PENYANDIAN EMAIL MENGGUNAKAN ALGORITMA KRIPTOGRAFI WAKE (WORD AUTO KEY ENCRYPTION)

Halasson Gultom (12110668)

Mahasiswa Program Studi Teknik Informatika STMIK Budi Darma Medan
Jl. Sisingamangaraja Np. 338 Simpang Limun Medan
http : //www.stmik-budidarma.ac.id // Email : goeltom2411@gmail.com

ABSTRAK

Dahulu komunikasi jarak jauh masih menggunakan cara yang konvensional, yaitu dengan cara saling mengirim surat, tetapi sekarang komunikasi jarak jauh dapat dilakukan dengan mudah dan cepat yaitu dengan adanya teknologi seperti Email, SMS (Short Messaging Service).

Salah satu dampak negatif dalam perkembangan teknologi adalah adanya penyadapan data, yang merupakan salah satu masalah yang paling ditakuti oleh para pengguna jaringan komunikasi.Karena itulah dibutuhkan suatu metode yang dapat menjaga kerahasiaan informasi ini, metode yang dimaksud adalah Kriptograpi.

Metode Kriptografi WAKE (Word Auto Key Encryption) merupakan salah satu metode yang telah digunakan secara komersial yang dapat digunakan untuk mengamankan data dimana dalam hal ini penulis ingin mengamankan isi dari email yang berupa teks.

Kata Kunci : Kriptografi, WAKE, EMAIL

1. Pendahuluan

1.1. Latar Belakang Masalah

Salah satu dampak negatif dalam perkembangan teknologi adalah adanya penyadapan terhadap data. Pada skripsi penulis ingin mengangkat masalah tentang penyadapan data pada isi sebuah email, dimana tindakan penyadapan tersebut merupakan salah satu masalah yang paling ditakuti oleh para pengguna jaringan komunikasi khususnya dalam proses pengiriman dan penerimaan email. Coba dibayangkan jika seseorang yang tidak bertanggung jawab telah mengetahui password dan user email , maka secara otomatis isi dari keseluruhan email kita tersebut tentu dapat diketahui oleh orang tersebut bukan. Karena itulah dibutuhkan suatu metode yang dapat menjaga kerahasiaan informasi ini, metode yang dimaksud adalah Kriptograpi.

Metode kriptografi dapat digunakan untuk mengamankan data yang bersifat rahasia agar data tersebut tidak diketahui oleh orang lain yang tidak berkepentingan. Metode WAKE merupakan salah satu metode yang telah digunakan secara komersial. WAKE merupakan singkatan dari *Word Auto Key Encryption*. Dalam algoritmanya, metode ini menggunakan operasi XOR, AND, OR dan *Shift Right*. Metode WAKE dapat dibagi menjadi beberapa proses yaitu proses pembentukan tabel dan kunci, enkripsi dan dekripsi. Proses penyelesaian metode ini cukup rumit dan sulit untuk dikerjakan secara manual berhubung karena algoritmanya yang cukup panjang dan kompleks.

1.2. Rumusan Masalah

Adapun yang menjadi rumusan masalah dalam penyusunan skripsi ini adalah sebagai berikut :

1. Bagaimana proses penyandian data pada email agar data tersebut tidak dapat diketahui oleh pihak-pihak yang tidak bertanggung jawab?
2. Bagaimana menerapkan metode WAKE (*Word Auto Key Encryption*) dalam proses enkripsi-deskripsi data plaintext?
3. Bagaimana merancang aplikasi penyandian email dengan metode WAKE (*Word Auto Key Encryption*)?

1.3. Batasan Masalah

Adapun yang menjadi batasan masalah dalam penyusunan skripsi ini adalah sebagai berikut :

1. Tipe data Email yang digunakan hanya berupa plaintext bukan berupa gambar dan *attachment file*.
2. Membahas enkripsi dan deskripsi email menggunakan algoritma kriptograpi WAKE saat mengirim dan menampilkan email yang telah diterima dalam kotak masuk.
3. Menggunakan mail server yahoo dan gmail.
4. Menggunakan protokol SMPT sebagai pengirim email ke server dan protokol IMAP sebagai penerima atau pengunduh email dari server.

5. Menggunakan Modem Smartfren CDMA untuk melakukan koneksi ke email server.
6. Bahasa Pemrogram yang digunakan adalah Visual Basic 6.0

1.4. Tujuan Dan Manfaat Penelitian

1.4.1. Tujuan Penelitan

Yang menjadi tujuan penelitan dalam penyusunan skripsi ini adalah :

1. Melakukan proses penyadian data pada email.
2. Menerapkan Metode WAKE dalam proses penyandian email.
3. Merancang aplikasi penyandian email dengan metode WAKE (*Word Auto Key Encryption*).

