PENGAMANAN DATA TEKS MENGGUNAKAN ALGORITMA MODULAR MULTIPLICATION BASED BLOCK CHIPER

H Khair [1)], J D M Saragih [2)], A M H Pardede [3*)]

[1]Teknik Informatika, STMIK Kaputama
E-mail: husnul.khair@gmail.com[1)]
[2]Teknik Informatika, STMIK Kaputama
E-mail: jhondarwis75@gmail.com[2)]
[3]Sistem Informasi, STMIK Kaputama
E-mail: akimmhp@live.com[3)]

**Penulis Korespondensi*

Abstract – Utilization of Information and Communication Technology (ICT) is currently a basic necessity for almost all inhabitants of this earth, one of the uses of ICT through the internet network is a way of sending text messages via email, social media, or other means of communication. The messages sent from sender to recipient are sometimes in the form of messages that are confidential in nature so that not all parties can see the message. However, when there is a violation or misuse in the security of the data sent, such as by destroying, tapping, changing the message for the purposes of the perpetrator's interests. This action can make information or messages that are confidential can be seen by people who are not responsible. In dealing with this data security problem, it can be done by securing data techniques using the Modular Multiplication based Block Chipper (MMB) algorithm, which is a simple method that is not too complex but the hidden messages are quite safe. In the implementation of the program, tests have been carried out on various texts in doc, txt, xls, and ppt formats, and it has been proven that all previously encrypted text can be re-decrypted.

***Keywords**: Security, Cryptography, MMB, Text*

Abstrak – Pemanfaatan Teknologi Informasi dan Komunikasi (TIK) saat ini menjadi kebutuhan pokok bagi hampir seluruh penduduk bumi ini, salah satu pemanfaatan TIK melalui jaringan internet adalah cara pengiriman pesan teks melalui email, sosial media, atau alat komunikasi lainnya. Pesan yang disampaikan dari pengirim ke penerima ada kalanya berupa pesan yang bersifat rahasia sehingga tidak semua pihak dapat melihat pesan tersebut. Namun, seiring terjadi pelanggaran atau penyalah gunaan dalam keamanan data yang dikirim seperti dengan cara merusak, menyadap, merubah pesan tersebut untuk tujuan kepentingan si pelaku. Tindakan tersebut dapat membuat informasi atau pesan yang bersifat rahasia dapat dilihat oleh orang yang tidak bertanggung jawab. Dalam menangani masalah keaman data ini, dapat dilakukan dengan teknik mengamankan data dengan menggunakan algoritma

Diterima <01092020>, Revisi <18012021>, Diterima untuk publikasi <27012021>.

Modular Multiplication based Block Chiper (MMB), yang merupakan metode yang sederhana tidak terlalu kompleks namun pesan yang disembunyikan cukup aman. Pada Implementasi program yang dilakukan telah dilakukan pengujian pada berbagai teks dengan format doc, txt, xls, dan ppt, dan telah berbukti dapat di dekrip kembali semua teks yang dienkrip sebleumnya.

Kata Kunci: *Keamanan, Kriptografi, MMB, Teks.*

PENDAHULUAN

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 [1].

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[2].

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 [3]. Keuntungan utama dari cipher yang diberikan adalah kemudahan implementasi dan kemungkinan enkripsi probabilistik. Ini berarti bahwa enkripsi teks akan melakukannya berbeda ketika kuncinya sama dan datanya sama. Jadi, kekuatannya enkripsi ditingkatkan. Selain itu, ukuran pesan yang disandikan sulit diprediksi [4].

Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat dirumuskan masalah dalam penelitian ini adalah bagaimana menerapkan metode *Modular Multiplication Based Block Cipher* (MMB) untuk melindungi keamanan data pada pesan teks yang bersifat rahasia, sehingga file teks tersebut tidak dapat dipecahkan

Tujuan Penelitian

Adapun tujuan dari penelitan ini adalah :

1. Untuk menerapkan kemanan file teks menggunakan metode *Modular Multiplication Based Block Cipher*
2. Merancang sebuah aplikasi yang dapat mengaman kan file teks yang bersifat rahasi.

