RANCANG BANGUN APLIKASI ENKRIPSI DAN DESKRIPSI FILE TEKS BERBASIS DESKTOP DENGAN MENGGUNAKAN METODE ALGORITMA *DATA ECRYPTION STANDART*

Disusun dan Diajukan Sebagai Salah Satu Syarat Untuk Menempuh Ujan Akhir Memperoleh
Gelar Sarjana Kompufer Pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi

SKRIPSI

OLEH :

NAMA : ADE CHINTIA NINGSIH
N.P.M : 1714370176
PROGRAM STUDI : SISTEM KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2021

LEMBAR PENGESAHAN

RANCANG BANGUN APLIKASI ENKRIPSI DAN DESKRIPSI FILE TEKS BERBASIS DESKTOP DENGAN MENGGUNAKAN METODE ALGORITMA *DATA ECRYPTION STANDART* UTARA

Disusun Oleh:

NAMA	**: ADE CHINTIA NINGSIH**
NPM	**: 1714370176**
PROGRAM STUDI	**: SISTEM KOMPUTER**

Skripsi Telah Disetujui Oleh Dosen Pembimbing Skripsi
Pada Tanggal 28 Juli 2021

Dosen Pembimbing I

Dr. Muhammad Iqbal, S.Kom.,M.Kom.

Dosen Pembimbing II

Arpan, S.Kom.,M.Kom.

Mengetahui,

Dekan Fakultas Sains Dan Teknologi

Hamdani, ST.,M.T.

Ketua Program Studi Sistem Komputer

Eko Hariyanto, S.Kom.,M.Kom.

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini:

Nama	: ADE CHINTIA NINGSIH
NPM	: 1714370176
Program Studi	: SISTEM KOMPUTER
Judul Skripsi	: RANCANG BANGUN APLIKASI ENKRIPSI DAN DESKRIPSI FILE TEKS BERBASIS DESKTOP DENGAN MENGGUNAKAN METODE ALGORITMA *DATA ECRYPTION STANDART*

Dengan ini menyatakan bahwa:

1. Tugas Akhir atau Skripsi saya bukan merupakan hasil plagiarisme.
2. Saya tidak akan menuntut perbaikan nilai indeks prestasi kumulatif (IPK) setelah menyelesaikan siding meja hijau.
3. Skripsi ini dapat di publikasikan oleh pihak lembaga dan saya tidak akan menuntut akibat dari publikasi tersebut.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya, terimakasih.

Medan, 4 Oktober 2021

ADE CHINTIA NINGSIH

1714370176

PERNYATAAN ORISINALITAS

Dengan ini menyatakan bahwa dalam skripsi ini tidak terdapat karya yang di ajukan untuk memperoleh gelar kesarjanaan di dalam perguruan tinggi, dan sepanjang sepengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis didalam skripsi ini dan disebut dalam daftar pustaka.

Medan, 02 September 2021

Yang Membuat Pernyataan

Ade Chintia Ningsih
1714370176

SURAT KETERANGAN PLAGIAT CHECKER

Dengan ini saya Ka.LPMU UNPAB menerangkan bahwa saurat ini adalah bukti pengesahan dari LPMU sebagi pengesah proses plagiat checker Tugas Akhir/ Skripsi/Tesis selama masa pandemi ***Covid-19*** sesuai dengan edaran rektor Nomor : 7594/13/R/2020 Tentang Pemberitahuan Perpanjangan PBM Online.

Demikian disampaikan.

NB: Segala penyalahgunaan/pelanggaran atas surat ini akan di proses sesuai ketentuan yang berlaku UNPAB.

Ka.LPMU

Ahmad Muhaimin Ritonga, BA., MSc

No. Dokumen : PM-UJMA-06-02	Revisi	: 00	Tgl Eff	: 23 Jan 2019

Analyzed document: ADE CHINTIA NINGSIH_1714370176_SISTEM KOMPUTER.docx Licensed to: Universitas Pembangunan Panca Budi_License03

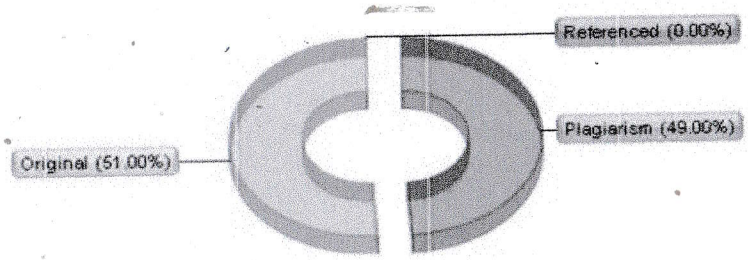
Comparison Preset: Rewrite Detected language:

Check type: Internet Check

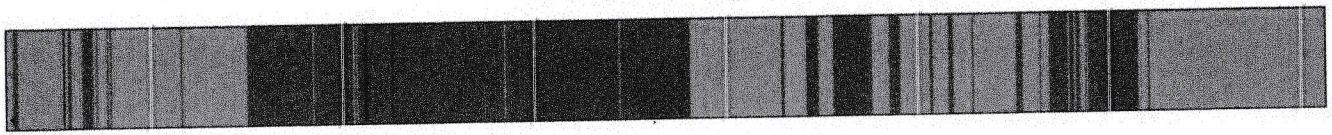
UNIVERSITAS PEMBANGUNAN PANCA BUDI
Beriman, Berilmu, Berkarya

Detailed document body analysis:

Relation chart:



Distribution graph:



Top sources of plagiarism: 44

27% 2095 1 https://makalah-update.blogspot.com/2012/11/makalah-pengertian-dan-sejarah-des-data.html

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km 4,5 Medan Fax. 061-8458077 PO.BOX : 1099 MEDAN

PROGRAM STUDI TEKNIK ELEKTRO	(TERAKREDITASI)
PROGRAM STUDI ARSITEKTUR	(TERAKREDITASI)
PROGRAM STUDI SISTEM KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI TEKNIK KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI AGROTEKNOLOGI	(TERAKREDITASI)
PROGRAM STUDI PETERNAKAN	(TERAKREDITASI)
PROGRAM STUDI TEKNOLOGI INFORMASI	(TERAKREDITASI)

PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR*

rtanda tangan di bawah ini :

	: ADE CHINTIA NINGSIH
Lahir	: BINJAI / 24 Oktober 1999
Mahasiswa	: 1714370176
	: Sistem Komputer
	: Keamanan Jaringan Komputer
yang telah dicapai	: 143 SKS, IPK 3.52
	: 085368393820
engajukan judul sesuai bidang ilmu sebagai berikut	:

Judul

mentasi Algoritma Data Encryptyon Standart pada Enkripsi dan Deskripsi File Teks Berbasis Dekstop

Oleh Dosen Jika Ada Perubahan Judul

Hal Perlu

Medan, 18 Juni 2021

Rektor I,

(Cahyo Pramono, S.E., M.M.)

Pemohon,

(Ade Chintia Ningsih)

Tanggal : .....
Disahkan oleh :
Dekan

(Hamdani, ST., MT.)

Tanggal : .....
Disetujui oleh :
Dosen Pembimbing I :

(Dr Muhammad Iqbal, S.Kom., M.Kom.)

Tanggal : .....
Disetujui oleh:
Ka. Prodi Sistem Komputer

(Eko Hariyanto, S.Kom., M.Kom)

Tanggal : .....
Disetujui oleh:
Dosen Pembimbing II:

(Arnan, S.Kom., M.Kom)

FM-BPAA-2012-041

rmohonan Meja Hijau

Medan, 19 Juni 2021
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

rmat, saya yang bertanda tangan di bawah ini :

	: ADE CHINTIA NINGSIH
Tgl. Lahir	: BINJAI / 24 Oktober 1999
rang Tua	: Edi Susianto
	: 1714370176
	: SAINS & TEKNOLOGI
Studi	: Sistem Komputer
	: 085368393820
	: Jl. T. Amir Hamzah Gang Ikhlas Lingkungan V Kelurahan Jati Utomo Kecamatan Binjai Utara Kota Binjai

ermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Implementasi Algoritma Data Encryptyon pada Enkripsi dan Deskripsi File Teks Berbasis Dekstop**, Selanjutnya saya menyatakan :

elampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
idak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah ulus ujian meja hijau.
elah tercap keterangan bebas pustaka
erlampir surat keterangan bebas laboratorium
erlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
erlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkipnya ebanyak 1 lembar.
erlampir pelunasan kwintasi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
kripsi sudah dijilid lux 2 examplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 examplar untuk penguji (bentuk dan warna penjilidan diserahkan berdasarkan ketentuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
oft Copy Skripsi disimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
erlampir surat keterangan BKKOL (pada saat pengambilan ijazah)
elah menyelesaikan persyaratan point-point diatas berkas di masukan kedalam MAP
ersedia melunaskan biaya-biaya uang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1.	[102] Ujian Meja Hijau	: Rp.	1,000,000
2.	[170] Administrasi Wisuda	: Rp.	1,750,000
Total Biaya		**: Rp.**	**2,750,000**

Ukuran Toga : M

rui/Disetujui oleh :

Hormat saya

m, ST., MT.
Fakultas SAINS & TEKNOLOGI

ADE CHINTIA NINGSIH
1714370176

Surat permohonan ini sah dan berlaku bila ;
- a. Telah dicap Bukti Pelunasan dari UPT Perpustakaan UNPAB Medan.
- b. Melampirkan Bukti Pembayaran Uang Kuliah aktif semester berjalan

Dibuat Rangkap 3 (tiga), untuk - Fakultas - untuk BPAA (asli) - Mhs.ybs.

YAYASAN PROF. DR. H. KADIRUN YAHYA
PERPUSTAKAAN UNIVERSITAS PEMBANGUNAN PANCA BUDI
Jl. Jend. Gatot Subroto KM. 4,5 Medan Sunggal, Kota Medan Kode Pos 20122

SURAT BEBAS PUSTAKA
NOMOR: 4385/PERP/BP/2021

Perpustakaan Universitas Pembangunan Panca Budi menerangkan bahwa berdasarkan data pengguna perpustakaan
na saudara/i:

: ADE CHINTIA NINGSIH
: 1714370176
Semester : Akhir
: SAINS & TEKNOLOGI
Prodi : Sistem Komputer

nnya terhitung sejak tanggal 16 Juni 2021, dinyatakan tidak memiliki tanggungan dan atau pinjaman buku sekaligus
terdaftar sebagai anggota Perpustakaan Universitas Pembangunan Panca Budi Medan.

Medan, 16 Juni 2021
Diketahui oleh,
Kepala Perpustakaan

Rahmad Budi Utomo, ST.,M.Kom

Dokumen : FM-PERPUS-06-01
si : 01
Efektif : 04 Juni 2015

YAYASAN PROF. DR. H. KADIRUN YAHYA
UNIVERSITAS PEMBANGUNAN PANCA BUDI
LABORATORIUM KOMPUTER
Jl. Jend. Gatot Subroto Km 4,5 Sei Sikambing Telp. 061-8455571
Medan - 20122

KARTU BEBAS PRAKTIKUM
Nomor. 1282BL/LAKO/2021

ertanda tangan dibawah ini Ka. Laboratorium Komputer dengan ini menerangkan bahwa :

a	: ADE CHINTIA NINGSIH
M.	: 1714370176
ad/Semester	: Akhir
tas	: SAINS & TEKNOLOGI
an/Prodi	: Sistem Komputer

tan telah menyelesaikan urusan administrasi di Laboratorium Komputer Universitas Pembangunan Panca Budi Medan.

Medan, 02 November 2021
Ka. Laboratorium

Melva Sari Panjaitan, S. Kom., M.Kom.

kumen : FM-LAKO-06-01	Revisi : 01	Tgl. Efektif : 04 Juni 2015

YAYASAN PROF. DR. H. KADIRUN YAHYA

UNIVERSITAS PEMBANGUNAN PANCA BUDI

JL. Jend. Gatot Subroto KM 4,5 PO. BOX 1099 Telp. 061-30106057 Fax. (061) 4514808
MEDAN - INDONESIA
Website : www.pancabudi.ac.id - Email : admin@pancabudi.ac.id

LEMBAR BUKTI BIMBINGAN SKRIPSI

Nama Mahasiswa : ADE CHINTIA NINGSIH

NPM : 1714370176

Program Studi : Sistem Komputer

Jenjang Pendidikan : Strata Satu

Dosen Pembimbing : Arpan, S.Kom., M.Kom

Judul Skripsi : Implementasi Algoritma Data Encryptyon Standart pada Enkripsi dan Deskripsi File Teks Berbasis Dekstop

Tanggal	Pembahasan Materi	Status	Keterangan
13 Maret 2021	Acc Sempro	Disetujui	
24 April 2021	Acc seminar hasil	Disetujui	
16 Juni 2021	Acc sidang meja hijau	Disetujui	
23 Agustus 2021	Acc Jilid	Disetujui	

Medan, 02 November 2021
Dosen Pembimbing,

Arpan, S.Kom., M.Kom

YAYASAN PROF. DR. H. KADIRUN YAHYA

UNIVERSITAS PEMBANGUNAN PANCA BUDI

JL. Jend. Gatot Subroto KM 4,5 PO. BOX 1099 Telp. 061-30106057 Fax. (061) 4514808
MEDAN - INDONESIA
Website : www.pancabudi.ac.id - Email : admin@pancabudi.ac.id

LEMBAR BUKTI BIMBINGAN SKRIPSI

Nama Mahasiswa : ADE CHINTIA NINGSIH

NPM : 1714370176

Program Studi : Sistem Komputer

Jenjang Pendidikan : Strata Satu

Dosen Pembimbing : Dr Muhammad Iqbal, S.Kom., M.Kom.

Judul Skripsi : Implementasi Algoritma Data Encryptyon Standart pada Enkripsi dan Deskripsi File Teks Berbasis Dekstop

Tanggal	Pembahasan Materi	Status	Keterangan
06 Maret 2021	Acc Sempro	Disetujui	
13 Maret 2021	Acc Sempro	Disetujui	
24 April 2021	Acc Bab 3	Revisi	
24 April 2021	Acc Bab IV dan V	Revisi	
24 April 2021	Acc Seminar Hasil	Disetujui	
16 Juni 2021	Acc Sidang Meja Hijau	Disetujui	
21 Agustus 2021	Acc jilid	Disetujui	

Medan, 02 November 2021
Dosen Pembimbing,

Dr Muhammad Iqbal, S.Kom., M.Kom.

ABSTRAK

Perkembangan teknologi komputer yang sangat pesat membawa perubahan yang signifikan bagi kehidupan manusia. Namun, hal ini masih sangat membutuhkan sistem keamanan dalam pengirimannya sehingga tidak bisa digunakan oleh pihak lain yang tidak berhak dan bisa merugikan pemilik informasi baik secara material maupun intematerial, salah satunya metode yang digunakan adalah kriptografi. Kriptografi ini berfungsi untuk menyamarkan isi dari suatu dokumen yang dikirimkan kepada sipenerima pesan, Autentifikasi penting untuk memastikan keaslian dokumen sehingga dapat diketahui apabila data masih terjaga keasliannya atau sudah disalah gunakan oleh pihak yang berwenang. Perancangan Aplikasi Enkripsi dan Deskripsi Dengan Metode DES ini dimaksudkan untuk membuat dokumen teks lebih aman dengan proses penyamaran, dimana bilangan yang digunakan bisa berbentuk abjad, angka, atau tanda perintah lainnya. Pada dasarnya penyamaran dokumen ini bisa membantu kita lebih efektif dalam penyimpanan dan sistem keamanan lebih terjaga. Mengetahui proses kerja dalam melakukan verifikasi terhadap suatu dokumen elektronik. Mengetahui cara merancang dan membuat aplikasi kriptografi Mengetahui kelebihan dan kekurangan kriptografi Sebagai bahan proposal pengajuan skripsi.

***Kata Kunci** : Kriptografi, Enkripsi, Deskripsi, Metode DES,*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Allah SWT, Tuhan Yang Maha Esa yang telah memberikan rahmat-Nya kepada peneliti, sehingga Skripsi ini dapat diselesaikan oleh peneliti tepat pada waktunya dengan judul **"RANCANG BANGUN APLIKASI ENKRIPSI DAN DESKRIPSI FILE TEKS BERBASIS DESKTOP DENGAN MENGGUNAKAN METODE ALGOR TMA *DATA ECRYPTION STANDART*"**

Skripsi ini disusun dengan maksud guna memenuhi salah satu syarat memperoleh gelar Sarjana Komputer pada Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan. Dalam penyusunan skripsi ini penulis masih banyak ketidak sempurnaan atas apa yang penulis lakukan tetapi penulis menyadari sebagai manusia memiliki keterbatasan kemampuan dan hal ini tidak dapat penulis hindari, penulis berharap adanya saran dan kritik demi sempurnanya skripis ini . Pada kesempatan ini, penulis menyampaikan rasa terima kasih dan penghargaan yang sebesar-besarnya kepada :Bapak Cahyo Pramono, SE, MM, selaku Rektor Universitas Pembangunan Panca Budi Medan.

1. Bapak Hamdani, ST., M.T., selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
2. Bapak Eko Haryanto,S.Kom.,M.Kom., selaku Ketua Program Studi Sistem Komputer Universitas Pembangunan Panca Budi Medan.
3. Bapak Dr. Muhammad Iqbal, S.Kom., M.Kom., selaku Dosen Pembimbing I yang telah memberikan arahan dan membimbing dalam peyelesaian skripsi ini. dan juga Bapak Arpan, S.Kom., M.Kom. selaku Dosen pembimbing II saya yang juga telah memberikan arahan dan membimbing dalam peyelesaian skripsi ini
4. Bapak/Ibu Dosen beserta seluruh staf Universitas Pembangunan Panca Budi Medan. yang telah mendidik dan membimbing penulis selama mengikuti perkuliahan
5. Teristimewa kepada Kedua Orang Tua Ayah dan Ibu dan terima kasih atas semua pengorbanannya , yang telah banyak memberikan bimbingan dan bantuan baik moril maupun materil selama peneliti mengikuti pendidikan hingga selesainya Tugas Akhir ini.
6. Kepada seluruh rekan-rekan di program Studi Sistem Komputer Universitas Pembangunan Panca Budi Medan yang telah memberikan dukungan moril kepada penulis.

Penulis menyadari bahwa Skripsi ini masih kurang sempurna. Oleh karena itu, penulis sangat mengharapkan dan menghargai saran maupun kritikan dari pembaca dan semua pihak yang mengarah kepada perbaikan Skripsi ini. Akhir kata, penulis berharap semoga penyusunan Skripsi ini dapat bermanfaat bagi pembaca.

Medan, Juni 2021

ADE CHINTIA NINGSIH

BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi komputer yang sangat pesat membawa perubahan yang signifikan bagi kehidupan manusia. Dengan semakin berkembangnya teknologi komputer, semakin banyak aktivitas manusia yang sebelumnya harus dilakukan secara manual, sekarang dapat dilakukan dengan bantuan computer untuk menghemat waktu terutama dalam melakukan pertukaran informasi. Namun, hal ini masih sangat membutuhkan sistem keamanan dalam pengirimannya sehingga tidak bisa digunakan oleh pihak lain yang tidak berhak dan bisa merugikan pemilik informasi baik secara material maupun intematerial, salah satunya metode yang digunakan adalah kriptografi.

