Journal of Information System, Informatics and Computing

Vol.4 No.1 bulan Juni 2020
e-ISSN : 2597-3673 *(Online)*
p-ISSN : 2579-5201 *(Printed)*

PENGAMANAN DATA FILE DOCUMENT MENGUNAKAN KRIPTOGRAFI ENCRYPTION SYSTEM (DES)

Nayuni Dwitri[1], Sukma Sindi[2], Irma Agustika Sihombing[3],Indra Gunawan[4]
Program Studi Teknik Informatika
STIKOM Tunas Bangsa Pematangsiantar
nayunidwitri997@gmail.com[1], skmsindi@gmail.com[2], irmasihombing006@gmail.com[3],indra@amiktunasbangsa.ac.id[4]

Abstrak

Banyak kasus penyadapan terhadap suatu informasi telah membuat para peneliti berpikir keras untuk mengamankan suatu data,dengan kriptografi informasi yang dianggap rahasia dapat disembunyikan dengan teknik penyandian,sehingga tidak dimengerti oleh oranglain atau pihak ketiga selain pengirim dan penerima yang dituju.Dengan mengunakan konsep Enkripsi dan Deskripsi,dimana *plaintext* yang dikirim dapat diubah terlebih dahulu menjadi *ciphertext.* Data *plaintext* dienkripsi 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.Pada penelitian ini dilakukan dengan melakukan proses enkripsi pada suatu file mengunakan cara kerja Algoritma Data Encryption Sistem (DES).Hasil dari penelitian ini adalah dapat mengamankan data dan keaslian dokumen tersebut

Kata Kunci: Kriptografi , Enkripsi , Deskripsi , Algoritma DES

I. PENDAHULUAN

Pada masa modern seperti sekarang,teknologi komputer sangat diperlukan oleh kehidupan manusia dalam urusan personal maupun kelompok.Oleh karena itu,dibuatlah sebuah keamanan bagi seluruh aspek – aspek terutama informasi dan data untuk menjaga kerahasian informasi tersebut.Dari keamanan tersebut ,timbullah sebuah tuntutan akan tersediannya suatu sistem pengamanan data yang lebih baik agar dapat melindungi informasi dari segala jenis serangan.Ini merupakan alasaan perkembangan suatu sistem pengamanan data yang berfungsi untuk melindungi data yang ditransmisikan melalui suatu jaringan perkomunikasian.

Banyak kasus penyadapan terhadap suatu informasi telah membuat para peneliti berpikir keras untuk mengamankan suatu data,dengan kriptografi informasi yang dianggap rahasia dapat disembunyikan dengan teknik penyandian,sehingga tidak dimengerti oleh oranglain atau pihak ketiga selain pengirim dan penerma yang dituju.[1]

Untuk menghindari kemungkinan data yang diserang dapat langsung dibaca oleh penyerang maka data yang dikirim diacak dengan mengunakan metode penyandian tertentu sehingga pesan atau data yang terkandung dalam suatu data yang dikirim menjadi lebih aman dan terjamin keasliannya.

II. LITERATUR DAN METODE

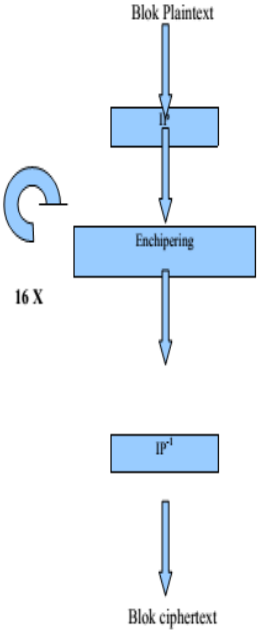
Salah satu cara untuk meningkatkan keamanan adalah mengunakan metode enkripsi.Data yang dikirim diubah sedemikian rupa hingga tidak mudah diserang.Sehingga dapat disimpulkan enkripsi adalah proses pengamanan data yang berupa *plaintext* (pesan asli) menjadi *ciphertext* (pesan tersandi)

Banyak layanan di internet yang masih menggunakan *plain text* untuk *authentication*, seperti penggunaan pasangan user id dan password. Informasi ini dapat dilihat dengan mudah oleh program penyadap.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

Ciphertext adalah pesan yang sudah tidak dapat dipahami lagi dengan mudah.Sedangkan sebaliknya,untuk mengubah *ciphertext* menjadi *plaintext* disebut dengan deskripsi.