Urgensi (Keutamaan) Penelitian

Penelitian ini sangat penting dilakukan, karena teknologi saat ini menggunakan cara pengiriman pesan atau file teks rahasia melalui internet sangat memungkinkan disadap oleh orang yang tidak bertanggung jawab, sehingga perlu dialukan analisa dan rancangan aplikasi keamanan file teks.

Dengan adanya penelitian ini diharapkan dapat memberikan kenyaman bagi pemilik pesan teks dalam melakukan pengiriman atau penyampaian pesan rahasia yang dimiliki dapat dihindari.

TINJAUAN PUSTAKA

Kriptografi menggunakan suatu algoritma (*chiper*) dan kunci (*key*). Chiper merupakan fungsi matematika yang digunakan untuk mengenkripsi dan

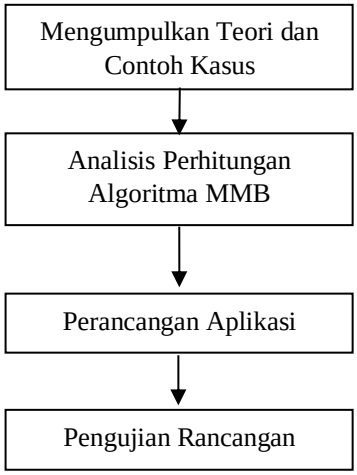
mendekripsi data. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi. Tidak sekedar mengandalkan keamanannya pada kerahasian algoritma tetapi kerahasian kunci [4]. Yang dimana pada kriptografi diperlukan untuk mengenkripsi blok teks $B = q1, q2,\ldots, qn$, yang memiliki n simbol ukuran b-bit masing-masing dengan kunci rahasia [5]. 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.

Jika teks biasa (X) atau kunci (Y) atau keduanya nol, maka output pengali adalah nol dan input bukan nol dapat menghasilkan output 216 yang juga diartikan sebagai nol. Ini menghasilkan output yang salah selama proses dekripsi [6], maka nol harus dideteksi dan diproses secara terpisah [6],Jika MMB memiliki 7 putaran itu masih rentan terhadap serangan yang berbeda [7]. Adapun kelebihan Metode Modular Multiplication Based Block Cipher (MMB) [8] :

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.

METODE PENELITIAN

Adapun langkah – langkah yang dilakukan dalam menyelesaikan masalah Analisis Dan Perancangan Pengaman Data Teks Menggunakan Algoritma *Modular Multiplication Based Block* Chiper, , terdiri dari beberapa tahapan seperti gambar 1 berikut:



Gambar 1. Kerangka Kerja Sistem

Berikut adalah penjelasan dari kerangka kerja sistem:

1. Mengumpulkan Teori dan Contoh – Contoh Kasus; Dalam hal ini dilakukan mengumpulkan teori-teori yang berhubungan dengan masalah teknik kriptografi, algoritma MMB. Teori-teori ini dikumpulkan dari beberapa sumber seperti jurnal-jurnal, buku-buku di perpustakaan, artikel-artikel di internet serta refrensi dari tugas akhir mahasiswa lain yang berhubungan dengan masalah yang dihadapi.
2. Analisa Perhitungan Algoritma MMB; Setelah teori-teori dan contoh kasus penunjang cukup, langkah

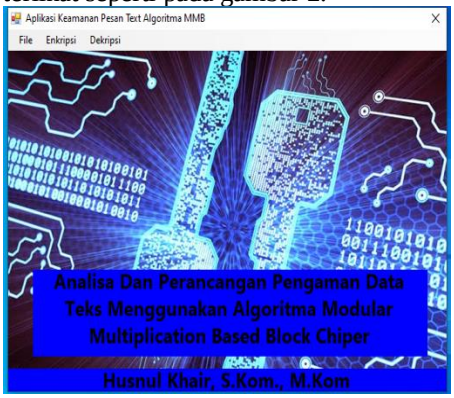
selanjutnya melakukan analisis perhitungan aloritma MMB, bagian ini dilakukan untuk pendalamam pemahaman cara kerja algoritma sesuai dengan tahapan-tahapanya.

