Jurnal Sistem Informasi (JSI), VOL. 3, NO. 2, Oktober 2011, *Halaman 371-387*
ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index

Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma *Data Encryption Standard* (DES)

Rifkie Primartha
Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Sriwijaya
e-mail: rifkie_p@yahoo.co.id

ABSTRAK

Kriptografi adalah bidang ilmu untuk menjaga keamanan pesan (message). Kriptografi telah banyak diimplementasikan di banyak hal. Smart card, Anjungan Tunai Mandiri (ATM), Pay TV, Mobile Phone, dan Komputer adalah beberapa contoh produk teknologi yang menggunakan kriptografi untuk keamanannya. Cara kerjanya adalah dengan mengubah pesan asli yang dapat dimengerti/dibaca manusia (plainteks) ke bentuk lain yang tidak dapat dimengerti/dibaca oleh manusia (cipherteks). Proses transformasi plainteks menjadi chiperteks diistilahkan dengan enkripsi. Sedang proses pengembalian pesan chiperteks menjadi plainteks diistilahkan dengan dekripsi. Ada banyak algoritma kriptografi, dalam penelitian ini aplikasi kriotografi yang dikembangkan menggunakan algoritma simetri DES (Data Encryption Standard) dengan bahasa pemrograman Java. DES menggunakan sandi blok kunci simetrik dengan ukuran blok 64-bit dan ukuran kunci 56-bit.

Kata Kunci: Plainteks, Chiperteks, Kriptografi, Enkripsi, Dekripsi.

1. PENDAHULUAN

Kemajuan teknologi internet sebagai media penghantar informasi telah diadopsi oleh hampir semua orang dewasa ini. Dimana informasi telah menjadi sesuatu yang sangat berharga. Bagi pelaku usaha, informasi bisa dianggap sebagai senjata untuk meningkatkan daya saing. Bagi militer, informasi bisa menjadi penentu kemenangan dalam perang. Bagi para wartawan, informasi menjadi sesuatu yang memiliki daya jual yang sangat mahal. Bagi perorangan, informasi menjadi sesuatu yang sangat pribadi. Bahkan informasi pun dapat menjadi alat untuk mempengaruhi perpolitikan bagi suatu negara.

Karena begitu berharganya suatu informasi, maka informasi telah menjadi target serangan oleh para *cracker*. Karenanya, keamanan suatu informasi menjadi sesuatu yang harus dijaga dengan baik. Pengamanan informasi pada prinsipnya berfungsi untuk melindungi informasi agar siapapun yang tidak berhak tidak dapat membaca, mengubahnya, atau menghapus informasi tersebut.

Begitu banyak kasus penyadapan terhadap suatu informasi telah membuat para peneliti berfikir keras untuk mengamankannya. Salah satu bidang ilmu untuk menjaga keamanan informasi adalah kriptografi. Dengan kriptografi, informasi yang dianggap

ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index

rahasia dapat disembunyikan dengan teknik penyandian, sehingga tidak dimengerti oleh orang lain, selain oleh pembuat dan penerimanya saja.

Banyak sekali jenis algoritma kriptografi, diantaranya adalah algoritma *Data Encryption Standard* (DES). Algoritma ini termasuk jenis simetri yang disebut juga sebagai algoritma konvensional, yaitu algoritma yang menggunakan kunci enkripsi dan kunci dekripsi yang sama.

M. Yuli Andri meneliti tentang implementasi algoritma kriptografi DES pada berkas *digital* (M. Yuli Andri, 2009). Irjatul Wardah meneliti tentang kriptografi algoritma DES untuk *image* yang dikirim menggunakan *telephone seluler* (Irjatul dan Wardah, 2010). Indra Syahputra meneliti tentang simulasi keamanan informasi menggunakan kriptografi algoritma DES (Indra Syahputra, 2009). William Mehuron meneliti tentang penggunaan algoritma DES dan Triple Data Encryption Algorithm (TDEA) untuk melindungi data rahasia (*Federal Information Processing Standars Publication, U.S. Department of Commerce/National Institute of Standars and Technology*, DES, 1999).

Pada penelitian-penelitian sebelumnya, penerapan algoritma DES baru menggunakan bahasa pemrograman C dan Pascal (Delphi). Adapun tujuan dari penelitian ini adalah mendesain dan membuat suatu aplikasi yang dapat melakukan penyandian (enkrip dan dekrip) menggunakan bahasa pemrograman Java. Harapannya, *software* tersebut dapat bermanfaat dalam mengamankan suatu informasi.

2. KONSEP ENKRIPSI dan DEKRIPSI

Salah satu mekanisme untuk meningkatkan keamanan adalah dengan menggunakan teknologi enkripsi. Data-data yang dikirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Jadi enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah **enkripsi** (*encryption*) **(Budi Raharjo, 2002)**. *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Terminologi yang lebih tepat digunakan adalah "*encipher*". Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut **dekripsi** (*decryption*). Terminologi yang lebih tepat untuk proses ini adalah "*decipher*".

Berdasarkan cara memproses teks (*plaintext*), *cipher* dapat dikategorikan menjadi dua jenis: *block cipher* and *stream cipher*. *Block cipher* bekerja dengan memproses data secara blok, dimana beberapa karakter/data digabungkan menjadi satu blok. Setiap proses satu blok menghasilkan keluaran satu blok juga. Sementara itu stream cipher bekerja

ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index

memproses masukan (karakter atau data) secara terus menerus dan menghasilkan data pada saat yang bersamaan.

