itu diperlukan suatu sistem keamanan yang dapat melindungi suatu informasi.

Keamanan data merupakan 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 bernilai sangat rahasia. Suatu hal yang dirasa perlu dan penting bagi pengguna adalah teknik dalam keamanan data, hal ini menunjukkan bahwa tingkat keamanan data haruslah ditingkatkan.

Teknologi keamanan data terus berkembang mulai dari penyandian data sampai kepenyisipan data. Salah satu teknik yang dapat digunakan untuk mengamankan data adalah dengan menggunakan algoritma *Modular Multiplication based Block Chiper* (MMB) merupakan metode yang sederhana tidak terlalu kompleks namun pesan yang disembunyikan cukup aman.

Dalam hal ini penulis mendapat referensi berdasarkan beberapa judul jurnal yang berkaitan dengan judul yang dipilih oleh penulis, yaitu penelitian yang dilakukan oleh Lambok Harry dengan judul "**Analisa Dan Implementasi Algoritma Modular Multiplication Based Block Cipher Pada Aplikasi Billing Warnet".** Dan penelitian yang dilakukan oleh Yudi, Albert dengan judul **"Perancangan Perangkat Lunak Bantu Pemahaman Kriptografi Menggunakan Metode MMB (*Modular Multiplication – Based Block Cipher*)"**

Berdasarkan latar belakang diatas maka penulis mencoba untuk menggabungkan dua metode berbeda ke dalam sebuah aplikasi yang akan dibangun yang bertujuan untuk lebih dapat mengamankan pesan yang akan dikirim. Dan disini penulis tertarik untuk mengangkat skripsi dengan judul "**Implementasi Algoritma Kriptografi *Modular Multiplication Based Block Cipher* (MMB) Pada Keamanan Data."**

1.1 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka dapat disimpulkan rumusan masalah yaitu:

1. Dengan menerapkan metode *Modular Multiplication Based Block Cipher* (MMB) bagaimana membuat suatu perangkat lunak yang dapat menyembunyikan dan melindungi keamanan data pada pesan teks ?
2. Bagaimana membangun sebuah aplikasi agar tidak terdapat pengaruh yang signifikan pada data?
3. Bagaimana mengamankan data pada pesan teks yang bersifat rahasia?

1.2 Batasan Masalah

Adapun Batasan Masalah adalah sebagai berikut:

1. Algoritma yang digunakan adalah Algoritma *Modular Multiplication Based Block Cipher* (MMB).
2. Data yang di amankan adalah pesan teks dengan format.doc, txt, xls, ppt.
3. Bahasa pemrograman yang digunakan adalah VB.net 2010

P-ISSN: 2548-9704
E-ISSN: 2686-0880

1.3 Tujuan Penelitian.

Adapun Tujuan adalah sebagai berikut:

1. Untuk membuat suatu perangkat lunak yang dapat menyembunyikan dan melindungi keamanan data pada pesan teks.
2. Membangun sebuah aplikasi agar tidak terdapat pengaruh yang signifikan pada data.
3. Untuk mengamankan data pada pesan teks yang bersifat rahasia.

1.4 Manfaat Penelitian

Adapun manfaat adalah sebagai berikut :

1. Dapat digunakan untuk menjaga kerahasiaan data pada pesan teks.
2. Dapat menjadi salah satu fasilitas yang digunakan untuk mengamankan data yang bersifat rahasia.
3. Aplikasi ini juga mampu memberikan keamanan yang baik terhadap data.

2. METODOLOGI PENELITIAN

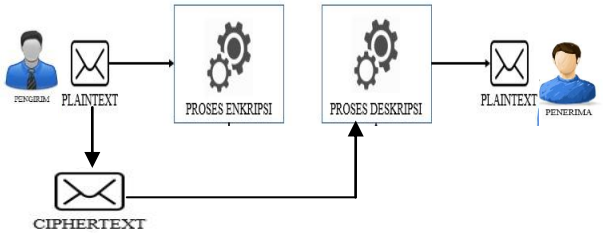
2.1 Pengertian Kriptografi

Menurut (M. Miftakul Amin, 2016) Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi sebuah kode yang tidak dapat dimengerti pihak lain.

Kriptografi menggunakan suatu algoritma (*cipher*) dan kunci (*key*). Cipher merupakan fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi data. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi. Tidak sekedar mengandalkan keamanannya pada kerahasian algoritma tetapi kerahasian kunci. *Plaintext* yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan *chipertext* yang berbeda pula. Artinya algoritma kriptografi yang digunakan boleh saja diketahui umum namun tanpa pengetahuan kunci, data tetap tidak terpecahkan.