Kriptografi ini berfungsi untuk menyamarkan isi dari suatu dokumen yang dikirimkan kepada sipenerima pesan, Autentifikasi penting untuk memastikan keaslian dokumen sehingga dapat diketahui apabila data masih terjaga keasliannya atau sudah disalah gunakan oleh pihak yang berwenang.

Namun permasalahan yang diangkat bagaimana suatu dokumen ini tidak dapat dibaca oleh orang lain tanpa persetujuan sipemilik dokumen, sehingga mengantisipasi dari pada penyalah gunaan dari pihak lain.

Perancangan Aplikasi Enkripsi dan Deskripsi Dengan Metode DES ini dimaksudkan untuk membuat dokumen teks lebih aman dengan proses penyamaran,

dimana bilangan yang digunakan bisa berbentuk abjad, angka, atau tanda perintah lainnya. Pada dasarnya penyamaran dokumen ini bisa membantu kita lebih efektif dalam penyimpanan dan sistem keamanan lebih terjaga.

1.2. Rurumusan Masalah

Adapun masalah yang akan dibahas dalam skripsi ini yaitu:

a. Bagaimana proses penyamaran dan memecahkan proses penyamaran *file* teks tersebut.

b. Bagaimana merancang dan membuat aplikasi enkripsi dan deskripsi file dengan menggunakan Bahasa Pemrograman Java Netbeans7.4

1.3. Batasan Masalah

Karena keterbatasan dan waktu maka penelitian ini penulis akan membatasi pokok permasalahan yang akan dibahas yaitu:

a. Bahasa Pemrograman yang digunakan adalah bahasa pemrograman Java Netbeans 7.4

b. Aplikasi yang dibuat berbasis desktop.

1.4 Tujuan Penelitian

Adapun tujuan dari penulisan ini sebagai berikut:

a. Mengetahui proses kerja dalam melakukan verifikasi terhadap suatu dokumen elektronik.

b. Mengetahui cara merancang dan membuat aplikasi kriptografi

c. Mengetahui kelebihan dan kekurangan kriptografi

d. Sebagai bahan proposal pengajuan skripsi.

1.5. Manfaat Penelitian

Hasil penelitian akan memberikan manfaat bagi :

1. Peneliti sendiri sebagai penerapan bidang ilmu untuk membantu pegguna dalam mengenskripsi data rahasia.
2. Dapat memberikan pemahaman mengenai metode *DES* untuk merahasiakan pesan teks.
3. Bagi penelitian berikutnya, sebagai referensi untuk melanjutkan penelitian berikutnya.

BAB II

LANDASAN TEORI

2.1 Enkripsi dan Deskripsi

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita [*bruce Schneier - Applied Cryptography*]. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data [*A. Menezes, P. van Oorschot and S. Vanstone - Handbook of Applied Cryptography*].Tidak semua aspek keamanan informasi ditangani oleh kriptografi. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

a) Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
b) Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
c) Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang

saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.

d) Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat

2.2 DES (Data Encryption Standard)

a) **Sejarah**

DES atau Singkatan dari Data Encryption Standard merupakan algoritma penyandian yang diadopsi dan dibakukan oleh NBS (National Bureau Standard) yang kini menjadi NIST (National Institute of Standards and Technology) pada tahun 1977 sebagai FIPS 46 (Federal Information Processing Standard). DES bermula dari hasil riset Tuchman Meyer yang diajukan sebagai kandidat Sandi Standard Nasional yang diusulkan oleh NBS. Konon katanya, algoritma yang dikembangkan oleh Tuchman Meyer ini merupakan algoritma terbaik dari semua kandidat Sandi Standard Nasional. Pada mulanya, algoritma yang kini disebut DES, memiliki panjang kunci sandi 128 bit. Namun selama proses pengadopsian, NBS melibatkan NSA (National Security Agency), dan algoritma sandi ini mengalami pengurangan ukuran kunci sandi dari 128 bit menjadi 56 bit saja. Sebagian orang mungkin mengira bahwa pengurangan panjang kunci

sandi ini merupakan usulan NSA untuk melemahkan algoritma Tuchman Meyer karena motif politik tertentu. Entah itu untuk mempermudah penyadapan atau untuk melemahkan pengamanan informasi lawan politik. Mungkin NSA menginginkan algoritma Tuchman Meyer ini "cukup aman" untuk digunakan warga sipil, tetapi mudah dipecahkan oleh organisasi besar semisal NSA dengan peralatan canggihnya. Bila dibandingkan dengan performa komputer personal pada saat itu, algoritma sandi dengan panjang kunci 56 bit dapat dikatakan cukup aman bila digunakan oleh orang-orang "biasa", tapi dapat dengan mudah dipecahkan dengan peralatan canggih dan tentunya kepemilikan alat canggih ini hanya dapat dijangkau oleh organisasi elit seperti NSA. Dengan dukungan dana yang melimpah, pembuatan alat brute-force DES bukanlah hal yang mustahil pada saat itu. Kini algoritma DES sudah usang dan keamanannya pun sudah tidak dapat dipertanggung jawabkan lagi. Kini komputer personal pun sudah cukup untuk membobol algoritma DES, apalagi dengan adanya teknologi parallel computing dan internet yang berkembang pesat. DES telah secara resmi digantikan fungsinya oleh AES (Advanced Encryption Standard) dengan panjang kunci sandi 128, 192 dan 256 bit. Kendatipun kita telah mengetahui bahwa algoritma AES sudah kuno dan tidak aman, tidak ada salahnya jika kita mempelajari algoritma ini untuk tujuan hobi atau pendidikan. Perlahan tapi pasti, belajar dari algoritma yang sederhana

dan perlahan-lahan menuju algoritma lain yang lebih kompleks. Algoritma DES merupakan algoritma enkripsi blok simetris. DES dikatakan enkripsi blok karena pemrosesan data baik enkripsi maupun dekripsi, diimplementasikan per blok (dalam hal ini 8 byte). DES dikatakan enkripsi simetris karena algoritma yang digunakan untuk enkripsi relatif atau bahkan sama persis dengan algoritma yang digunakan dalam proses dekripsi. Proses enkripsi dapat didefinisikan secara sederhana sebagai proses penterjemahan data “asli” yang “jelas” dan “kasat mata” yang dapat dipahami maknanya.

secara langsung menjadi data lain yang terlihat “ buram ” atau “acak” sehingga tidak dapat dipahami secara langsung, sedemikian rupa sehingga makna informasi yang disembunyikan tidak lagi dapat diketahui secara langsung kecuali dengan mengembalikan informasi tersebut ke bentuk aslinya. Sedangkan proses dekripsi dapat didefinisikan secara sederhana sebagai proses pengembalian bentuk data, dari data “buram” atau “acak” menjadi data “asli” yang “jelas” dan “kasat mata” yang dapat dipahami maknanya. Algoritma enkripsi umumnya dilengkapi semacam kata sandi (password), untuk memvariasikan fungsi enkripsi tersebut. Data yang sama, kunci yang sama dan algoritma yang sama akan menghasilkan data enkripsi yang sama. Dalam algoritma penyandian DES, kunci yang digunakan dalam proses enkripsi dan dekripsi haruslah sama, supaya data

dapat dikembalikan ke bentuk aslinya. Bisa jadi, karena “kesamaan” kunci inilah DES juga dinamakan algoritma enkripsi simetris. Inti dari proses enkripsi adalah penyembunyian data dengan mengaburkan data “asli” dan mengurangi keteraturan informasi, sehingga data tersebut tidak dapat “dibaca” kecuali oleh pihak yang berhak. Berbagai algoritma enkripsi sengaja dibuat untuk melindungi informasi dari penyadapan, karena ada kemungkinan terjadinya penyadapan saat data melewati media hantar (media hantar dapat berupa suara, surat, email, kabel, kertas, frekwensi radio atau apapun itu). Seandainya penyadap dapat menyadap semua informasi yang melalui media hantar, idealnya hasil sadapan tersebut hanya menghasilkan data “sampah” yang tidak berguna. Semua algoritma kriptografi diciptakan untuk mewujudkan kondisi ideal tersebut, tapi sayangya kondisi tersebut sangat sulit dicapai, karena selalu ada cara untuk membalikkan informasi sadapan ke bentuk aslinya.
Dalam DES, algoritma dekripsi tepatnya merupakan proses kebalikan (inverse) algoritma enkripsi. Dalam prakteknya proses pembalikan (proses dekripsi) ini diimplementasikan dengan membalikkan urutan sub kunci yang digunakan dalam proses enkripsi, selebihnya algoritma enkripsi dan dekripsi adalah sama. Algoritma enkripsi DES bekerja dengan mengolah blok data 8 byte (64 bit) dengan blok kunci 8 byte (64 bit). Proses penyandian dalam DES diawali dengan fungsi pengacakan bit yang dinamai IP (Initial Permutation) kemudian fungsi inti DES yang diulang

sebanyak 16 kali dan terakhir ditutup dengan fungsi pengacakan bit lain yang dikenal denagn nama IP-1 (Inverse Initial Permutation). Pada sisi lain algoritma penjadwalan sub kunci akan menghasilkan 16 sub kunci secara berurutan dari parameter kunci yang diberikan untuk digunakan pada setiap putaran fungsi inti DES. Sub kunci pertama untuk putaran pertama, sub kunci kedua untuk putaran kedua dan seterusnya hingga putaran ke 16. Perlu diingat, kendatipun slot kunci yang disediakan digunakan berukuran 8 byte (64 bit), ternyata pada faktanya ukuran kunci yang digunakan hanya sebanyak 56 bit saja, karena bit paling signifikan (MSB) dari setiap bit diabaikan.Jadi sebenarnya ukuran kunci DES adalah 56 bit. Adapun Ilustrasi penyandian DES dalam diagram blok dapat dilihat pada gambar di samping. Algoritma penjadwalan sub kunci dibentuk dari pengacakan bit dan pemutaran kiri ruas kanan dan kiri kunci. Pertama kali, bit-bit kunci diacak dengan Permutation Choice 1 dan dibagi dua menjadi ruas kiri dan ruas kanan. Kedua ruas tersebut kemudian diputar kiri dan diacak kembali dengan Permutation Choice 2 untuk menghasilkan sub kunci. Jumlah pemutaran ke kiri ditentukan secara spesifik untuk setiap sub kunci.

Rinciannya adalah sebagai berikut.

No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Jumlah	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Gambar 2.1 Rincian Permutation Choice

Untuk lebih lanjut, mari terlebih dahulu kita bahas detail algoritma penjadwalan sub kunci kemudian algoritma enkripsi dan terakhir algoritma dekripsi. Inti dari semua proses permutasi dalam DES adalah pengacakan bit. Sebagai contoh, jika masukan permutasi sebanyak n bit, maka akan ada sebanyak 2n kemungkinan masukan permutasi dan ada 2n kemungkinan hasil permutasi. Setiap satu kemungkinan masukan akan berpasangan dengan satu kemungkinan keluaran. Sebelum proses penjadwalan kunci dimulai, kunci terlebih dahulu dipetakan menjadi matriks 8x8 dan diberi indeks. Dalam setiap byte, indeks paling kecil melambangkan LSB dan indeks paling besar melambangkan MSB. Sebagai contoh, indeks ke 1 melambangkan LSB byte pertama, index ke 8 melambangkan MSB byte pertama, indeks ke 9 melambangkan LSB byte kedua, indeks ke 16 melambangkan MSB byte kedua dan seterusnya hingga indeks ke 64 yang melambangkan MSB byte ke 8. Mari kita perhatikan contoh dibawah ini.

Kunci = 0x01, 0x23, 0x45, 0x67, 0x89, 0xab, 0xcd, 0xef

Setelah pemetaan, hasilnya adalah sebagai berikut.

Matriks Indeks							
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Hasil Pemetaan							
1	0	0	0	0	0	0	0
1	1	0	0	0	1	0	0
1	0	1	0	0	0	1	0
1	1	1	0	0	1	1	0
1	0	0	1	0	0	0	1
1	1	0	1	0	1	0	1
1	0	1	1	0	0	1	1
1	1	1	1	0	1	1	1

Gambar 2.2 Hasil Pemetaan

Matriks Indeks Hasil Pemetaan

Pengacakan bit Permutation Choice-1 akan mengolah 8 byte blok kunci menjadi 56 bit sub kunci yang siap diproses lebih lanjut. Untuk lebih mudahnya, proses pengacakan bit dilambangkan dengan pengacakan indeks bit yang bersangkutan. Berikut ini adalah detail Permutation Choice 1.

Kunci

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

→

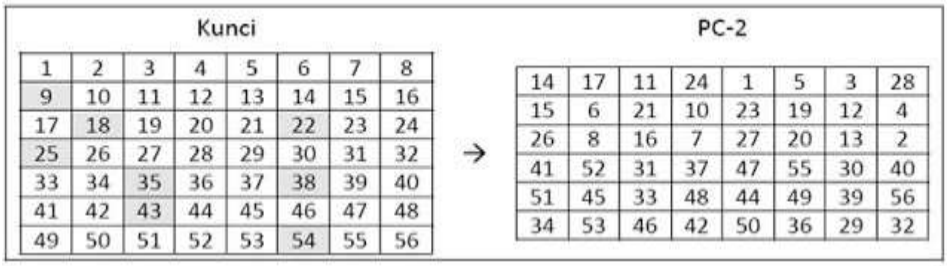
PC1

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
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Gambar 2.3 Detail Permutation Choice 1

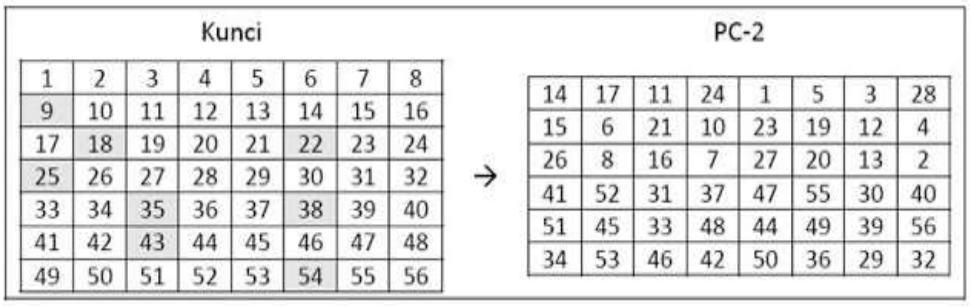
Setelah kunci diacak dengan Permutation Choice 1, hasil pengacakan bit tersebut kemudian dibagi 2, yakni ruas kiri dan ruas kanan, masing masing berukuran 28 bit (ditandai dengan garis tebal pada hasil Permutation Choice 1). Selanjutnya kedua ruas tersebut kemudian mengalami pemutaran kiri sebanyak jumlah yang tertera pada tabel penjadwalan jumlah pemutaran yang telah kita bahas sebelumnya.Berikut ini adalah ilustrasi pemutaran ke kiri sebanyak 1 kali (untuk ruas kiri atau ruas kanan kunci yang panjangnya 28 bit). Untuk pemutaran ke kiri dengan jumlah yang lebih besar, cukup mengulangi proses diatas sebanyak yang diinginkan.

Setelah ruas kiri dan ruas kanan diputar kiri dengan jumlah tertentu, selanjutnya hasil pemutaran tersebut digabungkan kembali menjadi 56 bit dan diacak dengan Permutation Choice-2 untuk menghasilkan sub kunci.Rincian Permutation Choice 2 adalah sebagai berikut.



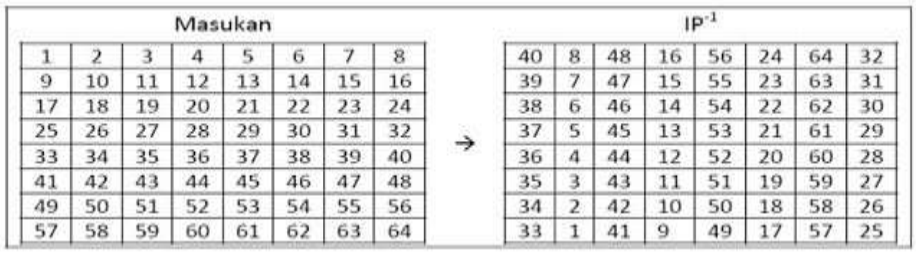
Gambar 2.4 Rincian Permutation Choice 2

Karena jumlah keluaran Permutation Choice 48 bit sementara masukannya 56 bit, dengan demikian ada 8 bit yang “dihilangkan”. Bit-bit yang tidak muncul dalam keluaran Permutation Choice 2 diwarnai abuabu. Selanjutnya, mari kita perjelas algoritma enkripsinya. Setelah melihat diagram blok secara keseluruhan proses enkripsi, ada tiga hal yang perlu digarisbawahi dan dibahas lebih lanjut yaitu, pertama IP (Initial Permutation), kedua detail fungsi F dan IP 1 (Inverse Initial Permutation. Selama proses enkripsi, pertama data dipetakan dan diberi indeks dengan prosedur sama persis seperti pemberian indeks pada penjadwalan kunci yang telah didiskusikan sebelumnya. Selanjutnya hasil pemetaan diacak dengan menggunakan Initial Permutation dengan rincian sebagai berikut Masukan IP



Gambar 2.5 Proses Initial Permutation

Setelah data melewati proses Initial Permutation, data yang akan disandikan kemudian dibagi menjadi dua ruas, yaitu ruas kiri dan ruas kanan yang masIng-masing lebarnya 4 byte (32 bit). Pada setiap putaran, ruas kanan dan sub kunci yang bersangkutan diproses dalam fungsi F dan hasilnya di XOR dengan ruas kiri ruas kanan dan kiri dipertukarkan. Proses ini diulang sebanyak 16 kali. Pada putaran terakhir ruas kiri dan ruas kanan dipertukarkan kembali untuk menghilangkan efek pertukaran pada putaran terakhir.Hasil ini kemudian diacak kembali dengan menggunakan IP 1 (Inverse Initial Permutation).XOR merupakan fungsi Boolean yang didefinisikan dengan table. Initial Permutatrion dan Inverse Initial Permutation memiliki karakter saling menetralkan. Dalam notasi matematika, IP−1(IP(A))= A. Inverse Initial Permutation didefinisikan sebagai berikut.



