APLIKASI ALGORITMA DES (*DATA ENCRYPTION STANDARD*) UNTUK PENGAMAN DATA

Gunawan Putrodjojo[1]
Julhan H. Purba[2]
Junawano Candra[3]
Dosen Jurusan Teknik Informatika STMIK Raharja[1], Peneliti Badan Tenaga Atom Nasional (BATAN)[2], Alumni STMIK Dharma Putra[3]
Email: gunawan.putrodjojo@gmail.com, purba_j_h@yahoo.com, junawanto.candra@gmail.com

Diterima: 6 Desember 2016/ Disetujui : 20 Desember 2016

ABSTRACT

Cryptography is a field of knowledge which uses a mathematical equation to perform the encryption and decryption process. This technique is used to convert the data into a specific code, with the aim that the stored information can not be read by anyone except those who are eligible. In this final project will be presented the design of cryptographic applications with cryptographic algorithm Data Encryption Standard. This cryptographic applications implementing encryption and decryption method using the DES algorithm.This research will presenting application design of crioptographic and its algorithm data of DES. This application will implementing the way of encryption and decription using DES. DES algorithm is adopted as standard algorithm. Since that, DES has been used in desimination information widely to protect data savely. In every day live, DES is using in many applications like to encrypt PIN (Personal Identity Number) in ATM and Banking transactions via internet. Even government organitations in US like Departmen of Energy, Justice Department, and Federal Reserve System are using DES to protect their data desiminations.
The principt of DES working is devides information in special blocks, so that DES is known as cipherblock. The messages will be randomly using standard matrix in DES alhgorithm. The first proces will generate DES key algorithm. Cipherblock with 64 bits block size. Because in this application we have designed internal key altogether in enription process. The next we will to do enription process. The steps in doine encryption will begin with choosing file .txt. This file contents will be changed as binery numbers using ASCII as reference. The changing file as binary will be devided into 64 bits. Its means automatically that in DES algorithm using 8-characters or 64-bits.
Next step, the deviding text will be permutated using first permutation matrix, the goal is to randomice plaintext. The randomice text will devivided into 2 blocks which 32-bits in length. Each block will use L_0 dan R_0 *as symbol. The next process will do 16-cycling process. After 16-cycling process, both blocks will put in unity. After that, we will final permutation with using permutation matrix* iP^{-1}

Key Words : *Cryptography, Encryption, Decryption, Cipher Block*

ABSTRAK

Kriptografi merupakan suatu bidang ilmu pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi. Teknik ini digunakan untuk mengkonversi data ke dalam bentuk kode-kode tertentu, dengan tujuan agar informasi yang tersimpan tidak dapat di baca oleh siapa pun kecuali orang-orang yang berhak. Tulisan ini akan menyajikan perancangan aplikasi kriptografi dengan algoritma kriptografi Data Encryption Standard (DES). Aplikasi kriptografi ini mengimplementasikan cara enkripsi dan dekripsi menggunakan algoritma DES. Algoritma DES diadopsi sebagai algoritma standar/baku. Sejak saat itu, DES banyak digunakan pada dunia penyebaran informasi untuk melindungi data agar tidak bisa dibaca oleh orang lain. Dalam kehidupan sehari – hari, DES banyak digunakan pada banyak aplikasi seperti pada enkripsi PIN (Personal Identification Number) pada mesin ATM dan transaksi perbankan lewat internet. Bahkan, organisasi – organisasi pemerintahan di Amerika Serikat seperti Departmen of Energy, Justice Department, dan Federal Reserve System menggunakan DES untuk melindungi penyebaran data mereka.

Prinsip kerja DES adalah pembagian informasi menjadi blok – blok tertentu oleh karena itu DES termasuk salah satu algoritma cipherblock. Pesan – pesan tersebut pun akan diacak menggunakan matriks – matriks standar yang ada pada algoritma DES. Proses pertama yang penulis lakukan adalah membangkitkan kunci pada algoritma DES. kriptografi cipherblock dengan ukuran blok 64 bit dan ukuran kuncinya 56 bit. Karena pada aplikasi yang penulis rancang kunci internalnya sudah dibuat bersamaan dengan proses enkripsi, maka proses selanjutnya yaitu proses enkripsi. Langkah – langkah enkripsi adalah sebagai berikut : Memilih file .txt yang akan dienkrip isi teksnya, selanjutnya, teks dalam isi file tersebut diubah menjadi bilangan biner dengan mengacu pada nilai indeks ASCII. Teks yang telah diubah menjadi bilangan biner dibagi menjadi 64 bit. Berarti pengerjaan untuk algoritma DES adalah setiap delapan karakter atau 64 bit. Kemudian teks yang telah dibagi tadi dipermutasikan dengan matriks permutasi awal, tujuannya adalah mengacak plaintext. Teks yang telah diacak kemudian dibagi menjadi dua blok, yang masing – masing panjangnya adalah 32 bit. Kedua blok tersebut dilambangkan dengan L_0 dan R_0. Selanjutnya, dilakukan putaran proses sebanyak 16 kali. Setelah dilakukan sebanyak 16 kali putaran, maka kedua blok tersebut akan digabungkan kembali. Setelah penggabungan kedua blok, maka proses terakhir adalah melakukan permutasi dengan menggunakan matriks permutasi IP^{-1}.

Kata kunci : kriptografi, Enkripsi, Dekripsi, Cipherblock

PENDAHULUAN

Perkembangan aplikasi dalam teknologi informasi sangat cepat dan sangat pesat, secara langsung maupun tidak langsung telah menjadi bagian yang tidak terpisahkan dalam berbagai bidang kehidupan. Karena banyak kemudahan yang ditawarkan, teknologi informasi tidak dapat lepas dari berbagai aspek kehidupan manusia, yang memungkinkan dapat berkomunikasi dan saling bertukar data maupun informasi. Seiring dengan kemajuan zaman maka sangat diperlukan sebuah keamanan data terhadap kerahasiaan data dan informasi yang saling dipertukarkan, apa lagi jika data tersebut dalam suatu jaringan komputer yang terhubung dengan jaringan lain. Hal tersebut tentu saja menimbulkan risiko bila data yang sensitif dan berharga diakses oleh orang yang tidak bertanggung jawab. Data dan Informasi yang terkandung didalamnya bisa saja diubah sehingga menyebabkan salah penafsiran oleh penerima pesan.