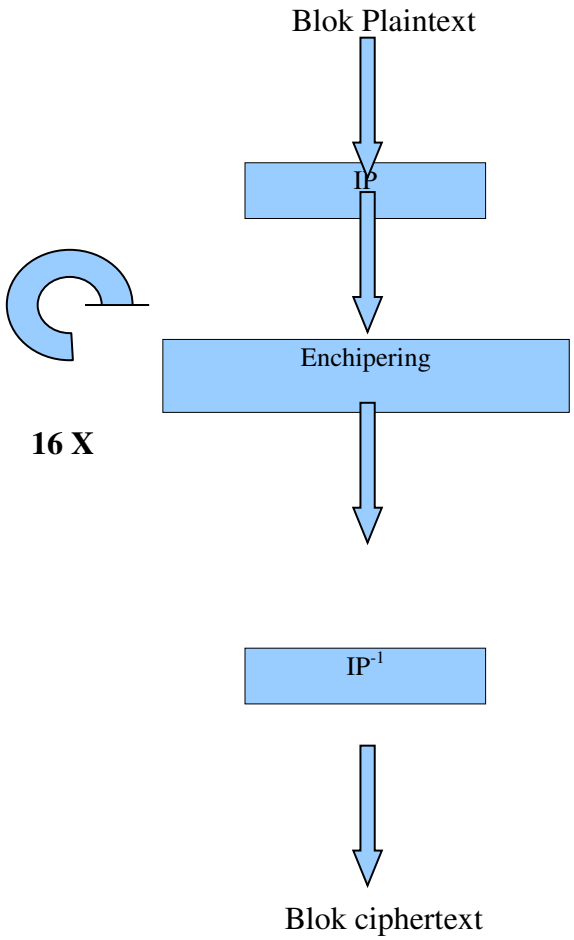
Banyak layanan di internet yang masih menggunakan "*plain text*" untuk *authentication*, seperti penggunaan pasangan userid dan password. Informasi ini dapat dilihat dengan mudah oleh program penyadap atau pengendus (*sniffer*).

Contoh layanan yang menggunakan *plaintext* antara lain:

- akses jarak jauh dengan menggunakan telnet dan rlogin
- transfer *file* dengan menggunakan FTP
- akses *email* melalui POP3 dan IMAP4
- pengiriman *email* melalui SMTP
- akses *web* melalui HTTP

Algoritma Enkripsi DES

Algoritma DES merupakan algoritma enkripsi yang paling banyak digunakan di dunia yang diadopsi oleh NIST (National Institue of Standards and Technology) sebagai standar pengolah informasi Federal AS. Data *plaintext* dienkrip dalam blok-blok 64 bit menjadi 64 bit data *ciphertext* menggunakan kunci 56 bit kunci internal (*internal key*). DES mentransformasikan input 64 bit dalam beberapa tahap enkripsi ke dalam output 64 bit. Dengan demikian, DES termasuk *block cipher*. Dengan tahapan dan kunci yang sama, DES digunakan untuk membalik enkripsi. Kunci internal pada algoritma DES dibangkitkan dari kunci eksternal (*external key*) 64 bit. Skema global dari proses algoritma DES dapat dilihat pada gambar 1.