3. Perancangan Aplikasi; Perancangan terhadap program dimelakukan dengan menggunakan teknik keamanan data pada pesan teks, dimana teknik yang digunakan adalah algoritma MMB. Langkah pertama dalam perancangan program ini adalah merancang proses kerja sistem menggunakan sebuah bagan alir (flowchart) yang menjelaskan secara rinci proses-proses yang akan dilakukan program dalam keamanan data pada pesan teks.
4. Pengujian Rancangan; Pada tahap akhir ini dilakukan serangkaian pengujian terhadap rancangan program yang dihasilkan. Pengujian – pengujian ini dilakukan untuk mencari kesalahan – kesalahan (*error*) pada rancangan program dan melakukan perbaikan – perbaikan yang dibutuhkan.

HASIL DAN PEMBAHASAN

Tampilan *Form* Utama

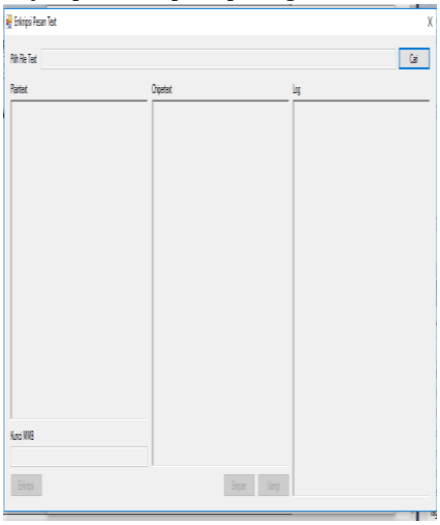
Ketika penerapan aplikasi implementasi algoritma kriptografi *modular multiplication based block cipher* (MMB). Dijalankan, maka tampilan akan terlihat seperti pada gambar 2.



Gambar 2. Tampilan *Form* Awal

Tampilan *Form Encryption*

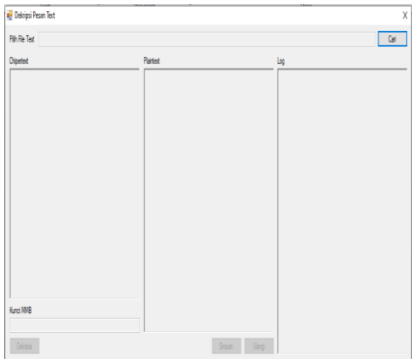
Tampilan form enkripsi merupakan halaman yang akan digunakan oleh pengirim pesan untuk mengenkrip file dengan mencari file dari media penyimpanan, kemudian memasukkan kunci pada kotak yang tersedia, dan mengklik tombol "*encrypt*" untuk mengenkrip pesan, setelah hasil enkrip keluar, maka tersimpan ke dalam media penyimpanan, seperti pada gambar 3.



Gambar 3. *Form Encryption*

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 4.



Gambar 4. *Form Description*

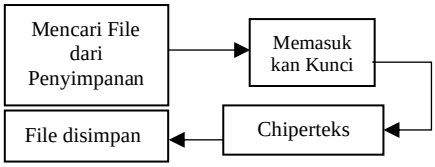
Implementasi

Implementasi merupakan kelanjutan dari kegiatan perancangan sistem. Tahap ini merupakan tahap meletakkan sistem supaya siap untuk di operasikan dan dapat dipandang sebagai usaha untuk mewujudkan sistem yang telah di rancang. Langkah-langkah dalam tahap implementasi ini adalah urutan kegiatan awal sampai akhir yang harus dilakukan dalam mewujudkan sistem yang telah di rancang. Setelah perancangan sistem selesai, maka menampilkan hasil dari sistem yang telah dirancang berikut akan dibahas tentang implementasi uji coba aplikasi yang dibangun.