1.4.2. Manfaat Penelitian

Adapun yang menjadi manfaat yang diperoleh dari penyusunan skripsi ini adalah sebagai berikut :

1. Pemahaman proses enkripsi dan deskripsi data berupa plaintext.
2. Pemahaman metode WAKE dalam proses penyandian data plaintext pada email.
3. Dengan menggunakan aplikasi penyandian email ini, user dapat mengirim dan menerima email yang dienkripsi, dimana pada saat penampilan data akan dilakukan proses deskripsi untuk menampilkan data yang sebenarnya.

2. Landasan Teori

2.1. WAKE (*Word Auto Key Encryption*)

Metode WAKE menggunakan kunci 128 bit dan sebuah tabel 256 x 32 bit. Dalam algoritmanya, metode ini menggunakan operasi XOR, AND, OR dan *Shift Right*. Dalam prosesnya metode ini memiliki proses yang sederhana dan cepat, untuk menghasilkan chipertext kunci yang telah diputar sebanyak n putaran di XOR kan dengan plaintext dan untuk menghasilkan plaintext kunci yang diputar sebanyak n putaran di XOR kan dengan chipertext yang telah dihasilkan pada saat melakukan enkripsi. Metode ini ditemukan oleh David J. Wheeler pada tahun 1993. Inti dari metode WAKE terletak pada proses pembentukan tabel *S-Box* dan proses pembentukan kunci. Tabel *S-Box* dari metode WAKE bersifat fleksibel dan berbeda-beda untuk setiap putaran.

2.2.1. Proses Pembentukan Tabel S-Box

Langkah-langkah untuk membentuk tabel S-Box adalah sebagai berikut :

1. Inisialisasi nilai TT[0] … TT[7] :
   TT[0] = 726A8F3B (dalam heksadesimal)
   TT[1] = E69A3B5C (dalam heksadesimal)
   TT[2] = D3C71FE5 (dalam heksadesimal)
   TT[3] = AB3C73D2 (dalam heksadesimal)
   TT[4] = 4D3A8EB3 (dalam heksadesimal)
   TT[5] = 0396D6E8 (dalam heksadesimal)
   TT[6] = 3D4C2F7A (dalam heksadesimal)
   TT[7] = 9EE27CF3 (dalam heksadesimal)
2. Inisialisasi nilai awal untuk T[0] … T[3] :
   T[0] = K[0] T[2] = K[2]
   T[1] = K[1] T[3] = K[3]
   K[0], K[1], K[2], K[3] dihasilkan dari kunci yang dipecah menjadi 4 bagian yang sama panjang.
3. Untuk T[4] sampai T[255], lakukan proses berikut :
   X = T[n-4] + T[n-1]
   T[n] = X >> 3 XOR TT(X AND 7)
4. Untuk T[0] sampai T[22], lakukan proses berikut :
   T[n] = T[n] + T[n+89]
5. Set nilai untuk beberapa variabel di bawah ini :
   X = T[33]
   Z = T[59] OR (01000001h)
   Z = Z AND (FF7FFFFFh)
   X = (X AND FF7FFFFFh) + Z
6. Untuk T[0] … T[255], lakukan proses berikut :
   X = (X AND FF7FFFFFh) + Z
   T[n] = T[n] AND 00FFFFFFh XOR X
7. Inisialisasi nilai untuk beberapa variabel berikut ini :
   T[256] = T[0]
   X = X AND 255
8. Untuk T[0] … T[255], lakukan proses berikut :
   Temp = (T[n XOR X] XOR X) AND 255
   T[n] = T[Temp]
   T[X] = T[n+1]

2.1.2. Proses Pembentukan Kunci

Proses pembentukan kunci dari metode WAKE dapat ditentukan sendiri yaitu sebanyak n putaran. Semakin banyak putaran dari proses pembentukan kunci, maka keamanan datanya akan semakin terjamin. Fungsi yang digunakan dalam proses pembentukan kunci adalah **M(X, Y) = (X + Y) >> 8 XOR T[(X + Y) AND 255].** Pertama-tama, kunci yang di-*input* akan dipecah menjadi 4 bagian dan di-set sebagai nilai awal dari variabel A_0, B_0, C_0, dan D_0. Nilai dari variabel ini akan diproses dengan melalui langkah berikut :

$A_{i+1} = M(A_i, D_i)$
$B_{i+1} = M(B_i, A_{i+1})$
$C_{i+1} = M(C_i, B_{i+1})$
$D_{i+1} = M(D_i, C_{i+1})$

Nilai dari D_i merupakan nilai dari kunci K_i.