2.1.1 Pengertian Metode *Modular Multiplication Based Block Cipher* (MMB)

Metode MMB menggunakan kunci sepanjang 128 *bit*. Proses pembentukan kunci pada metode MMB ini sangat sederhana. Kunci yang di-*input* hanya dibagi menjadi empat (4) buah sub *block* kunci dengan panjang masing-masing 32 *bit*. Desain arsitektur sistem pesan chat menggunakan kriptografi MMB yang dibangun. Lihat Gambar II.1



Gambar II.1 Desain Arsitektur Pesan Chat Kriptografi MMB

Kelebihan Metode *Modular Multiplication Based Block Cipher* (MMB) :

1. Pada MMB, Kunci yang digunakan pada proses enkripsi dan dekripsi sama. Sedangkan pada IDEA Kunci yang digunakan pada proses enkripsi dan dekripsi tidak sama. Kunci dekripsi merupakan operasi kebalikan dari kunci enkripsi
2. Pada MMB, Proses enkripsi dan dekripsi menggunakan operasi perkalian modulo $2^{32} - 1$ sehingga tingkat sekuritas lebih tinggi.Sedangkan IDEA, Proses enkripsi dan dekripsi menggunakan operasi perkalian modulo $2^{16} + 1$.
3. Pada MMB, Proses enkripsi dan dekripsi jauh lebih cepat daripada IDEA yaitu hanya terdiri dari 2 putaran saja. Sedangkan IDEA, Proses enkripsi dan dekripsi lebih panjang yaitu terdiri dari 8 putaran sehingga lebih memakan waktu.

P-ISSN: 2548-9704
E-ISSN: 2686-0880

2.2.1 Operasi XOR

Operasi *XOR* dalah singkatan dari *Exclusive OR* yang terdiri dari dua (2) masukan (*input*) dan satu (1) keluaran (*output*) logika. Gerbang *XOR* akan menghasilkan keluaran (output) logika satu (1)
jika semua masukan-masukannya (input) mempunyai nilai logika yang berbeda. Jika nilai logika *input*nya sama, maka akan memberikan hasil keluaran logika nol (0).

2.2.2 Enkripsi Metode MMB

Metode MMB menggunakan *plaintext* dan kunci dengan panjang 128 *bit*. Inti proses enkripsi dari metode MMB adalah sebagai berikut :

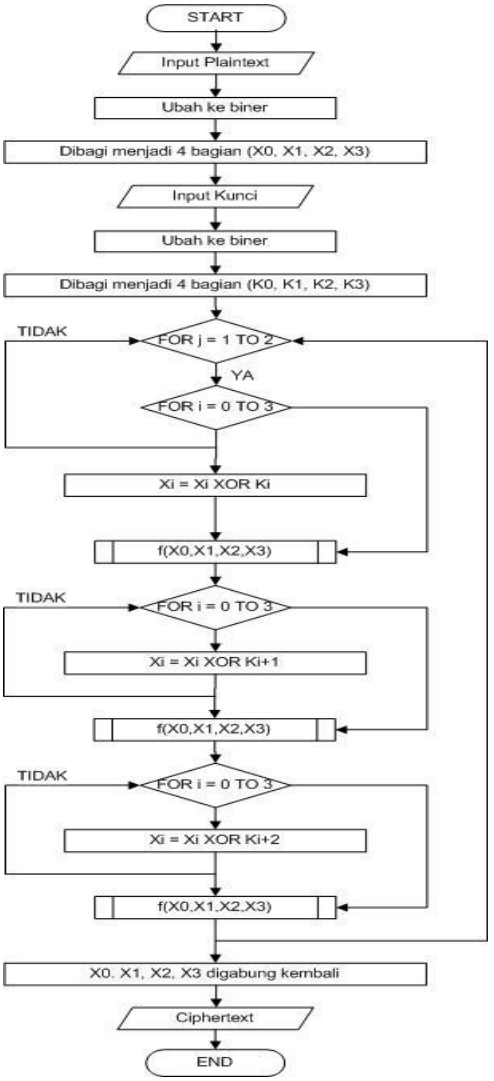
1. *Plaintext* dibagi menjadi empat (4) sub *block* yang sama besar (x0, x1, x2, x3).
2. Lakukan proses berikut ini sebanyak 2 kali :

for i = 0 to 3
xi = xi XOR ki
next i
f(x0,x1,x2,x3)
for i = 0 to 3
xi = xi XOR ki+1
next i

f(x0,x1,x2,x3)
for i = 0 to 3
xi = xi XOR ki+2
next i

f(x0,x1,x2,x3)

Proses enkripsi tersebut dapat ditunjukkan dalam bentuk bagan seperti Gambar II.2 berikut ini :



