PROTOTYPE MODEL KEAMANAN DATA MENGGUNAKAN KRIPTOGRAFI DATA ENCRYPTION STANDAR (DES) DENGAN MODE OPERASI *CHIPER BLOCK CHAINING* (CBC)

Ari Muzakir
Fakultas Ilmu Komputer, Universitas Bina Darma
Jl. A. Yani No. 12 Plaju Palembang
email: ariemuzakir@mail.binadarma.ac.id

Abstrak *– Model keamanan data menjadi topik yang selalu dibicarakan, karena semakin banyaknya isu keamanan yang terus mengancam dalam pemanfaatan teknologi informasi. Sehingga keamanan data menjadi aspek yang sangat penting untuk terus diselesaikan. Salah satu upaya yang dapat dilakukan dalam pengamanan data pada sistem informasi adalah dengen memanfaatkan teknik kriptografi. Tujuan dari penelitian ini adalah untuk dapat membuat suatu prototype model keamanan data pada suatu aplikasi yang berfungsi sebagai pengamanan suatu data atau informasi. Model keamanan yang dilakukan adalah dengan mengubah struktu pesan asli suatu data menjadi pesan yang disandikan menggunakan algoritma kriptografi dan mengembalikan pesan yang telah disandikan ke bentuk semula. Algoritma kriptografi yang dimanfaatkan dalam penelitian ini adalah kriptografi Data Encryption Standard (DES). Hasil dari pengujian aplikasi ini dapat diketahui bahwa model enkripsi dekripsi suatu data dapat dilakukan dengan baik antara lain file dengan format txt,rtf,dan doc.*

Kata Kunci: keamanan data, kriptografi Data Encryption Standard

I. PENDAHULUAN

Pertukaran data menjadi topik penting dalam perkembangan teknologi informasi saat ini. Teknologi berperan penting dalam membantu setiap pekerjaan diberbagai organisasi maupun pekerjaan pribadi, sehingga faktor keamanan menjadi sangat penting. Salah satu upaya yang dapat dilakukan dalam mengatasi masalah keamanan adalah dengan menggunakan teknik penyandian data yang disebut kriptografi.

Kriptografi merupakan teknik pengamanan data atau ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Rinaldi, 2008). Banyak sekali teknik kriptografi yang digunakan untuk proses enkripsi dan dekripsi pesan. Salah satu kriptografi ini adalah data encryption standard (DES). Metode DES merupakan algoritma kriptografi yang paling banyak digunakan. Kriptografi ini pertama kali di adopsi oleh National Institute of Standard and Technology (NIST) sebagai standar pengolahan informasi federal AS. Kriptografi DES ini membagi menjadi tiga kelompok, yaitu pemrosesan kunci, enkripsi data 64 bit, dan dekripsi 64 bit yang mana antar kelompok tersebut saling terintegrasi satu sama lainnya.

Faktor keamanan menjadi hal yang sulit untuk dipecahakan, dimana teknik kriptografi yang beredar saat ini sudah semakin banyak. Namun penggunaan kriptografi dalam teknologi informasi masih sangat sedikit sekali. Apalagi untuk pengguna yang belum mengetahui fungsi keamanan data sendiri.

Pada penelitian ini, kriptografi DES akan digunakan dalam membuat prototype keamanan dalam penyandian data tanpa membandingkan dengan algoritma lain yang dapat digunakan untuk tujuan yang sama. Sehingga tujuan dari penelitian ini adalah membuat prototype untuk memberikan keamanan pada data yang berformat rtf,txt, maupun doc dalam proses enkripsi dan dekripsi.

II. LANDASAN TEORI

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu Cryptós yang artinya " secret " (yang tersembunyi) dan gráphein yang artinya " writting " (tulisan). Jadi, kriptografi berarti " secret writting " (tulisan rahasia). Definisi yang dikemukakan oleh Bruce Schneier (1996), kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (Cryptography is the art and science of keeping messages secure). Selanjutnya menurut Menezes,dkk (1996) mengartikan Kriptografi adalah ilmu yang mempelajari teknik – teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data.