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 lakukan meliputi proses penyisipan teks melalui sisip dan membaca pesan melalui tobol baca.



Gambar 5. Langkah – Langkah Enkripsi

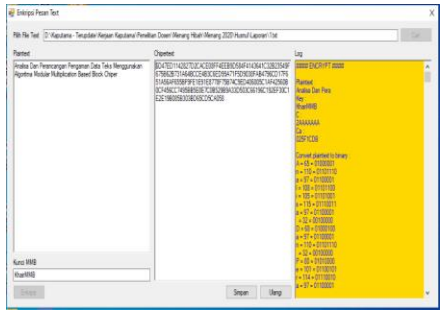
Untuk proses enkripsi, file teks dibuka dari media penyimpanan dan memasukkan kunci, selanjutnya hasil chiperteks akan ditampilkan dan disimpan kedalam media penyimpanan.

Gambar 6. Langkah – Langkah Deskripsi

Teks enkripsi di deskripsi dengan algoritma MMB, kemudian teks dibaca menggunakan metode MMB yang sebelumnya akan dibaca kunci sebagai tanda pengenal, selanjutnya teks asli (plainteks) akan tampil sebagai hasil.

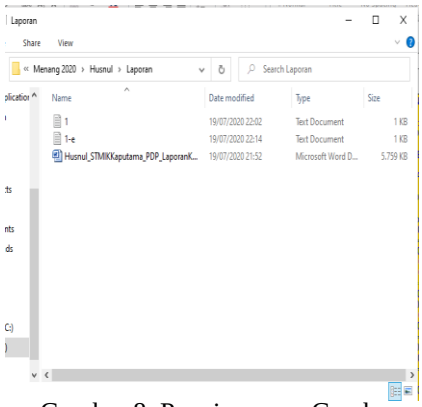
Uji Coba *Encryption*

Pada tahap proses uji coba enkripsi pesan yang dilakukan 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 7. 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 8 .

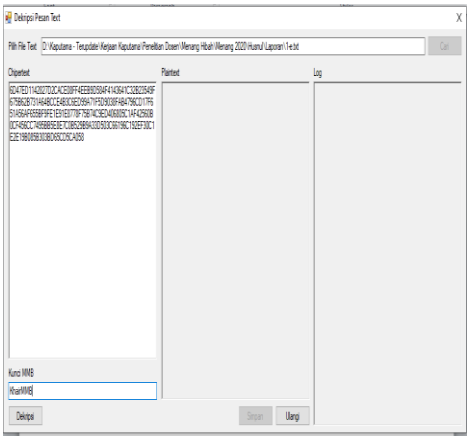


Gambar 8. Penyimpanan Gambar

Pada *form* di atas berfungsi sebagai tempat penyimpanan file hasil dari *enkripsi*. File yang sudah dienkrip akan diberi nama sesuai yang diiginkan.

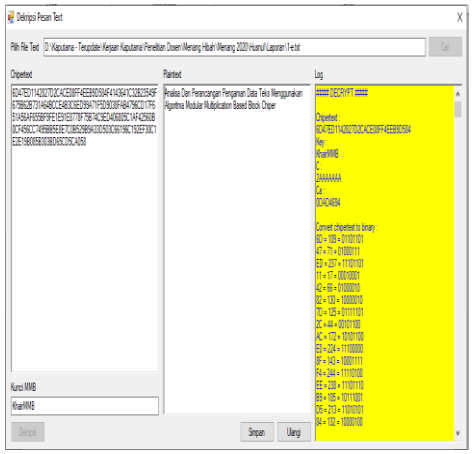
Uji Coba *Description*

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 9. Uji Coba *Description*

Setelah itu klik tombol decrypt untuk melakukan pembacaan teks pada gambar, seperti terlihat pada gambar 10.