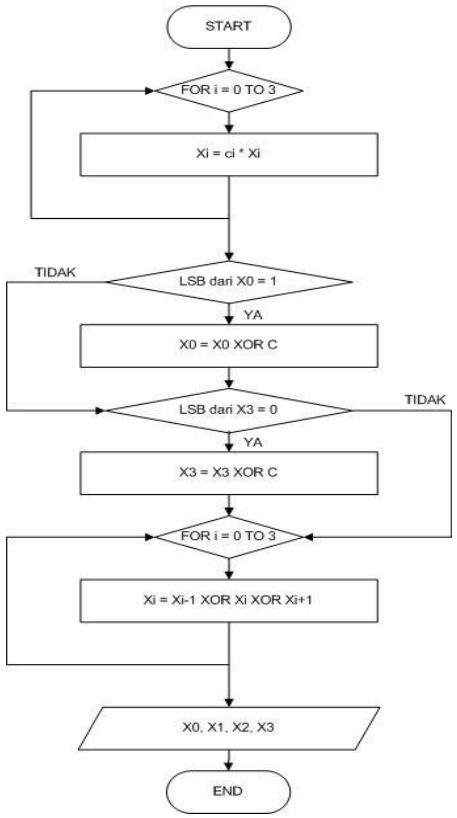
Gambar II.2 Flowchart Proses enkripsi pada metode MMB

Fungsi f yang digunakan memiliki 3 langkah yaitu :

For i = 0 to 3
Xi = ci * xi
Next i
Jika *Least Significant Bit (LSB)* dari x0 = 1, maka x0 = x0 *XOR* C.
Jika *LSB* dari x3 = 0, maka x3 = x3 *XOR* C.
for i = 0 to 3
xi = xi-1 XOR xi XOR xi+1
next i

Fungsi f diatas dapat digambarkan dalam bentuk bagan seperti Gambar II.3 berikut ini :

P-ISSN: 2548-9704
E-ISSN: 2686-0880



Gambar II.3 Flowchart Fungsi f pada operasi enkripsi metode MMB

Operasi perkalian yang digunakkan merupakan operasi perkalian. Sedangkan konstanta yang digunakan dapat di rincikan sebagai berikut :

- C = (2AAAAAAA)16
- c0 = (025F1CDB)16
- c1 = 2 * c0
- c2 = 23 * c0
- c3 = 27 * c0

2.2.3 Dekripsi Metode MMB

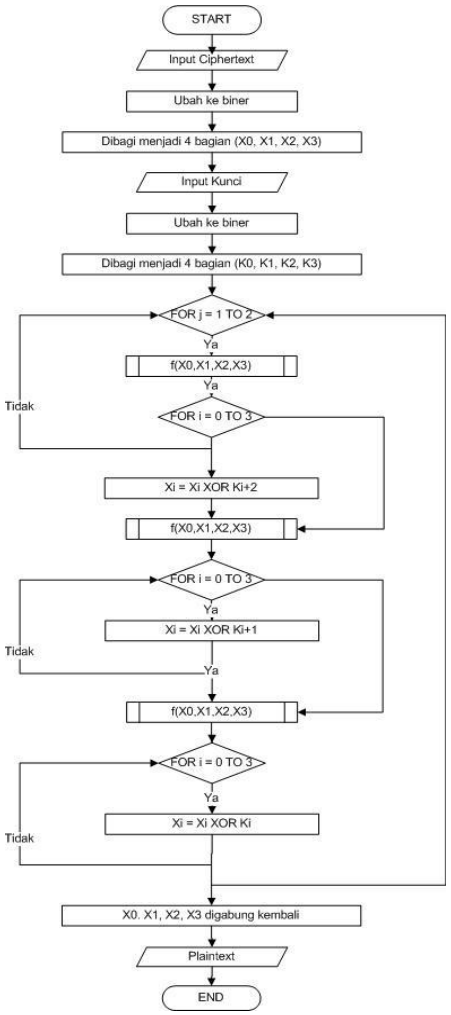
Algoritma yang digunakan pada proses dekripsi berbeda dengan proses enkripsi. Inti proses dekripsi dari metode MMB dapat dijabarkan seperti berikut :

1. *Ciphertext* dibagi menjadi empat (4) sub *block* yang sama besar (x0, x1, x2, x3).
2. Lakukan proses berikut ini sebanyak 2 kali :

f(x0,x1,x2,x3)
for i = 0 to 3
xi = xi XOR ki+2
next i
f(x0,x1,x2,x3)
for i = 0 to 3
xi = xi XOR ki+1
next i

f(x0,x1,x2,x3)
for i = 0 to 3
xi = xi XOR ki
next i

Proses dekripsi tersebut dapat ditunjukkan dalam bentuk bagan seperti Gambar II.4 berikut ini :



