ENKRIPSI SURAT ELEKTRONIK MENGGUNAKAN METODE XXTEA

Oris Krianto Sulaiman[1], Khairuddin Nasution, Satria Yudha Prayogi[2]
[12]*Program Studi Teknik Informatika Universitas Islam Sumatera Utara*
Jl. Sisingamangaraja, Teladan Barat, Medan Kota, Kota Medan, Sumatera Utara 20216
[1]*oris.ks@ft.uisu.ac.id*

Abstrak—**Pesatnya perkembangan teknologi komputer saat ini sering mengakibatkan penyalahgunaan teknologi tersebut dalam tindakan kriminal. Salah satu yang paling sering terjadi adalah pencutian data yang terkandung dalam surat elektronik (email), account pribadi hingga dokumen-dokumen rahasis. Untuk itu, dirasakan perlunya suatu bentuk pengamanan terhadap hal-hal di atas guna kenyamanan user dalam menggunakan teknologi komputer, yaitu dengan melakukan enkripsi. Enkripsi surat elektronik ini dilakukan dengan menggunakan metode XXTEA. XXTEA adalah sebuah algoritma penyandian yang sederhana, tapi kuat yang berbasis iterasi Feistel dan menggunakan banyak ronde untuk mendapatkan keamanan. Enkripsi dan dekripsi dilakukan terhadap surat elektronik yang menggunakan server google mail (Gmail) yaitu smpt.gmail.com dengan port number 587. Namun sistem ini belum bisa digunakan untuk enkripsi surat elektronik yang menggunakan inbox akun e-mail melalui aplikasi di luar situs www.gmail.com, sehingga masih membutuhkan pengembangan lebih lanjut.**

Kata Kunci— **Surat Elektronik, Enkripsi, Metode XXTEA**.

I. PENDAHULUAN

Perkembangan teknologi yang semakin hari kian pesat membuat banyaknya aplikasi dan perangkat yang dapat memudahkan pekerjaan manusia. Saat ini hampir semua aplikasi tersebut terhubung melalui akun yang di verifikasi lewat email. Email atau perangkat elektronik merupakan kerahasiaan pemakaian yang harus dijaga keaslian isinya.

Keamanan data di dalam surat elektronik tidaklah terjamin dan selalu ada resiko terbuka untuk umum, dalam artian semua isinya dapat dibaca oleh orang lain. Hal ini disebabkan oleh karena surat elektronik itu akan melewati banyak server sebelum sampai di tujuan. Tidak tertutup kemungkinan ada orang yang menyadap surat elektronik yang dikirimkan tersebut. Untuk mengurangi potensi surat elektronik disadap, surat dapat diamankan dengan menggunakan teknik pengacakan (enkripsi) [1].

Salah satu metode yang digunakan untuk enkripsi adalah corrected block tiny encryption algorithm atau lebih dikenal dengan nama XXTEA. XXTEA adalah sebuah algoritma penyandian yang sederhana, tapi kuat yang berbasis iterasi Feistel dan menggunakan banyak ronde untuk mendapatkan keamanan. XXTEA dirancang berupa program kecil yang dapat berjalan pada banyak mesin dan mengenkripsi dengan aman. Algoritma ini menggunakan banyak iterasi dibandingkan program yang rumit sehingga algoritma ini dapat diterjemahkan ke dalam banyak bahasa pemrograman dengan mudah.

II. TINJAUAN PUSTAKA

A. Sistem Pengamanan Data

Heading pada level kedua dituliskan dengan *boldface italics* dengan menggunakan huruf besar dan huruf kecil. *Heading* dituliskan rata kiri.

Data adalah suatu istilah majemuk dari kata datum, yang berarti fakta atau bagian fakta yang mengandung arti, yang dihubungkan dengan kenyatan, simbol-simbol, gambar-gambar, kata-kata, angka-angka, huruf-huruf, atau simbol-simbol yang menunjukkan suatu ide, objek, kondisi atau situasi dan lain sebagainya[2].

