PENGAMANAN E-MAIL MENGGUNAKAN ALGORITMA BLOCK CIPHER DAN FUNGSI XOR

Respati Bayuadi (1110651231)[1], Ari Eko Wardoyo S.T, M.Kom [2],
Deni Arifianto, S.Kom [3], Sistem Bisnis Cerdas,
Program Studi Teknik Informatika, Fakultas Teknik,
Universitas Muhammadiyah Jember
E-mail : breeze_boyz@yahoo.co.id [1],

ABSTRAK

E-mail merupakan telekomunikasi dengan standar terbuka yang artinya dipergunakan banyak pihak, sehinggan dimungkinkan terjadinya penyadapan informasi. Penelitian ini berusaha untuk memberikan keamanan dalam bertukar informasi atau pesan dengan mengubah teks asli manjadi pesan tersandi atau yang dikenal dengan istilah Kriptografi. Pengamanan ini ditekankan pada *body* dan *attachment e-mail*. Dalam pengamanan penulis menggunakan algoritma *block cipher* dan fungsi *xor*. Dengan pesan yang tersandi maka keamanan pengguna *e-mail* dalam bertukan informasi dan pesan menjadi lebih aman, dan menjaga keaslian data yang dikirim oleh pengguna.

Kata kunci : *e-mal, body, attachment, block cipher, xor,* Kriptografi

1. PENDAHULUAN

Salah satu perkembangan yang sangat pesat adalah penggunaan *e-mail* dalam bertukar informasi atau pesan melalui jaringan internet. Namun tingkat keamanan dalam penggunaan media *e-mail* harus diperhatikan, karena *e-mail* merupakan bentuk telekomunikasi dengan standar terbuka yang artinya dipergunakan banyak pihak, sehingga dimungkinkan terjadi penyadapan informasi. Oleh karena itu dikembangkan cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi. Kriptografi merupakan seni menyembunyikan pesan. Dengan pesan yang tersandi maka keamanan pengguna *e-mail* dalam bertukar data menjadi lebih aman, dan menjaga keaslian data yang di kirim oleh pengguna

2. METODOLOGI PENELITIAN

2.1 Kriptografi

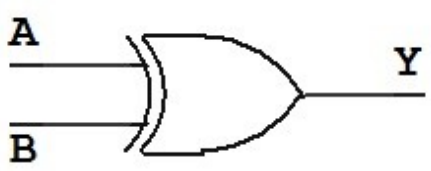
Kriptografi berasal dari bahasa yunani, *crypto* dan *graphia*. Crypto berarti rahasia dan *graphia* berarti menulis. *Kriptografi* adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirim, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam buku "*Applied Cryptography"*, kriptografi adalah ilmu pengetahuan dan seni menjaga pesan agar tetap aman. Menurut William Stallings mendefinisikan *kriptografi* sebagai "*the art and science of keeping messages secure"*

2.2 Block cipher

Pada *cipher* blok, rangkaian bit-bit plaintex dibagi menjadi blok-blok bit dengan panjang sama. Hasil enkripsi dari blok plainteks akan sama bila menggunakan kunci yang sama.

2.3 Fungsi *Xor*

Fungsi Xor berasal dari kata *Exclusive OR*. Fungsi ini berjalan pada mode bit, keluaran fungsi ini bernilai 1 jika nilai masukan-masukannya mempunyai keadaan yang berbeda. Simbol standar gerbang logika Xor adalah seperti tampak pada gambar dibawah:



Gambar 3.5 Gerbang logika Xor

3. HASIL DAN PEMBAHASAN

3.1 Proses Enkripsi

Langkah-langkah proses Enkripsi :

1. Menyiapkan file dan teks yang akan digunakan.
2. Plainteks di geser sesuai dengan posisi plainteks
3. Membuat kunci berdasarkan hasil jumlah *ASCII* mod 16
4. Merubah plainteks dan kunci menjadi biner
5. Membuat blok pada plainteks dan kunci sebesar 32bit (32 digit biner)
6. Plainteks *XOR* dengan kunci pada blok pertama, dan seterusnya.
7. Hasil *XOR* dirubah menjadi basis16 (*hex)*
8. Merubah jumlah *ASCII* menjadi basis16 (*hex)*
9. Merubah panjang plainteks menjadi basis16 (*hex)*
10. Menggabungkan semua hasil basis16 menjadi satu bagian
11. Menyisipkan jumlah *ASCII* dan panjang plainteks ditengah dari ciphertext

3.2 Proses Dekripsi

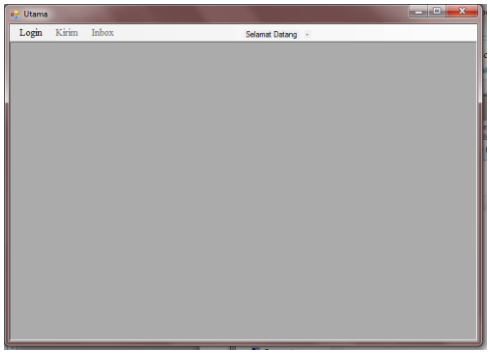
Langkah – langkah proses dekripsi

1. Menyiapkan file dan teks (cipherteks) yang akan digunakan.
2. Memisahkan ciper, jumlah *ASCII*, dan panjang plainteks
3. Jumlah *ASCII* dirubah menjadi basis 10 kemudian di mod 16
4. Pembentukan kunci
5. Binerisasi kunci dari basis
6. Pembentukan kunci 32bit
7. Membuat blok cipher dengan ukuran 2 digit *hex*
8. Binerisasi cipher
9. Melakukan operasi *XOR* antara cipher dan kunci (sama-sama biner)
10. Melakukan pemisahan biner dengan ukuran 8 bit
11. Merubah 8 bit biner menjadi desimal (basis 10)
12. Pergeseran baris tiap cipher sesuai dengan posisi karakter chiper, dengan pergeseran minus (keatas).
13. Merubah hasil pergeseran menjadi karakter

14. Menggabungkan semua karakter untuk membentuk plainteks

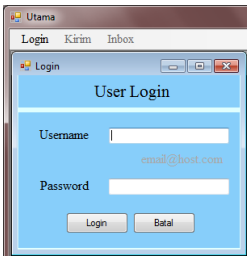
4. Impementasi Program

(1) Menu utama program adapun tampilan menu utama pada saat program dijalankan ditunjukkan pada Gambar 1.