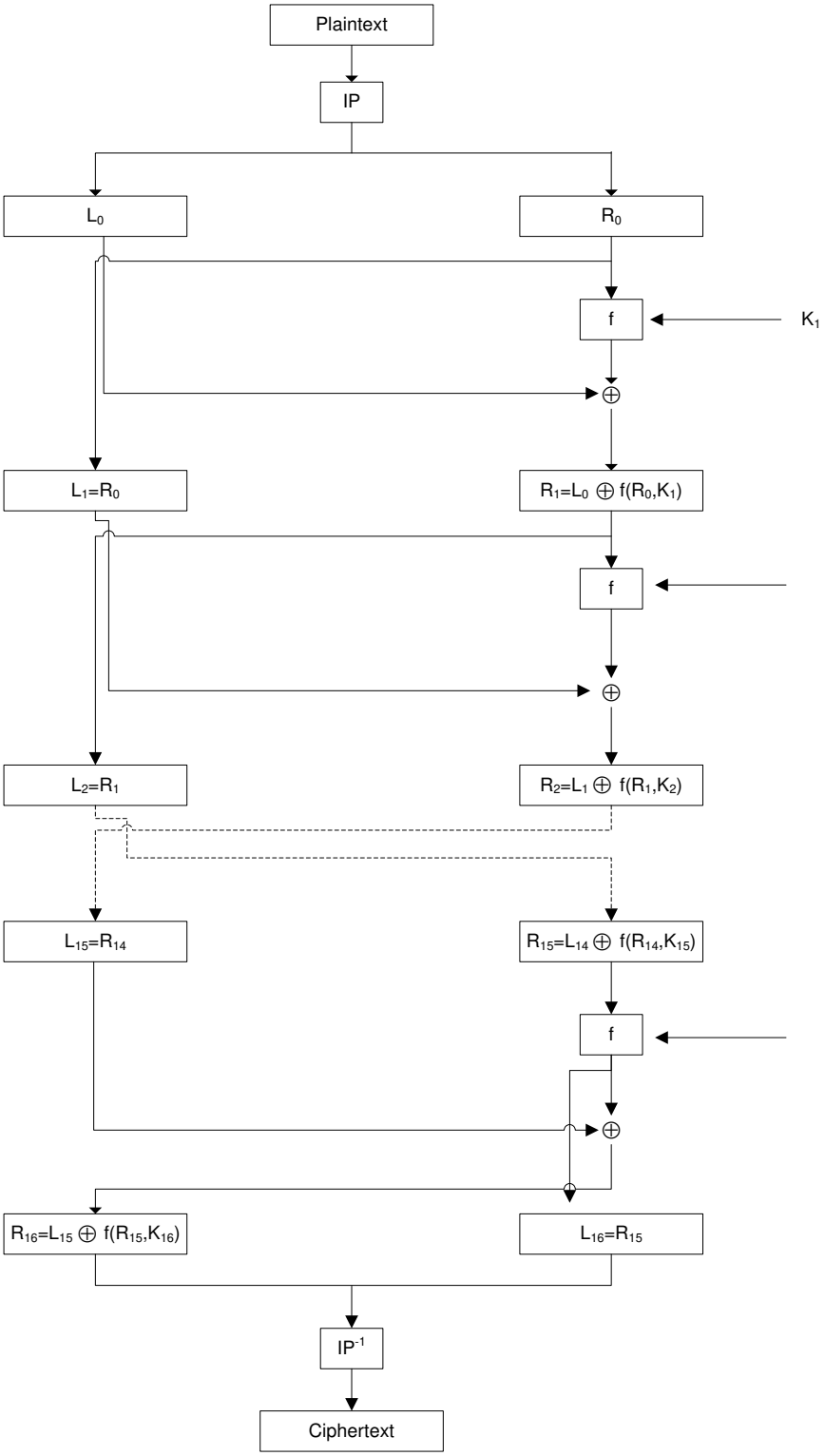


Gambar 1. Skema Global Algoritma DES (M. Yuli Andri, 2009)

6.1. Skema global dari algoritma DES adalah sebagai berikut:

1. Blok *plaintext* dipermutasi dengan matriks permutasi awal (initial permutation atau IP).
2. Hasil permutasi awal kemudian di enchipering sebanyak 16 kali putaran. Setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil *enchipering* kemudian dipermutasi dengan matriks permutasi balikan (*invers initial permutation* atau IP^{-1}) menjadi blok *chipertext*.
4. Skema algoritma DES dapat dilihat pada gambar 2.

ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index



Gambar 2. Skema Dasar Algoritma DES (M. Yuli Andri, 2009)

ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index

Dalam algoritma DES, terdapat kunci eksternal dan kunci internal. Kunci internal dibangkitkan dari kunci eksternal yang diberikan oleh pengguna. Kunci internal dapat dibangkitkan sebelum proses enkripsi ataupun bersamaan dengan proses enkripsi. Kunci eksternal panjangnya 64 bit atau 8 karakter. Karena ada 16 putaran, maka kunci internal yang dibutuhkan sebanyak 16 buah, yaitu K_1, K_2, ..., K_{16}. Untuk mengaitkan kunci internal diperlukan beberapa langkah.

Kunci eksternal 64 bit, dikompresi terlebih dahulu menjadi 54 bit menggunakan matriks permutasi kompresi PC-1. Dalam permutasi tiap bit ke-8 dari 8 *byte* kunci akan diabaikan. Sehingga akan ada penggunaan 8 bit dari 64 bit awal kunci eksternal.

Setelah didapatkan 56 bit hasil permutasi, selanjutnya 56 bit ini akan dibagi menjadi 2 bagian, kiri dan kanan, yang masing-masing panjangnya 28 bit. Lalu ke-2 bagian tersebut akan disimpan ke dalam C_0 dan D_0.

C_0 : berisi bit-bit dari K pada posisi :

57, 49, 41, 33, 25, 17, 9, 1, 58, 50, 42, 34, 26, 18
10, 2, 59, 51, 43, 35, 27, 19,11, 3, 60, 52, 44, 36

D_0 : berisi bit-bit dari K pada posisi :

63, 55, 47, 39, 31, 23, 15, 7, 62, 54, 46, 38, 30, 22
14, 6, 61, 53, 45, 37, 29, 21, 21, 13, 5, 28, 20, 12

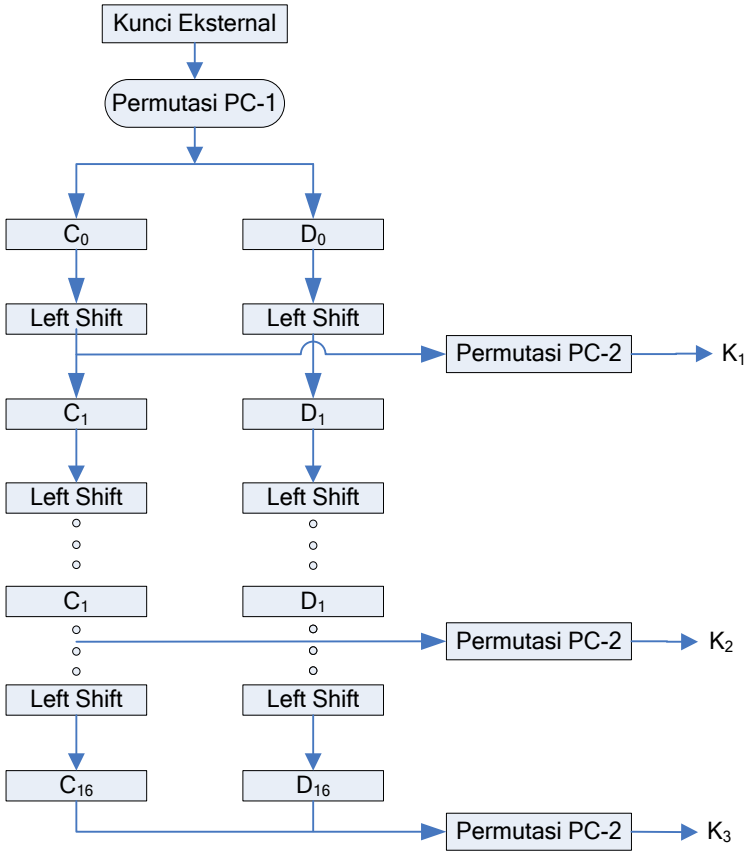
Proses selanjutnya adalah ke-2 bagian (C_0 dan D_0) digeser ke kiri (*left shift*) sepanjang 1 atau 2 bit, tergantung pada tiap putaran. Perputaran ini bersifat *wrapping* atau *round-shift*.