Journal of Information System, Informatics and Computing
Vol.4 No.1 bulan Juni 2020
e-ISSN : 2597-3673 *(Online)*
p-ISSN : 2579-5201 *(Printed)*



Gambar 1 , Proses Enkripsi

Berdasarkan cara memproses *plaintext*,penyandian dapat dibagi menjadi 2 yaitu:

1) *Block cipher*,bekerja dengan memproses data secara blok,dimana beberapa data digabungkan menjadi satu blok.Dan hasil yang didapat menghasilkan satu blok pula.
2) *Stream cipher*,bekerjadengan memasukkan data secara terus menerus dan menghasilkan data padaa saat yang bersamaaan

III. METODE

Algoritma DES merupakan algoritma enkripsi yang paling banyak digunakan di dunia yaang diadopsi oleh NIST (National Institue of Standards and Technology) sebagai standar pengolah informasi Federal AS.

Data plaintext dienkripsi 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

Enkripsi

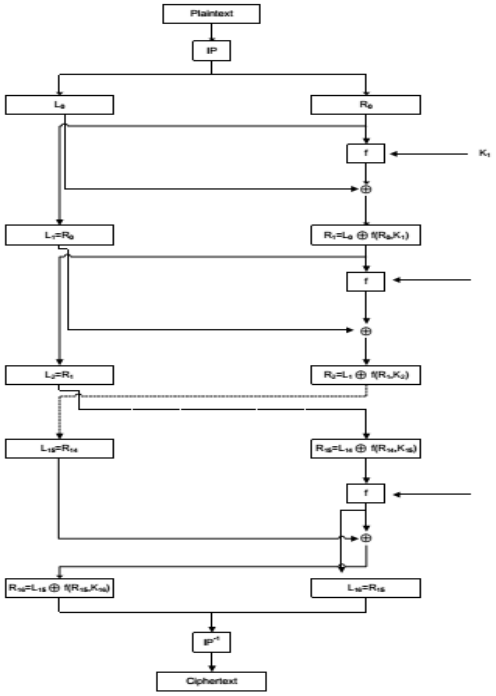
Skema global dari algoritma DES adalah sebagai berikut:

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.



Gambar 2. Skema Algoritma DES

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.

Journal of Information System, Informatics and Computing
Vol.4 No.1 bulan Juni 2020
e-ISSN : 2597-3673 *(Online)*
p-ISSN : 2579-5201 *(Printed)*

Kunci eksternal panjangnya 64 bit atau 8 karakter. Karena ada 16 putaran, maka kunci internal yang dibutuhkan sebanyak 16 buah, yaitu K1, K2, ..., K16.

Mengaitkan kunci internal diperlukan beberapa langkah.

1. Kunci eksternal 64 bit, dikompresi terlebih dahulu menjadi 54 bit menggunakan matriks permutasi kompresi PC-1.
2. Dalam permutasi tiap bit ke-8 dari 8 *byte* kunci akan diabaikan. Sehingga akan ada penggunaan 8 bit dari 64 bit awal kunci eksternal.
3. Setelah didapatkan 56 bit hasil permutasi, selanjutnya 56 bit ini akan dibagi menjadi 2 bagian, kiri dan kanan, yang masing-masing panjangnya 28 bit.
4. Lalu ke-2 bagian tersebut akan disimpan ke dalam C0 dan D0.