Data tidak dapat langsung dipakai untuk pengambilan keputusan. Data dapat dimanfaatkan setelah diolah menjadi informasi. Kegunaan data adalah sebagai bahan dasar dari informasi yang dapat digunakan sebagai referensi pengambilan keputusan oleh berbagai pihak. Komputer dapat menyimpan data apabila telah diperinci dan disusun hirarki, susunan data secara hirarki[2] adalah :

1. Bit
2. Byte
3. Karakter
4. Field
5. Record
6. File
7. Database

Sedangkan system pengamanan data/informasi dalam komunikasi komputer menjadi penting karena nilai informasi itu sendiri dan meningkatnya penggunaan Kcomputer di berbagai sektor. Melihat pada kenyataan semakin banyak data yang diproses

dengan komputer dan dikirim melalui perangkat komunikasi elektronik maka ancaman terhadap pengamanan data akan semakin meningkat. Beberapa pola ancaman terhadap komunikasi data dalam komputer menurut [1]:

1. Interruption

Interruption terjadi bila data yang dikirimkan dari A tidak sampai pada orang yang berhak (B). Interruption merupakan pola penyerangan terhadap sifat availability (ketersediaan data).

2. Interception

Serangan ini terjadi bila pihak ketiga C berhasil membaca data yang dikirimkan. Interception merupakan pola penyerangan terhadap sifat confidentiality (kerahasiaan data).

3. Modification

Pada serangan ini pihak ketiga C berhasil merubah pesan yang dikirimkan. Modification merupakan pola penyerangan terhadap sifat integrity (keaslian data).

4. Fabrication

Pada serangan ini, penyerang berhasil mengirimkan data ke tujuan dengan memanfaatkan identitas orang lain. Fabrication merupakan pola penyerangan terhadap sifat authenticity.

Ancaman-ancaman tersebut di atas menjadi masalah terutama dengan semakin meningkatnya komunikasi data yang bersifat rahasia seperti pemindahan dana secara elektronik kepada dunia perbankan / pengiriman dokumen rahasia pada instansi pemerintah. Untuk mengantisipasi ancaman-ancaman tersebut perlu dilakukan usaha untuk melindungi data yang dikirim melalui saluran komunikasi salah satunya adalah dengan teknik enkripsi, serta untuk masalah kekuatan pengamanannya tergantung pada algoritma metode enkripsi tersebut dan juga kunci yang digunakan di dalamnya.

B. Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (Cryptography is the art and science of keeping messages secure).

Sebagai pembanding, selain definisi tersebut di atas, terdapat pula definisi lain, yaitu : “Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi”.[3][4]

Kata “seni” di dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan. Cara-cara unik tersebut mungkin berbeda-beda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia pesan mempunyai nilai estetika tersendiri sehingga kriptografi berkembang menjadi sebuah seni merahasiakan pesan (kata “graphy” di dalam “cryptography” itu sendiri sudah menyiratkan sebuah seni). [5]

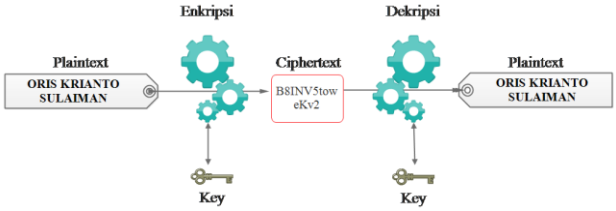
Pada perkembangan selanjutnya, kriptografi berkembang menjadi sebuah disiplin ilmu sendiri karena teknik-teknik kriptografi dapat diformulasikan secara matematik sehingga menjadi sebuah metode yang formal.

Di dalam kriptografi akan sering ditemukan berbagai istilah atau terminologi. Beberapa istilah yang penting untuk diketahui adalah sebagai berikut :

1. Pesan, Plainteks, dan Cipherteks

Pesan (message) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plainteks (*plaintext*) atau teks-jelas (cleartext). Pesan dapat berupa data atau informasi yang dikirim (melalui kurir, saluran telekomunikasi, dan sebagainya) atau yang disimpan di dalam media perekaman (kertas, storage, dan sebagainya). Pesan yang tersimpan tidak hanya berupa teks, tetapi juga dapat berbentuk citra (image), suara/bunyi (audio), dan video, atau berkas biner lainnya. [6], [7]

Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut cipherteks (*ciphertext*) atau kriptogram (cryptogram). Cipherteks harus dapat ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima bisa dibaca. Gambar 1 memperlihatkan contoh dari plainteks, masing-masing berupa teks dan gambar, serta cipherteks yang berkoresponden. Perhatikan bahwa plainteks dapat dibaca dengan jelas, tetapi cipherteks sudah tidak dapat lagi dimengerti maknanya. Melalui proses yang berkebalikan, cipherteks dapat ditransformasikan kembali menjadi plainteks semula atau disebut dengan dekripsi.