2.1.3. Proses Enkripsi dan Dekripsi

Inti dari metode WAKE tidak terletak pada proses enkripsi dan dekripsinya, karena proses enkripsi dan dekripsinya hanya berupa operasi XOR dari *plaintext* dan kunci untuk menghasilkan

ciphertext atau operasi XOR *ciphertext* dan kunci untuk menghasilkan *plaintext*.

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

Dimana : P = plaintext
K = Kunci
C = Chiepertext

Sumber : Skripsi Christian Sudibyo,2012 : 15-19

2.2. Defenisi Email

Email (*Electronic mail*) merupakan salah satu layanan yang tersedia di internet. Dimana layanan ini digunakan untuk saling korespondensi antar teman, relasi, lembaga dan lain sebagainya. Dengan Email data dikirim secara elektronik sehingga sampai di tujuan dengan sangat cepat. Konsep E-mail adalah seperti kita mengirim surat dengan pos biasa, dimana kita mengirimkan ke kantor pos dengan dibubuhi alamat yang kita tuju. Dari Kantor Pos tersebut akan disampaikan ke Kantor Pos yang terdekat dengan alamat yang dituju dan akhirnya sampai ke alamat tersebut.

3. Analisa Dan Perancangan

3.1. Analisa Penerapan Metode WAKE

Proses penyandian dengan menggunakan algoritma kriptografi WAKE terdiri atas 4 (empat) proses utama, yaitu :

1. Proses Pembentukan Tabel *S-Box*.
2. Proses Pembentukan Kunci.
3. Proses Enkripsi.
4. Proses Dekripsi.

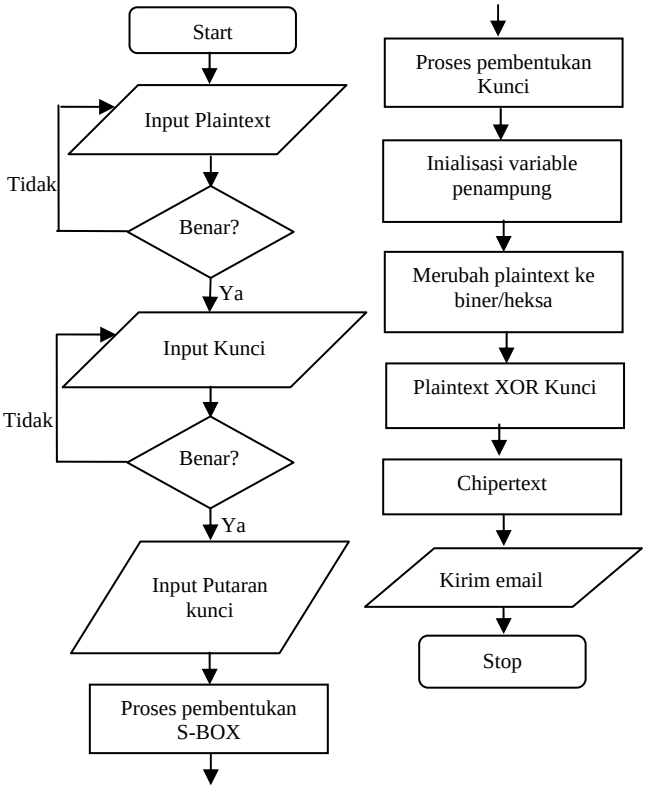
Dimana Inti dari metode WAKE terletak pada proses pembentukan tabel *S-Box* (*Substitution Box*) dan proses pembentukan kunci. Proses enkripsi dan dekripsi hanya berupa operasi XOR dari *plaintext* dan kunci untuk menghasilkan *ciphertext* dan operasi XOR dari *ciphertext* dan kunci untuk menghasilkan *plaintext*.

3.2. Perancangan Sistem Dan Aplikasi

Perancangan sistem merupakan gambaran dari perancangan dan pembuatan sketsa, sehingga dapat menjadi satu kesatuan. Pada tahap ini, alat bantu yang digunakan adalah *Flowchart diagram*. Perancangan penyandian email menggunakan algoritma kriptografi WAKE yang dikembangkan dapat berjalan sesuai dengan prosedur yang ada.