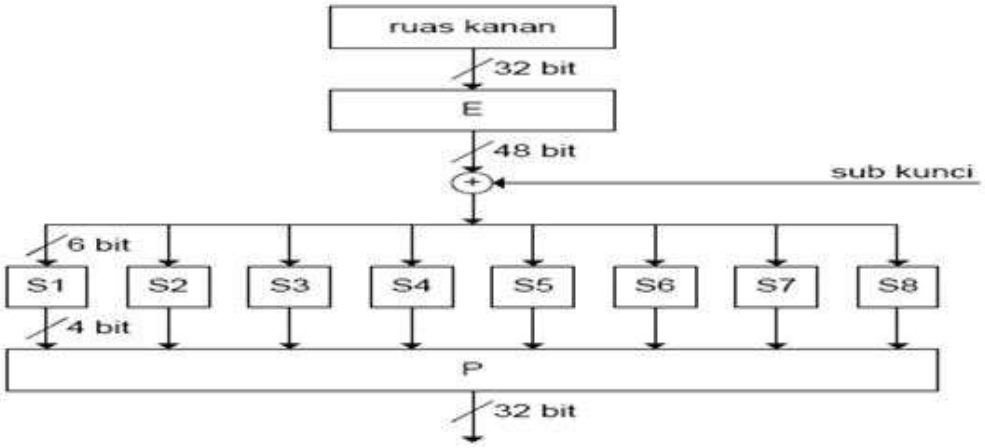
Masukan							
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

→

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Gambar 2.6 Inverse Initial Permutation

Fungsi F merupakan fungsi inti kompleks yang terdiri dari beberapa proses. Fungsi F menerima dua parameter, yaitu sub kunci dan ruas kanan data yang akan dienkripsi. Berikut ini adalah diagram blok detail fungsi F. Pada fungsi F, ruas kanan (32 bit) diacak sekaligus diperluas dengan permutasi E menjadi 48 bit. Hasil pengacakan tersebut kemudian di XOR dengan sub kunci yang telah ditetapkan dengan putaran yang bersangkutan. Hasil XOR kemudian dipecah menjadi 8 unit yang masing-masing lebarnya 6 bit.Setiap unit tersebut kemudian disubstitusikan dalam SBOX S1 hingga S8. 6 bit paling kiri disubstitusikan ke dalam S1 dan 6 bit paling kanan disubstitusikan ke dalam S8. Hasil setiap substitusi kemudian digabungkan menjadi data selebar 48 bit yang kemudian diacak dan diperpendek dengan permutasi P menjadi 32 bit. Hasil permutasi P kemudian dinyatakan sebagai keluaran fungsi F yang nantinya akan di XOR kan dengan ruas kiri data yang akan dienkripsi.



Gambar 2.7 Hasil Permutasi P

Sekarang mari kita bahas detail fungsi F satu per satu. Pertama, permutasi E memetakan 32 bit masukan menjadi 48 bit keluaran. Karena lebar keluaran lebih besar dari lebar masukan, maka ada beberapa bit masukan yang digandakan untuk mengisi kekosongan. Permutasi E didefinisikan sebagai berikut

Ruas kanan

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

→

E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Gambar 2.8 Permutasi E

Kedua, DES memiliki 8 buah SBOX (S1 hingga S8) yang memiliki masukan selebar 6 bit dan keluaran selebar 4 bit. Karena lebar keluaran SBOX lebih kecil daripada lebar masukannya, maka adakemungkinan beberapa kombinasi masukan yang berbeda akan menghasilkan keluaran yang sama. Seandainya masukan setiap SBOX adalah 1 2 3 4 5 6 x x x x x x maka S1 hingga S8 didefinisikan

S1	$x_1x_2x_3x_4$															
x_5x_6	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	e	4	d	1	2	f	b	8	3	a	6	c	5	9	0	7
01	0	f	7	4	e	2	d	1	a	6	c	b	9	5	3	8
10	4	1	e	8	d	6	2	b	f	c	9	7	3	a	5	0
11	f	c	8	2	4	9	1	7	5	b	3	e	a	0	6	d

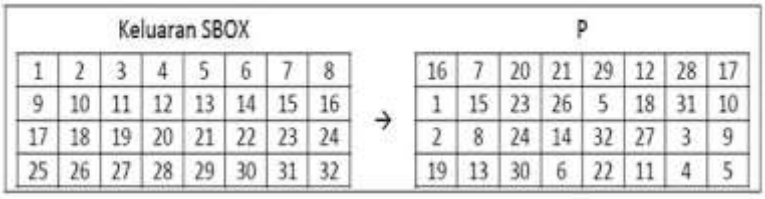
S2	$x_1x_2x_3x_4$															
x_5x_6	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	f	1	8	e	6	b	3	4	9	7	2	d	c	0	5	a
01	3	D	4	7	f	2	8	e	c	0	1	a	6	9	b	5
10	0	e	7	b	a	4	d	1	5	8	c	6	9	3	2	f
11	d	8	a	1	3	f	4	2	b	6	7	c	0	5	e	9

S3	$x_1x_2x_3x_4$															
x_5x_6	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	a	0	9	e	6	3	f	5	1	d	c	7	b	4	2	8
01	d	7	0	9	3	4	6	a	2	8	5	e	c	b	f	1
10	d	6	4	9	8	f	3	0	b	1	2	c	5	a	e	7
11	1	a	d	0	6	9	8	7	4	f	e	3	b	5	2	c

S4	$x_1x_2x_3x_4$															
x_5x_6	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	7	d	e	3	0	6	9	a	1	2	8	5	b	c	4	f
01	d	8	b	5	6	f	0	3	4	7	2	c	1	a	e	9
10	a	6	9	0	c	b	7	d	f	1	3	e	5	2	8	4
11	3	f	0	6	a	1	d	8	9	4	5	b	c	7	2	e

Gambar 2.9 Hasil SBOX

Ketiga, hasil substitusi SBOX kemudian digabungkan menjadi 32 bit dan diacak dengan permutasi P dan hasil permutasi P merupakan keluaran fungsi F yang nantinya di XOR dengan ruas kiri. Permutasi P didefinisikan sebagai berikut.



Gambar 2.10 Hasil Permutasi P

Dalam DES, algoritma yang digunakan dalam proses enkripsi sama persis dengan algoritma yang digunakan dalam proses dekripsi, hanya saja penggunaan sub kuncinya saja yang berbeda. Dalam proses dekripsi, urutan sub kunci yang digunakan merupakan kebalikan urutan sub kunci yang digunakan dalam proses enkripsi. Implementasi Operasi yang digunakan dalam algoritma DES merupakan operasi-operasi sederhana semisal move, bit copy, XOR, lookup, shift dan rotate. Semua operasi tersebut tersedia dalam mikroprosesor/mikrokontroler 8 bit.Dengan demikian dapat kita simpulkan bahwa DES dapat diterapkan dalam platform 8 bit.Semua operasi permutasi dalam DES, baik IP, IP 1, PC 1, PC 2, E dan P, pada intinya hanyalah operasi penyalinan bit. Jika instruksi penyalinan bit tidak tersedia, maka permutasi juga dapat diimplementasikan dengan operasi shift, dengan memanfaatkan carry yang timbul dari setiap instruksi shift. Selain itu, operasi substitusi dengan SBOX juga dapat dengan mudah diimplementasikan menggunakan table lookup dengan ukuran yang masih dapat dijangkau. Dalam platform 32 atau 64 bit, DES dapat diimplementasikan lebih effektif lagi, tapi sayangnya operasi bit

per bit seperti permutasi mungkin sedikit menyita performa prosesor dan memperlambat laju enkripsi per detik.

2.3 Algoritma Sandi

Algoritma sandi adalah algoritma yang berfungsi untuk melakukan tujuan kriptografis. Algoritma tersebut harus memiliki kekuatan untuk melakukan (dikemukakan oleh Shannon):

konfusi/pembingungan (confusion), dari teks terang sehingga sulit untuk direkonstruksikan secara langsung tanpa menggunakan algoritma dekripsinya difusi / peleburan (difusion), dari teks terang sehingga karakteristik dari teks terang tersebut hilang. sehingga dapat digunakan untuk mengamankan informasi. Pada implementasinya sebuah algoritmas sandi harus memperhatikan kualitas layanan/Quality of Service atau QoS dari keseluruhan sistem dimana dia diimplementasikan.Algoritma sandi yang handal adalah algoritma sandi yang kekuatannya terletak pada kunci, bukan pada kerahasiaan algoritma itu sendiri.Teknik dan metode untuk menguji kehandalan algoritma sandi adalah kriptanalisa.Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu yang berisi elemen teks terang /plaintext dan yang berisi elemen teks sandi/ciphertext. Enkripsi dan dekripsi merupakan fungsi transformasi antara himpunan-himpunan tersebut. Apabila elemen-elemen teks terang dinotasikan dengan P, elemen-elemen teks sandi dinotasikan dengan C, sedang untuk proses enkripsi dinotasikan dengan E, dekripsi dengan notasi D.

Enkripsi : E(P) = C

Dekripsi : D(C) = P atau D(E(P)) = P

Secara umum berdasarkan kesamaan kuncinya, algoritma sandi dibedakan menjadi :

A. kunci-simetris/symetric-key, sering disebut juga algoritma sandi konvensional karena umumnya diterapkan pada algoritma sandi klasik
B. kunci-asimetris/asymetric-key

Berdasarkan arah implementasi dan pembabakan jamannya dibedakan menjadi

A. algoritma sandi klasik classic cryptography
B. algoritma sandi modern modern cryptography

Berdasarkan kerahasiaan kuncinya dibedakan menjadi :

A. algoritma sandi kunci rahasia secret-key
B. algoritma sandi kunci publik publik-key

Pada skema kunci-simetris, digunakan sebuah kunci rahasia yang sama untuk melakukan proses enkripsi dan dekripsinya. Sedangkan pada sistem kunci-asimentris digunakan sepasang kunci yang berbeda, umumnya disebut kunci public (public key) dan kunci pribadi (private key), digunakan untuk proses enkripsi dan proses dekripsinya. Bila elemen teks terang dienkripsi dengan menggunakan kunci pribadi maka elemen teks sandi yang dihasilkannya hanya bisa didekripsikan dengan menggunakan pasangan kunci pribadinya. Begitu juga sebaliknya, jika kunci pribadi

digunakan untuk proses enkripsi maka proses dekripsi harus menggunakan kunci publik pasangannya.

A. **algoritma sandi kunci - simetris**

Beberapa contoh algoritma yang menggunakan kunci-simetris:

DES - Data Encryption Standard

blowfish

twofish

MARS

IDEA

3DES - DES diaplikasikan 3 kali

AES - Advanced Encryption Standard, yang bernama asli rijndael.

B. Algoritma Chaum's Blind Signature

Algoritma Chaum's Blind Signature adalah penandatanganan pesan yang dibuat oleh sipengirim pesan, dan ditandatangani oleh penerima pesan. Pada *Blind signature*, pesan ditandatanganin si penandatanganan tanpa mengetahui isi pesan yang akan ditandatangani terlebih dahulu. Mekanisme *Blind Signature* sebagai berikut:

a. Pihak pengirim pesan membangkitkan factor blinding secara acak terhadap dokumen yang bersangkutan, kemudian mengirimkan dokumen yang telah disamarkan tersebut ke pihak penerima.

b. Pihak penerima menerima pesan dan langsung menandatanganinya.

Pengirim pesan mengeluarkan *factor blinding* dari dokumen sehingga yang tertinggal pada dokumen tersebut adalah isi pesan yang sebenarnya dan tanda tangan

penerima pesan.Sebenarnya mekanisme ini dapat dimanfaatkan oleh pihak-pihak tertentu untk kepentingan sepihak yang mungkin dapat merugikan si pemberi tanda tangan, misalnya untuk menandatangani bukti bahwa si pemberi tanda tangan berhutang kepada seseorang, dan sebagainya.Karena itu untuk mencegah dampak negatif yang ditumbulkan dari adanya *Blind Signature* ini adalah dengan menerapkan konsep probabilitas, yaitu dengan mengambil sampel dokumen. Jika sampel dokumen yang dipilih berisi pesan yang wajar menurut penerima pesan, maka pesan lainnya dianggap sama wajarnya. Mekanismenya adalah sebagai berikut:

a. Pengirim mengirimkann pesan yang telah disisipkan factor blinding didalamnya kepada penerima, kemudian penerima memilih pesan sejumlah n-1.
b. Penerima meminta *factor blinding* dari sejumlah n-1 dokumen yang dipilihnya ke pengirim.
c. Penerima dapat membuka pesan tersebut setelah menghilangkan *factorblinding.*

Berdasarkan prinsip yang dimilikinya, *Blind Signature* dapat digunakan di aplikasi seperti Sistem *Cash Payment dan Sistem Voting* Elektronik.Misalnya pada system voting setiap kotak suara harus disahkan oleh pihak yang berwenang terhadap pemilihan sebelum diperhitungkan. Di luar system pihak ini seharusnya mengecek apakah pemilih memang memenuhi syarat sebagai pemilih dan tidak memilih lebih dari satu kali dengan memasukkan ke kotak suara lain. Dalam hal ini penghitung suara tidak

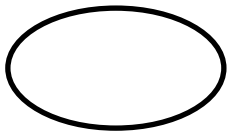
mengetahui bahwa subjek S dipilih pemilih mana saja, atau bahkan apakah subjek S dipilih oleh P.

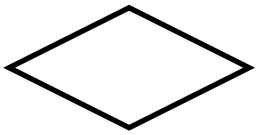
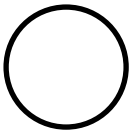
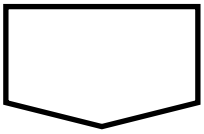
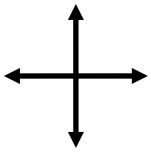
Proses pada *Blinding Signature* membutuhkan komputasi untuk mengantisipasi seluruh kemungkinan jenis tanda tangan. Untuk sebuah jenis kurang lebih ada sekitar lebih dari satu tanda tangan yang harus diantisipasi.

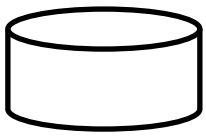
1. Flowchart

adalah sekumpulan simbol-simbol atau skema yang menunjukkan atau menggambarkan rangkaian kegiatan-kegiatan program dari awal hingga akhir. *Flowchart* digunakan untuk menggambarkan urutan langkah-langkah pekerjaan suatu algoritma. Berikut penjelasan lambang-lambang yang digunakan pada *flowchart* sebagai berikut.

Tabel 2.1 Simbol - Simbol Flowchart

No.	Simbol	Fungsi
1.		*Terminal* berfungsi untuk memulai dan mengakhiri suatu program.
2.		Proses suatu symbol yang menunjukkan setiap pengolahan yang dilakkan oleh komputer.
3.		*Input-Ouput* berfungsi untuk memasukkan atau menunjukkan hasil dari proses.

4.		*Decission* suatu kondisi yang akan menghasilkan beberapa kemungkinan jawaban atau pilihan.
5.		*Connector* suatu prosedur akan masuk atau keluar melalui symbol ini dalam lembar yang sama.
6.		*Predifined Process* suatu symbol untuk menyediakan tempat-tempat pengolahan dalam storage.
7.		*Off Line Connector* merupakan symbol untuk masuk atau keluarnya suatu prosedur pada lebar kertas yang lain.
8.		*Arus atau Flow* Prosedur yang akan dapat dilakukan.
9.		*Document* merupakan symbol untuk data yang berbentuk kertas maupun informasi.
10.		Simbol untuk output yang ditentukan kesuatu device, seperti printer ataupun plotter.
11.		Untuk menyatakan sekumpulan langkah proses yang ditulis secara prosedur.

12.		*Storage* untuk menyimpan data

2. Data Flow Diagram (DFD)

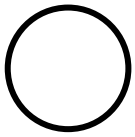
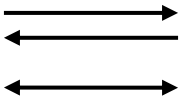
*Data Flow Diagram*atau*DFD* merupakan gambaran suatu sistem yang telah ada atau sistem baru yang dikembangkan secara logika tanpa mempertimbangkan lingkungan fisik dimana data tersebut mengalir.Dengan adanya Data Flow Diagram maka pemakai sistem yang kurang memahami dibidang komputer dapat mengerti sistem yang sedang berjalan.z

Pada tahun 1967, Martin dan Estrin memperkenalkan suatu algorima program dengan menggunakan simbol lingkaran dan panah untuk mewakili arus data. E. Yourdan dan L. L. Constantine juga menggunakan notasi simbol ini untuk menggambarkan arus data dalam perancangan program. G.E. Whitehouse tahun 1973 juga menggunakan notasi semacam ini untuk membuat model-model sistem matematika. Penggunaan notasi dalam diagram arus data ini sangat membantu sekali untuk memahami suatu sistem pada semua tingkat kompleksitasnya seperti yang diungkapkan oleh Chris Gane dan Trish Sarson. Pada tahap analisis, penggunaan notasi ini sangat membantu sekali di dalam komunikasi dengan pemakai sistem untuk memahami sistem secara logika.

DFD sering digunakan untuk menggambarkan suatu sistem yang telah ada atau sistem baru yang akan dikembangkan secara logika tanpa mempertimbangkan

lingkungan fisik dimana data tersebut mengalir (misalnya lewat telpon, surat dan sebagainya) atau lingkungan fisik dimana data tersebut akan disimpan (misalnya *file* kartu, microfile, harddisk, tape, disket dan lain sebagainya). DFD merupakan alat yang cukup populer sekarang ini, karena dapat menggambarkan arus data di dalam sistem dengan terstruktur dan jelas. Ada beberapa simbol Data Flow Diagram, yaitu :

Tabel 2.2 Simbol Data Flow Diagram (DFD)

Simbol	Nama	Keterangan
	Entitas Eksternal	Dapat berupa orang/unit terkait yang berinteraksi dengan sistem tetapi di luar sistem
	Proses	Orang, unit yang mempergunakan atau melakukan transformasi data. Komponen fisik tidak didefenisikan.
	Aliran Data	Aliran data dengan arah khusus dari sumber ke tujuan.
	*Data Store*	Penyimpanan data atau tempat data direfer oleh proses
	*Display*	Menunjukkan *output* yang ditampilkan
	Penghubung	Digunakan untuk menunjukkan sambungan bagan alir

3. Netbeans 7.4

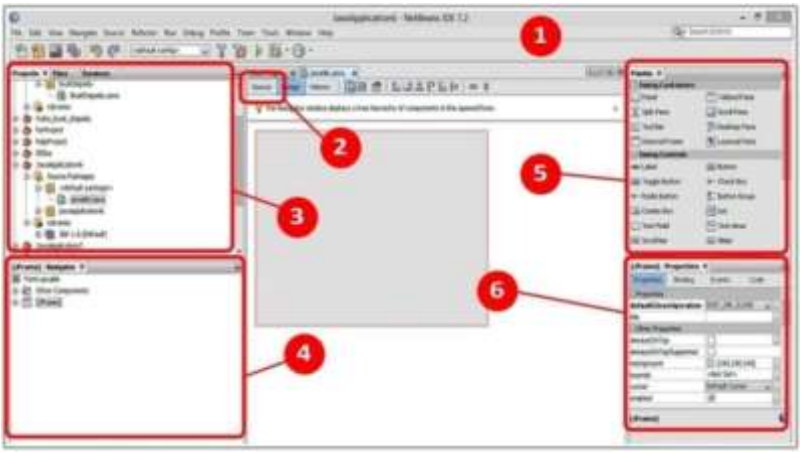
Netbeans merupakan sebuah aplikasi *Integrated Development Environment* (IDE) yang berbasiskan Java dari Sun Microsystems yang berjalan di atas swing. Swing merupakan sebuah teknologi Java untuk pengembangan aplikasi *desktop* yang dapat berjalan pada berbagai macam *platform* seperti Windows, Linux, Mac OS X dan Solaris. Sebuah IDE merupakan lingkup pemrograman yang di integrasikan ke dalam suatu aplikasi perangkat lunak yang menyediakan Graphic User Interface (GUI), suatu kode editor atau teks, suatu *compiler* dan suatu *debugger*.

Netbeans juga digunakan oleh sang programmer untuk menulis, meng-*compile*, mencari kesalahan dan menyebarkan program Netbeans yang ditulis dalam bahasa pemrograman Java namun selain itu dapat juga mendukung bahasa pemrograman lainnya dan program ini pun bebas untuk digunakan dan untuk membuat professional *desktop, enterprise*, *web*, dan *mobile applications* dengan Java *language*, C/C++, dan bahkan *dynamic languages* seperti PHP, JavaScript, Groovy, dan Ruby.