Gbr 1. Proses enkripsi dan dekripsi menggunakan kunci

Proses pada gambar diatas merupakan proses enkripsi dan dekripsi menggunakan kunci publik dimana si pengirim akan enkripsi *plaintext* dengan menggunakan kunci dan kemudian disisi penerima juga akan mendekripsikan *ciphertext* dengan menggunakan kunci.

Kunci (key) adalah parameter yang digunakan untuk transformasi enciphering dan dechipering. Kunci biasanya berupa string atau deretan bilangan.

Dengan menggunakan kunci K, maka fungsi enkripsi dan dekripsi dapat ditulis sebagai

EK(P) = C dan DK(C) = P

dan kedua fungsi ini memenuhi

DK(EK(P)) = P

C. Surat Elektronik (Email)

Surat elektronik (disingkat ratel atau surel atau surat-e) atau pos elektronik (disingkat pos-el) atau nama umumnya dalam bahasa Inggris "e-mail atau email" (ejaan Indonesila: imel) adalah sarana kirim mengirim surat melalui jalur *Internet*. Dengan surat biasa umumnya pengirim perlu membayar per pengiriman (dengan membeli perangko), tetapi surat elektronik umumnya biaya yang dikeluarkan adalah biaya untuk membayar sambungan *Internet*.

Contoh alamat e-mail:

1. oris.ks : nama kotak surat (mailbox) atau nama pengguna (username) yang ingin dituju dalam mailserver.

2.ft.uisu.ac.id: nama mailserver tempat pengguna yang dituju, rinciannya:

a. ft.uisu: subdomain (milik pemegang nama domain), biasanya merujuk ke suatu komputer dalam lingkungan pemilik domain.
b. ac.id: menunjukkan bahwa domain ini termasuk kategori akademisi.

D. Corrected Block Tiny Encryption (XXTEA)

Metode corrected block tiny encryption algorithm atau lebih dikenal dengan nama XXTEA adalah sebuah algoritma penyandian yang sederhana, tapi kuat yang berbasis iterasi Feistel dan menggunakan banyak ronde untuk mendapatkan keamanan. XXTEA dirancang berupa program kecil yang dapat berjalan pada banyak mesin dan mengenkripsi dengan aman. Algoritma ini menggunakan banyak iterasi dibandingkan program yang rumit sehingga algoritma ini dapat diterjemahkan ke dalam banyak bahasa pemrograman dengan mudah.[8], [9].

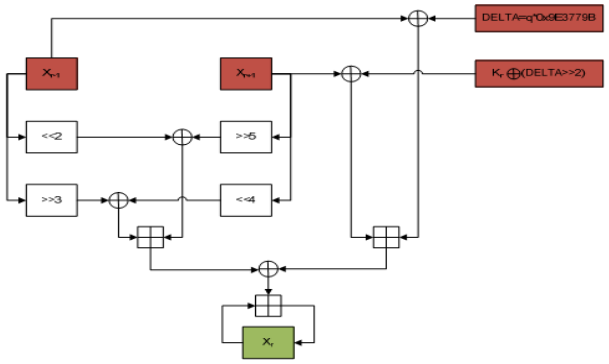
XXTEA juga merupakan sebuah algoritma enkripsi efektif yang mirip dengan DES yang dapat digunakan untuk aplikasi web yang membutuhkan keamanan. Ketika menggunakan algoritma ini, sebuah perubahan dari teks asal akan mengubah sekitar setengah dari teks hasil tanpa meninggalkan jejak di mana perubahan berasal.