Hasil dari pergeseran C_0 dan D_0 akan didapatkan nilai dari C_1 dan C_2. Begitu seterusnya, hingga proses tersebut menghasilkan C_{16} dan D_{16}. Untuk mendapatkan kunci internal pertama (K_1), maka bit dari C_0 dan D_0 tadi dilakukan permutasi kompresi dengan menggunakan matriks PC-2.

Jadi setiap kunci K_i, mempunyai panjang 48 bit. Apabila proses pergeseran bit-bit dijumlahkan semuanya, maka jumlah seluruhnya sama dengan 28 putaran. Jumlah ini sama dengan jumlah bit pada C_i dan D_i. Oleh karena itu, setelah putaran ke-16 akan didapatkan

ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index

kembali $C_{16} = C_0$ dan $D_{16} = D_0$. Gambar 3 akan memperlihatkan bagaimana cara pembangkitan kunci internal pada algoritma DES.



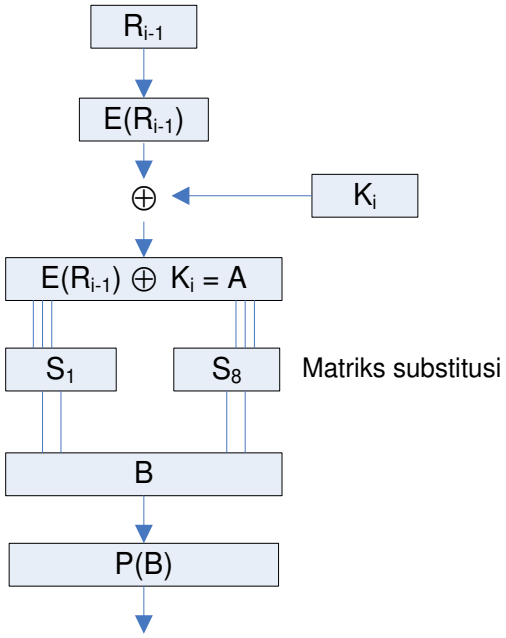
Gambar 3. Proses Pembangkitan Kunci Internal Pada Algoritma DES (M. Yuli Andri, 2009)

Proses *enciphering* terhadap blok *plaintext* dilakukan setelah permutasi awal. Setiap blok *plaintext* mengalami 16 kali putaran *enciphering*. Setiap putaran *enciphering* secara matematis dinyatakan sebagai:

$$L_i = R_{i-1} \quad (2.1)$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \quad (2.2)$$

Diagram fungsi *f* diperlihatkan pada gambar 4.



Gambar 4. Rincian Komputasi Fungsi f (M. Yuli Andri, 2009)

E merupakan fungsi ekspansi yang memperluas blok R_{i-1} yang mempunyai panjang 32 bit menjadi blok 48 bit.

Hasil ekspansi *E(Ri-1)*, yang panjangnya 48 bit di-XOR-kan dengan K_i yang panjangnya 48 bit menghasilkan vektor A yang panjangnya juga 48 bit. Kemudian vektor A dikelompokkan menjadi 8 bagian, yang masing-masing bagian berisi 6 bit, dan merupakan masukkan dari proses substitusi.

Proses substitusi menggunakan 8 buah kotak-S (*S-box*). Kotak-S adalah matriks yang berisi substitusi sederhana yang memetakan satu atau lebih bit dengan satu atau lebih bit lainnya.

Dalam algoritma DES kotak-S yang digunakan adalah 6x4 *S-box* yang berarti menerima masukkan 6 bit dan menghasilkan keluaran 4 bit. Kelompok 6 bit pertama menggunakan S_1, kelompok 6 bit berikutnya menambahkan S_2 dan seterusnya sampai menggunakan S_8, sehingga secara keseluruhan akan menghasilkan 32 bit keluaran yang dinamakan dengan vektor B.