Netbeans merupakan sebuah proyek kode terbuka yang sukses dengan pengguna yang sangat luas, komunitas yang terus tumbuh, dan memiliki hampir 100 mitra (dan terus bertambah). Sun Microsystems mendirikan proyek kode terbuka Netbeans pada bulan Juni 2000 dan terus menjadi sponsor utama. Dan saat ini pun netbeans memiliki 2 produk yaitu Platform Netbeans dan Netbeans IDE. Platform Netbeans merupakan *framework* yang dapat digunakan kembali (*reusable*) untuk menyederhanakan pengembangan aplikasi *desktop* dan Platform NetBeans juga menawarkan layanan-

layanan yang umum bagi aplikasi *desktop*, mengijinkan pengembang untuk fokus ke logika yang spesifik terhadap aplikasi.

Dalam Netbeans terbagi beberapa komponen GUI yang umum digunakan, antara lain:

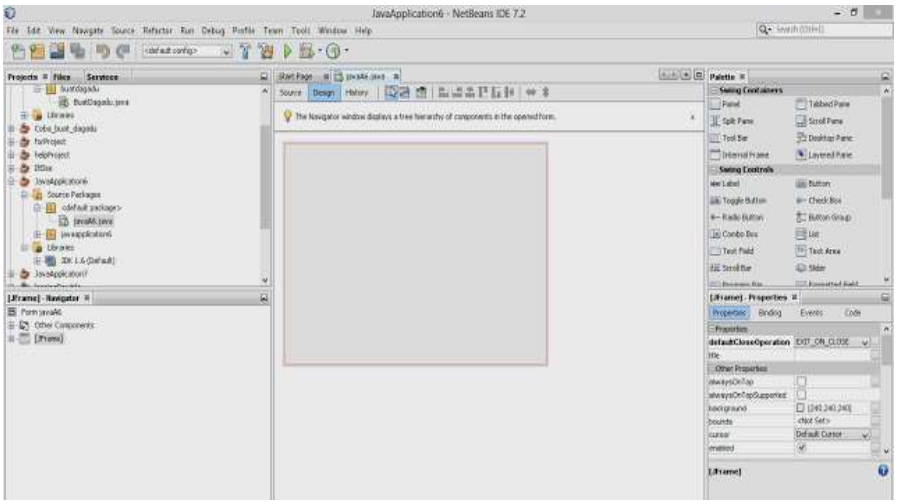


Gambar 2.11 GUI Netbeans 7.4

Keterangan:

1. GUI Builder

   GUI Builder merupakan jendela utama yang di dalamnya terdapat komponen untuk merancang GUI.



Gambar 2.12 GUI Builder

2. Source Area

   Source Area merupakan jendela yang digunakan untuk menambahkan atau mengubah kode program yang ada pada pemograman Java.

Gambar 2.13 Source Area

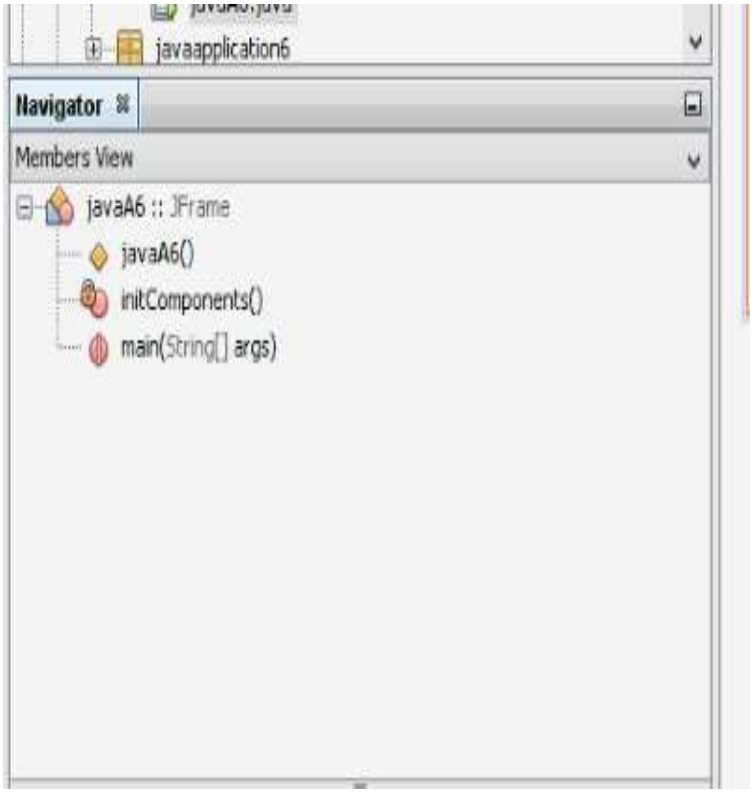
3. Panel Project

   Panel Project menampilkan Project yang dirancang.

Gambar 2.14 Panel Project

4. Panel Navigator

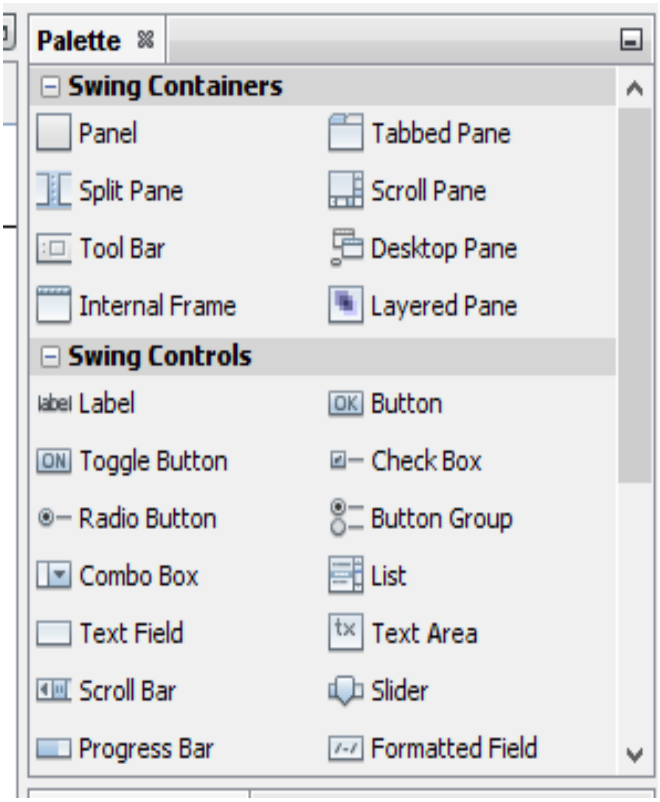
   Panel Navigator merupakan jendela yang menampilkan pohon pewarisan dari semua komponen *form* yang di buka seperti button, label, menu, timer, dan sebagainya.



Gambar 2.15 Panel Navigator

5. Panel Palette

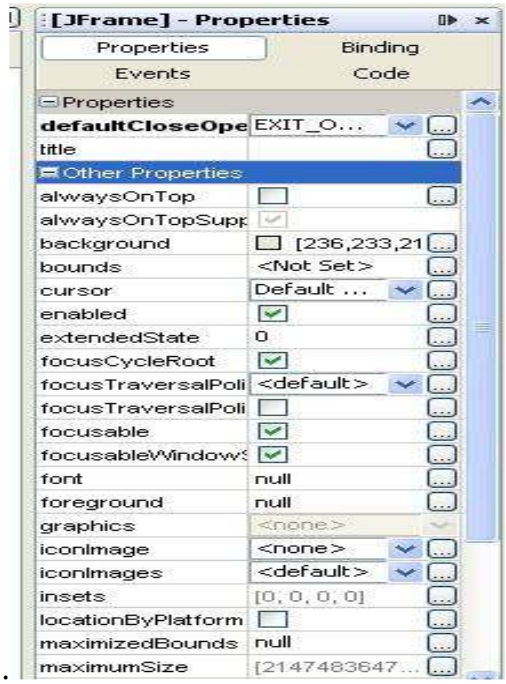
Panel Pallete merupakan panel yang menydiakan tool-tool untuk mendesain *form* berbasis grafis (GUI). Dimana setiap kategori menyediakan tool-tool GUI Builder sesuai dengan kategorinya.Untuk menggunakannya, tinggal klik dan menyeret tool-tool kedalam area desain.



Gambar 2.16 Panel Palette

6. Panel Properties

Panel Properties berfungsi untuk menampilkan *property* komponen yang aktif untuk mengatur *property* yang dimiliki oleh suatu komponen



Gambar 2.17 Panel Properties

IDE Netbeans sangatlah diperlukan dalam pembangunan program perangkat lunak, Karena Netbeans merupakan platform yang baik untuk sebuah pembangunan program perangkat lunak.Oleh karena itu IDE Netbeans sering dipakai di kalangan programmer karena User Friendly. IDE Netbeans sendiri adalah sebuah GUI (Graphical User Interface) atau pembangunan program perangkat lunak secara visual(berbasis Desktop). Manfaat dari pada Netbeans sendiri adalah Mempermudah user untuk mendesain programnya sendiri serta menghemat source code yang akan ditulis dan juga menghemat waktu.IDE Netbeans juga memiliki banyak fasilitas di

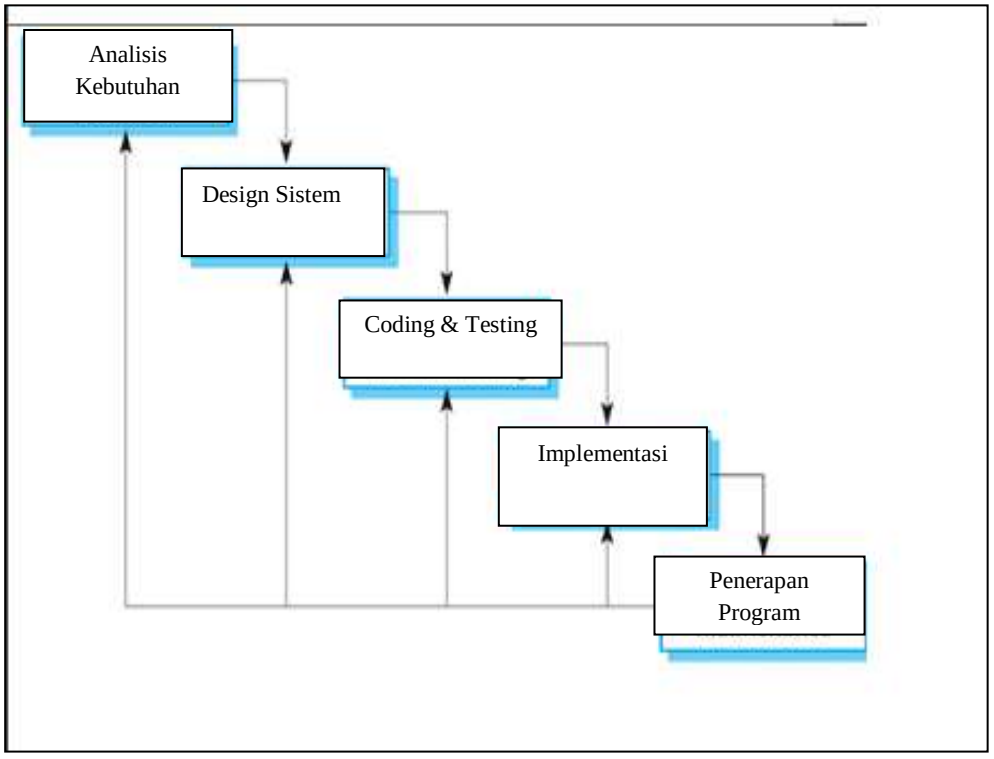
dalamnya yaitu Java Application, Java Web, Java EE(Enterprise Edition), PHP dan lain-lain.

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Tahapan penelitian yang penulis lakukan dalam penelitian ini ialah sebagai berikut :



Gambar 3.1 Tahapan Penelitian

1. Pada tahapan analisis kebutuhan merupakan pengumpulan data dan melakukan sebuah penelitian, wawancara atau studi literatur. Tahapan ini juga akan

menghasilkan sebuah dokumen dimana sebagai acuan sistem analisis untuk menerjemahkan kedalam bahasa pemograman.

2. Design sistem merupakan sebuah perancangan dari perangkat lunak yang dapat diperkirakan sebelum dibuat kesebuah coding. Proses ini terdapat struktur data, arsitektur perangkat lunak, interface, dan detail (algoritma) prosedural.
3. Coding dan Testing merupakan dalam bahasa yang bisa dikenali oleh sebuah komputer. Dimana tahapan ini secara nyata dalam mengerjakan suatu sistem. Setelah pengkodean selesai maka dilakukan tahap testing dimana tujuannya untuk menemukan kesalahan terhadap sistem.
4. Implementasi merupakan suatu rencana yang telah disusun secata terperinci dari sebuah sistem itu sendiri.
5. Penerapan program merupakan final dalam pembuatan sistem setelah melakukan analisa, design dan pengkodean maka sistem yang sudah jadi digunakan oleh user.

3.2 Metode Pengumpulan Data

dalam metode penelitian terdapat beberapa tahapan, diantaranya adalah :

1. Studi Literatur/ Studi Kepustakaan

   Studi pustaka digunakan untuk mendapatkan teori penunjang aplikasi yang akan dibuat, yaitu dengan pengumpulan bahan – bahan refrensi dari buku, artikel, jurnal, makalah maupun situs internet yang berkaitan dengan pencapaian tujuan penelitian, adapun studi literatur yang dilakukan ialah :

a. Kriptografi,

b. DES.

c. Konsep dasar teori probabilitas.

2. Enkripsi dan Dekripsi data dengan DES.

   Yaitu mendeskripsikan algoritma DES yang digunakan untuk mengenkripsi suatu plaintext yang berupa 16 digit hexadesimal menjadi chipertext yang juga berupa 16 digit hexadesimal, dan sebaliknya. Selanjutnya diaplikasikan dalam sebuah contoh kasus.

3. Analisis Data

   Pada tahap ini bertujuan untuk mengumpulkan data secara langsung yang diperoleh dari proses enskripsi dan deskripsi dari pengiriman pesan tersebut.

4. Merancang Desain Sistem

   Merancang desain *user interface* dan aplikasi yang di rancang

5. Implementasi Sistem

   Program ini di implementasikan dalam bentuk perangkat lunak menggunakan bahasa pemograman JAVA Netbeans.

3.3 Analisis Sistem berjalan

Adapun sistem yang berjalan saat ini dilakukan dengan keadaan manual yaitu tanpa adanya filter keamanan dalam pengiriman pesan sehingga memungkinkan adanya kerahasiaan pada pesan yang dikirim terungkap, pada pengiriman pesan tertentu misalkan antara pegawai dan pimpinan, dimana pesan

tersebut hanya layak diketahui oleh pimpinan sehingga diperlukan keamanan data atau *enskripsi* data yang di kirim tersebut .

Dalam merancang suatu sistem harus mempunyai analisis terhadap sistem yang akan dirancang tersebut terlebih dahulu. Aplikasi enkripsi ini dapat mengubah pesan atau kata-kata menjadi karakter yang disamarkan. Aplikasi ini juga dapat membuat file yang diisi dengan pesan atau kata-kata menjadi file yang tidak dapat dibaca sama sekali kecuali dengan menggunakan aplikasi ini ataupun aplikasi sejenis yang dilingdungi dengan *key password* yang di input oleh user.

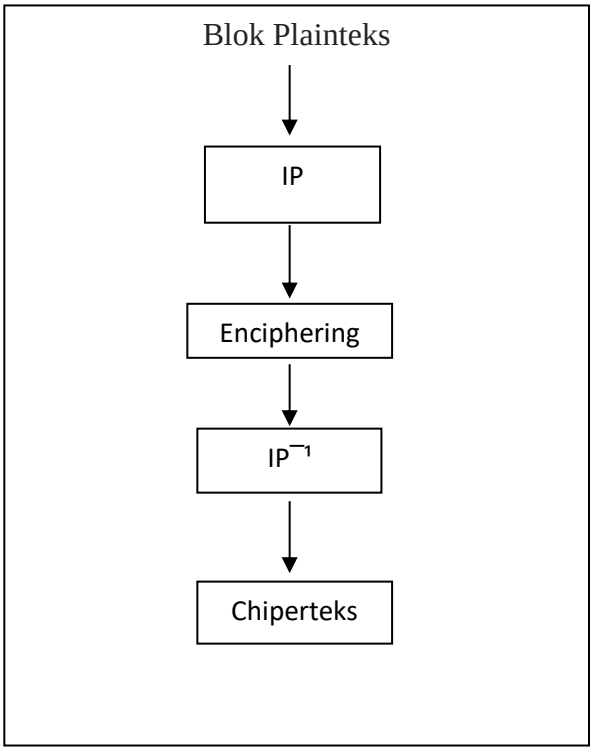
3.4. Analisis Sistem Yang Diusulkan

3.4.1. Analisis Algoritma DES

Prinsip kerja Des adalah pembagian informasi menjadi blok-blok tertentu oleh karna itu DES termasuk salah satu algoritma chipper blok. Pesan-pesan tersebutpun akan diacak dengan menggunakan matriks-matriks standart yang ada pada algoritma DES. Proses yang pertama penulis lakukan adalah membangkitkan kunci pada algoritma DES langkah-langkah Enkripsi dan dekripsi adalah sebagai berikut:

a. Skema Data Encryption Standart

   Skema Data Encyption standart merupakan skema dasar dari perhitungan algoritma DES, dimana proses enskripsi menentukan blok plainteks terlebih dahulu yang kemudian dilakukan enskripsi sehingga menampilkan chiperteks, begitu juga sebaliknya dalam proses deskrpsi, berikut gambaran skema data encryption standart.

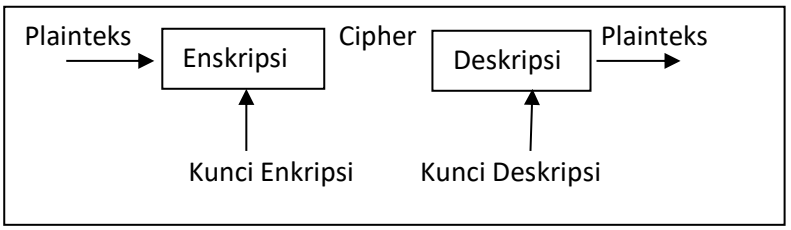


Gambar 3.2 Skema Proses Des

1. Blok plainteks dipermutasi dengan matriks permutasi awal (*Initial Permutation* atau *IP*)
2. Hasil permutasi awal kemudiandi *Enciphering* sebanyak 16 putaran, setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan menjadi blokcipherteks.

b. Proses Enskripsi dan Deskripsi

Proses Enkripsi adalah proses pengacakan data menggunakan sebuah key agar tidak dapat dibaca oleh pihak lain. adapun gambar diagram proses plainteks ke enkripsi dan cipterteks ke deskipsi dapat dilihat pada gambar berikut.



Gambar 3.3 Diagram Proses Enkripsi dan Deskripsi

3.5. Analisis Data

Analisis data merupakan tahapan dimana dilakukannya analisis terhadap data-data apa saja yang diolah dalam sistem atau prosedur sebuah rancangan, dalam hal ini data yang akan di enkripsi pada aplikasi kriptografi adalah berupa file Txt, Doc.