Kriptografi mempunyai sejarah yang panjang dan menakjubkan. Informasi yang lengkap mengenai sejarah kriptografi dapat ditemukan di dalam buku David Kahn yang berjudul The Codebreakers . Buku tersebut menulis secara rinci sejarah kriptografi, mulai dari penggunaan kriptografi oleh Bangsa Mesir 4000 tahun yang lalu (berupa hieroglyph pada piramid) hingga penggunaan kriptografi abad ke – 20 (Dony ,2009).

.

2.2 Data Encryption Standard (DES)

Data Encryption Standard (DES) merupakan salah satu algoritma kriptografi cipher block dengan ukuran blok 64bit dan ukuran kuncinya 56 bit. Algoritma DES dibuat di IBM, dan merupakan modifikasi daripada algoritma terdahulu yang bernama Lucifer. Lucifer merupakan algoritma cipher block yang beroperasi pada blok masukan 64 bit dan kuncinya beru kuran 128 bit (Rinaldi, 2008). Pengurangan jumlah bit kunci pada DES dilakukan dengan alasan agar mekanisme algoritma ini bisa diimplementasikan dalam satu chip. DES pertama kali dipublikasikan di Federal Register pada 17 Maret 1975. Setelah melalui banyak diskusi, akhirnya algortima DES diadopsi sebagai algoritma standar yang digunakan oleh NBS (National Bureau of Standards) pada 15 Januari 1977. Sejak saat itu, DES banyak digunakan pada dunia penyebaran informasi untuk melindungi data agar tidak bisa dibaca oleh orang lain.

2.2.1 Algoritma DES

Algoritma utama DES terbagi menjadi 3 kelompok, yaitu :

1. Pemrosesan Kunci

a. Meminta sebuah kunci 64-bit (8 karakter) dari pengguna. Setiap bit ke 8 digunakan sebagai *bit parity*.
b. Penjadwalan kunci rahasia (*secret key–scheduling*) dimaksudkan untuk menyusun 16 buah kunci yang akan dimasukkan pada setiap iterasi DES, baik pada enkripsi maupun dekripsi.
   1. Permutasi dilakukan pada kunci 64-bit. Pada tahapan ini, *bit-bit parity* tidak dilibatkan, sehingga bit kunci tereduksi menjadi 56-bit. Bit 1 pada kunci 56 merupakan bit 57 kunci awalnya, bit 2 adalah bit 49, dan seterusnya hingga bit 56 adalah bit 4 kunci 64. Hasil permutasi yang dikenal dengan nama *Permuted Choice* 1 (PC-1).
   2. Output PC-1 kemudian dibagi menjadi dua bagian. 28-bit pertama disebut C[0] dan 28-bit terakhir disebut D[0].
   3. Dari C[0] dan D[0] kemudian dihitung sub-sub kunci untuk setiap iterasi, yang dimulai dengan j = 1.
   4. Untuk setiap j, rotasi ke kiri sekali atau dua kali dijalankan pada C[j – 1] dan D[j –1] untuk mendapatkan C[j] dan D[j]. Tabel berikut menunjukkan step rotasi yang dilakukan pada setiap iterasi.
   5. Pada setiap hasil C[j]D[j], kunci untuk iterasi ke-j didapat dengan melakukan permutasi kembali pada C[j]D[j]. Permutasi tersebut dikenal dengan nama *Permuted Choice* 2 (PC-2).
   6. Iterasi dilakukan terus hingga ke-16 kunci berhasil disusun.