3.2.1. Proses Enkripsi Email

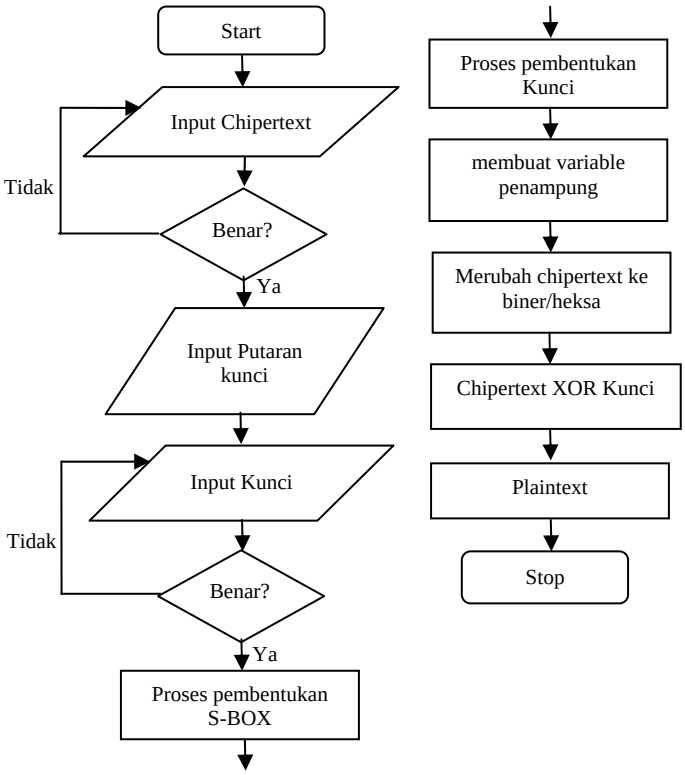
Sistem berjalan ketika sistem aplikasi mulai dijalankan, dimana sebelum user mengirimkan email, user akan menginput plaintext pada textboxt yang tersedia sebelum melakukan proses penyandian data dan pengiriman email. Kemudian user akan memasukkan inputan kunci yang akan digunakan untuk melakukan pembentukan tabel s-box dan proses pembentukan kunci. User juga akan memasukkan jumlah putaran yang akan digunakan dalam proses pembentukan kunci, dimana jumlah putaran user akan mempengaruhi hasil kunci yang didapatkan. Untuk lebih jelasnya kita dapat melihat proses ini pada gambar 3.1. Proses enkripsi dari metode WAKE untuk menghasilkan *ciphertext* adalah berupa hasil operasi XOR dari *plaintext* dan 32 bit kunci yang dihasilkan dari proses pembentukan kunci.



Gambar 1. Flowchart proses enkripsi email

3.2.2. Proses Deskripsi Email

Sistem berjalan ketika sistem aplikasi mulai dijalankan, dimana sebelum user melakukan proses deskripsi terhadap email, user akan akan terlebih dahulu melakukan proses *download* email dari email server dengan melakukan login pada mail server, kemudian menginput *chipertext* pada *textboxt* yang tersedia. Kemudian user akan memasukkan inputan kunci yang sama pada saat proses enkripsi file sebanyak 16 karakter yang akan digunakan untuk melakukan pembentukan tabel s-box dan proses pembentukan kunci. User juga akan memasukkan jumlah putaran yang akan digunakan dalam proses pembentukan kunci, dimana jumlah putaran user akan mempengaruhi hasil kunci yang didapatkan. Untuk lebih jelasnya kita dapat melihat proses ini pada gambar Proses dekripsi dari metode WAKE untuk menghasilkan *plaintext* adalah berupa hasil operasi XOR dari *ciphertext* dan 32 bit kunci yang dihasilkan dari proses pembentukan kunci.



Gambar 2. Flowchart Deskripsi Email

4. Algoritma Dan Implementasi

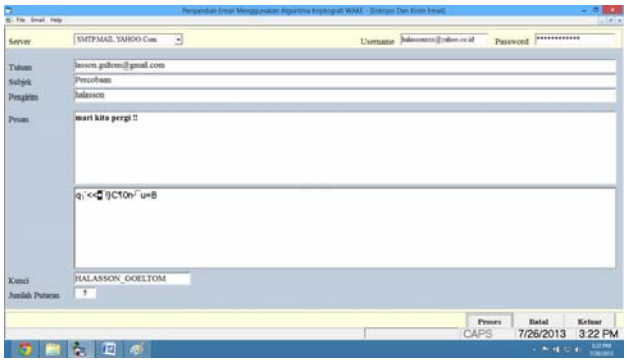
4.1. Algoritma

Untuk menghasilkan sebuah program aplikasi, hal pertama yang harus dilakukan adalah membentuk algoritma yang akan menggambarkan bagaimana program itu bekerja. Dalam menggambarkan dibutuhkan langkah-langkah logika untuk menyelasaikan masalah serta berfungsi untuk penelusuran program untuk keperluan perbaikan atau pengembangan akan lebih mudah dan terarah. Adapun algoritma yang digunakan dalam program ini adalah :

1. Algoritma pembentukan tabel S-box
2. Algoritma pembentukan kunci.
3. Algoritma enkripsi.
4. Algoritma Deskripsi.
5. Algoritma pengiriman email.
6. Algoritma penerimaan/download email.