Ilmu yang mempelajari tentang pengamanan data adalah kriptografi. Kriptografi telah menjadi suatu bagian yang tidak dapat dipisahkan dari sistem keamanan jaringan, salah satu metodenya adalah *Data Encryption Standard (DES). Data Encryption Standard (DES)* merupakan algoritma *cipher block* yang populer karena algoritma ini dijadikan standar algoritma enkripsi kunci-simetri. Sebenarnya *DES* adalah nama standar enkripsi simetri, nama algoritma enkripsinya sendiri adalah *DEA (Data Encryption Algorithm)*, namun nama *DES* lebih populer dibandingkan dengan *DEA*.

PERMASALAHAN

Permasalahan yang akan dibahas dalam tulisan ini adalah bagaimana meningkatkan keamanan data melalui Proses Enkripsi - Dekripsi. Agar pembahasan masalah ini tidak menyimpang, penulis akan memberikan beberapa batasan masalah, sebagai berikut :

- Algoritma Enkripsi Dekripsi yang akan digunakan adalah DES.
- Aplikasi ini hanya dapat digunakan pada *file* text (.txt) saja
- Aplikasi bahasa yang digunakan adalah pemrograman Visual Studio 2015 dengan compiler Visual Basic.

LANDASAN TEORI

Algoritma

Algoritma adalah urutan langkah – langkah logis penyelesaian masalah yang disusun secara sistematis dan logis. Kata logis merupakan kata kunci dalam algoritma. Langkah – langkah dalam algoritma harus logis dan harus dapat ditentukan nilai salah atau benar. (Munir, 2002).

Kriptografi

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan (*Cryptography is the art and science of keeping messages secure*) selain itu ada pengertian lain tentang kriptografi yaitu ilmu yang mempelajari teknik – teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, serta integritas data. Kata "seni" di dalam definisi di atas maksudnya adalah mempunyai cara yang unik untuk merahasiakan sebuah pesan. Kata "*graphy*" di dalam "*cryptography*" itu sendiri sudah menyiratkan arti seni. (Munir, 2006).

Menurut (Munir, 2006), ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

1. *Convidentiality* (kerahasiaan), yaitu memberikan kerahasiaan pesan dan menyimpan data dengan menyembunyikan data dengan menyembunyikan informasi lewat teknik-teknik enkripsi.
2. *Message intergrity* (integritas data), yaitu memberikan jaminan bahwa dari setiap bagian tidak mengalami perubahan dari saat data dibuat/ dikirim sampai dengan saat data tersebut dibuka.
3. *Non-repudiation* (tidak dapat disangkal), yang memberikan cara untuk membuktikan apabila seseorang mencoba menyangkal jika ia memiliki dokumen tersebut.
4. *Auntentication* (autentikasi), yang memberikan dua layanan. Yang pertama mengidentifikasi keaslian dari suatu pesan dan memberikan jaminan keotentikannya. Kedua, untuk meguji identitas seseorang apabila ia akan memasuki sebuah sistem.

Enkripsi dan Dekripsi

Enkripsi merupakan proses pengamanan suatu data dengan cara mengkonversi data (*plaintext*) menjadi bentuk yang tidak dapat dibaca (*ciphertext*). sementara Dekripsi merupakan kebalikan dari enkripsi yaitu mengkonversi data yang sudah dienkripsi (*ciphertext*) kembali ke data aslinya (*plaintext*) sehingga dapat dibaca kembali.

Pesan merupakan data atau informasi yang dimengerti maknanya. Nama lain dari pesan adalah *plaintext*. Pesan tersebut dapat dikirim (melalui kurir, saluran telekomunikasi, dan lain – lain) dan dapat juga disimpan dalam media penyimpanan. Pesan dapat berupa teks, video, gambar, dan lain – lain. Agar pesan tersebut tidak dapat dimengerti maknanya bagi pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang telah tersandikan tersebut dinamakan dengan *ciphertext*. Perbandingan antara *plaintext* dan *ciphertext* dapat dilihat pada gambar 1.

Gambar 1. perbandingan antara *plaintext* dan *ciphertext*

Data Encryption Standard (DES)

DES memiliki beberapa elemen pembangun, diantaranya :

- Aritmatika Modular

Aritmatika Modular merupakan operasi matematika yang banyak diimplementasikan pada metode kriptografi. Pada metode kriptografi simetris, operasi aritmatika modular yang sering dipakai adalah proses penjumlahan modulo dua dan operasi XOR (*exclusive-or*) dengan symbol □□□Operasi modulo dua ini melibatkan bilangan-bilangan 0 dan 1 saja sehingga identik dengan bit pada komputer.

- Jaringan Feistel

Jaringan Feistel adalah metode yang umum digunakan pada algoritma kriptografi *block cipher*. Bagian utama dari jaringan Feistel adalah fungsi f, yaitu fungsi pemetaan string input menjadi string output. Pada setiap putaran, blok sumber merupakan input bagi fungsi *f* , kemudian output dari fungsi *f* tersebut di XOR-kan dengan blok tujuan. Setelah itu kedua blok tersebut ditukar. Alasan digunakan jaringan Feistel yaitu *cipher* yang dibuat dengan fungsi ini dijamin dapat dikembalikan untuk proses dekripsi. Jaringan Feistel ini banyak digunakan oleh algoritma enkripsi seperti DES, Lucifer, FEAL, Khufu, LOKI, GOST, CAST, Blowfish dan lain-lain.

S-Box

S-Box merupakan suatu tabel subtitusi yang banyak digunakan pada kebanyakan algoritma blok cipher. Dalam algoritma DES digunakan 8 buah S-Box yang dalam masing–masing tabelnya terdiri dari 4 baris dan 16 kolom. Setiap S-Box menerima input 6 bit dan menghasilkan output 4 bit. Kelompok 6 bit pertama menggunakan S_1, kelompok 6 bit kedua menggunakan S_2, dan seterusnya sampai 6 bit kedelapan menggunakan S_8.

Jumlah putaran DES

Penentuan banyak putaran pada algoritma kriptografi didasarkan atas atas keseimbangan. Semakin sedikit jumlah putaran akan menyebabkan algoritma kriptografi menjadi mudah untuk dipecahkan. Tetapi jika jumlah putaran semakin banyak akan menyebabkan kecepatan proses enkripsi atau dekripsi semakin berkurang. Putaran yang digunakan dalam Algoritma DES adalah 16 kali putaran. Hal ini didasarkan pada penelitian yang menunjukkan DES dengan jumlahputaran kurang dari 16 kali dengan mudah dapat dipecahkan dengan *known-plaintext attack*.