C0 : 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

D0 ***: berisi bit-bit dari K pada posisi :***

63, 55, 47, 39, 31, 23, 15, 7, 62, 54, 46, 38, 30, 22

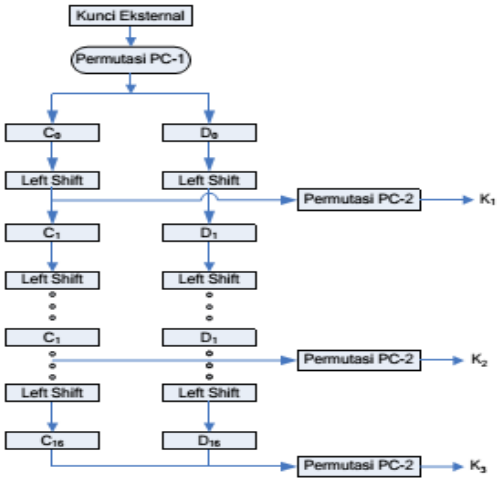
14, 6, 61, 53, 45, 37, 29, 21, 21, 13, 5, 28, 20, 12

5. Proses selanjutnya adalah ke-2 bagian (C0 dan D0) digeser ke kiri (*left shift*) sepanjang 1 atau 2 bit, tergantung pada tiap putaran. Perputaran ini bersifat *wrapping* atau *round-shift*.
6. Hasil dari pergeseran C0 dan D0 akan didapatkan nilai dari C1 dan C2. Begitu seterusnya, hingga proses tersebut menghasilkan C16 dan D16.
7. Untuk mendapatkan kunci internal pertama (K1), maka bit dari C0 dan D0 tadi dilakukan permutasi kompresi dengan menggunakan matriks PC-2.

Jadi setiap kunci Ki, 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 Ci dan Di.

Oleh karena itu, setelah putaran ke-16 akan didapatkan kembali C16 = C0 dan D16 = D0.

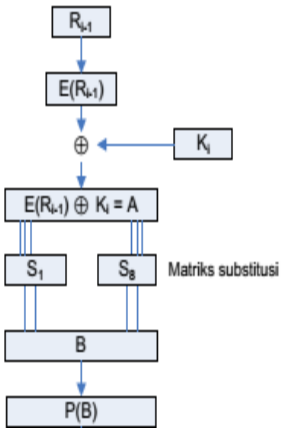
Gambar 3 akan memperlihatkan bagaimana cara pembangkitan kunci internal pada algoritma



Gambar 3.Pembangkitan Kunci Internal

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

Li = Ri-1 (2.1)
Ri = Li-1 f (Ri-1, Ki) (2.2)



Gambar 4. Diagram Fungsi f

Fungsi ekspansi yang memperluas blok Ri-1 yang mempunyai panjang 32 bit menjadi blok 48 bit. Hasil ekspansi *E(Ri-1)*, yang panjangnya 48 bit di-XOR-kan

Journal of Information System, Informatics and Computing
Vol.4 No.1 bulan Juni 2020
e-ISSN : 2597-3673 *(Online)*
p-ISSN : 2579-5201 *(Printed)*

dengan Ki 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. Keluarannya menghasilkan *P(B)* yang juga merupakan keluaran dari fungsi *f*.

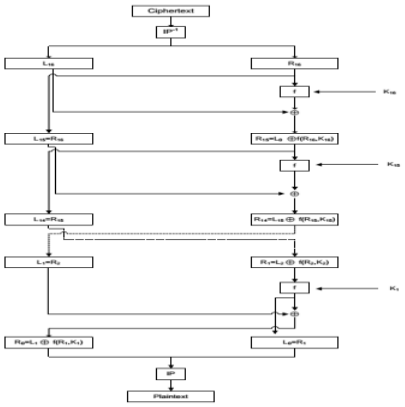
Proses selanjutnya yaitu bit-bit *P(B)* diXOR-kan dengan Li-1 untuk mendapatkan *Ri*.
Proses selanjutnya yaitu permutasi terakhir yang dilakukan setalah 16 kali putaran terhadap gabungan dari blok kiri (*L*) dan blok kanan (*R*). Proses permutasi dilakukan dengan menggunakan matriks permutasi balikan (invers initial permutation) atau IP-1.