***Gambar II.4 Flowchart Proses dekripsi pada* metode MMB**

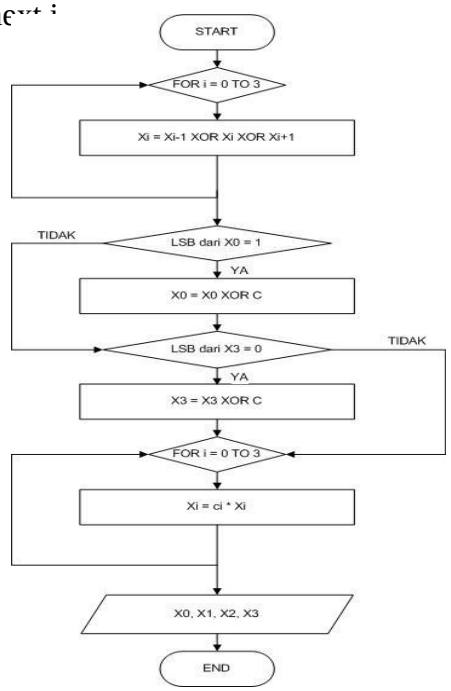
Fungsi f yang digunakan juga berbeda dan dapat dijabarkan seperti berikut :

for i = 3 to 0 step -1
xi = xi-1 XOR xi XOR xi+1
next i

Jika *Least Significant Bit (LSB)* dari x0 = 1, maka x0 = x0 *XOR* C.
Jika *LSB* dari x3 = 0, maka x3 = x3 *XOR* C.

P-ISSN: 2548-9704
E-ISSN: 2686-0880

for i = 0 to 3
xi = ci * xi
next i



Gambar II.5 Flowchart Fungsi f pada operasi dekripsi metode MMB

Operasi perkalian yang digunakkan merupakan operasi perkalian. Sedangkan konstanta yang digunakan dapat di rincikan sebagai berikut :

- C = (2AAAAAAA)16
- c0-1 = (0DAD4694)16
- c1-1 = 2-1 * c0-1
- c2-1 = 2-3 * c0-1
- c3-1 = 2-7 * c0-1

2.2.4 Perhitungan Matematis Manual Enkripsi–Dekripsi Metode MMB

Proses enkripsi dari metode MMB ini memiliki input data plaintext 128 bit yang identik dengan 32 digit heksadesimal atau 16 karakter. Proses enkripsi dari metode MMB dapat dilihat pada contoh tahapan proses enkripsinya berikut ini :

A. Pembentukan Knci
1. Masukkan Kunci (plaintext 128 bit, 32 digit heksadesimal atau 16 karakter).
2. Ubah ke bentuk biner.
3. Pecah teks biner menjadi 4 bagian.

B. Enkripsi
1. Masukkan pesan (plaintext 128 bit, 32 digit heksadesimal atau 16 karakter).
2. Ubah ke bentuk biner.
3. Pecah teks biner menjadi 4 bagian.
4. Algoritma inti proses MMB sebagai berikut :

a. Tahap 1 : Melakukan proses Exclusive OR (XOR) antara kunci (K) dengan pesan (X) untuk mencari hasil (Xa). Contoh Hitung XOR : 1 XOR 1 = 0 1 XOR 0 = 1 0 XOR 1 = 1 0 XOR 0 = 0

b. Tahap 2 : Perhitungan biner dengan rumus
Hitung Xb = C * Xa MOD ((2^32) - 1)
((2^32) – 1) = 4.294.967.295
Konversi ke biner = 11111111111111111111111111111111

c. Input Ca
Ca = 025F1CDB untuk menentukan Ca(0), Ca(1) ,Ca(2), Ca(3)
Konversi ke hasil biner
Hitung C(0) – C(3) :
Ca(0) :
Konversi “025F1CDB” ke hasil biner.
Ca(1) = 2*C(0)
To Bineri hasil Perkalian bineri.
Ca(2) : 2^3*C(0)
To Bineri hasil Perkalian bineri.
Ca(3) :

d. Tahap 3 (Mengambil digit terakhir bilangan biner yang identik yaitu 1 dan 0) :
Input Cb : 2AAAAAAA
Konversi ke hasil biner
(Dicari digit 1 dibelakang, didapat di X(1))
(Dicari digit 0 dibelakang, didapat di X(3))
LSB(Xb(1)) = 1 = 1 --> TRUE
Xc(1) = Xb(1) XOR Cb
LSB(Xc(3)) = 0 = 0 --> TRUE
Xc(3) = X(3) XOR Cb
Xc(0) = Xa(0) XOR Cb =10011000000000001110000000011010
Xc(2) = Xa(2) XOR Cb =10111101110111110111101111001001