Panjang kunci DES

Panjang kunci eksternal DES adalah 64 bit atau 8 karakter. Kunci eksternal adalah kunci yang diberikan oleh pengguna sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Setelah melalui proses permutasi, dari 64 bit kunci eksternal hanya 56 bit yang digunakan, sehingga dikatakan panjang kunci DES adalah 56 bit.

Pada awal perancangan DES, panjang kunci yang diusulkan IBM 128 bit, tetapi atas permintaan NSA panjang kunci diperkecil menjadi 56 bit. Algoritma DES merupakan algoritma simetris yang paling banyak digunakan di dunia untuk proses enkripsi. DES bekerja pada bit atau bilangan biner yaitu 0 dan 1. Sebelum dienkripsi menggunakan algoritma DES, sebuah *plaintext* yang berupa bilangan hexadesimal (bilangan berbasis 16) akan dikonversi terlebih dahulu kedalam 64 bit bilangan biner dengan masing-masing grup tersusun dari 4 bit. Sebagai contoh, bilangan hexadesimal “0” akan dikonversi kedalam bilangan biner “0000”, bilangan hexadesimal “6” akan dikonversi ke dalam bilangan biner “0110” dan bilangan hexadesimal “B” akan dikonversi ke dalam bilangan biner “1011”. Hasil enkripsi yang berupa bilangan biner dikonversi kedalam bilangan hexadesimal. Jadi *plaintext* dan *ciphertext* yang merupakan input dan output dalam algoritma DES ini berupa bilangan hexadesimal.

DES Merupakan algoritma *cipher block* yang termasuk kedalam sistem kriptografi simetri. DES beroperasi pada ukuran blok 64 bit. DES mengenkripsi 64 bit *plaintext* menjadi 64 bit *ciphertext* dengan menggunakan 56 bit kunci internal (*internal key*). Kunci internal pada algoritma DES dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit.

Skema global dari algoritma *DES* adalah sebagai berikut :

- Blok *plaintext* dipermutasikan dengan *metric* permutasi awal (*initial permutation* atau *IP*).
- Hasil permutasi awal kemudian dilakukan *enciphering* sebanyak 16 kali (16 putaran) dimana setiap putaran menggunakan kunci internal yang berbeda.
- Hasil *enciphering* kemudian dipermutasikan dengan matriks permutasi balikan (*invers initia l permutation* atau ip^{-1}) menjadi blok *ciphertext*.

Di dalam proses enkripsi, blok *plaintext* dibagi menjadi dua bagian yaitu 32 bit kiri (blok *L*) dan 32 bit kanan (Blok *R*). Kemudian kedua bagian ini masuk ke dalam 16 putaran DES.

Pada setiap putaran *i*, blok*R* merupakan *input* untuk fungsi transformasi yang disebut *f*. Pada fungsi *f*, blok *R* dikombinasikan dengan kunci internal K_i. *Output* dari fungsi *f* di XOR-kan dengan blok*L* untuk mendapatkan blok *R* yang baru. Sedangkan untuk blok*L* yang baru, langsung di ambil dari blok *R* sebelumnya. Ini adalah satu putaran DES yang secara matematis dinyatakan sebagai berikut :

$L_i = R_{i-1}$

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

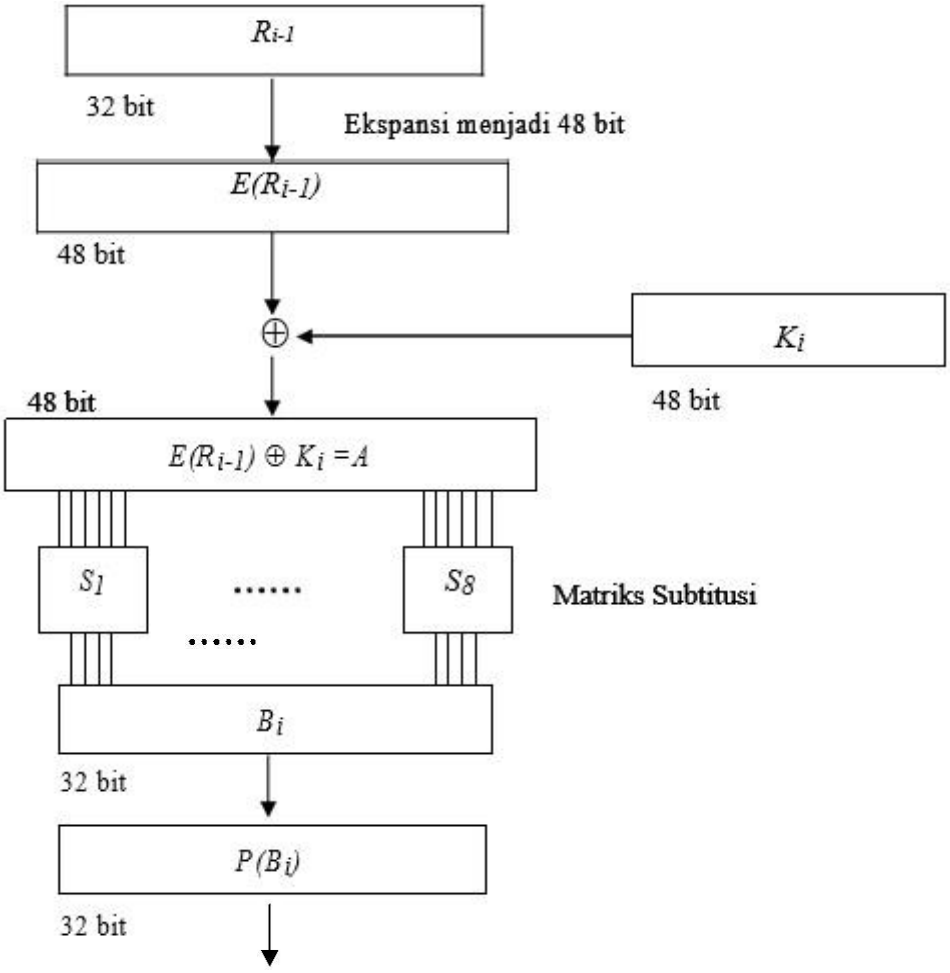
Satu putaran DES ini akan diulang sebanyak 16 kali putaran.

Pembangkitan Kunci Internal

Setiap blok *plaintext* mengalami 16 kali putaran pada proses enkripsi, untuk itu dibutuhkan kunci internal sebanyak 16 buah, yaitu $K_1, K_2, \ldots, K_{16}$. Kunci-kunci internal ini dapat dibangkitkan dari kunci eksternal yang diberikan oleh pengguna sebelum proses enkripsi atau bersamaan dengan proses enkripsi. Kunci eksternal yang panjangnya 64 bit atau 8 karakter menjadi input untuk permutasi menggunakan permutasi kompresi 1 (PC-1).