3.6. Analisis keamanan data

Pertukaran informasi setiap detik di internet membuat banyak terjadi pencurian informasi itu sendiri oleh pihak-pihak yang tidak bertanggung jawab. Oleh karna itu agar data yang dikirim aman dari orang yang tidak bertanggung jawab, data tersebut harus disembunyikan dengan cara menyandikan data tersebut menggunakan algoritma kriptografi DES. Pertukaran data baik di jaringan lokal maupun di jaringan internet membawa informasi berupa pesan (message) yaitu suatu data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan disebut juga plainteks (plaintext) atau teks-jelas (cleartext). Pesan dapat berupa data atau informasi yang dikirimkan atau disimpan di dalam media perekaman, adapun pesan yang tersimpan tidak hanya berupa teks, tetapi dapat juga

berbentuk citra (image), suara/bunyi (audio), dan juga video, atau pun berkas biner lainnya, namun hal ini penulis meneliti pesan berupa teks.

Agar pesan tidak dapat dimengerti maknanya oleh pihak lain, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut chiperteks atau kriptogram. Chiperteks harus dapat ditransformasikan kembali menjadi plainteks semula agar pesan yang diterima bisa dibaca. Algoritma kriptografi yang digunakan disebut juga cipher yaitu suatu bentuk aturan untuk enciphering dan deciphering, atau fungsi matematika yang digunakan untuk proses enkripsi dan deskripsi. Beberapa cipher memerlukan algoritma yang berbeda untuk enciphering dan deciphering. Keamanan suatu data sering diukur dari banyaknya kerja (work) yang dibutuhkan untuk memecahkan chiperteks menjadi plainteksnya tanpa mengetahui kunci yang digunakan. Semakin banyak kerja yang diperlukan, semakin lama waktu yang dibutuhkan, maka semakin kuat algoritma kriptografi tersebut.

3.7. Langkah – Langkah Penyelesaian

Menurut (Munir, 2006) Dari permasalahan diatas, maka penulis mencoba untuk membuat sebuah rancangan yang berguna untuk mengamankan sebuah data dengan menggunakan algoritma kriptografi DES. Langkah – langkah simulasi dalam penyelesaian pada masalah diatas yaitu ;

a. Proses Enkripsi

- Langkah – langkah sebagai berikut :

1. Blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation atau IP).
2. Hasil permutasi awal kemudian di-enciphering- sebanyak 16 kali (16 putaran).
3. Setiap putaran menggunakan kunci internal yang berbeda.

Hasil *enciphering* kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation atau IP-1) menjadi blok cipherteks.

b. Proses Deskripsi

Dengan langkah-langkah sebagai berikut ;

1. Proses dekripsi terhadap cipherteks merupakan kebalikan dari proses enkripsi. DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah K1, K2,…, K16, maka pada proses dekripsi urutan kunci yang digunakan adalah K16, K15, …, K1.
2. Untuk tiap putaran 16, 15, …, 1, keluaran pada setiap putaran deciphering adalah ;

   Li = Ri – 1

   Ri = Li – 1 □ f(Ri – 1, Ki)

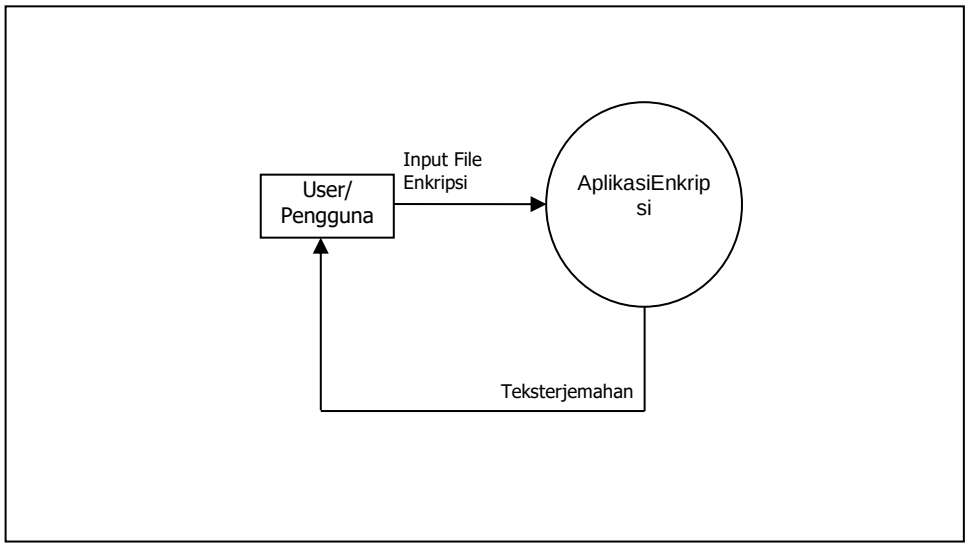
3. Yang dalam hal ini, (R16, L16) adalah blok masukan awal untuk deciphering, Blok (R16, L16) diperoleh dengan mempermutasikan cipherteks dengan matriks permutasi IP-1. Pra-keluaran dari deciphering adalah adalah (L0, R0). Dengan permutasi awal IP akan didapatkan kembali blok plainteks semula.
4. Tinjau kembali proses pembangkitan kunci internal pada Gambar Selama deciphering, K16 dihasilkan dari (C16, D16) dengan permutasi PC-2. Tentu saja (C16, D16) tidak dapat diperoleh langsung pada permulaan deciphering. Tetapi karena (C16, D16) = (C0, D0), maka K16 dapat dihasilkan dari (C0, D0) tanpa perlu lagi melakukan pergeseran bit. Catatlah bahwa (C0, D0) yang merupakan bit-bit dari kunci eksternal K yang diberikan pengguna pada waktu dekripsi.
5. Selanjutnya, K15 dihasilkan dari (C15, D15) yang mana (C15, D15) diperoleh dengan menggeser C16 (yang sama dengan C0) dan D16 (yang sama dengan C0) satu bit ke kanan. Sisanya, K14 sampai K1 dihasilkan dari (C14, D14) sampai (C1, D1). Catatlah bahwa (Ci – 1, Di – 1) diperoleh dengan menggeser Ci dan Di dengan cara yang sama seperti pada Tabel 1, tetapi pergeseran kiri (left shift) diganti menjadi pergeseran kanan (right shift).

3.8. Rancangan Aplikasi

Aplikasi enkripsi ini dapat mengubah pesan atau kata-kata menjadi karakter yang disamarkan. Aplikasi ini juga dapat membuat file yang diisi dengan pesan atau kata-kata menjadi file yang tidak dapat dibaca sama sekali kecuali dengan menggunakan aplikasi ini ataupun aplikasi sejenis yang dilingdungi dengan *key password* yang di input oleh user.

c. Diagram Konteks

Diagram konteks merupakan diagram yang berisi gambaran umum dari aplikasi yang akan dibuat. Berikut adalah diagram konteks aplikasi enkripsi yang akan dibuat.

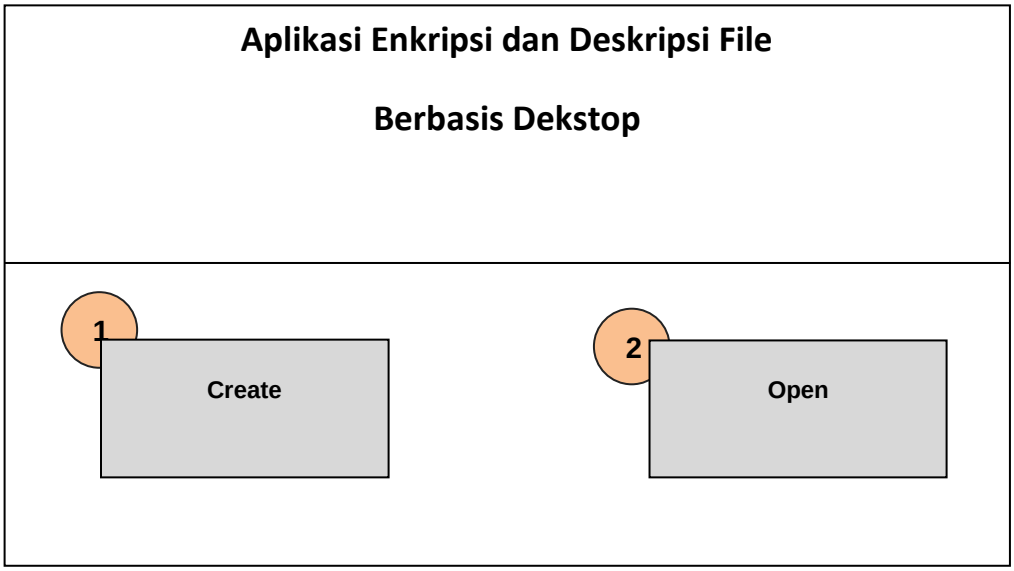


Gambar 3.4 Diagram Konteks

d. Hasil Desain Aplikasi

1) Hasil Desain Form Utama

Desain form menu utama meruapakan rancangan tampilan awal untuk memulai menjalankan sistem aplikasi ini, dimana proses dari enskripsi akan terlihat pada gambaran rancangan di bawah ini ;

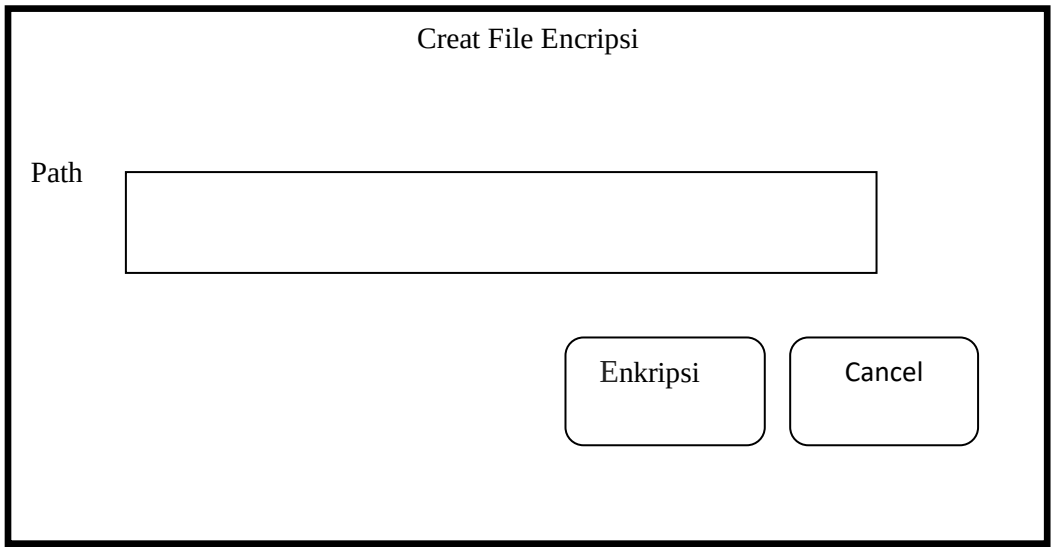


Gambar 3.5 Desain Form Utama

Keterangan :

1. **Tombol Buat Create**, untuk menginput file yang akan di enkripsikan.
2. **Tombol Open**, untuk membuka dan menerjemahkan berupa pesan file yang di enkripsikan menjadi file yang dapat dibaca.

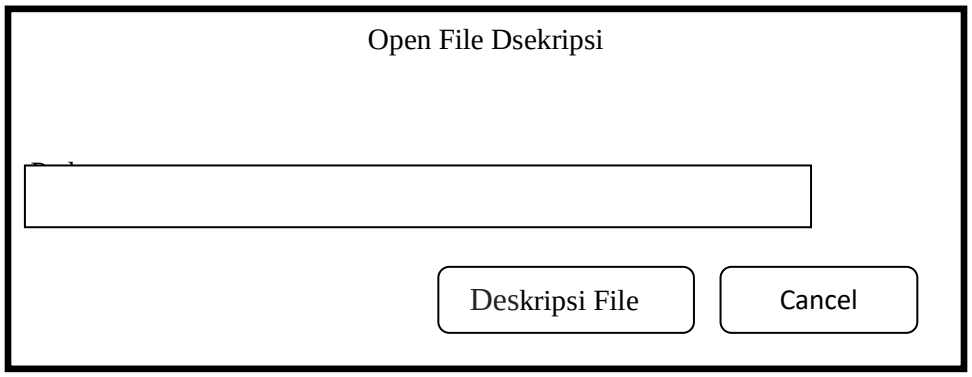
2) Hasil Desain Form Enkripsi



Gambar 3.6 Form Enkripsi File

1. Tombol Enkripsi file untuk memilih file teks yang akan di enkripsikan
2. Tombol Cancel untuk membatalkan jalanya program
3. JTeksArea tempat dimana file teks yang akan dienkripsi tersimpan

3) Desain Form untuk Deskripsi



Gambar 3.7 Form Untuk Deskripsi File

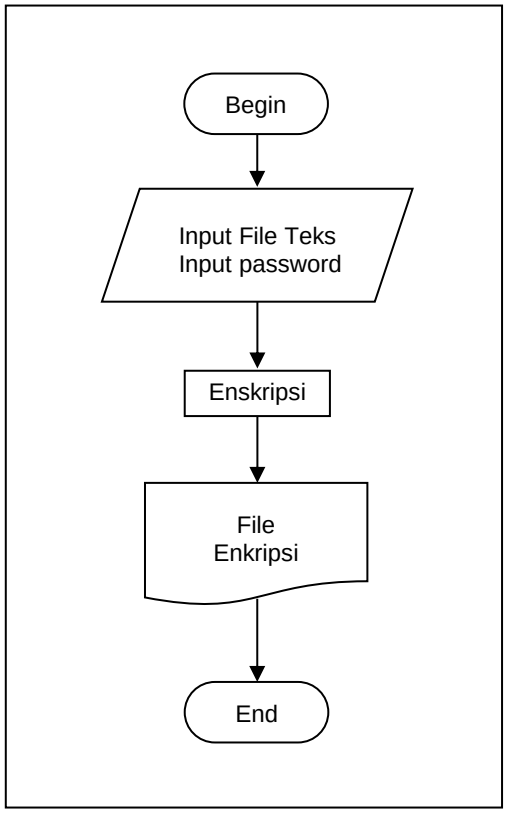
1. Tombol Deskripsi File untuk mengkonvert file teks enkripsi
2. Tombol Cancel untuk membatalkan program yang sedang berjalan

3. JTeksArea tempat dimana file teks yang akan dideskripsikan tersimpan

e. Flowchart

Flowchart adalah gambar atau skema yang menunjukkan langkah operasi dari suatu algoritma mulai dari awal hingga akhir.Sebelum suatu program diciptakan, maka terlebih dahulu dibuat flowchart.

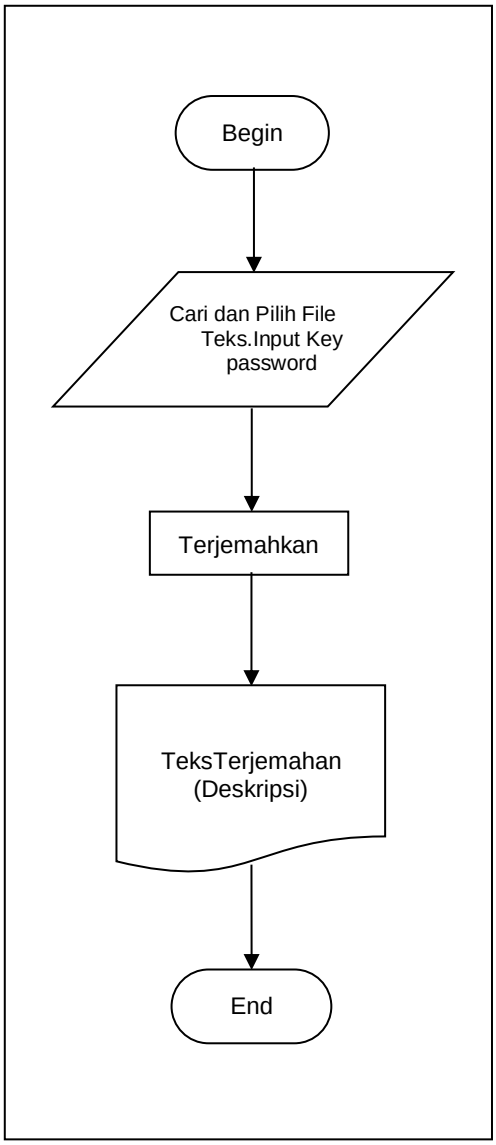
1) Flowchart Buat File Enkripsi



Gambar 3.8 Flowchart Buat File Enkripsi

User harus membuat file encripsi dan menginput key password dahulu setelah itu user menyimpan file enkripsi di directori yang di ingin akan.

2) Flowchart Buka dan Terjemahkan File Enkripsi



Gambar 3.9 Flowchart Buka dan Terjemahkan File Enkripsi

Untuk menterjemahkan file enskripsi user harus memilih file setelah itu masukan key password yang telah dibuat oleh user yang lain. Setelah itu pilih terjemahkan maka akan muncul tulisan yang telah di terjemahkan.