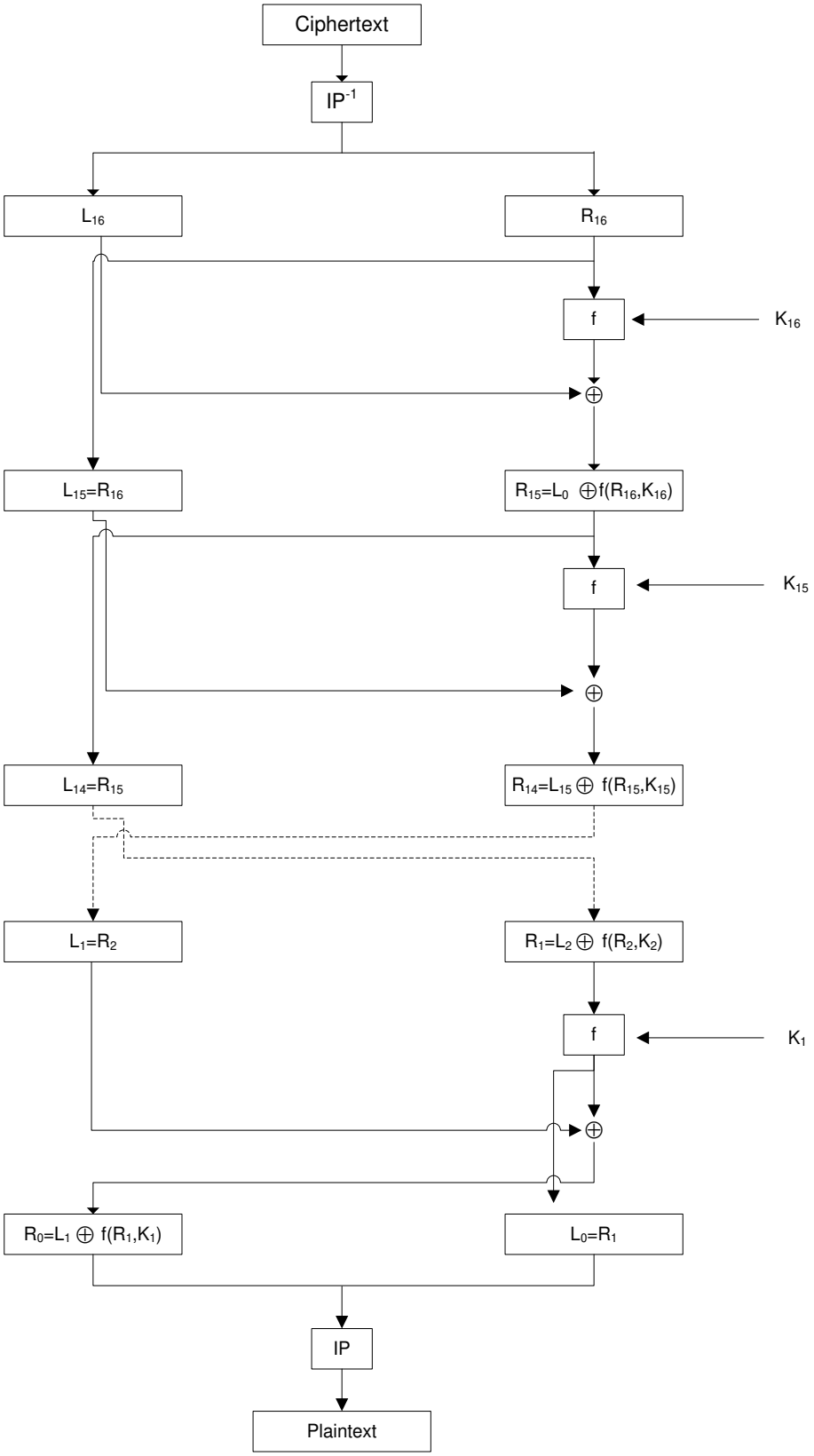
Setelah didapat vektor B, maka selanjutnya pada vektor B dilakukan proses permutasi, yang bertujuan untuk mengacak hasil proses substitusi kotak-S. Permutasi dilakukan dengan menggunakan matriks permutasi P *(P-box)*. Keluarannya menghasilkan *P(B)* yang juga merupakan keluaran dari fungsi *f*. Proses selanjutnya yaitu bit-bit *P(B)* di-XOR-kan dengan L_{i-1} untuk mendapatkan R_i.

ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index

Proses selanjutnya yaitu permutasi terakhir yang dilakukan setalah 16 kali putaran terhadap gabungan dari blok kiri (*L*) dan blok kanan (*R*). Proses permutasi dilakukan dengan menggunakan matriks permutasi balikan (invers initial permutation) atau IP^{-1}.

Algoritma Dekripsi DES

Pada algoritma DES proses dekripsi dan enkripsinya menggunakan kunci yang sama. Proses dekripsi pada ciphertext merupakan proses kebalikan dari proses enkripsi. Jika pada proses enkripsi urutan kunci yang digunakan adalah K1, K2, …, K16, maka untuk proses dekripsi urutan kunci yang digunakan adalah K16, K15, …, K1. Masukkan awalnya adalah R16 dan L16 untuk deciphering. Blok R16 dan L16 diperoleh dengan mempermutasikan ciphertext dengan matriks permutasi IP-1. Skema proses dekripsi diperlihatkan pada gambar 5.