Proses Enkripsi DES

Proses enkripsi terhadap blok*plaintext* yang panjangnya 64 bit dilakukan setelah permutasi awal terhadap blok *plaintext* tersebut. Setelah itu blok *plaintext* dibagi menjadi dua bagian yaitu kiri (*L*) dan kanan (*R*) yang masing-masing panjangnya 32 bit. Kemudian kedua bagian ini mengalami 16 kali putaran dengan setiap putaran menggunakan kunci internal yang berbeda. Setiap satu putaran merupakan jaringan Feistel yang secara matematis dinyatakan dalam Persamaan (1). Dalam persamaan tersebut fungsi *f* merupakan fungsi tranformasi yang merupakan inti dari algoritma DES, diperlihatkan dalam Gambar 2.



Gambar 2. Diagram alir fungsi *f* algoritma DES

Pada gambar tersebut R_{i-1} diperoleh dari blok kanan sebuah *plaintext* kemudian menjadi input dari

transformasi *f*. Fungsi ekspansi *E* berguna untuk memperluas blok R_{i-1} yang panjangnya 32 bit menjadi blok yang panjangnya 48 bit dengan matriks permutasi ekspansi *(expansion permutation).*

Proses Dekripsi DES

Pada algoritma DES proses dekripsi dan enkripsinya menggunakan kunci yang sama. Proses dekripsi pada *ciphertext* merupakan kebalikan dari proses enkripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah

$K_1, K_2, \ldots, K_{16}$, maka pada proses dekripsi urutan kunci yang digunakan adalah $K_{16}, K_{15}, \ldots, K_1$.

Proses dekripsi DES dimulai dengan putaran ke-16, 15,…,2, 1. Untuk setiap putaran dalam proses dekripsi, dihasilkan output yang secara matematis dapat dinyatakan dalam Persamaan 2.6. Persamaan ini diturunkan dari Persamaan 2.1 yang merupakan output dari setiap putaran dalam proses enkripsi.

$$R_{i-1} = L_i$$

$$Li\text{-}1 = Ri \; f(Li, Ki) \quad (2.)$$

Dalam hal ini (R_{16}, L_{16}) adalah input awal untuk proses dekripsi. Untuk memperoleh blok (R_{16}, L_{16}) maka dilakukan permutasi terhadap ciphertext menggunakan matriks permutasi IP^{-1} seperti dalam Tabel 9. Output terakhir dari proses dekripsi adalah (L_0,R_0). Selanjutnya dilakukan permutasi terhadap (L_0,R_0) menggunakan matriks permutasi awal pada Tabel 2.3 sehingga diperoleh kembali blok plaintext semula.

LITERATURE REVIEW

Terdapat beberapa penelitian yang memiliki korelasi yang searah dengan penelitian yang dibahas dalam tulisan ini, antara lain :

1. -Penelitian yang dilakukan oleh Rifkie Primartha (2011)
   Penelitian ini berjudul "Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma *Data Encryption Standard* (DES)".Hasil dari penelitian ini adalah berupa suatu aplikasi perangkat lunak yang bertujuan untuk melakukan enkripsi dan dekripsi suatu informasi berbentuk *file* atau teks sederhana.
2. -Penelitian yang dilakukan oleh I Putu Herryawan (2008)
   Penelitian ini berjudul "Analisis Dan Penerapan Algoritma DES Untuk Pengamanan Data Gambar". Hasil dari penelitian ini adalah berupa aplikasi perangkat lunak yang bertujuan untuk melakukan enkripsi pada gambar dengan mengacak bit pada gambar tersebut.
3. -Penelitian yang dilakukan oleh Deni Mustofa (2007)
   Penelitian ini berjudul "Perancangan Program Keamanan Data Dengan Menggunakan Algoritma Kriptografi DES". Hasil penelitian ini berupa aplikasi perangkat lunak yang bertujuan untuk mengenkipsi dan dekripsi sebuah *file* dengan menampilkan isi *file* asli dan isi *file* setelah di enkripsi pada layar antar muka aplikasi tersebut.
4. -Penelitian yang dilakukan oleh Indra Syahputra (2009)
   Penelitian ini berjudul "Simulasi Kerahasiaan / Keamanan Informasi Dengan Menggunakan Algoritma DES". Hasil dari penelitian ini berupa aplikasi perangkat lunak yang mensimulasikan metode DES.
5. -Penelitian yang dilakukan oleh M. Yuli Andri (2009)
   Penelitian ini berjudul "Implementasi Algoritma Kriptografi DES Pada File Digital".Hasil dari penelitian ini berupa aplikasi perangkat lunak yang bertujuan untuk mengenkipsi dan dekripsi sebuah *file* dengan meminta kunci internal sebelum proses enkripsi dilakukan.

PEMBAHASAN

DES merupakan salah satu algoritma kriptografi *cipherblock* dengan ukuran blok 64 bit dan ukuran kuncinya 56 bit. Setelah melalui banyak diskusi, akhirnya algoritma DES diadopsi sebagai algoritma standar. Sejak saat itu, DES banyak digunakan pada dunia penyebaran informasi untuk melindungi data agar tidak bisa dibaca oleh orang lain. Dalam kehidupan sehari – hari, DES banyak digunakan pada banyak aplikasi seperti pada enkripsi PIN (*Personal Identification Number*) pada mesin ATM (*Automatic Teller Machine*) dan transaksi perbankan lewat internet. Bahkan, organisasi – organisasi pemerintahan di Amerika Serikat seperti *Departmen of Energy, Justice Department,* dan *Federal Reserve System* menggunakan DES untuk melindungi penyebaran data mereka.