P-ISSN: 2548-9704
E-ISSN: 2686-0880

e. Tahap 4 Triple XOR : untuk menentukan nilai Xd :
Xd(0) = Xc(3) XOR Xc(0) XOR Xc(1)
Xd(1) = Xc(0) XOR Xc(1) XOR Xc(2)
Xd(2) = Xc(1) XOR Xc(2) XOR Xc(3)
Xd(3) = Xc(2) XOR Xc(3) XOR Xc(0)

f. Tahap 5 Penggabungan X(0) -X(3)
Xd(0)=01110001000100111001000111101001
Xd(1)=00000011101011001000111011110110
Xd(2)=01101100100011000000101000111010
Xd(3)=01110010101111111001111100000001
Hasil : 01110001000100111001000111101001000000011101011001000111011110110011011001000110000001010001110100111001010111111100111110000000 1 And then konversikan biner ke ASCII

3. ANALISA DAN PEMBAHASAN

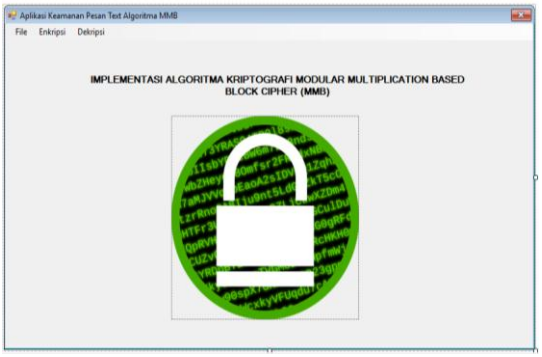
Program aplikasi implementasi algoritma kriptografi *modular multiplication based block cipher* (MMB) pada keamanan data dengan tujuan untuk menyembunyikan dan melindungi keamanan data yang dikirimkan ke user lain dengan cara mengamankan isi pesan tersebut dan membaca kembali teks tersebut agar pesan asli dapat dibaca, dalam hal ini user harus memiliki aplikasi ini.

Tampilan Layar Antar Muka (*Interface*)

Berikut ini adalah tampilan dan penjelasan dari form pada penerapan aplikasi implementasi algoritma kriptografi *modular multiplication based block cipher* (MMB).

1. Tampilan *Form* Utama

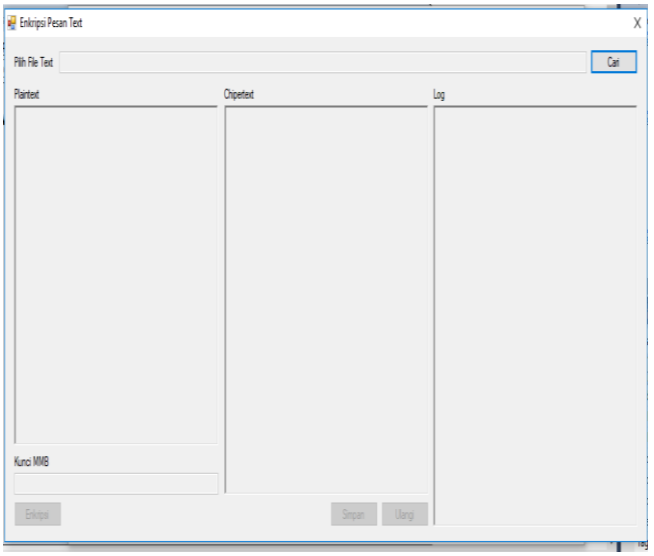
Ketika penerapan aplikasi implementasi algoritma kriptografi *modular multiplication based block cipher* (MMB). Dijalankan, maka tampilan akan terlihat seperti pada gambar III.1



Gambar III.1 Tampilan *Form* Awal

Tampilan *Form Encryption*

Tampilan form enkripsi merupakan halaman yang akan digunakan oleh pengirim pesan untuk mengenkrip file dengan mencari file dari media penyimpanan, kemudian memasukkan kunci pada kotak yang tersedia, dan mengklik tombol "*encrypt*" untuk mengenkrip pesan, setelah hasil enkrip keluar, maka tersimpan ke dalam media penyimpanan, seperti pada gambar III.2