Gambar 10. Hasil PembacaanTeks

Hasil Uji Coba

Berdasarkan rangkaian perencanaan dan uji coba setiap form yang ada, peneliti menyampaikan hasil uji coba aplikasi program berjalan sesuai dengan perenacanaan. Program dapat mengenkrip file , kemudian dapat membaca file menjadi file asli pada penerima pesan tersebut. Dan pada teks yang di enkrip akan kembali 100% seperti teks semula setelah didekrip.

Kelebihan dan Kekurangan

Kelebihan dari hasil program Implementasi Algoritma Kriptografi *Modular Multiplication Based Block Cipher* (MMB) Pada Keamanan Data adalah sebagai berikut:

1. Dapat proteksi kunci yang panjangnya tidak terbatas
2. Teks rahasia sulit untuk dipecahkan, bila tidak mengetahui metodenya, kecuali orang yang bersangkutan melalukan pelacakan semua kombinasi
3. Ukuran Teks yang disembunyikan tidak terbatas
4. Menjaga keamanan isi teks yang akan dikirim
5. File Teks berformat doc,txt,xls,ppt.

Kekurangan dari program Implementasi Algoritma Kriptografi *Modular Multiplication Based Block Cipher* (MMB) Pada Keamanan Data adalah sebagai berikut:

1. Hanya mengamankan pesan teks berformat doc,txt,xls,ppt.
2. Aplikasi hanya bisa berjalan pada sistem operasi widows

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..

UCAPAN TERIMA KASIH

Kami menyampaikan terima kasih yang sebesar-besarnya kepada Direktorat Riset dan Pengabdian Kepada Masyakat (DRPM) Ditjen Penguatan Riset dan Pengembangan Kementerian Riset, Teknologi, dan Pendidikan Tinggi atas dukungan dana berupa hibah Penelitian Dosen Pemula (PDP) tahun anggaran 2020. Kami juga mengucapkan terimakasih kepada STMIK Kaputama atas dukungan dalam pelaksanaan kegiatan penelitian ini.

DAFTAR PUSTAKA

[1] A. M. H. Pardede, H. Manurung, and D. Filina, “Algoritma Vigenere Cipher Dan Hill Cipher Dalam Aplikasi Keamanan Data Pada File DOKUMEN,” *JTIK (Jurnal Tek. Inform. Kaputama)*, vol. 1, no. 1, pp. 26–33, 2017.

[2] F. W. Christanto, A. Nugroho, and W. Adhiwibowo, “Implementasi Kemanan Jaringan LAN Berbasis ACLS dan VLAN,” *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 7, no. 2, p. 121, Sep. 2018, doi: 10.32736/sisfokom.v7i2.568.

[3] F. Dewandaru and C. Rahmad, “Aplikasi Keamanan Data Menggunakan Metode Mmb Dan Lsb,” *J. Inform. Polinema*, 2016.

[4] I. A. Ilyas, “Kriptografi,” *Kriptografi fFle Menggunakan Metod. AES Dual Password*, 2014, doi: 10.1046/j.1364-3703.2000.00031.x.

[5] S. Krendelev, N. Zbitnev, D. Shishlyannikov, and D. Gridin, “Block cipher based on modular arithmetic and methods of information compression,” 2017, doi: 10.1088/1742-6596/913/1/012009.

[6] S. Elagooz, N. Hamdy, K. Shehata, and M. Helmy, “Design and implementation of high and low modulo (216 + 1) multiplier used in idea algorithm on FPGA,” 2003, doi: 10.1109/NRSC.2003.1217343.

[7] K. Jia, J. Chen, M. Wang, and X. Wang, “Practical attack on the full MMB block cipher,” 2012, doi: 10.1007/978-3-642-28496-0_11.

[8] D. Ariyus, “Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi.,” *Journal of Chemical Information and Modeling*. 2008, doi: 10.1017/CBO9781107415324.004.