2. Enkripsi data 64-bit.

a. Ambil blok data 64-bit. Apabila blok data kurang dari 64-bit, maka penambahan harus dilakukan agar memadai untuk penggunaan.
b. Permutasi awal (*Initial Permutation*) dilakukan pada blok data tersebut.
c. Blok data dibagi menjadi dua bagian. 32-bit pertama disebut L[0] dan 32-bit kedua disebut R[0].
d. Ke-16 sub kunci dioperasikan dengan blok data, dimulai dengan j = 1, dengan cara :
   1. R[j – 1] dikembangkan menjadi 48-bit menurut fungsi pemilihan ekspansi berikut :
   2. E(R[j – 1]) di-XOR dengan K[j]
   3. Hasil E(R[j – 1]) XOR K[j] dipecah menjadi delapan blok 6-bit. Kelompok bit 1-6 disebut B[1], bit 7-12 disebut B[2], dan seterusnya bit 43-48 disebut B[8].
   4. Jumlah bit dikurangi dengan penukaran nilai-nilai yang ada dalam tabel S untuk setiap B[j]. Dimulai dengan j = 1, setiap nilai dalam tabel S memiliki 4 bit.
   a. Ambil bit ke 1 dan ke 6 dari B[j] bersama-sama menjadi nilai 2 bit. Misalkan m, yang menunjukkan baris dalam tabel S[j] .
   b. Ambil bit ke 2 hingga 5 dari B[j] sebagai nilai 4 bit, misalkan n, yang menunjukkan kolom dalam S[j].
   c. Hasil proses ini adalah S[j][m][n] untuk setiap B[j] sehingga iterasi yang diperlukan sebanyak 8 kali.
   5. Permutasi dilakukan kembali pada gabungan hasil substitusi di atas S[1][m1][n1] hingga S[8][m2][n2] dengan menggunakan tabel berikut :
   6. Hasil permutasi kemudian di XOR dengan L[j-1], selanjutnya hasil ini menjadi R[j]

$$R[i] = L[i-1]\ XOR\ P(S[1](B[1]\ldots S[8](B[8]))\ldots\ldots (1)$$

yang mana B[j] merupakan blok 6-bit hasil E(R[i-1]) XOR K[i]. Fungsi ini biasa ditulis pula sebagai

$$R[i] = L[i-1]\ XOR\ f(R[i-1], K[i]) \quad \ldots\ldots (2)$$

   7. $L[i] = R[i-1]$ .... (3)
   8. Loop kembali ke 4.a hingga K[16].

e. Permutasi akhir dilakukan kembali dengan tabel permutasi yang merupakan invers dari permutasi awal. Tabel ini disebut tabel permutasi akhir atau tabel inver permutasi awal (*IPinverse*).

3. Dekripsi data 64-bit.

Pada bagian sebelumnya telah diuraikan algoritma DES dalam mengenkrip satu blok data 64-bit. Untuk dekripsi, proses yang sama dilakukan kembali, hanya saja digunakan kunci K[j] dalam urutan yang berlawanan, yaitu memasukkan K[16] terlebih dahulu, kemudian K[16], seterusnya hingga K[1].

III. PEMBAHASAN

3.1 Analisis Kebutuhan Sistem

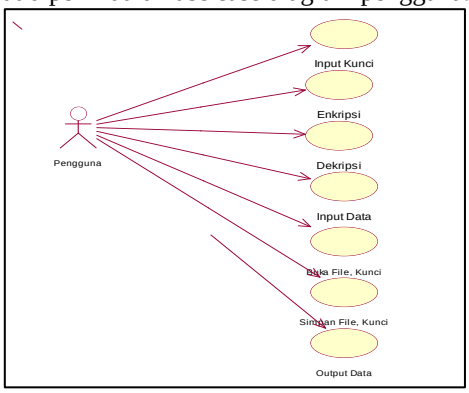
Menganalisis suatu kebutuhan merupakan

langkah awal dari suatu rangkaian sistem dimana letak keberhasilan dari suatu sistem sangat bergantung dari hasil analisa yang diharapkan. Dalam pembuatan sistem yang akan dilakukan adalah sebagai berikut:

a. Bagian Masukan Data (Input)
   Melakukan pemasukan data, data yang dimasukkan berupa abjad, angka, dan tanda baca yang nantinya akan dilakukan enkripsi maupun dekripsi pada bagian proses, data juga bisa berasal dari file yang sudah ada.
b. Bagian Proses
   Pada bagian ini data yang dimasukkan akan dilakukan proses sesuai pilihan yaitu enkripsi atau dekripsi untuk mendapatkan keluaran.
c. Bagian Keluaran (Output)
   Proses akan menghasilkan keluaran yaitu :
   1. Enkripsi (Plaintext menjadi Ciphertext)
   2. Dekripsi (Ciphertext menjadi Plaintext)