BAB IV

HASIL DAN PEMBAHASAN

1. Analisa Kebutuhan Sistem

a) Kebutuhan Perangkat Keras

Dalam merancang perangkat lunak ini, programmer harus memiliki komputer/laptop yang digunakan untuk memprogram perangkat lunak. Adapun spesifikasi minimum untuk membuat dan menjalankan perangkat lunak ini nantinya antara lain sebagai berikut:

Tabel 4.1 Kebutuhan *Hardware*

No.	Nama Perangkat	Spesifikasi
1	Prosesor	Pentium IV atau yang lebih baru
2	Ram	1 GB
3	VGA Card	128 MB / lebih tinggi
4	Hard disk	50 GB
5	Resolusi Layar	1024 x 768 pixel
6	Perangkat input	Keyboard dan mouse.

b) Kebutuhan Perangkat Lunak

Sedangkan aplikasi pendukung yang dibutuhkan untuk membangun perangkat lunak *Encripsi deskripsi* ini adalah sebagai berikut:

Tabel 4.2 Kebutuhan *Software*

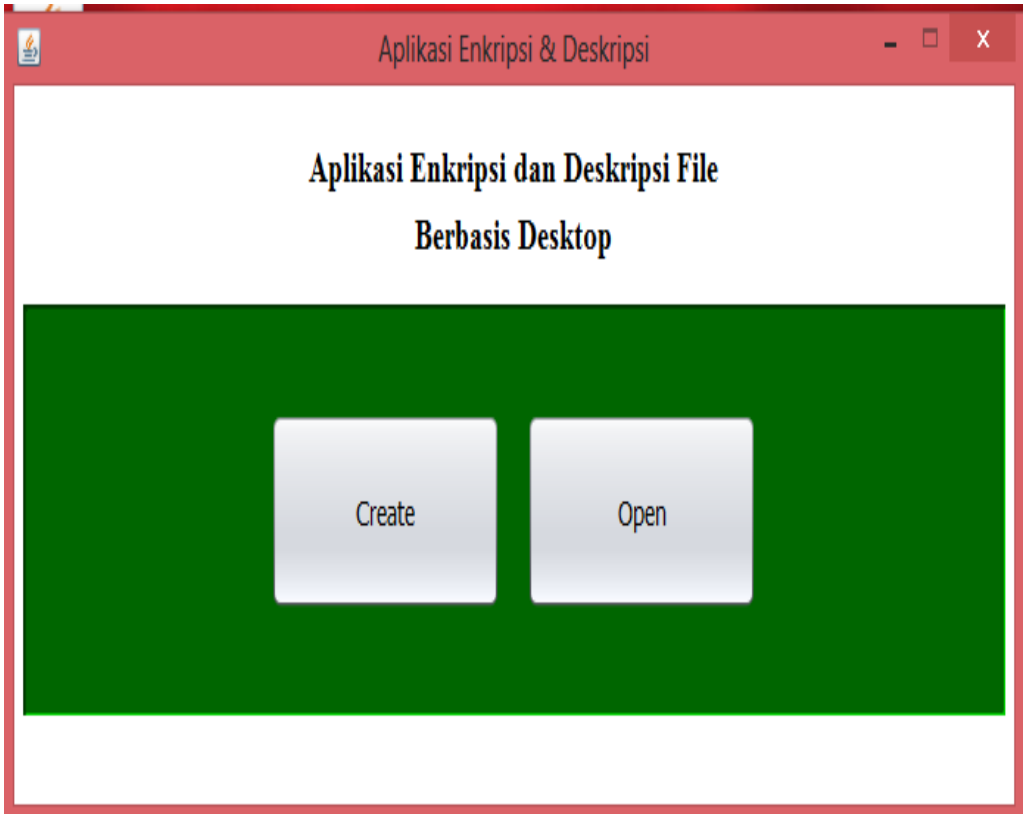
No.	Nama Perangkat	Fungsi
1	Java Netbeans 7,4	Untuk membuat *Script* Program Java
2	Toolkit	Untuk mempercantik *control* perangkat lunak

2. Perancangan Sistem

Perangkat lunak aplikasi enskripsi dan deskripsi file adalah aplikasi computer mengubah pesan atau kata-kata menjadi karakter yang disamarkan. Aplikasi ini juga dapat membuat file yang diisi dengan pesan atau kata-kata menjadi file yang tidak dapat dibaca sama sekali kecuali dengan menggunakan aplikasi ini ataupun aplikasi sejenis yang dilingdungi dengan *key password* yang diinput oleh user.

3. Hasil Rancangan

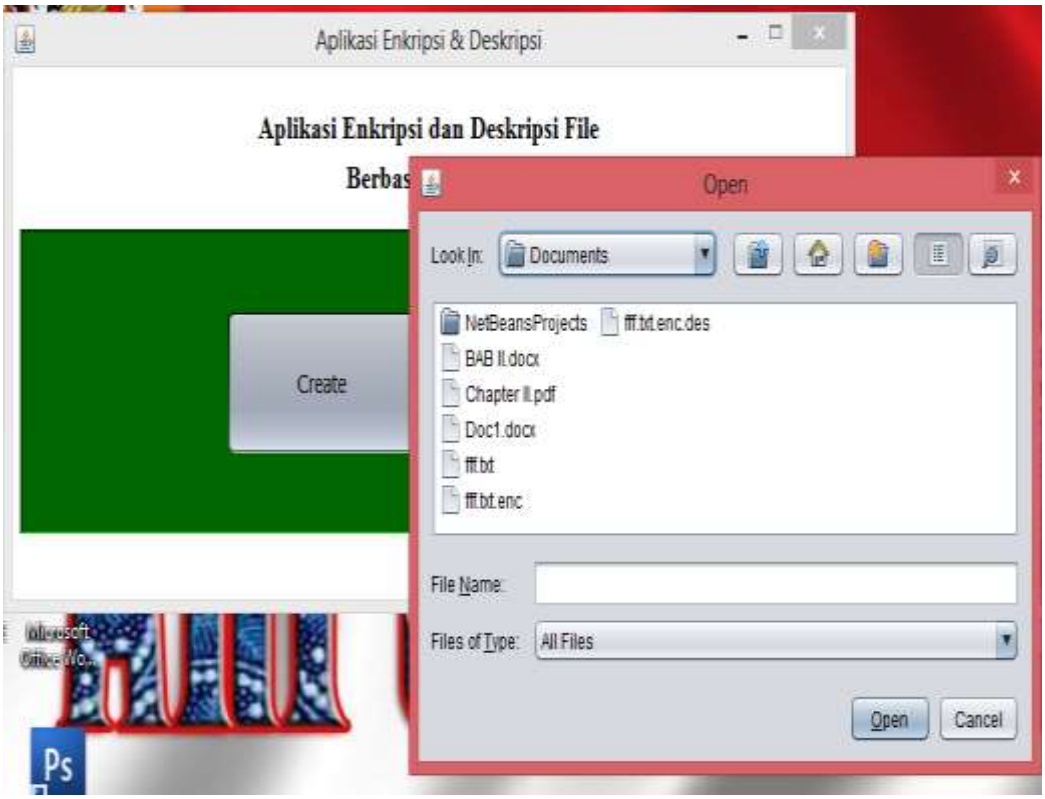
a. Tampilan Form Utama



Gambar 4.1 Tampilan Form Utama

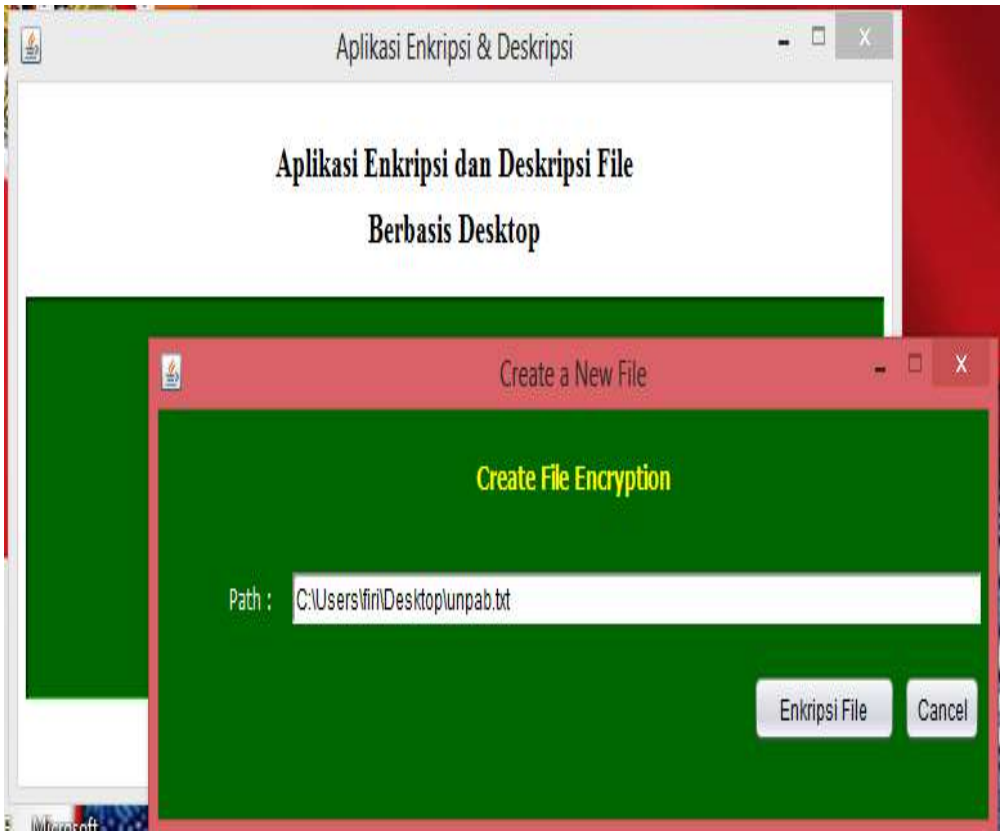
User harus memilih tombol mana yang akan dipilih, Tombol *create* untuk membuat file enkripsi, Tombol open untuk membuka file yang telah di enskripsi yang disimpan dilocal disk pada komputer.

b. Tampilan Form Buat File Pesan Enskripsi



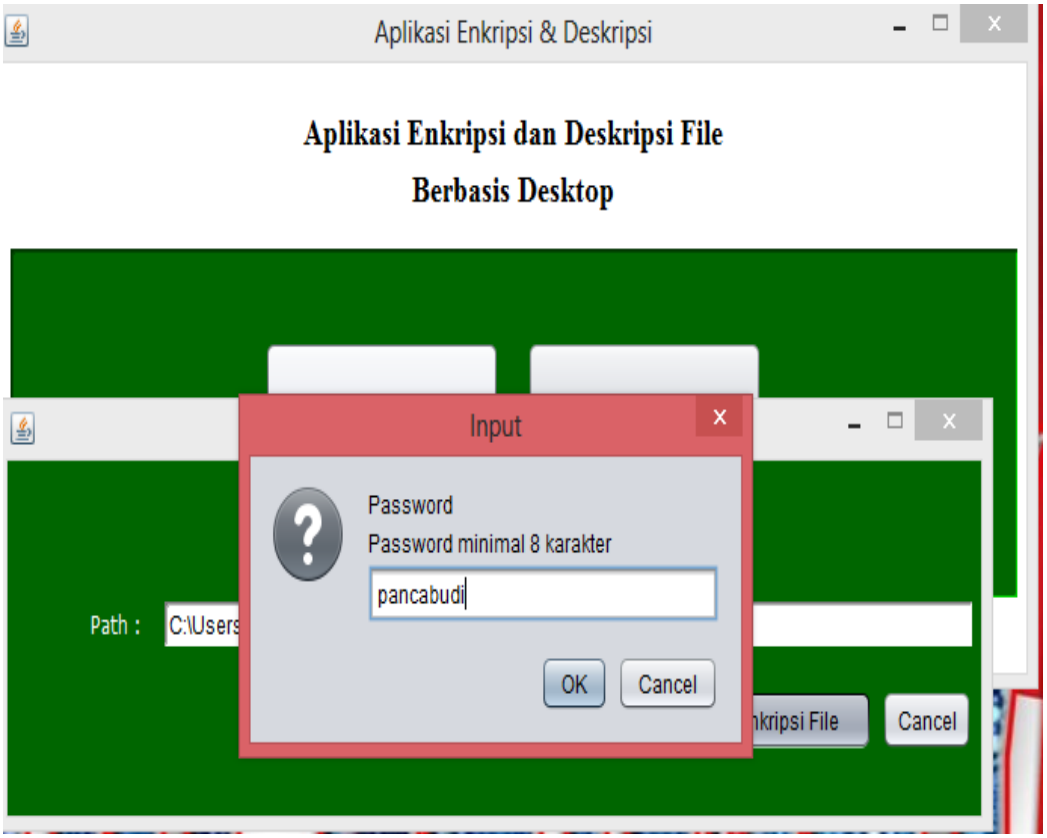
Gambar 4.2 Tampilan JFileChooser Cari File

User harus menginput isi pesan dan menyimpan di local disk mana kita simpan kata – kata yang akan kita Enkripsi, setelah itu user memilih button create setelah itu akan muncul seperti gambar yang diatas, user tinggal memilih file teks yang telah disimpan. Setelah terpilih maka akan muncul gambar sebagai berikut.



Gambar 4.3 Tampilan Create File Enkripsi

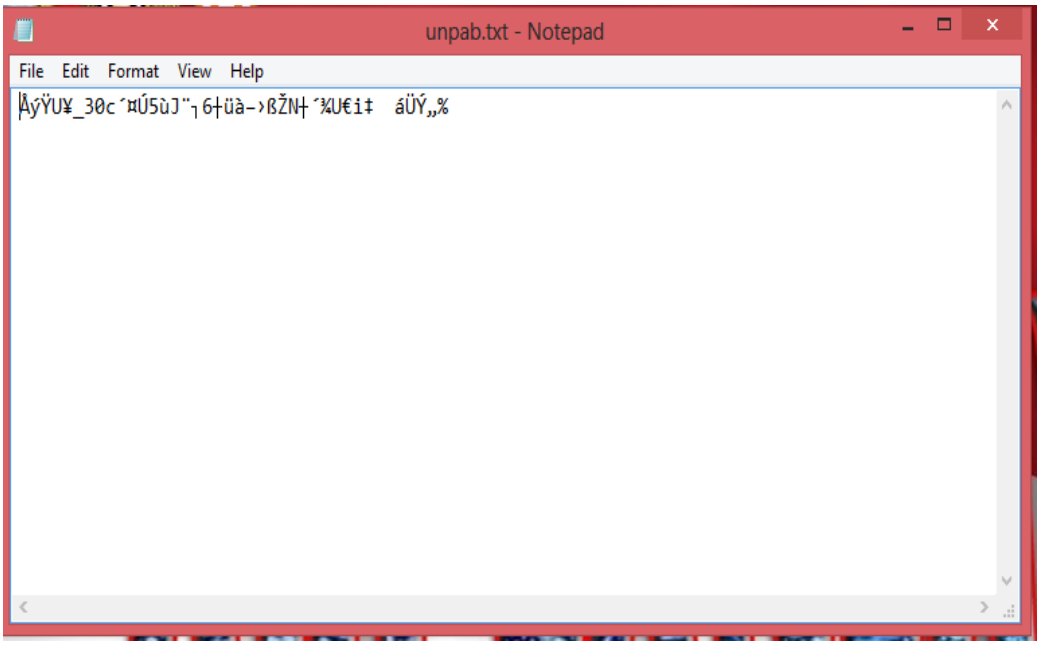
Setelah itu user memilih Button Enkripsi File maka akan muncul *JFileChooser* untuk user menentukan dimana file enskripsi tersebut user simpan. Setelah menentukan tempat maka user dituntut untuk memasukan password sebelum menyimpan enskripsi file teks. Seperti gambar dibawah ini.



Gambar 4.4 Tampilan Input Password

Pada gambar diatas ini user disuruh memasukan password untuk menjaga keamanan file teks yang dibuat..

Setelah itu file teks yang telah dienkripsi kan akan berubah isinya. Seperti gambar berikut.

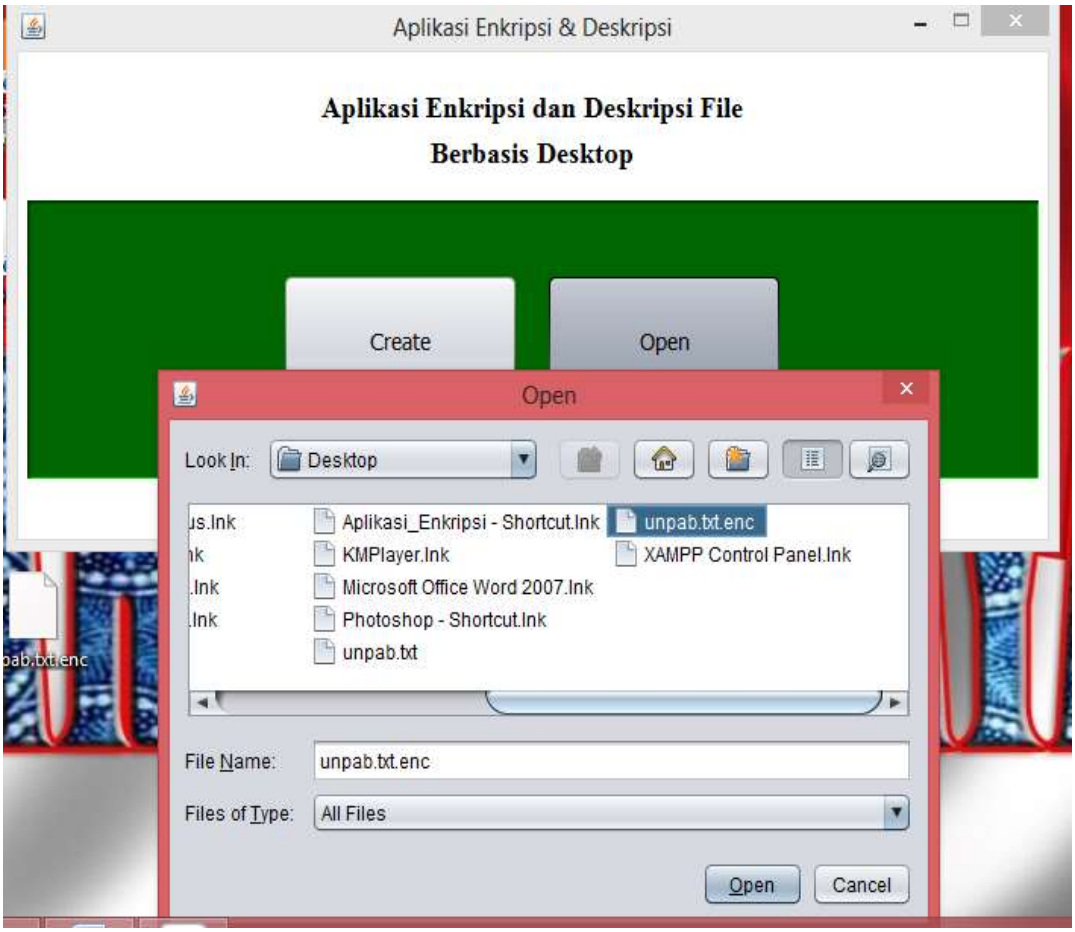


Gambar 4.5 Hasil Dari File Teks Yang Telah Dienskripsi

Ini adalah hasil dari file teks yang telah di enkripsikan bisa kita liat kalimat yang kita buat menjadi berubah sehingga tidak bisa dibaca oleh orang lain.

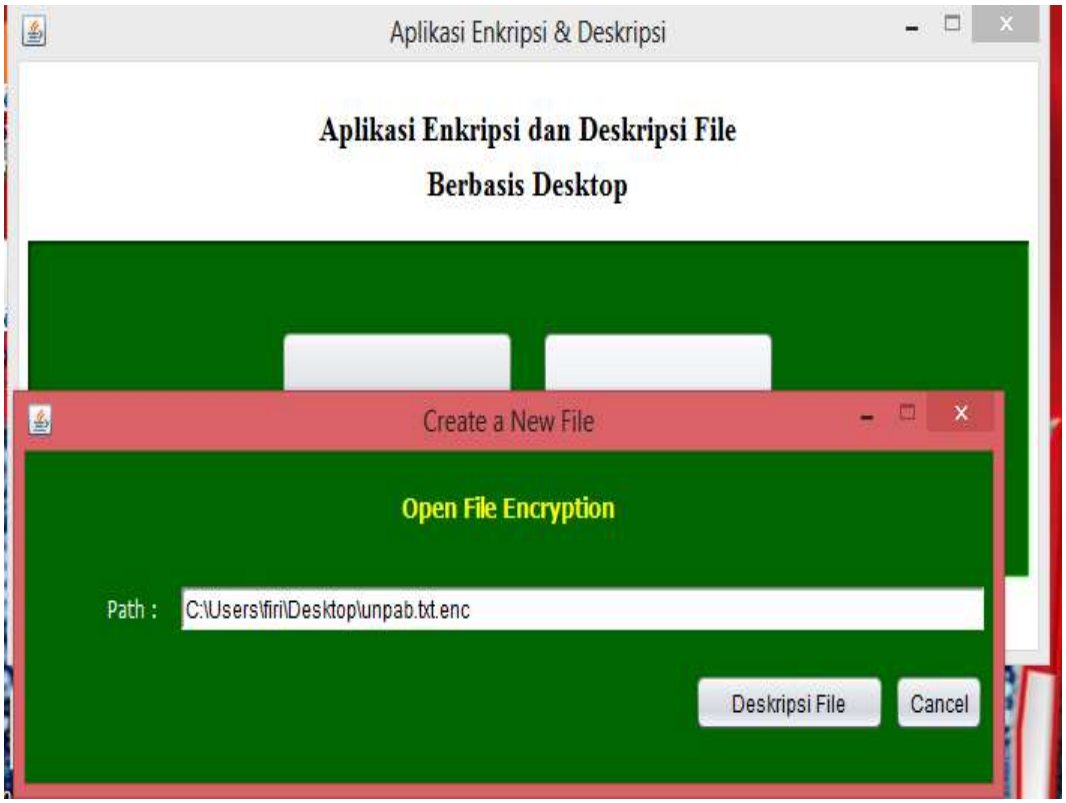
c. Tampilan File Pesan Deskripsi

Apabila user ingin membuka file teks yang telah di enkripsikan, user harus meilih button Open pada tampilan awal, setelah memilih button Open maka akan muncul ***JFileChooser*** seperti gambar berikut.