XXTEA beroperasi pada blok yang berukuran tetap yang merupakan kelipatan 32 bits dengan ukuran minimal 64 bits. Jumlah dari putaran lengkap bergantung pada ukuran blok, tetapi terdapat minimal 6 (bertambah terus hingga 32 untuk ukuran blok yang lebih kecil). Algoritma ini menggunakan lebih banyak fungsi pengacakan yang menggunakan kedua blok tetangganya dalam pemrosesan setiap kata dalam blok.[10]

Untuk kemudahan penggunaan dan keamanan secara umum, XXTEA lebih tepat digunakan ketika dapat dipakai untuk kondisi berikut:

1. Perubahan satu bit pada *plaintext* akan mengubah sekitar setengah dari total bits dari seluruh blok tanpa meninggalkan jejak di mana perubahan di mulai.
2. Walaupun terdapat perubahan yang teratur pada *plaintext* (misalkan nomor pesan), hanya pesan yang sama yang akan memberikan *ciphertext* yang sama dan kebocoran informasi minimal.
3. Jika tidak memungkinkan untuk memasukkan pesan yang panjang, pesan tersebut dapat dipecah menjadi beberapa bagian yang masing-masing berukuran 60 kata.

Sedangkan algoritma XXTEA dalam satu iterasi dapat dilihat pada Gambar berikut :



Gbr 2. Satu Iterasi dalam Algoritma XXTEA

Keterangan simbol pada Gambar :

1. X_r, X_{r-1},… X_{r+1} : blok *plaintext*, di mana r adalah urutan blok yang sedang diacak.
2. q : jumlah iterasi yang sedang dilakukan.
3. DELTA : q dikalikan dengan konstanta yang bernilai 0x9E3779B.
4. Kr : blok kata kunci ke-r, di mana r sama dengan keterangan di atas.
5. <<n : pergeseran bit ke kiri sebanyak n kali.
6. >>n : pergeseran bit ke kanan sebanyak n kali.
7. : operasi XOR.
8. : operasi penambahan.

Keterangan warna pada Gambar :

1. Kotak berwarna merah : input user.
2. Kotak berwarna hijau : output program.

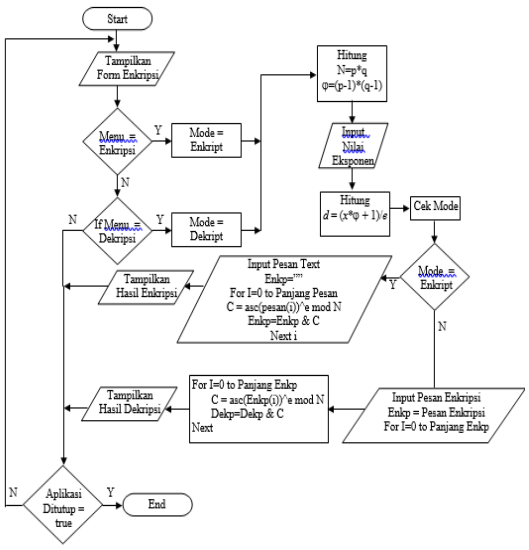
Gambar menampilkan proses pengacakan yang dilakukan pada satu iterasinya. Proses iterasi dalam XXTEA dilakukan dalam 2 kali iterasi yang dilakukan secara bersarang. Pada iterasi teratas, iterasi dilakukan sebanyak q, di mana: q = 6 +25/n

Proses pengacakan yang dilakukan dalam satu iterasi XXTEA adalah :

1. Algoritma akan mengacak blok ke-r dari *plaintext*.
2. Proses akan mengambil x_{r-1}, x_{r+1}, DELTA, dan kata kunci sebagai *input.*
3. Pengacakan pertama: x_{r-1}<<2 di-XOR-kan dengan x_{r+1}>>5.
4. Pengacakan kedua : x_{r-1}>>3 di-XOR-kan dengan x_{r+1}<<4.
5. Hasil yang di dapat dari tahap 4 dan 5 ditambahkan.
6. Pengacakan ketiga: x_{r-1} di-XOR-kan dengan D yang merupakan perkalian antara konstanta DELTA yang bernilai 0x9E3779B dengan jumlah iterasi pertama yang telah dilakukan.
7. Pengacakan keempat: x_{r+1} di-XOR-kan dengan salah satu blok kata kunci, yaitu blok ke-(r XOR D>>2).
8. Hasil yang didapat dari tahap ke 6 dan 7 ditambahkan.
9. Hasil yang didapat dari tahap 5 dan 8 di-XOR-kan.
10. Hasil yang didapat pada tahap 9 ditambahkan ke blok *plaintext* ke-r.