4.2. Implementasi Sistem

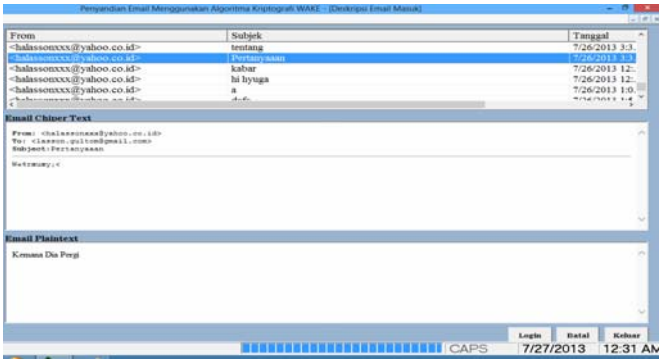
Ketika user memilih sub menu enkripsi email maka tampilan enkripsi dan kirim email akan ditampilkan seperti gambar 3 dibawah ini. Pada tampilan ini user dapat menyandikan email dengan proses enkripsi dan mengirim email tersebut dengan cara mengklik tombol proses.



Gambar 3. Tampilan Form Login

4.3. Tampilan Email Masuk dan Deskripsi Email

Ketika user memilih salah satu email maka sistem memeriksa apakah email tersebut dalam keadaan terenkripsi atau tidak. Jika email tersebut dienkripsi maka sistem akan melakukan proses deskripsi, dimana proses deskripsi tersebut memerlukan sebuah kunci dan jumlah putaran kunci, tentunya terlebih dahulu user harus menginput kunci dan jumlah putaran kunci yang sama pada saat user (pengirim email) melakukan proses enkripsi. Setelah proses deskripsi selesai, maka sistem akan menampilkan isi email terebut seperti pada gambar 4.



Gambar 4 Tampilan Form Login

5. Kesimpulan Dan Saran

5.1. Kesimpulan

Dari pembahasan yang penulis lakukan pada penulisan skripsi ini dapat ditarik beberapa kesimpulan antara lain :

1. Proses penyandian email berupa plainteks dapat dilakukan dengan teknik enkripsi-

deskripsi dengan menggunakan algoritma kriptografi WAKE (*Word Auto Key Encryption*) sehingga pihak-pihak yang tidak bertanggung jawab tidak dapat mengetahui isi email dengan mudah.

2. Dalam penerapan metode WAKE (*Word Auto Key Encryption*) pada penyandian email berupa plainteks, pengirim dan pernerima harus menggunakan kunci dan jumlah rotasi kunci yang sama.
3. Penyandian email menggunakan algoritma kriptografi WAKE (*Word Auto Key Encryption*) dapat dilakukan dengan menggunakan bahasa pemograman *visual basic 6.0*

5.2. Saran

Adapun yang menjadi saran dalam penulisan skripsi ini adalah sebagai berikut:

1. Diharapkan pada masa yang akan datang email yang disandikan dapat berupa gambar dan *file attachment.*
2. Diharapkan penambahan variasi desain pada tampilan aplikasi penyandian email ini agar lebih menarik dan lebih bagus lagi dengan menggunakan bahasa pemograman yang lain, misalnya visual studio 2008, java dan lain-lain.

DAFTAR PUSTAKA

1. Rinaldi Munir, ***Kriptografi***, Penerbit Informatika Bandung, 2006.
2. Dony Ariyus,Kriptografi, ***Keamanan Data dan Komunikasi***, Penerbit Graha Ilmu, 2006.
3. Achmad Basuki, ***Algoritma Pemograman 2 Menggunakan Visual Basic 6.0***, Institut Teknologi Sepuluh November Surabaya, 2006.
4. Ryan Maulana A, 2012, ***Penerapan Algoritma Kriptografi WAKE pada Aplikasi Chating & Internet Monitor Berbasis LAN.***
5. Christian Sudibyo, 2012, ***Implementasi dan Analisis Performa Kriptografi Metode WAKE Pada Kombinasi Data Numerik dan Karakter.***
6. *http://yudhim.blogspot.com/2010/08/pengenalan-tentang-e-mail-electronic.html, tanggal 20 Mei 2013*
7. *http://computer-muter.blogspot.com/2012/11/smtp-simple-mail-transfer-protocol.html,tanggal 20 Mei 2013*.