Gambar 5. Skema Dasar Proses Dekripsi Algoritma DES (M. Yuli Andri, 2009)

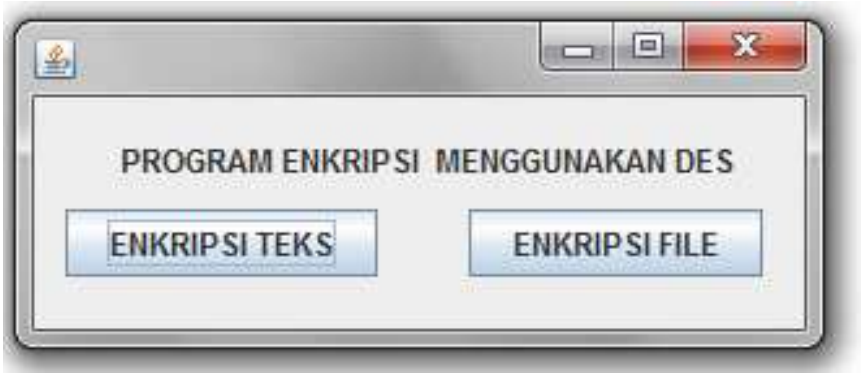
ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index

3. PERANCANGAN PERANGKAT LUNAK

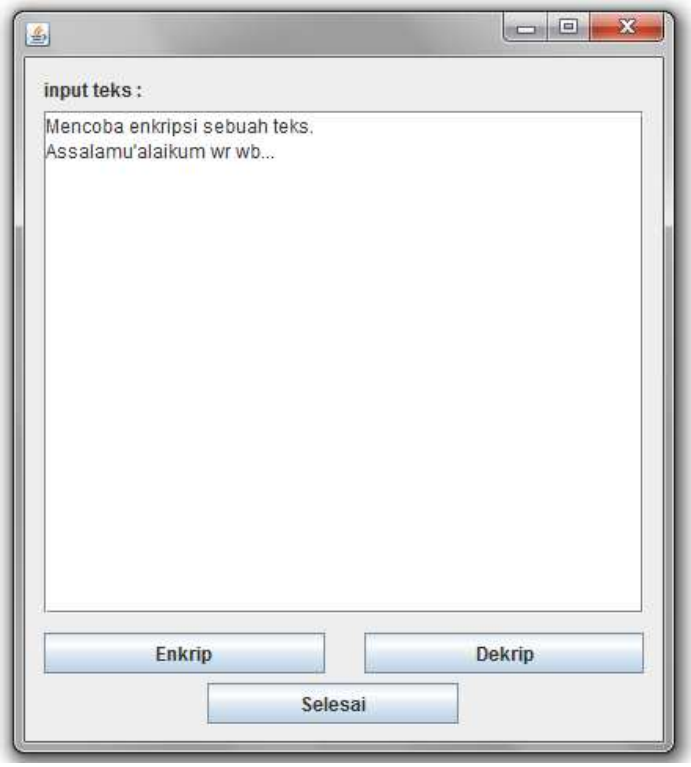
Pada perancangan ini terdiri dari perancangan desain antar muka perangkat lunak dan perancangan kode program perangkat lunak. Perancangan desain antar muka dimaksudkan agar user diberikan kemudahan dalam menggunakan perangkat lunak dalam melakukan enkripsi dan dekripsi pesan baik berupa teks maupun berupa file.

Adapun perancangan kode program adalah melakukan konversi algoritma DES ke dalam bahasa pemrograman Java.