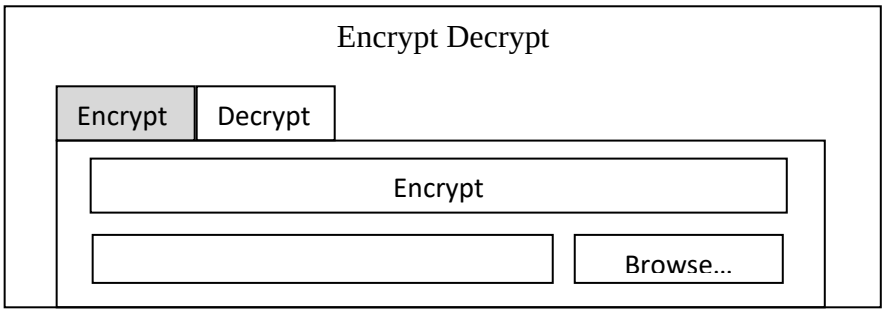
Analisis Algoritma DES

Prinsip kerja DES adalah pembagian informasi menjadi blok – blok tertentu oleh karena itu DES termasuk salah satu algoritma *cipherblock*. Pesan – pesan tersebut pun akan diacak dengan menggunakan matriks – matriks standar yang ada pada algoritma DES. Proses pertama yang penulis lakukan adalah membangkitkan kunci pada algoritma DES. Karena pada aplikasi yang penulis rancang kunci internalnya sudah dibuat bersamaan dengan proses enkripsi, maka proses selanjutnya yaitu proses enkripsi algoritma DES. Langkah – langkah proses enkripsi adalah sebagai berikut :

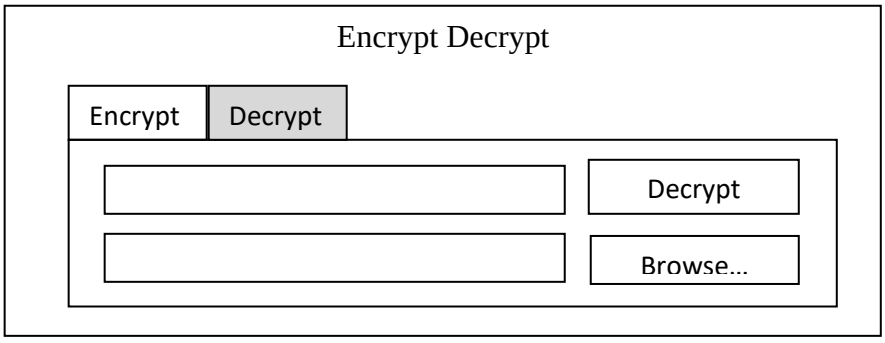
1. – Pertama, adalah memilih *file* .txt yang akan yang akan dienkrip isi teksnya.
2. – Kedua, teks dalam isi *file* tersebut akan diubah menjadi bilangan biner dengan mengacu pada nilai indeks *ASCII*. Teks yang telah diubah menjadi bilangan biner tersebut dalam hal pengerjaan enkripsi dibagi menjadi 64 bit. Berarti pengerjaan untuk algoritma DES adalah setiap delapan karakter atau 64 bit.
3. – Ketiga, teks yang telah dibagi tadi kemudian dipermutasikan dengan matriks permutasi awal.
4. – Keempat, yaitu teks yang telah diacak tadi kemudian dibagi menjadi dua blok, yang masing – masing panjangnya adalah 32 bit. Kedua blok tersebut dilambangkan dengan L_0 dan R_0.
5. – Kelima, yaitu melakukan putaran proses sebanyak 16 kali. Proses yang dilakukan dalam setiap putaran adalah sebagai berikut :
   $L_i = R_{i-1}$
   $R_i = L_{i-1}$ □ □ K_i
6. Setelah dilakukan sebanyak 16 kali, maka pada proses selanjutnya kedua blok tersebut akan digabungkan kembali.
7. Setelah penggabungan kedua blok, maka proses terakhir adalah melakukan permutasi dengan menggunakan matriks permutasi IP^{-1}.

Perancangan Antar Muka (*Interface)*

Perancangan bertujuan untuk memberikan gambaran secara terperinci. Perancangan merupakan tahap lanjutan dari analisis, dimana pada perancangan digambarkan rancangan yang akan dibangun sebelum dilakukan pengkodean/penyandian ke dalam suatu bahasa pemrograman.
Berikut adalah gambar dari rancangan yang akan penulis buat :