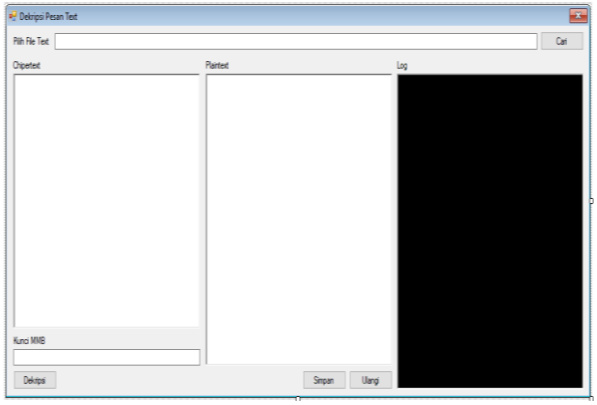
Gambar III.2 *Form Encryption*

P-ISSN: 2548-9704
E-ISSN: 2686-0880

Tampilan *Form Description*

Tampilan form baca pesan merupakan halaman yang akan digunakan oleh penerima pesan untuk membaca pesan yang telah diterima. Untuk membaca pesan yaitu dengan memasukkan file dari media penyimpanan dan tampillah pesan berupa hasil enkrip, selanjutnya jika ingin

membaca pesan asli, maka harus memasukkan kunci yang sama dengan pengirim pesan dan klik "*decrypt*" maka tampillah pesan asli, seperti pada gambar III.3

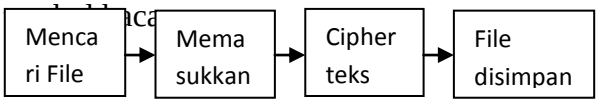


Gambar III.3 *Form Description*

3.1. Jalannya Uji Coba

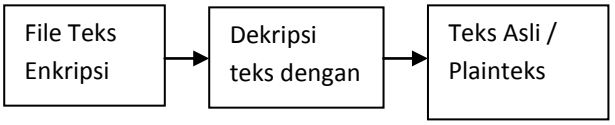
Uji coba terhadap program dilakukan dengan menggunakan *Visual Basic.Net* 2010 yang sudah ada. VB.Net 2010 digunakan untuk membuat aplikasi di dalam komputer sehingga aplikasi yang dibuat dapat dijalankan dan diuji coba langsung di dalam komputer.

Proses uji coba yang penulis lakukan meliputi proses penyisipan teks melalui sisip dan membaca pesan melalui



Gambar III.4 Langkah – Langkah Enkripsi

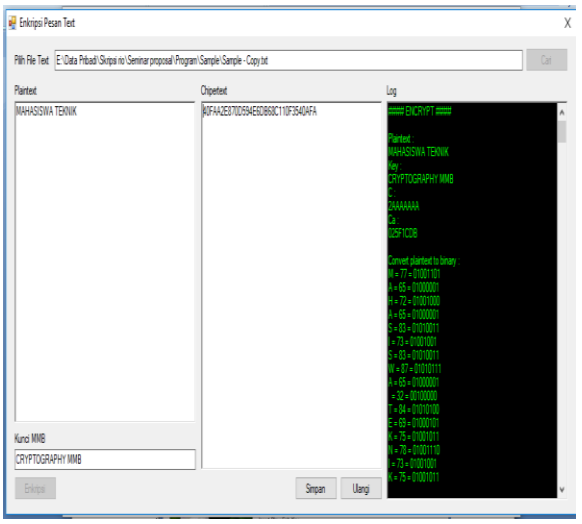
Untuk proses enkripsi, file teks dibuka dari media penyimpanan dan memasukkan kunci, selanjutnya hasil cipherteks akan ditampilkan dan disimpan kedalam media penyimpanan.



Gambar III.5 Langkah – Langkah Dekripsi

3.2 Uji Coba *Encryption*

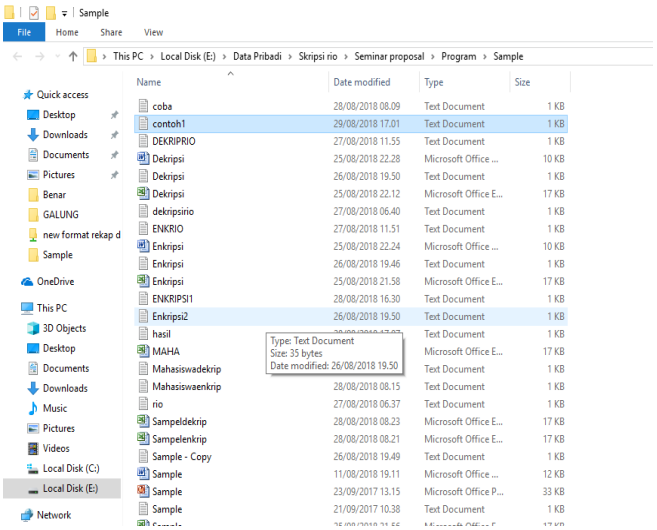
Pada tahap proses uji coba enkripsi pesan yang penulis lakukan adalah melakukan proses *enkripsi*. Untuk mengamankan file pesan dengan klik tombol cari, kemudian akan muncul isi pesan file teks pada kotak teks dan isi kunci pada kotak kunci, selanjutnya klik tombol *encrypt* dan tampillah hasil *enkrip* teks.