Gambar Perancangan Antar Muka Perangkat Lunak

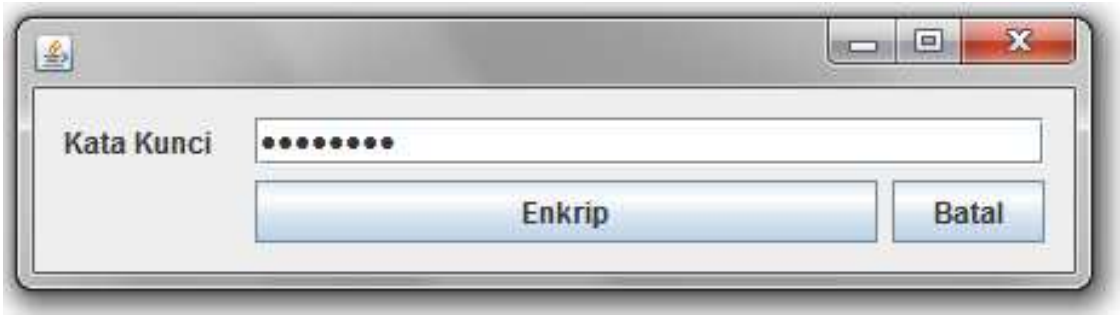


Gambar 6. Menu Utama Aplikasi

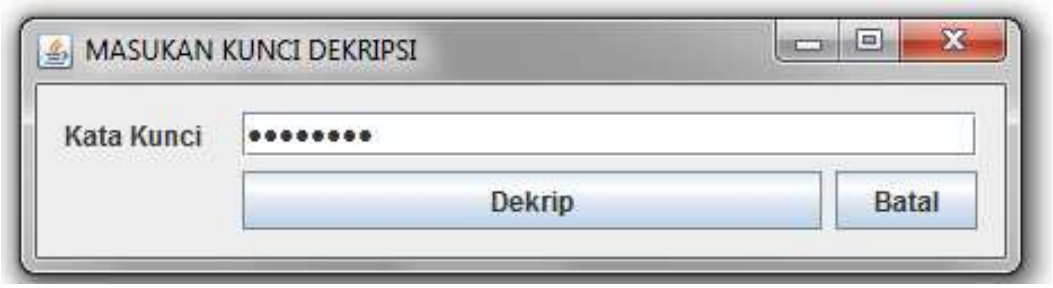


Gambar 7. Antar Muka Enkripsi Teks

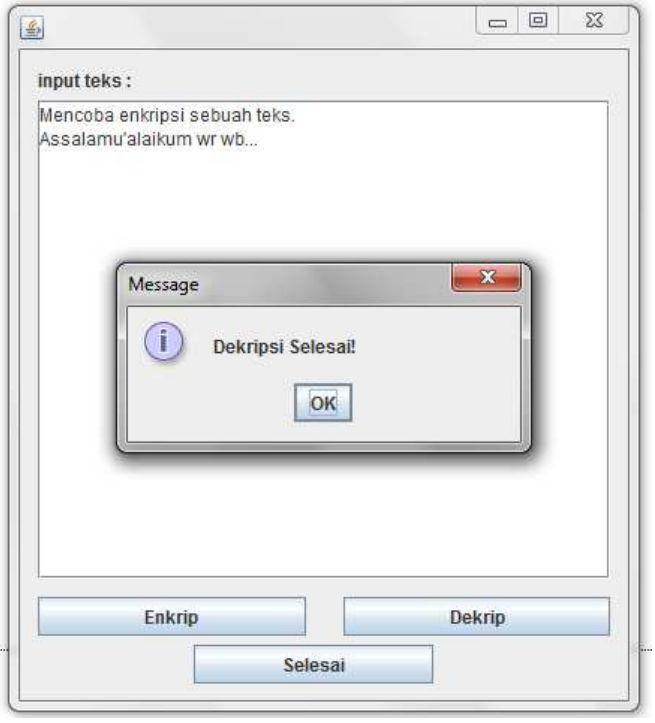
ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index



Gambar 8. Antar Muka Input Password



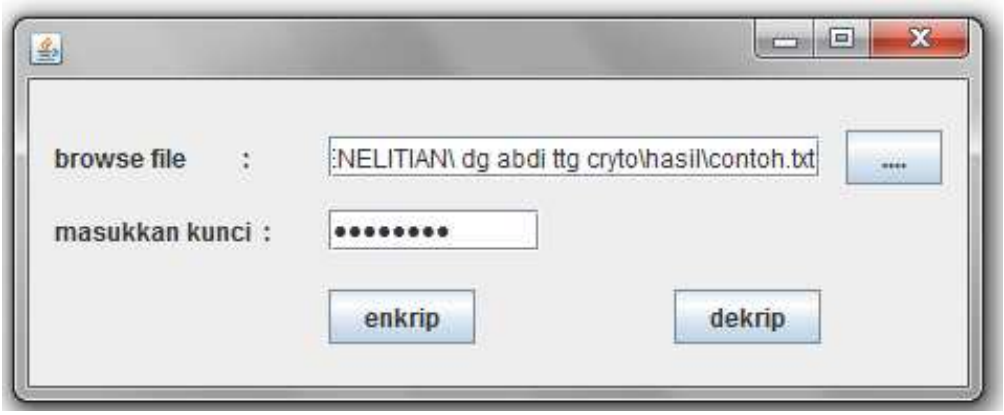
Gambar 9. Antar Muka Dekripsi



Gambar 10. Antar Muka Hasil Dekripsi Teks

ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index

Gambar 11. Antar Muka Enkripsi File

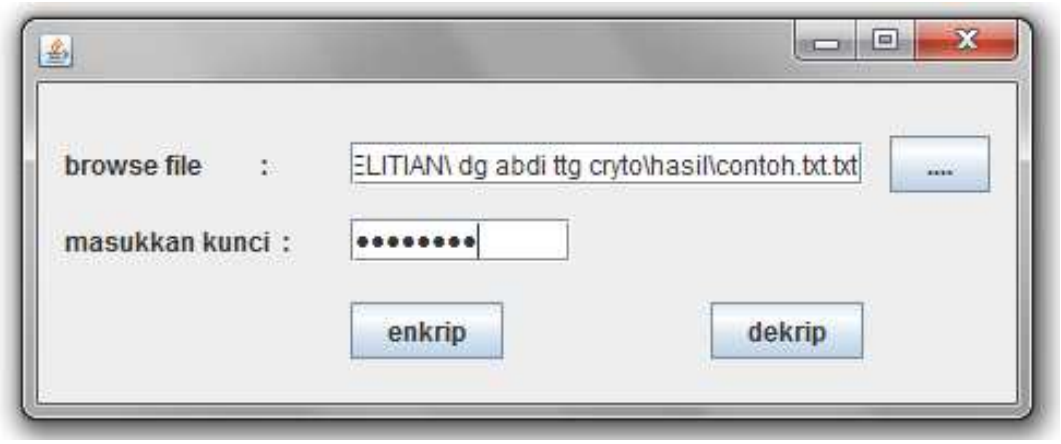


Gambar 12. Lokasi File dan Password untuk enkripsi file

Gambar 13. Antar Muka hasil Enkripsi File

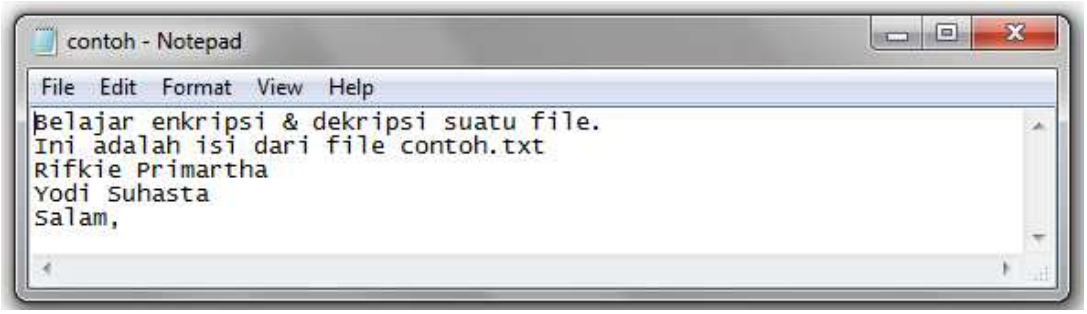
ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index