III. PERANCANGAN

Adapun metodologi penelitian yang diterapkan dalam penelitian ini mengacu kepada analisa data yang akan di amankan dalam kasus ini adalah kerahasiaan pesan pada surat elektronik atau *email*. Sistem kriptografi menggunakan algoritma XXTEA, metode ini digunakan untuk mengenkripsi dan dekripsi surat elektronik yang dipilih oleh pengguna. Penggunaan metode ini diharapkan dapat digunakan untuk mengurangi kemungkinan penyalahgunaan isi surat elektronik oleh pihak lain yang tidak berhak.



Gbr 3. *Flowchart* Kriptografi Metode XXTEA

Dari flowchart diatas dapat dilihat bahwasannya sistem ini di mulai dari munculnya form enkripsi dan dekripsi ketika sistem pertama kali dijalankan, kemudian apabila user memilih mode enkript maka sistem akan melakukan enkripsi teks yang terdapat dalam surat elektronik sesuai dengan metode yang dipilih yaitu metode XXTEA, sedangkan apabila memilih menu dekript maka akan dilakukan proses sebaliknya yaitu proses dekripsi teks yang telah di enkripsi sebelumnya.

Proses enkripsi dilakukan dengan menggunakan kunci dimana sebelum pengiriman pesan elektronik terjadi maka *plaintext* akan di konversi ke bilangan binner dan dilakukan perhitungan dengan menggunakan metode XXTEA dari bilangan binner dengan kunci maka jadilah *ciphertext*. *Ciphertext* yang dikirim akan diterima oleh sipenerima dan yang harus di lakukan yaitu proses dekripsi untuk mengembalikan teks dari *ciphertext* menjadi *plainteks* dengan kunci yang sama.

Adapun metode pengujian sistem yang penulis lakukan adalah metode statis (static technique) dimana pengujian dibagi dalam beberapa tahapan.

1. Menetapkan Parameter Pengujian

Adapun paramaeter pengujian yang penulis gunakan dalam pengujian sistem ini adalah sebagai berikut :

a. Kestabilan Sistem
   Parameter ini digunakan untuk menguji apakah sistem masih mengalami error pada saat dieksekusi atau pada saat melakukan proses enkripsi dan dekripsi.
b. Kecepatan Proses
   Parameter ini digunakan untuk menguji kecepatan sistem dalam melakukan enkripsi dan dekripsi pada isi sebuah pesan dalam bentuk e-mail.
c. Ketepatan Hasil
   Parameter ini digunakan untuk menguji apakah sistem telah dapat bekerja seperti apa yang diharapkan dalam perancangan.

2. Menyiapkan Perangkat Pengujian

Dalam tahap ini, penulis menyiapkan sebuah modem GSM dan dua buah akun G-Mail (fairystrawhat@gmail.com dan darkfairystrawhat@gmail.com). fairystrawhat@gmail.com akan digunakan sebagai akun e-mail pengirim, sedangkan darkfairystrawhat@gmail.com akan digunakan sebagai akun e-mail penerima.

IV. HASIL DAN PEMBAHASAN

Pengujian dilakukan dengan cara pengiriman pesan elektronik dimulai dari proses *plaintext* menjadi *ciphertext* kemudian *ciphertext* otomatis akan dikirimkan via email dan sipenerima akan menerima

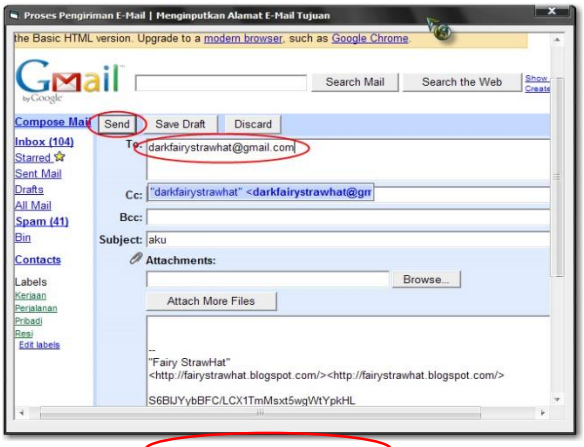
ciphertext tersebut dan mendekripsi dengan kunci tertentu untuk mendapatkan *plaintext* adapun tampilan program untuk enkripsi dan dekripsi adalah sebagai berikut adalah sebagai berikut :