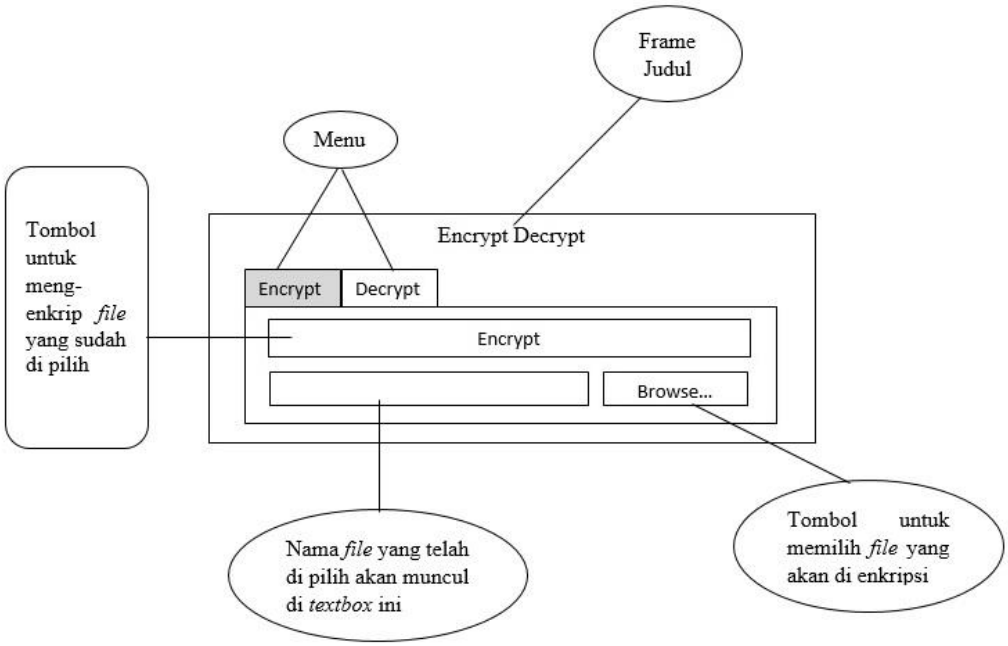


Gambar 3. Rancangan dari tampilan Antar muka untuk Enkripsi

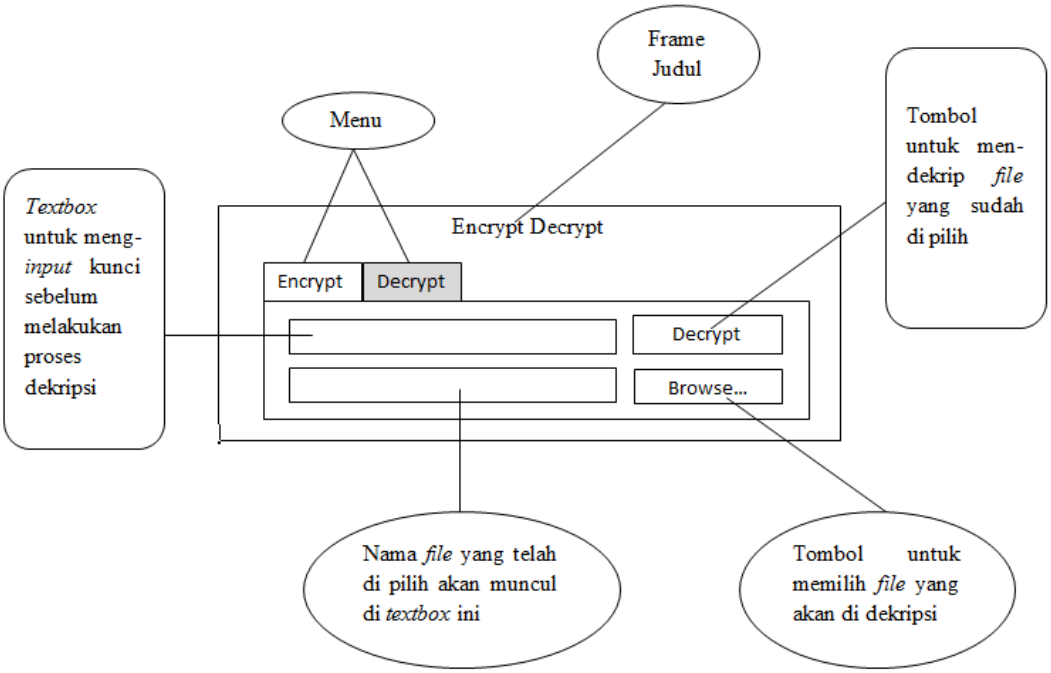


Gambar 4. Rancangan dari tampilan Antar muka untuk Dekripsi

Dan berikut adalah keterangan dari rancangan Antar muka yang dibuat



Gambar 5 Keterangan dari Antar muka enkripsi yang dibuat



Gambar 6. Keterangan dari Antar muka dekripsi yang dibuat

IMPLEMENTASI

Pada implementasi ini secara keseluruhan penulis membuat tiga buah form, yang akan dijelaskan secara terperinci satu per satu. Pada form pertama terdapat dua buah menu yaitu menu enkripsi dan menu dekripsi, Lebih jelasnya akan diperlihatkan pada gambar 7.

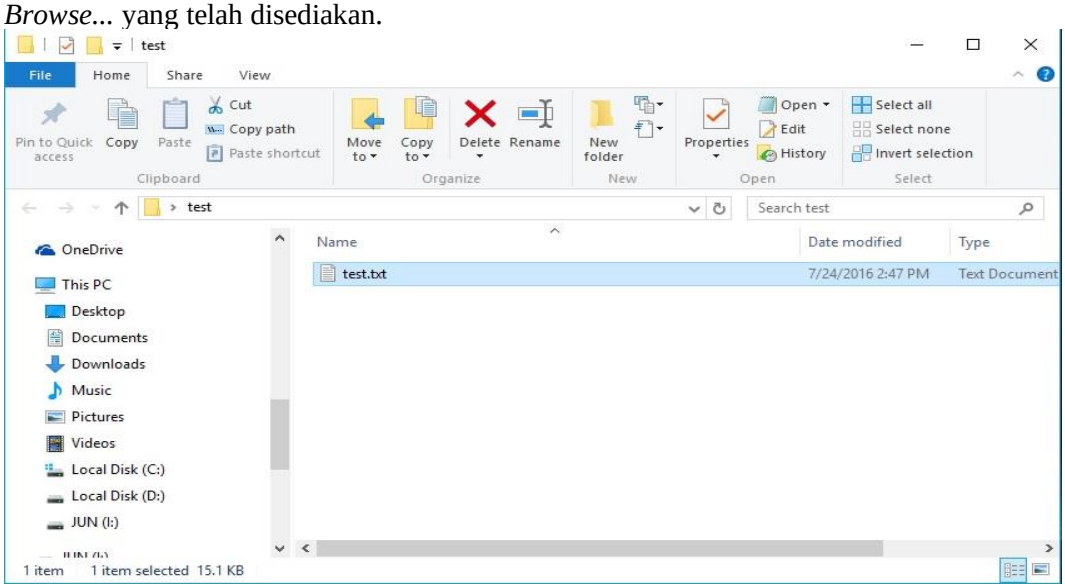
Gambar 7. Antar muka Form utama : menu enkripsi dan menu dekripsi

Proses Enkripsi

Proses Enkripsi yaitu proses dimana perubahan informasi yang dapat kita baca (*plaintext*) menjadi informasi yang tidak dapat dimengerti (*ciphertext)*

Gambar 8. Antar muka Menu Enkripsi

Pada menu ini user hanya perlu memilih *file* yang akan dienkripsi dengan menggunakan tombol *Browse...* yang telah disediakan.



Gambar 9. Antar muka proses enkripsi ketika membuka *file*

Setelah memilih *file*, selanjutnya user hanya perlu menggunakan tombol *Encrypt* yang telah disediakan. Secara otomatis kunci akan muncul pada form kedua karena pada sistem ini proses pembangkitan kunci dilakukan bersamaan dengan proses enkripsi, jadi user hanya perlu meng-*copy* kunci tersebut. Lebih jelasnya akan diperlihatkan pada gambar 10.

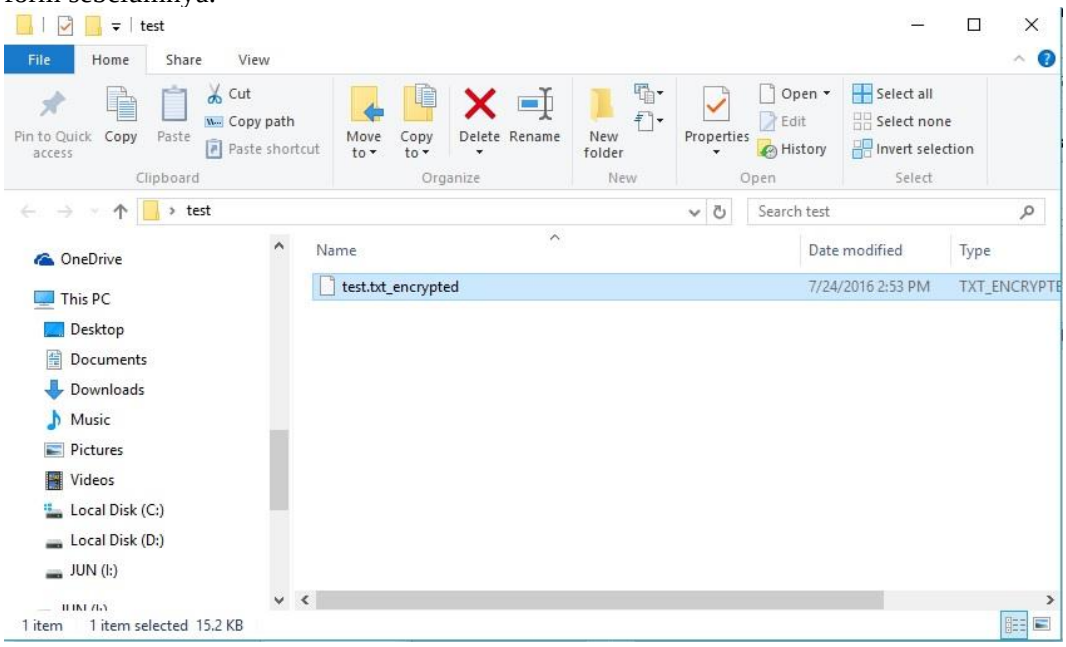
Gambar 10. antar muka proses pembangkitan kunci