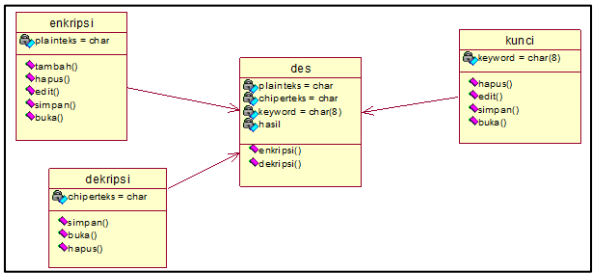
3.2 Analisa Perancangan Sistem

Pada analisis perancangan sistem yang akan dilakukan dalam penelitian ini yaitu menggunakan pemodelan Unified Modeling Language (UML). Berikut diperlihatkan use case diagram pengguna.



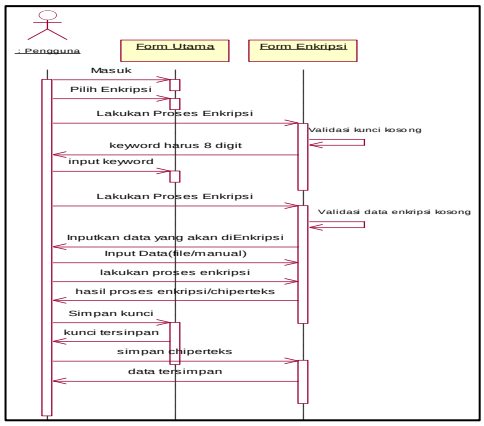
Gambar 1. Use Case Diagram

Pada Gambar tesebut terdapat beberapa proses yang dapat dilakukan oleh pengguna antara lain yaitu input kunci, enkripsi data, dekripsi data, input data, buka file kunci, simpan file kunci, dan output data. Sedangkan jika dilihat dengan menggunakan pemodelan class diagram seperti Gambar berikut:



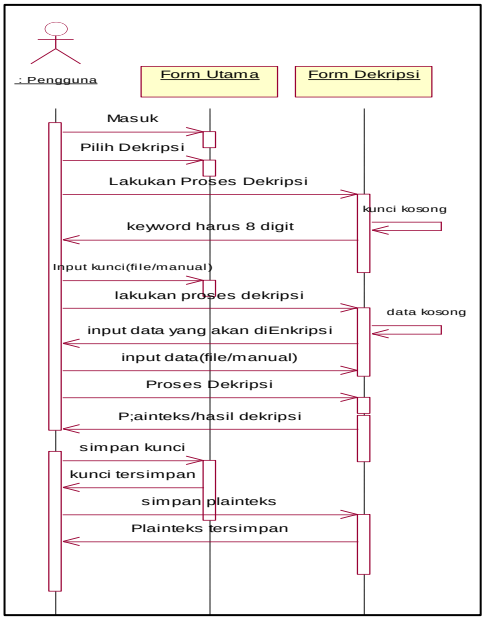
Gambar 2. Class Diagram

Dari gambar class diagram tersebut terdapat empat class yang digunakan yaitu class enkripsi, class dekripsi, class des, dan class kunci. Kemudian untuk alur proses proses enkripsi diperlihatkan pada Gambar berikut:



Gambar 3. Sequence Diagram pada Proses Enkripsi

Selanjutnya pada proses dekripsi diperlihatkan pada Gambar berikut.



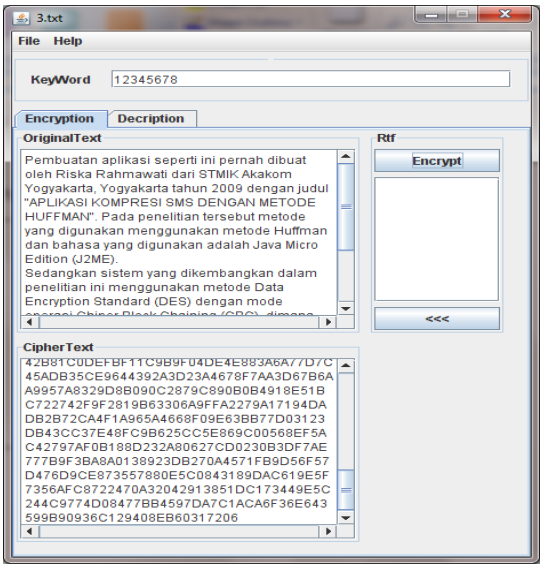
Gambar 4. Sequence Diagram pada Proses Dekripsi