Deskripsi

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 Proses Deskripsi

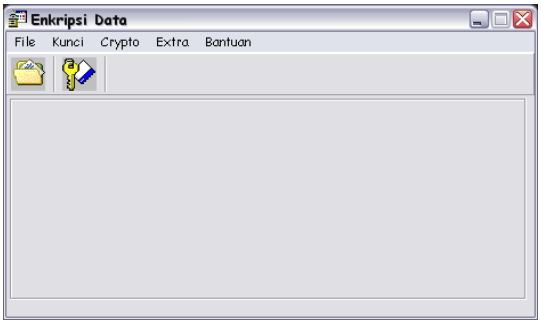
IV. HASIL DAN PEMBAHASAN

Proses

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.

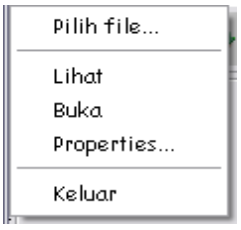
Pada saat melakukan dekripsi suatu file, lokasi (path) file yang telah dienkripsi harus diketahui oleh aplikasi. Setelah itu akan diminta untuk memasukkan password yang sama ketika melakukan enkripsi. Data file yang telah didekripsi akan kembali seperti aslinya.

a. Menu Utama



Gambar diatas adalah contoh rancangan tampilan dari form utama yang berisi file, kunci, crypto, extra dan bantuan.

b. Menu File



Pada Menu *File* dilakukan proses enkripsi dan dekripsi. Terdapat lima sub menu yaitu: *Pilih File.., lihat, buka, properties* dan *keluar.*

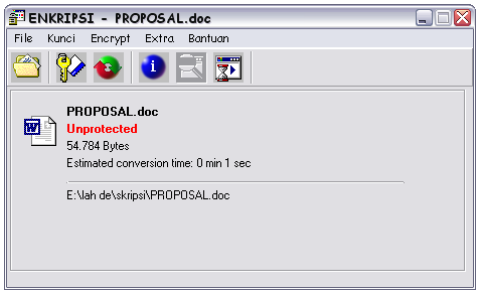
Journal of Information System, Informatics and Computing
Vol.4 No.1 bulan Juni 2020
e-ISSN : 2597-3673 *(Online)*
p-ISSN : 2579-5201 *(Printed)*

c. Menu Kunci

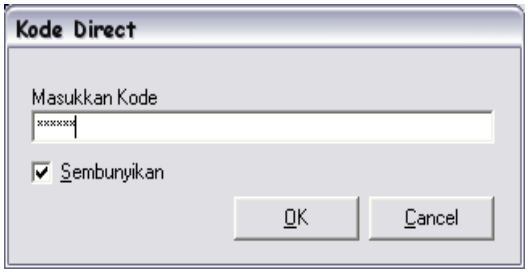
Digunakan untuk memberikan password atau kunci pada file yang akan di enkripsi maupun di dekripsi.