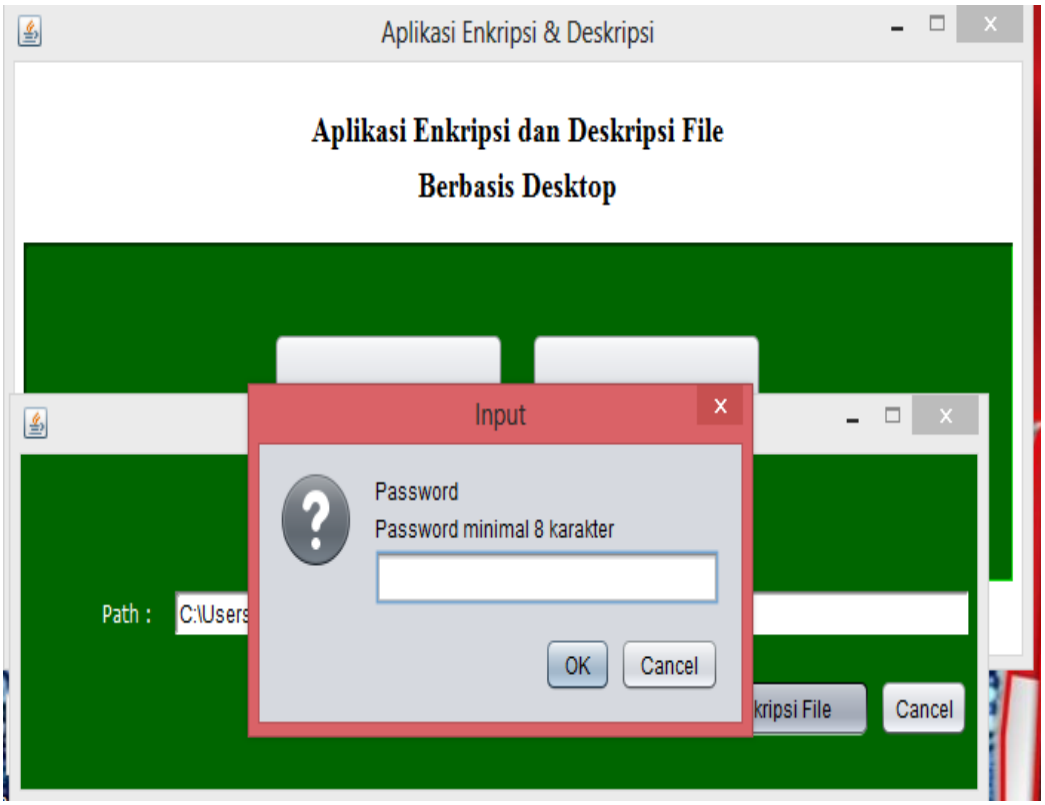
Gambar 4.6 Tampilan *JFileChooser* Untuk Mendeskripsi

Setelah muncul seperti gambar diatas user tinggal memilih file teks yang akan di deskripsikan kemudian klik tombol open. Maka akan muncul pemberitahuan seperti gambar berikut.



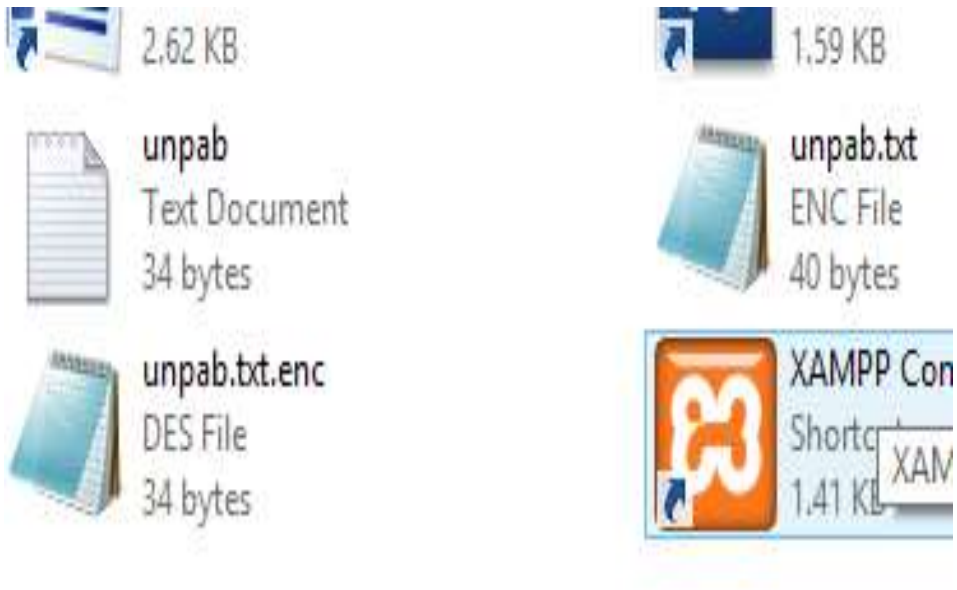
Gambar 4.7 Tampilan open file Enkripsi

Setelah muncul seperti pada gambar diatas user tinggal mengklik button Deskripsi maka akan masuk ketampilan input password. Seperti gambar berikut



Gambar 4.8 Tampilan Input Password

Setelah muncul seperti pada gambar diatas user harus memasukan password sesuai dengan password pada saat mengenkripsikan file teks. setelah itu maka akan muncul file teks yang telah di deskripsikan seperti pada gambar berikut.



Gambar 4.9 File Enkripsi Dan Deskripsi

pada gambar diatas adalah gambar dimana hasil enkripsi dan deskripsi telah disimpan bisa kita liat pada gambar yang mana hasil enkripsi dan yang mana hasil deskripsi.

BAB IV

HASIL DAN PEMBAHASAN

1. Analisa Kebutuhan Sistem

a) Kebutuhan Perangkat Keras

Dalam merancang perangkat lunak ini, programmer harus memiliki komputer/laptop yang digunakan untuk memprogram perangkat lunak. Adapun spesifikasi minimum untuk membuat dan menjalankan perangkat lunak ini nantinya antara lain sebagai berikut:

Tabel 4.1 Kebutuhan *Hardware*

No.	Nama Perangkat	Spesifikasi
1	Prosesor	Pentium IV atau yang lebih baru
2	Ram	1 GB
3	VGA Card	128 MB / lebih tinggi
4	Hard disk	50 GB
5	Resolusi Layar	1024 x 768 pixel
6	Perangkat input	Keyboard dan mouse.

b) Kebutuhan Perangkat Lunak

Sedangkan aplikasi pendukung yang dibutuhkan untuk membangun perangkat lunak *Encripsi deskripsi* ini adalah sebagai berikut:

Tabel 4.2 Kebutuhan *Software*

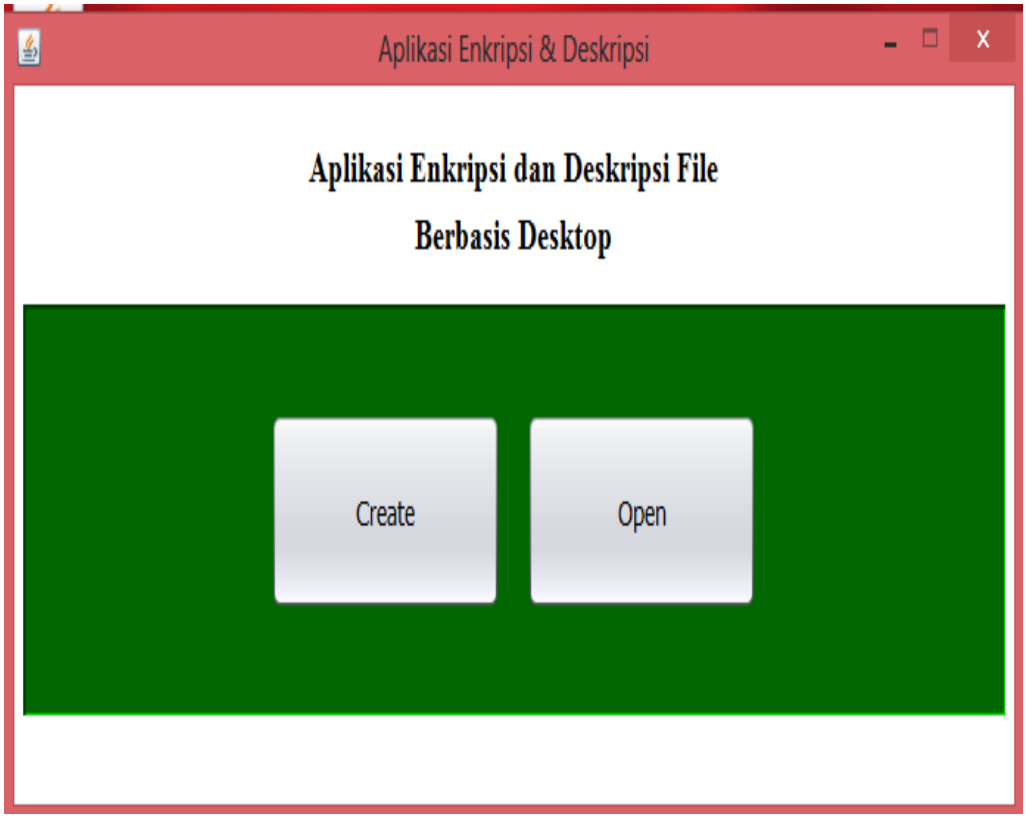
No.	Nama Perangkat	Fungsi
1	Java Netbeans 7,4	Untuk membuat *Script* Program Java
2	Toolkit	Untuk mempercantik *control* perangkat lunak

2. Perancangan Sistem

Perangkat lunak aplikasi enskripsi dan deskripsi file adalah aplikasi computer mengubah pesan atau kata-kata menjadi karakter yang disamarkan. Aplikasi ini juga dapat membuat file yang diisi dengan pesan atau kata-kata menjadi file yang tidak dapat dibaca sama sekali kecuali dengan menggunakan aplikasi ini ataupun aplikasi sejenis yang dilingdungi dengan *key password* yang diinput oleh user.

3. Hasil Rancangan

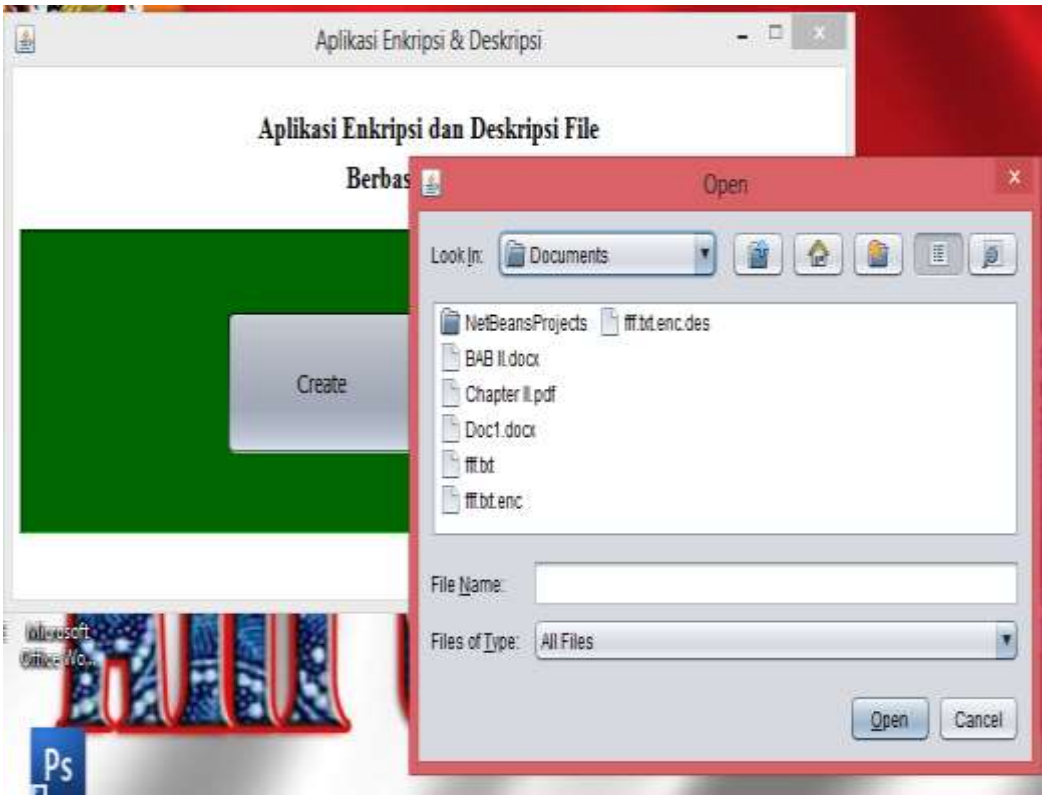
a. Tampilan Form Utama



Gambar 4.1 Tampilan Form Utama

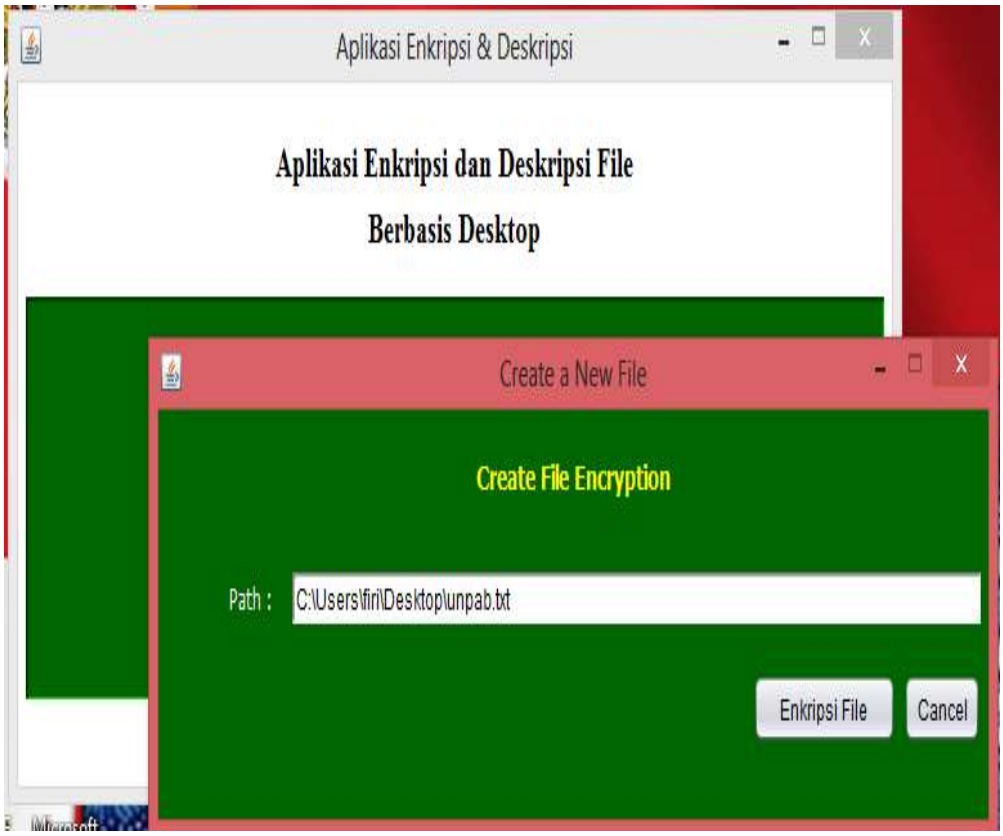
User harus memilih tombol mana yang akan dipilih, Tombol *create* untuk membuat file enkripsi, Tombol open untuk membuka file yang telah di enskripsi yang disimpan dilocal disk pada komputer.

b. Tampilan Form Buat File Pesan Enskripsi



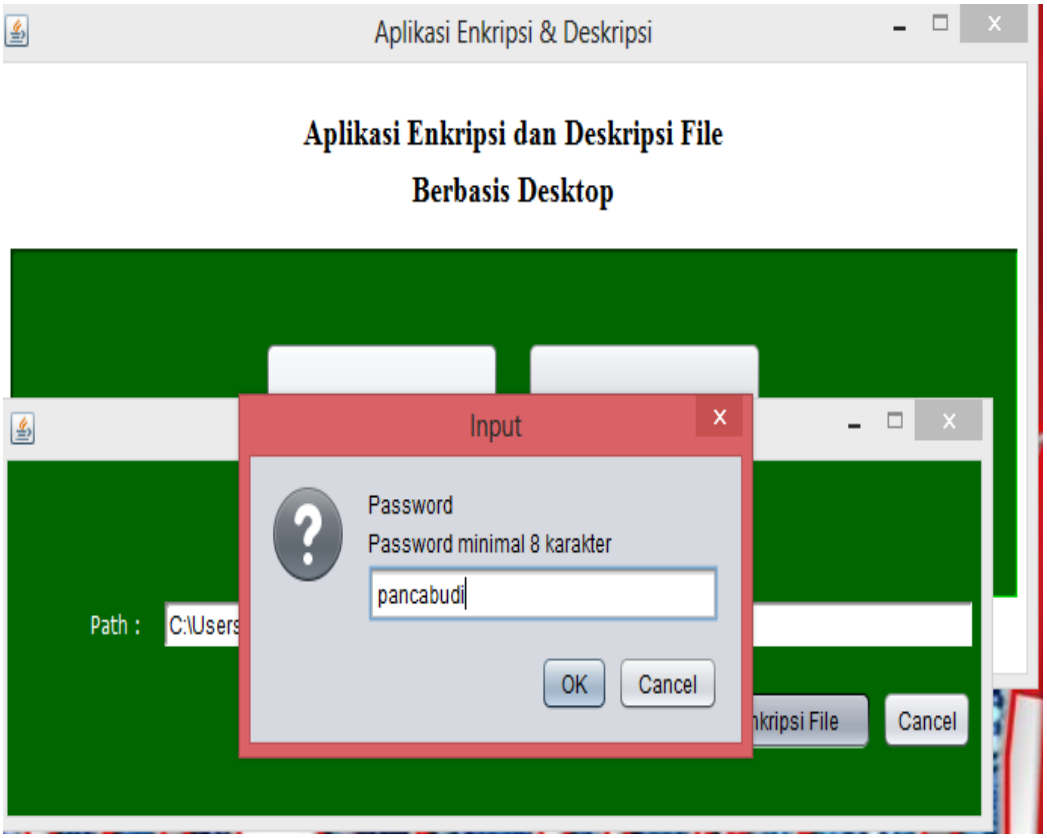
Gambar 4.2 Tampilan JFileChooser Cari File

User harus menginput isi pesan dan menyimpan di local disk mana kita simpan kata – kata yang akan kita Enkripsi, setelah itu user memilih button create setelah itu akan muncul seperti gambar yang diatas, user tinggal memilih file teks yang telah disimpan. Setelah terpilih maka akan muncul gambar sebagai berikut.