3.3 Implementasi

Hasil implementasi dari prototype model keamanan data menggunakan kriptografi DES ini adalah suatu aplikasi yang dapat digunakan sebagai simulasi dari model keamanan data. Pada penelitian ini terdapat dua kelas penting yang berperan penting, yaitu kelas enkode dan kelas dekode. Kelas enkode digunakan untuk mendekodekan karakter yang dituliskan atau dari suatu file yang dibuka yang kemudian akan dilakukan proses enkrip menjadi bentuk pesan tersandikan (chipertext). Kemudian kelas dekode digunakan untuk mengembalikan karakter yang berupachipertext menjadi karakter asli (plaintext).

3.4. Simulasi Program Aplikasi

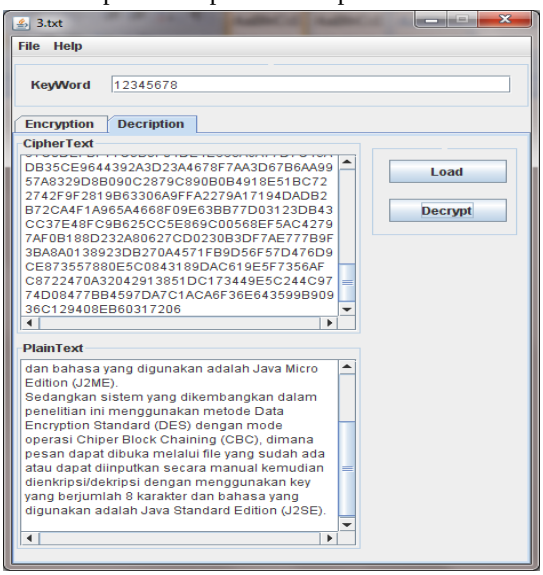
Berikut merupakan hasil dari tampilan aplikasi enkripsi dan dekripsi menggunakan algoritma kriptografi DES.



Gambar 5. Form Inputan Untuk Enkripsi Data

Pada form inputan untuk enkripsi data tersebut terdapat beberapa form inputan antara lain keyword yang digunakan sebagai input key, kemudian terdapat menu yang dapat digunakan sebagai inputan berupa file misalnya rtf maupun doc. Sedangkan untuk text atau txt dapat copy paste pada inputan original text.

Untuk proses dekripsi sendiri langkahnya sama dengan proses enkripsi yang membedakan adalah struktur tampilan, dimana proses inputan berupa chipertext atau file yang sudah terenkripsi sebelumnya. Berikut tampilan dari proses dekripsi.



Gambar 6. Form Inputan Untuk Dekripsi Data

IV. KESIMPULAN

Setiap makalah harus memiliki kesimpulan. Judul tambahan untuk ucapan terima kasih dapat diletakkan setelah bagian kesimpulan. Daftar referensi diletakkan paling akhir dan menggunakan nomor urut sesuai dengan dengan IEEE style.

DAFTAR REFERENSI

[1] A. Menezes, Paul C. van Oorcshot dan Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press. USA. 1996.

[2] A. Dony. Computer Security. Yogyakarta:Andi Offset.2005

[3] M. Rinaldi, Belajar Ilmu Kriptografi, Yogyakarta : Andi offset, 2008.

[4] S. Bruce. The Blowfish Encryption Algorithm -- one year Later. Dr. Dobb's Journal.1995.

Biodata Penulis

Ari Muzakir, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informasi Universitas Bina Darma Palembang, lulus tahun 2009. Memperoleh gelar Master of Computer Science (M.Cs) Program Pasca Sarjana Magister Ilmu Komputer Universitas Gadjah Mada Yogyakarta, lulus tahun 2012. Saat ini menjadi Dosen di Universitas Bina Darma Palembang.