d. Menu Crypto

Enkripsi



Deskripsi

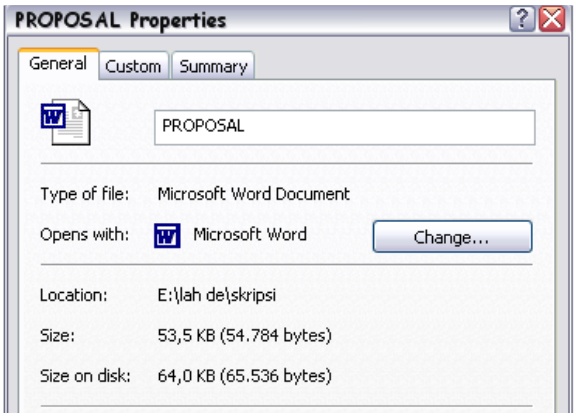


e. Menu Extra

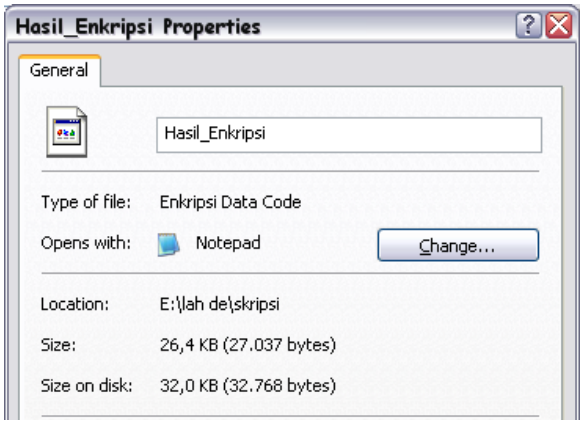
Didalam menu ini terdapat submenu Options yang berfungsi untuk melakukan pengaturan default folder dan kunci.

Hasil

Dengan mengenkripsi suatu data dokumen yang dibuat menggunakan Microsoft word (*.doc). Disini akan dilakukan proses enkripsi terhadap file yang bernama "Proposal.doc".dokumen tersebut memiliki properties seperti pada gambar berikut



File ini akan dienkripsi dan hasilnya akan disimpan dengan nama "Hasil_Enkripsi.edc". Untuk proses enkripsinya, akan diberikan kata kunci "akakom" untuk file tersebut. Setelah dienkrip ukuran file akan berubah, hal ini di karenakan pada saat proses enkripsi terjadi proses kompresi, sehingga file hasil enkripsi akan berukuran lebih kecil dibandingkan dengan file aslinya.



V. KESIMPULAN

Proses Pengamanan data berupa file document pada peneitian ini meliputi proses enkripsi dan deskripsi.Masukan file dan kunci,yang menghasilkan *ciphertext*.Penelitian dilakukan dengan proses pencocokan bit.

Untuk mengenkripsi dan mendekripsi data yang sama, dilakukan dengan menggunakan kunci yang sama.

Ukuran file hasil enkripsi cenderung lebih kecil dari ukuran file asli.

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.

REFERENASI

[1]Primartha,Rifki.2011.*Penerapan Enkripsi Dan Deskripsi File mengunakan Algoritma DES*.Palembang: *Jurnal Sistem Informasi (JSI), VOL. 3, NO. 2, Oktober 2011,*

[2]Budiawan,I Gede Agus.2008.*Aplikasi Pengamanan Data Mengunakan Algoritma RC4*.Yogyakarta: Jurnal Telematika Vol. 1 No. 2 Agustus 2008

[3] Arisantoso , dkk.2017. *PENERAPAN APLIKASI PENGAMANAN DATA/FILE DENGAN METODE ENKRIPSI DAN DEKRIPSI ALGORITMA 3DES DALAM JARINGAN LOKAL AREA*.Jakarta: Seminar Nasional Teknologi Informasi dan Multimedia 2017

[4]Herryawan,I Putu.2017. *ANALISA DAN PENERAPAN ALGORITMA DES UNTUK PENGAMANAN DATA GAMBAR DAN VIDEO*.Bali:Universitas Udayana

[5]Prasetiyo,Budi , dkk.2014.*Kombinasi Steganografi Berbasis Bit Matching dan Kriptografi DES untuk Pengamanan Data*.Semarang: Scientific Journal of Informatics, Vol. 1, No. 1, Mei 2014 ISSN 2407-7658

[6]Aribowo,Eko.2008.*APLIKASI PENGAMANAN DOKUMEN OFFICE DENGAN ALGORITMA KRIPTOGRAFI KUNCI ASIMETRIS ELGAMAL*.Yogyakarta: JURNAL INFORMATIKA Vol 2, No. 2, Juli 2008

[7]Sasongko,Jati.2005.*Pengamanan Data Informasi menggunakan Kriptografi Klasik*.Semarang: Jurnal Teknologi Informasi DINAMIK *Volume X, No.3, September 2005 : 160-167*