Gambar III.6 Uji Coba *Encryption*

Setelah itu klik tombol simpan untuk melakukan penyimpanan file yang telah dienkrip, dengan nama sesuai yang diinginkan dan kemudian akan muncul pesan,seperti terlihat pada gambar IV.7 .

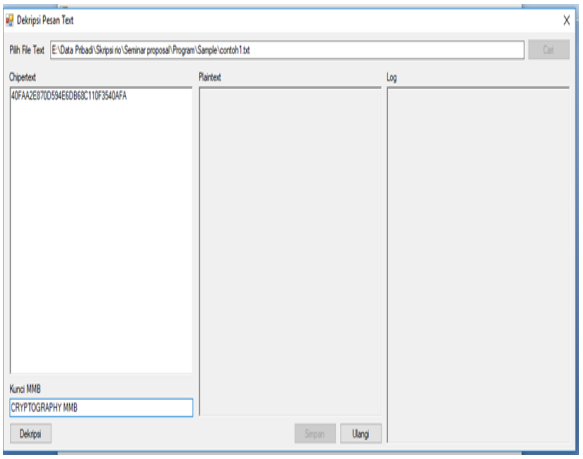
P-ISSN: 2548-9704
E-ISSN: 2686-0880



Gambar III.7 Penyimpanan Gambar

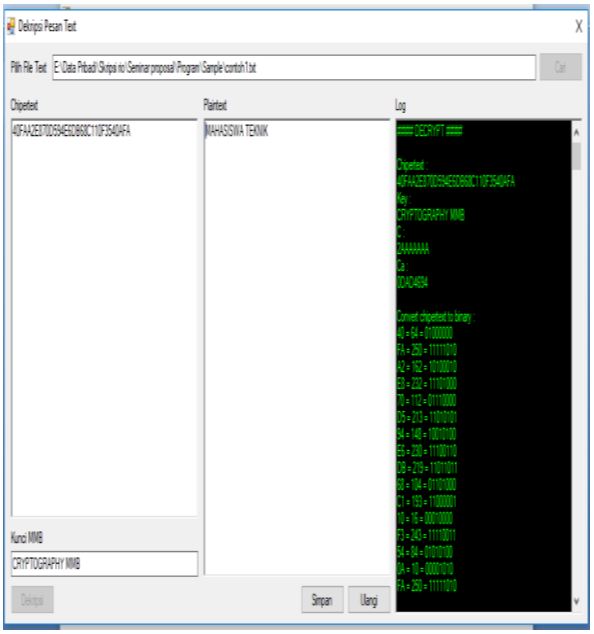
3.3. Uji Coba *Decription*

Proses uji coba selanjutnya adalah proses pembacaan pesan yang berada pada file. Penerima pesan klik tombol cari sebagai
pengambilan file yang telah dienkrip dan mengisi kunci yang sesuai pada saat proses mengenkrip file.



Gambar III.8 Uji Coba *Decription*

Setelah itu klik tombol decrypt untuk melakukan pembacaan teks pada gambar, seperti terlihat pada gambar III.9.



Gambar III.9 Hasil Pembacaan Teks

3.4. Hasil Uji Coba

Berdasarkan rangkaian perencanaan dan uji coba setiap form yang ada, penulis merasa aplikasi program berjalan sesuai dengan perenacanaan. Program dapat mengenkrip file , kemudian dapat membaca file menjadi file asli pada penerima pesan tersebut. Untuk lebih jelasnya terlihat pada tabel III. 1 dan tabel III. 2 berikut:

Tabel III.1 Uji Coba *Encryption*

No	Plain text	Kunci	Ciphertext	Keterangan
1.	MAHASISWA TEKNIK	CRYPTOGRAPHY MMB	40FAA2E870D594E6DB68C110F3540AFA	Berhasil di jalankan
2.	Saya Mahasiswa KAPUTAMA	STMIK KAPUTAMA22	8E33B9F7A2851AE0E7A1EA489EDBE89F130D5E6BBCBD9385BDB77559FD0108015E149130D5B81DF4DFCDB71D4FF143FF	Berhasil di jalankan
3.	Hello World 123441241	TEKNIK KOMPUTER	CA8E847B64D5931F9BB21784A4D587C876AF041EC21D0C87BA7D9B7D77	Berhasil di jalankan