Proses Dekripsi

Proses dekripsi merupakan proses pengembalian *fileciphertext* menjadi *fileplaintext*. Jadi secara umum proses dekripsi merupakan kebalikan dari proses enkripsi.

Gambar 11. Antar muka menu dekripsi

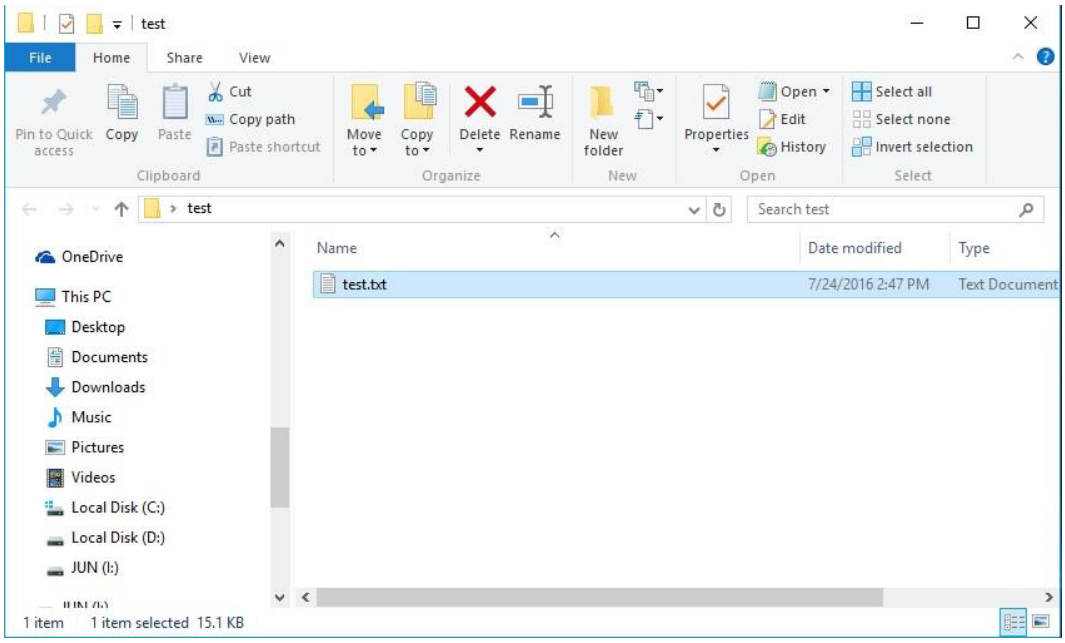
Pada menu ini user hanya perlu memilih *file* yang akan didekripsi menggunakan tombol *Browse...* yang telah disediakan dan meng-*paste* kan kunci yang sudah di *copy* pada saat proses enkripsi pada form sebelumnya.



Gambar 12. Antar muka proses dekripsi ketika membuka *file*

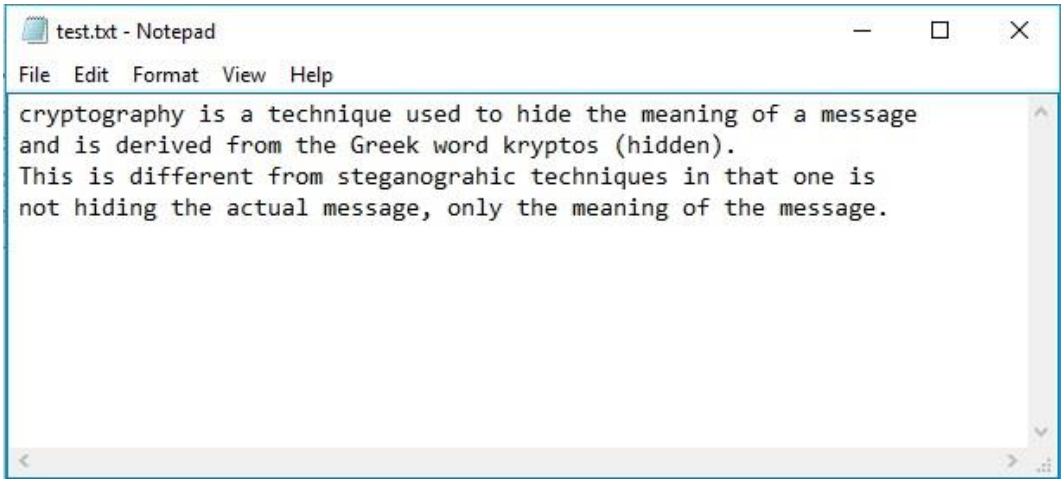
Gambar 13. Antar muka setelah memilih *file* dan mem-*paste* kunci

File yang berhasil didekripsi akan disimpan pada direktori *folder* yang samadan akan kembali menjadi nama asli *file* sebelum dilakukan proses enkripsi.Setelah di dekripsi, *file* yang sudah di enkripsi tadi akan di hapus secara otomatis