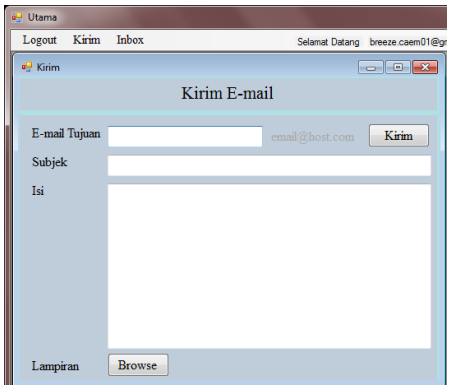
Gambar 1 Form Menu Utama

(2) Form Login, tampilan form ini digunakan untuk login kedalam *e-mail.*



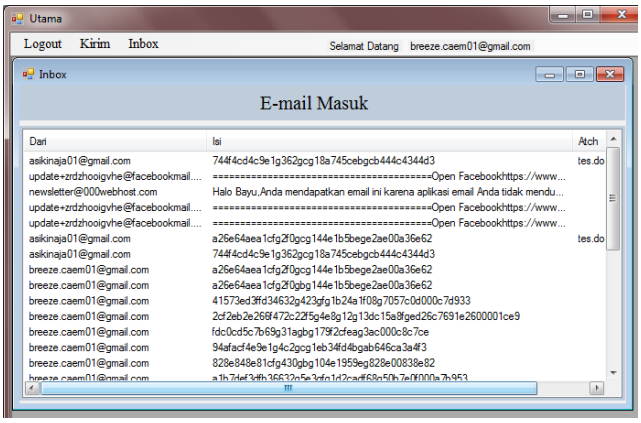
Gambar 2 Form Login

(3) Form kirim *e-mail*, tampilan form ini digunakan untuk melakukan pengiriman *e-mail*



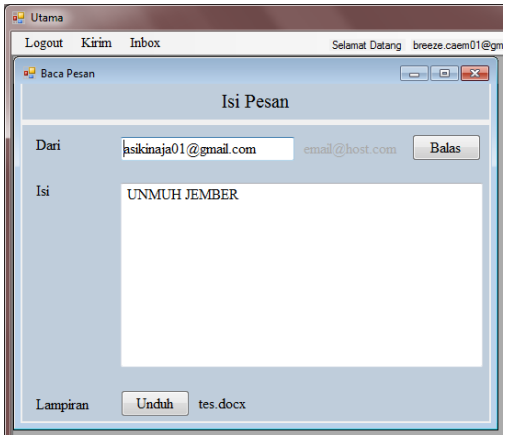
Gambar 3 Form Kirim *e-mail*

(4) Form inbox, tampilan form ini digunakan untuk melihat sema surat yang ada pada *e-mail.*



Gambar 4 form inbox

(5) Form baca, tampilan form ini digunakan untuk membaca pesan pada *e-mail.*



Gambar 5 form baca

Teks	Enkrip	Dekrip	Keterangan
UNMUH JEMBER	744F4CD4C9E1G362GCG18A745CEBGCB444C4344D3	UNMUH JEMBER	Berhasil
MAKAN MALAM	a26e64aea1cfg2f0gbg144e1b5bege2ae00a36e62	MAKAN MALAM	Berhasil
SELAMAT BERBUKA	41573ed3ffd34632g423gfg1b24a1f08g7057c0d000c7d933	SELAMAT BERBUKA	Berhasil
KULIAH	2cf2eb2e266f472c22f5g4e8g12g13	KULIAH	Berhasil

KERJA NYATA	dc15a8fged26c7691e2600001ce9	KERJA NYATA	
TIDUR SIANG	fdc0cd5c7b69g31agbg179f2cfeag3ac000c8c7ce	TIDUR SIANG	Berhasil

Tabel 1 Uji coba

5. Kesimpulan dan Saran

a. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan pada bab-bab sebelumnya dapat diambil kesimpulan sebagai berikut :

1. Tingkat kesuksesan algoritma ini dari 6 kali uji coba terhadap 300 kata sebesar 100%
2. Algoritma ini terbukti efektif dan aman untuk segala jenis teks.
3. Program ini efisien dalam mengirim *e-mail* yang ter-enkripsi.

b. Saran

Beberapa saran yang dapat diberikan untuk pengembangan lebih lanjut yaitu :

1. Untuk jenis file lampiran nantinya bisa dilengkapi dengan jenis file lain seperti excell, dan lain lain.
2. Agar dapat menjaga keaslian format penulisan teks yang terkirim

REFERENSI

- A Darto Iwan S, 2009. *Pengenalan Kriptografi*, Buletindo
- A Irawan, 2011, *Stone Morse*, From amikom.ac.id/index.php/karyailmiahdosen/article/view/2222/538, 7 Februari 2015
- Ariyus,Dony. 2006. *Computer Security*, Andi Offset, Yogyakarta
- Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi*, Andi Offset-STMIK AMIKOM, Yogyakarta
- Munir, Rinaldi, 2006. *Kriptografi*, Informatika, Bandung