Gambar 14. File yang telah dienkripsi tidak dapat dibaca



Gambar 15. Antar Muka Dekripsi File

Gambar 16. Antar Muka Hasil Dekripsi File



Gambar 17. File yang telah di dekrip dapat dibaca kembali

ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index

4. HASIL dan PEMBAHASAN

Hasil dari penelitian ini adalah berupa suatu aplikasi perangkat lunak yang dibangun dengan bahasa pemrograman Java yang bertujuan untuk melakukan enkripsi serta dekripsi suatu informasi berbentuk file maupun teks sederhana.

Pengujian pertama, melakukan enkripsi dan dekripsi sebuah teks.

Data berupa teks diketikkan di tempat input teks, setelah itu klik tombol Enkrip. Selanjutnya muncul tampilan untuk memasukkan password enkripsi.

Data teks yang telah dienkripsi menghasilkan karakter-karakter acak yang tidak dapat dibaca/dimengerti.

Selanjutnya, akan dilakukan proses pengembalian/dekripsi agar karakter-karakter acak tersebut kembali seperti semula. Setelah klik tombol dekripsi, lalu memasukkan password yang sama saat melakukan enkripsi maka data teks kembali seperti bentuk aslinya dan dapat dibaca.

Pengujian kedua, melakukan enkripsi-dekripsi data berbentuk file.

Melakukan pencarian lokasi file yang hendak dienkripsi. Setelah file ditemukan, maka masukkan password. Lalu tekan tombol enkrip.

Sama seperti proses enkripsi-dekripsi teks, pada proses enkripsi-dekripsi File pun diminta untuk memasukkan password.

Pada saat melakukan dekripsi suatu file, lokasi (path) file yang telah dienkripsi harus diketahui oleh aplikasi. Setelah itu akan diminta untuk memasukkan password yang sama ketika melakukan enkripsi. Data file yang telah didekripsi akan kembali seperti aslinya.

5. KESIMPULAN DAN SARAN

5.1. KESIMPULAN

Dari penelitian ini didapatkanlah beberapa kesimpulan, antara lain:

- Dengan adanya aplikasi kriptografi yang dikembangkan berdasarkan algoritma DES, maka data-data penting dapat diamankan (dienkripsi) ketika hendak dikirim melalui media internet.
- Proses enkripsi dan dekripsi file maupun teks, pada prinsipnya memiliki mekanisme proses yang sama.

- Waktu yang dibutuhkan untuk melakukan enkripsi maupun dekripsi file/teks sederhana adalah relatif sama.

5.2. SARAN

Penelitian yang telah dilakukan baru membuat suatu aplikasi kriptografi DES menggunakan bahasa pemrograman Java. Perlu dilakukan penelitian untuk membuat aplikasi berdasarkan algoritma kriptografi DES menggunakan bahasa pemrograman yang berbeda. Bahasa C, C++ atau Pascal dirasa perlu untuk dicoba mengingat masing-masing bahasa pemrograman memiliki karakteristik serta kelebihannya masing-masing.

Antar muka aplikasi ini masih sangat standar, diharapkan pada penelitian selanjutnya dapat dibuat antar muka aplikasi yang lebih menarik dibanding yang sekarang.

6. DAFTAR PUSTAKA

Abd Rahim Mat Sidek Dan Ahmad Zuri Sha'ameri, "*Comparison Analysis Of Stream Cipher Algorithms For Digital Communication*", Jurnal Teknologi, Universitas Teknologi Malaysia, 2007.

Andri, M Yuli, "Implementasi Algoritma Kriptografi DES, RSA dan Algoritma Kompresi LZW pada Berkas Digital", Skripsi, Universitas Sumatera Utara, 2009.

Andrizal, "Algoritma Enkripsi Rivest Code 5 (RC-5)", Journal Teknik Elektro ITB, Bandung, 2010.

Budi Rahardjo," Keamanan Sistem informasi Berbasis Internet", PT Insan Komunikasi Indonesia, Bandung, 2002.

E. Biham and A. Biryukov, "*An Improvement of Davies' Attack on DES*," *Journal of Cryptology*, vol. 10, no. 3, pp. 195–206, 1997.

Federal Information Processing Standards Publication, U.S. Department of Commerce/National Institute of Standards and Technology, *Data Encryption Standard* (DES), October 1999.

L. R. Knudsen and J. E. Mathiassen, "*A chosen-plaintext linear attack on* DES," in Fast Software Encryption, FSE 2000 (B. Schneier, ed.), vol. 1978 of Lecture Notes in Computer Science, pp. 262–272, Springer-Verlag, 2001.

ISSN Print : 2085-1588
ISSN Online : 2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index

Syahputra, Indra, "Simulasi Kerahasiaan/Keamanan Informasi dengan Menggunakan Algoritma *Data Encryption Standard* (DES)", Skripsi, Universitas Sumatera Utara, 2009.

Wardah, Irjatul, "Kriptografi Pengiriman Image pada *Telephone* Seluler Menggunakan Algoritma DES", Skripsi, UIN Maulana Malik Ibrahim, Malang, 2010.