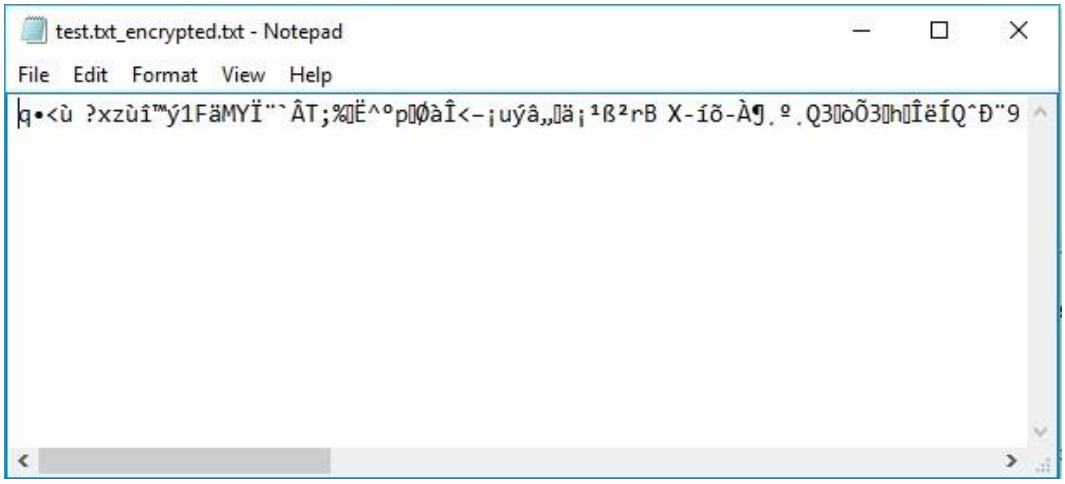


Gambar 14. nama *file* setelah di dekripsi akan kembali menjadi nama *file* asli

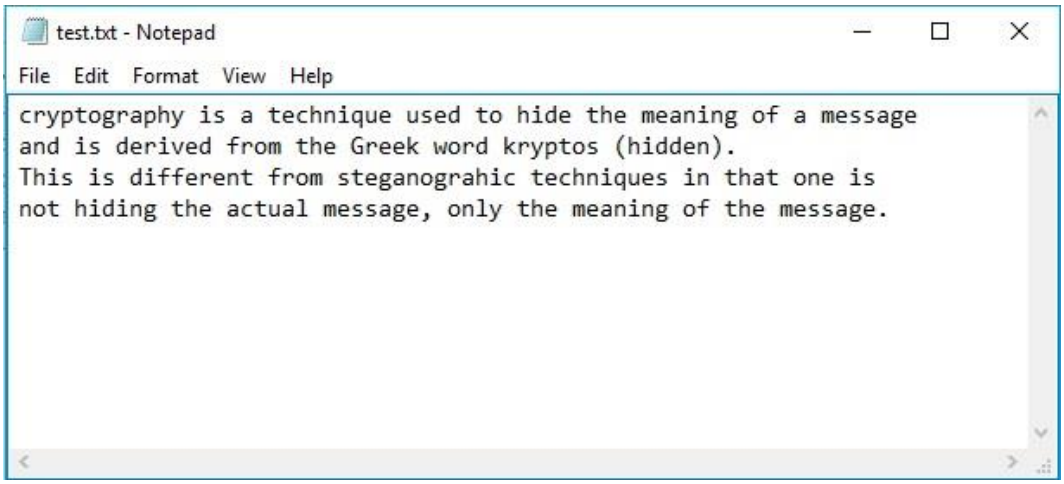
Berikut akan ditampilkan hasil pengujian masing – masing dari *file* semula, *file* setelah dienkripsi dan *file* yang telah didekripsi.



Gambar 15. *File* asli sebelum dilakukan proses enkripsi ataupun dekripsi



Gambar 16. *file* setelah dilakukan proses enkripsi



Gambar 17. *file* setelah dilakukan proses dekripsi ke bentuk semula

Tiga gambar di atas membuktikan bahwa *file* asli berhasil dienkripsi dan didekipsi dengan baik.

KESIMPULAN

Berdasarkan hasil analisis dan penelitian dari uraian-uraian yang telah dikemukakan maka dapat ditarik kesimpulan sebagai berikut :

Keamanan data/teks dapat ditingkatkan menggunakan algoritma DES yaitu melalui proses Enkripsi - Dekripsi.

Aplikasi yang dibangun merupakan aplikasi yang praktis untuk melaksanakan proses Enkripsi maupun proses Dekripsi menggunakan algoritma DES dimana dengan hanya memilih menu yang dibutuhkan semuanya bisa dilakukan.

Secara umum proses DES terbagi menjadi tiga kelompok, yaitu pemrosesan kunci, pemrosesan enkripsi data 64 bit, dan dekripsi data 64 bit.

Penggunaan kunci merupakan sesuatu yang sangat penting dalam proses enkripsi dan dekripsi, sehingga dibutuhkan suatu kerahasiaan dalam pemakaian kuncinya.

Aplikasi dibangun menggunakan bahasa pemrograman Visual Studio 2015 dengan compiler Visual Basic.

DAFTAR PUSTAKA

[1]. Agus Mulyanto. 2009. *Sistem Informasi Konsep dan Aplikasi*. Yogyakarta : Pustaka Belajar

[2]. Andi, Sunyoto. 2007. *Pemrograman Database dengan Visual Basic dan Microsoft SQL*. Yogyakarta: Andi Offset.

[3]. Dony, Ariyus. 2008. *Pengantar Ilmu Kriptografi*. Yogyakarta:ANDI

[4]. Kurniawan, Yusuf, 2004. *Kriptografi kemanan internet dan jaringan komunikasi*. Bandung: Informatika Bandung

[5]. Rinaldi, Munir, 2002. *Algoritma dan pemrograman dalam bahasa Pascal dan C buku 2*. Bandung: Informatika Bandung

[6]. Rinaldi, Munir, 2006. *Kriptografi*. Bandung: Informatika Bandung

[7]. http://ilmu-kriptografi.blogspot.co.id/2009/05/algoritma-des-data-encryption-standart.htmldiakses pada tanggal 10 Mei 2016

[8]. http://studyinformatics.blogspot.co.id/2012/07/des-data-encryption-standard.htmldiakses pada tanggal 10 Mei 2016

[9]. https://id.wikipedia.org/wiki/Enkripsi diakses pada tanggal 7 Juni 2016

[10].https://id.wikipedia.org/wiki/Keamanandiakses pada tanggal 7 Juni 2016

[11].https://en.wikipedia.org/wiki/Microsoft_Visual_Studiodiakses pada tanggal 5 July 2016

[12].http://www.ekowiner.web.id/2015/04/pengertian-dasar-pemrograman-visual-basic-6.0.htmldiakses pada tanggal 5 July 2016

[13].http://ilmu-kriptografi.blogspot.co.id/2011/05/kriptografi-dalam-kehidupan-sehari-hari.htmldiakses pada tanggal 20 July 2016