Gbr 4. Tampilan GUI dari aplikasi kriptografi

Dalam pengujian ini digunakan 2 email gmail dengan email fairystrawhat@gmail.com sebagai email pengirim dan darkfairystrawhat@gmail.com sebagai email penerima. Pengujian dilakukan dengan mengirimkan pesan "*pesan ini sangat rahasia jadi jangan sampai tau!!!"* kemudian pesan ini akan dienkripsi dengan metode XXTEA dengan menggunakan kunci "54321"

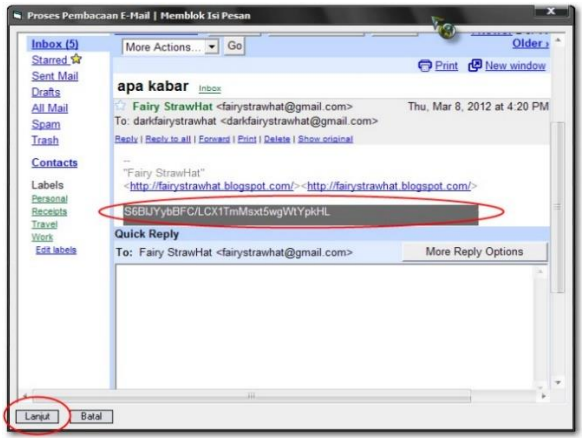
Gbr 5. Proses Pengiriman *Plaintext*

Plaintext tersebut akan di enkripsi dan hasil enkripsi akan dikirimkan kepada email penerima yaitu darkfairystrawhat@gmail.com. Hasil enkripsi dari *plaintext* tersebut adalah S6BIJYybBFC/LCX1TmMsxt5wgWtYpkHL terlihat pada gambar berikut bahwa tampilan form menggunakan form gmail dan di bagian isi email terdapat text S6BIJYybBFC/LCX1TmMsxt5wgWtYpkHL yang merupakan enkripsi dari *plaintext.*



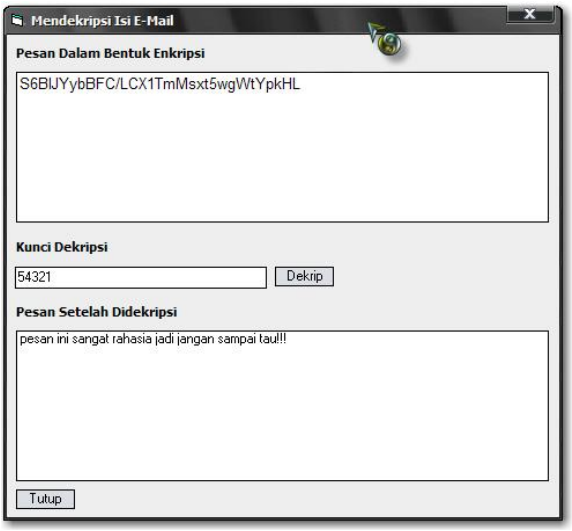
Gbr 6. Proses pengiriman *ciphertext* ke penerima

Kemudian si penerima yaitu darkfairystrawhat@gmail.com akan memilih mode proses dekripsi E-mail untuk merubah *ciphertext* menjadi *plaintext* atau teks asli.



Gbr 7. Tampilan kotak masuk penerima *ciphertext*

Kemudian penerima diharuskan dekripsi pesan tersebut dengan menggunakan kunci yang sama yaitu kunci 54321.



Gbr 8. Tampilan hasil dekripsi *ciphertext*

Berdasarkan hasil pengujian yang dilakukan, beberapa poin penting mengenai proses enkripsi dan dekripsi e-mail melalui server Gmail dengan menggunakan metode XXTEA, sebagai berikut :

1. Server Gmail menyediakan port server yang dapat digunakan untuk mengirimkan e-mail selain dengan cara mengakses situs gmail.com. adapun port ini adalah smtp.gmail.com dengan nomor port 587.
2. Dengan memanfaatkan port di atas, dapat dilakukan enkripsi terhadap sebuah pesan melalui metode kriptografi yang ada, sebagai contoh XXTEA. XXTEA akan mengubah isi pesan asli menjadi pesan terenkripsi.
3. Walaupun menyediakan port untuk mengirimkan e-mail selain dengan cara mengakses situs gmail.com, server Gmail tidak menyediakan port untuk melakukan pembacaan terhadap isi inbox dari sebuah akun. Hal ini menyebabkan isi pesan yang akan didekripsi harus di copy secara manual setelah melakukan pengaksesan terhadap inbox akun Gmail yang bersangkutan.
4. Kecepatan dan stabilitas koneksi internet sangat berpengaruh pada proses pengiriman e-mail terenkripsi, maupun pada proses dekripsi e-mail tersebut. Jika delay waktu akses terlalu lama, maka port smtp.gmail.com akan secara otomatis memutus koneksi tersebut, sehingga proses harus diulang dari awal.

V. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian ini, maka penulis mengambil kesimpulan sebagai berikut :

1. Server google mail (Gmail) menyediakan sebuah port server yang dapat digunakan untuk mengirimkan e-mail melalui aplikasi di luar situs www.gmail.com, yaitu smtp.gmail.com dengan nomor port 587. Namun, Gmail tidak menyediakan port server untuk mengakses inbox akun e-mail melalui aplikasi diluar situs www.gmail.com.
2. Metode XXTEA dapat digunakan untuk menyamarkan isi pesan asli yang akan dikirimkan melalui e-mail, sehingga menjaga kerahasiaan isi pesan tersebut.
3. Sering terjadinya kegagalan pengiriman e-mail atau pendekripsian e-mail melalui perangkat lunak ini diakibatkan tidak stabilnya koneksi modem GSM yang digunakan. Ketidak stabilan ini menyebabkan delay akses yang cukup lama, sehingga gmail secara otomatis memutus hubungan koneksi melalui smtp.gmail.com.

Berdasarkan kesimpulan di atas, maka penulis memberikan saran sebagai berikut :

1. Dalam menggunakan perangkat lunak ini, sebaiknya digunakan jaringan internet yang stabil dalam hal kecepatan koneksi. Hal ini untuk mencegah terputusnya hubungan koneksi dengan port smtp.gmail.com.
2. Perangkat lunak ini dapat dikembangkan sehingga pada proses dekripsi e-mail tidak perlu dilakukan secara manual dengan cara mengakses situs www.gmail.com.
3. Perangkat lunak ini dapat dikembangkan dengan mengubah metode enkripsi lain selain XXTEA, sehingga dapat dibandingkan hasilnya dengan metode yang digunakan dalam perangkat lunak ini.

REFERENSI

[1] R. E. Blahut, *Cryptography and secure communication*, vol. 9781107014275. 2012.

[2] H. M. Jogiyanto, *Analisis & Disain Sistem Informasi Pendekatan Terstruktur Teori Dan Praktek Aplikasi Bisnis*, 2nd ed. Yogyakarta: Penerbit Andi, 2015.

[3] M. Ihwani, "Model Keamanan Informasi Berbasis Digital Signature Dengan Algoritma Rsa," *CESSJournal Comput. Eng. Syst. Sci.*, vol. 1, no. 1, pp. 15–20, 2016.

[4] H. Delfs and H. Knebl, *Introduction to Cryptography*. 2007.

[5] L. Van Houtven, "Crypto 101," p. 243, 2014.

[6] O. K. Sulaiman, M. Ihwani, and S. F. Rizki, "MODEL KEAMANAN INFORMASI BERBASIS TANDA TANGAN DIGITAL DENGAN DATA ENCRYPTION STANDARD (DES) ALGORITHM," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 14–19, Sep. 2016.

[7] A. Widarma, "Kombinasi Algoritma AES, RC4, dan Elgamal dalam Skema Hybrid untuk Keamanan Data," *J. Comput. Eng. Syst. Sci.*, vol. 1, no. 1, pp. 1–8, 2016.

[8] M. Natsir, "Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java," *J. Sist. Inf.*, vol. 6, pp. 87–105, 2017.

[9] H. Nasution, P. Studi, T. Informatika, and U. Tanjungpura, "Implementasi Algoritma Kriptografi XXTEA untuk Enkripsi dan Dekripsi Query Database pada Aplikasi Online Test (Studi Kasus : SMK Immanuel Pontianak)," vol. 1, no. 1, pp. 1–5, 2017.

[10] J. HOLDEN, *The Mathematics of Secrets. Cryptography from Caesar Ciphers to Digital Encryption*. 2017.