P-ISSN: 2548-9704
E-ISSN: 2686-0880

			241C5A	
4.	MAHASISWA KAPUTAMA	KAPUTAMA BINJAI1	3D5C2C0031B50588692FB68B2E3D84616FBCA8AE2A4321E14F1A293DB27C433B	Berhasil di jalankan

Tabel III.2 Uji Coba *Description*

No	Ciphertext	Kunci	Plaintext	Keterangan
1.	40FAA2E870D594E6DB68C110F3540AFA	CRYPTOGRAPHY MMB	MAHASISWA TEKNIK	Berhasil di jalankan
2.	8E33B9F7A2851AE0E7A1EA489EDBE89F130D5E6BBCBD9385BDB77559FD0108015E149130D5B81DF4DFCDB71D4FF143FF	STMIK KAPUTAMA 22	Saya Mahasiswa Kaputama	Berhasil di jalankan
3.	CA8E847B64D5931F9BB21784A4D587C876AF041EC21D0C87BA7D9B7D77241C5A	TEKNIK KOMPUTER	HelloWorld 123441241	Berhasil di jalankan
4.	3D5C2C0031B50588692FB68B2E3D84616FBCA8AE2A4321E14F1A293DB27C433B	KAPUTAMA BINJAI1	MAHASISWA KAPUTAMA	Berhasil di jalankan

4. KESIMPULAN

Dari implementasi metode kriptografi *Modular Multiplication-based Block cipher (*MMB*)* pada keamanan data yang dilakukan pada penelitian ini, maka dapat diambil kesimpulan sebagai berikut :

1. Program aplikasi yang telah dibangun hanya mengenkripsi *plaintext* dengan format doc, txt, xls, ppt.
2. Kata kunci dan panjang kunci dibuat dinamis sehingga pengirim pesan dapat merubah kata kunci sesuai dengan keinginan mereka.
3. Ukuran panjang teks (total karakter) tidak berpengaruh (tidak ada batasan) terhadap algoritma MMB, jadi dengan kata lain tidak ada masalah untuk ukuran panjang teks pesan.

5. SARAN

Sistem yang penulis telah kembangkan belumlah sempurna seperti yang diharapkan dikarenakan keterbatasan pengetahuan dan waktu. Adapun saran penulis untuk pengembangan sistem ini adalah sebagai berikut :

1. Aplikasi ini masih belum sempurna dalam hal implementasi, baik dalam segi tampilan program maupun fasilitas dalam program.
2. Aplikasi ini masih perlu dikembangkan lagi supaya dapat mengamankan data pada berbagai format media digital sebagai media penampung dan pesan yang diamankan tidak hanya berbentuk doc, txt, xls, ppt, masih ada beberapa media yang dapat diamankan.
3. Perlu dilakukan penelitian lebih lanjut agar file yang telah di *enkripsi* ini bisa tahan terhadap proses konversi format ke dalam ke dalam format lainnya.
4. Untuk kedepannya dapat memperbaiki atau mengembangkan program yang dibuat misalnya menggunakan metode yang lebih efisien, mengubah keamanan datanya dengan teknik yang lebih canggih lagi, mengenkripsi pesan yang dirahasiakan.
5. Implementasi perancangan sistem dapat di uji coba menggunakan bahasa pemograman visual selain, VB.Net 2010 misalnya: Delphhi 7.0, Visual C++, C# dan sebagainya dengan tambahan basis-data.

DAFTAR PUSTAKA

[1]. Harry. 2013. *Analisa Dan Implementasi Algoritma Modular Multiplication Based Block Chiper Pada Aplikasi Billing Warnet*. Pelita Informatika Budi Darma .Volume III, Maret 2013, ISSN 2301 – 9425

[2] Larry, 2012. *Jurus Kilat Mahir Visual Basic*. Dunia Komputer, Jakarta Timur.

P-ISSN: 2548-9704
E-ISSN: 2686-0880

[3] Miftakul Amin, 2016. *Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Web.* Jurnal Pseudocode.Volume III, No. 2, September 2016, ISSN 2355-5920

[4] Sugiarti, Yuni. 2013. *Analisis dan Perancangan UML (Unified Modeling Language) Generated VB.6*. Graha Ilmu, Yogyakarta

[5] Yatini B, 2010. *Flowchart, Algoritma, dan Pemrograman menggunakan Bahasa C++ Builder.* Graha Ilmu ,Yogyakarta.

[6] Yudi, Albert. Perancangan Perangkat Lunak Bantu Pemahaman Kriptografi Menggunakan Metode MMB (*Modular Multiplication – Based Block Chiper*) STMIK IBBI, ISSN 2339 – 1766