Gambar 4.3 Tampilan Create File Enkripsi

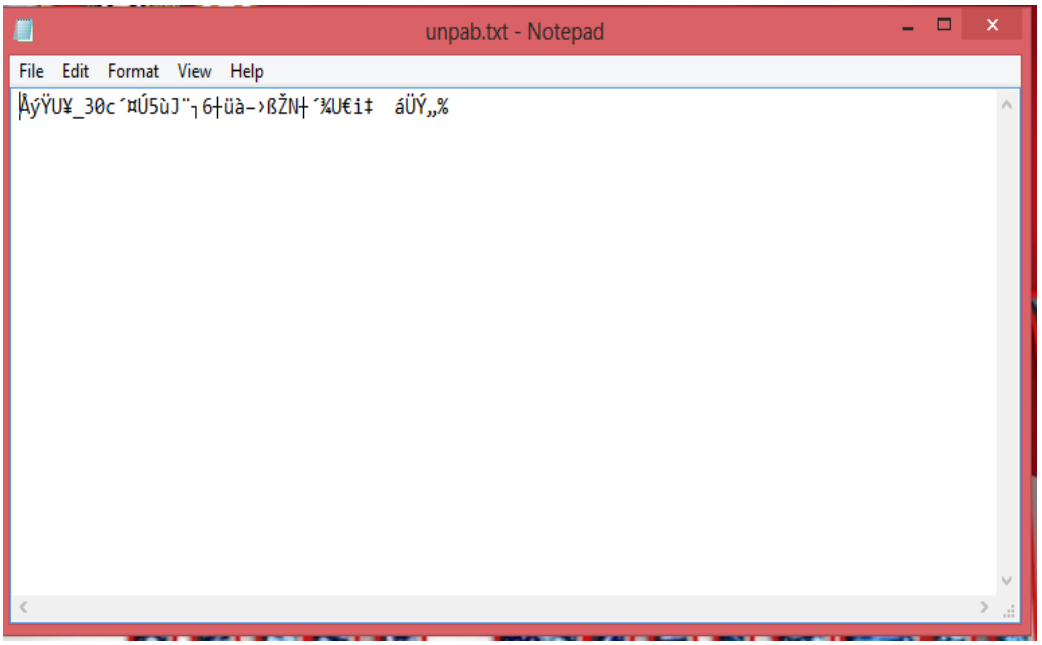
Setelah itu user memilih Button Enkripsi File maka akan muncul *JFileChooser* untuk user menentukan dimana file enskripsi tersebut user simpan. Setelah menentukan tempat maka user dituntut untuk memasukan password sebelum menyimpan enskripsi file teks. Seperti gambar dibawah ini.



Gambar 4.4 Tampilan Input Password

Pada gambar diatas ini user disuruh memasukan password untuk menjaga keamanan file teks yang dibuat..

Setelah itu file teks yang telah dienkripsi kan akan berubah isinya. Seperti gambar berikut.

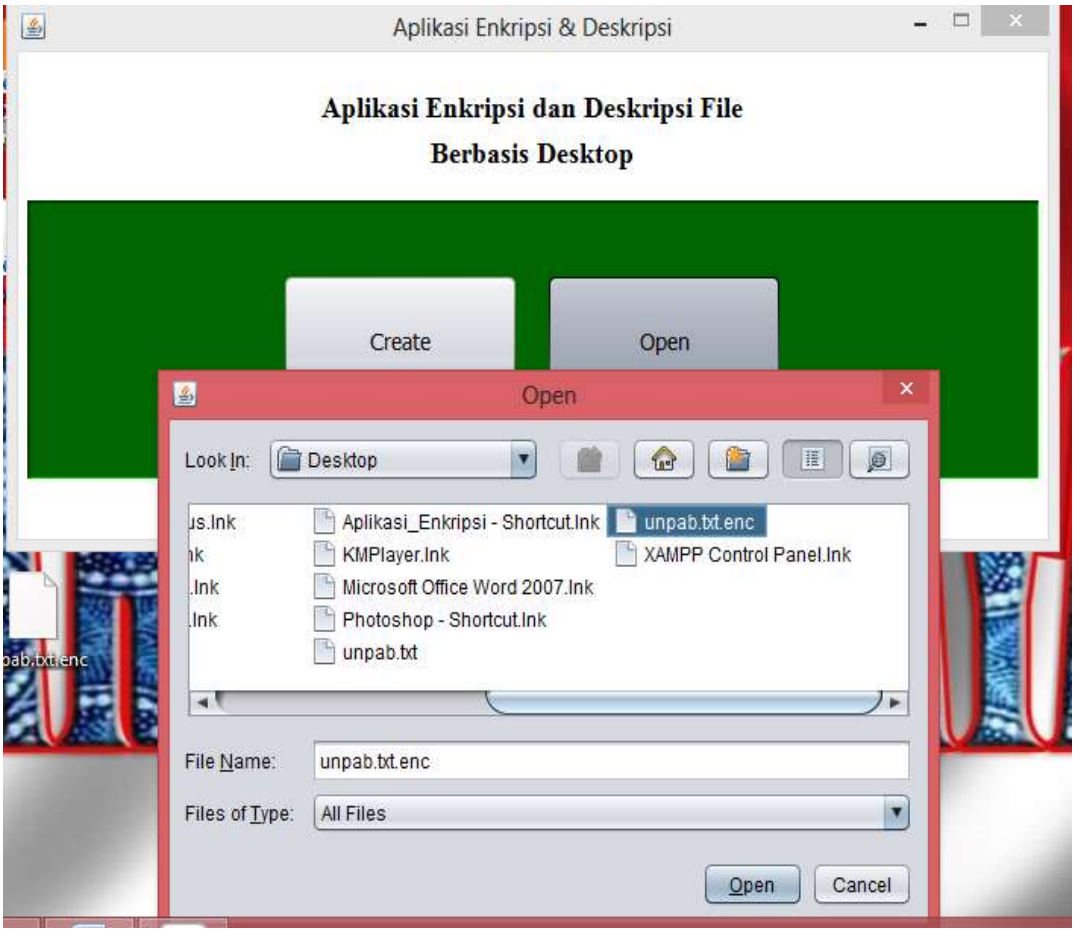


Gambar 4.5 Hasil Dari File Teks Yang Telah Dienskripsi

Ini adalah hasil dari file teks yang telah di enkripsikan bisa kita liat kalimat yang kita buat menjadi berubah sehingga tidak bisa dibaca oleh orang lain.

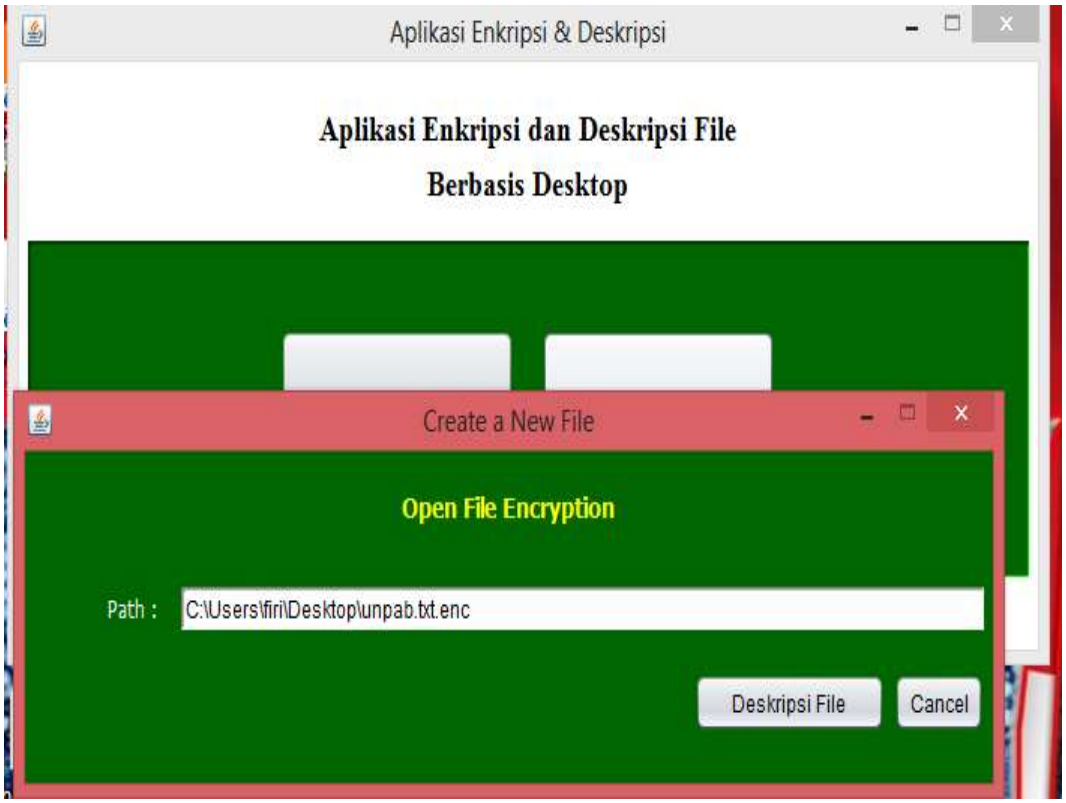
c. Tampilan File Pesan Deskripsi

Apabila user ingin membuka file teks yang telah di enkripsikan, user harus meilih button Open pada tampilan awal, setelah memilih button Open maka akan muncul ***JFileChooser*** seperti gambar berikut.



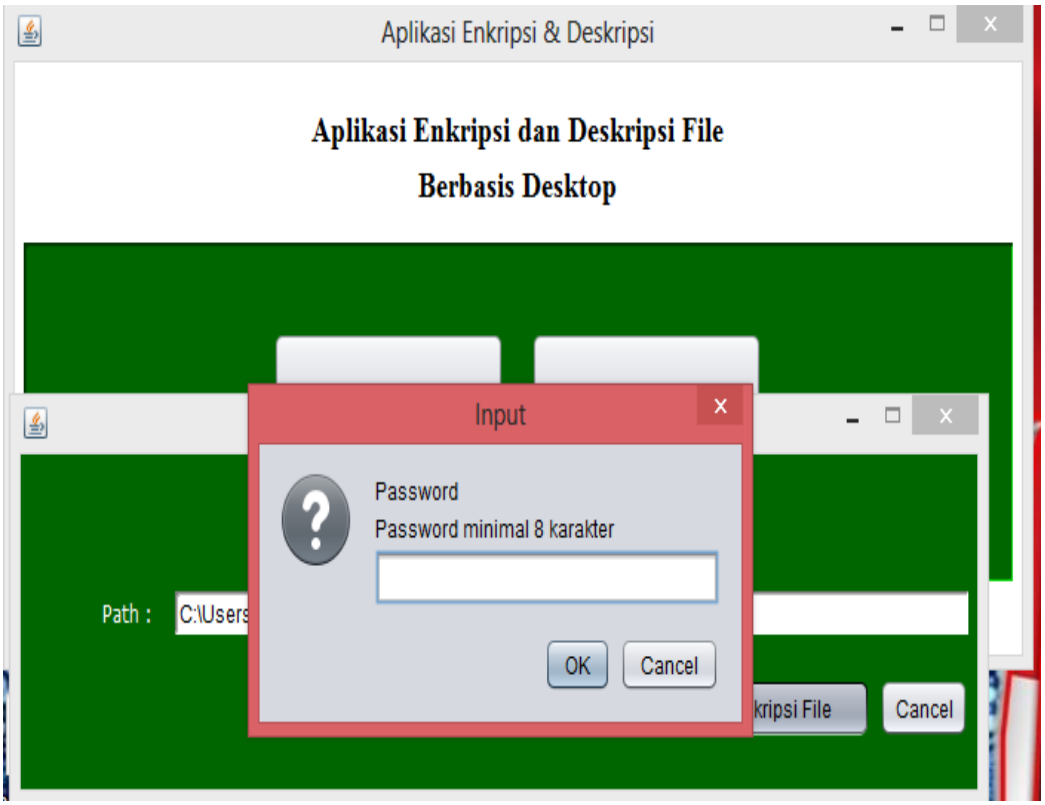
Gambar 4.6 Tampilan *JFileChooser* Untuk Mendeskripsi

Setelah muncul seperti gambar diatas user tinggal memilih file teks yang akan di deskripsikan kemudian klik tombol open. Maka akan muncul pemberitahuan seperti gambar berikut.



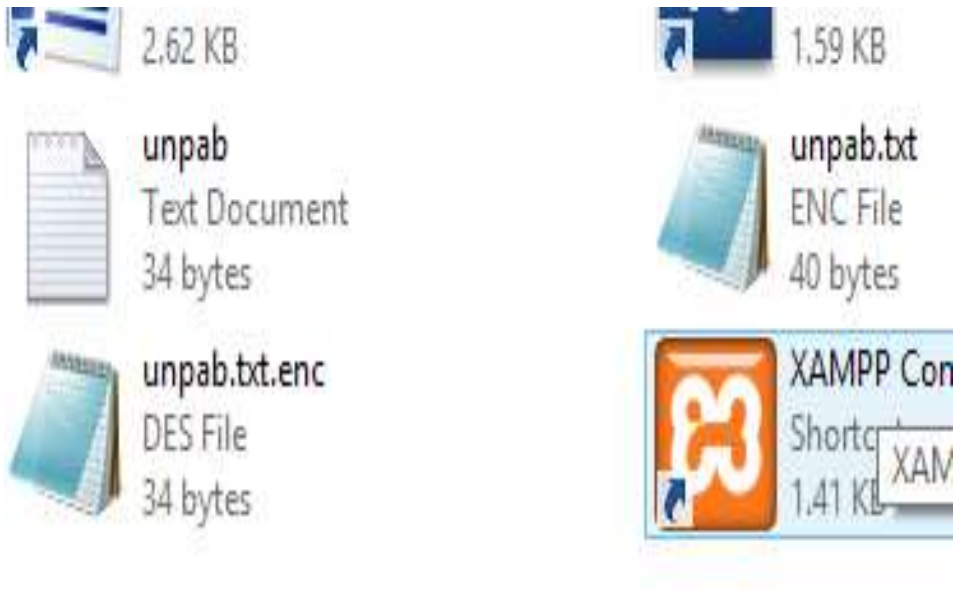
Gambar 4.7 Tampilan open file Enkripsi

Setelah muncul seperti pada gambar diatas user tinggal mengklik button Deskripsi maka akan masuk ketampilan input password. Seperti gambar berikut



Gambar 4.8 Tampilan Input Password

Setelah muncul seperti pada gambar diatas user harus memasukan password sesuai dengan password pada saat mengenkripsikan file teks. setelah itu maka akan muncul file teks yang telah di deskripsikan seperti pada gambar berikut.



Gambar 4.9 File Enkripsi Dan Deskripsi

pada gambar diatas adalah gambar dimana hasil enkripsi dan deskripsi telah disimpan bisa kita liat pada gambar yang mana hasil enkripsi dan yang mana hasil deskripsi.

BAB V

PENUTUP

1. Kesimpulan

Berdasarkan hasil implementasi dan pembahasan yang dilakukan pada penelitian ini, ada beberapa kesimpulan yang dapat ditarik yaitu:

a. Enskripsi dan Deskripsi ini merupakan aplikasi yang membantu menjaga file text menjadi aman dari orang yang akan masalah gunakan file dari isi dokumen.

b. Proses penyamaran pada algoritma ini memanfaatkan metode kriptografi berbasi DES dimodifikasi sehinggahanya membutuhkan satu kunci privat saja. Kunci privat tersebut hanya dibutuhkan oleh pihak yang akan melihat dokumen digital.

c. Hasil penyamaran dokumen dalam bentuk deret bilangan merupakan salah satu cirri khas kriptografi yang memiliki tingkat pengamanan yang tinggi. Dengan menggunakan deret bilangan, akan mempersulit proses kriptanalis terhadap dokumen yang disamarkan.

2. Saran

Adapun saran yang ingin penulis berikan sehubungan dengan penelitian ini adalah sebagai berikut:

a. Aplikasi ini dapat dikembangkan dalam bentuk *user*, sehingga perlu dilakukan *re-login* untuk setiap proses penterjemahan dokumen oleh pengguna yang bersangkutan.

b. Dapat ditambahkan format dokumen digital lain selain TXT, sehingga menambah variasi dokumen digital yang dapat diakses dalam aplikasi ini.

c. Untuk bahan perbandingan, dapat dipergunakan basis kriptografi lain seperti elgamal, sehingga dapat dilihat perbedaannya dengan basis DES yang digunakan.

DAFTAR PUSTAKA

Ardhi. C.K. 2018. ***Perancangan Alat Pendeteksi Gempa Menggunakan Sensor Accelerometer Dan Sensor Getar*.** Publikasi Tugas Akhir Program Studi S1 Teknik Elektro Universitas Telkom.

Aprianah, Desi. 2013. ***Program Kendali Intensitas Cahaya Lampu dan Pintu Via Short Message Service*.** Laporan Akhir Politeknik Negeri Sriwijaya.

Aristiawan. H, & Setiadi. H. 2006. ***Pemanfaatan Levitasi Magnet Sebagai Sensor Gerak Vertikal Untuk Deteksi Getaran*.** ITB, 2006

Amin, M., & Novelan, M. S. (2020). Sistem Kendali Obstacle Avoidance Robot Sebagai Prototype Social Distancing Menggunakan Sensor Ultrasonic dan Arduino. InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 5(1), 148-153.

Anwaruddin. M. 2019. ***Rancang Bangun Prototype Tempat Tidur Tanggap Gempa Menggunakan Arduino Uno***. Skripsi. Universitas Islam Negeri Syarif Hidayatullah. Jakarta. 2019.

Batubara, S., Wahyuni, S., Hariyanto, E., & Lubis, A. (2021). Webinar Menangkal Cyberporn pada Internet dan Android memanfaatan add ons dan aplikasi antipornografi parental control di SMA Panca Budi. Jurnal Abdimas BSI: Jurnal Pengabdian Kepada Masyarakat, 4(1), 164-173.

Jamal. Z. 2011. ***Pendeteksi Gempa Dengan Metode FM Berbasis Personal Komputer***. Jurnal Informatika, Vol. 11, No. 1, Juni 2011.

Maharani, D., Helmiah, F., Harahap, R. R., & Fachri, B. (2018). Pelatihan Komputer Dalam Meningkatkan Tahfidz Qur'an Menggunakan Al-Qur'an Digital Tajwid. Jurdimas (Jurnal Pengabdian Kepada Masyarakat) Royal, 1(2), 95-100.

Novianta. M.A. 2012. ***Sistem Deteksi Dini Gempa Dengan Piezo Elektrik Berbasis Mikrokontroler AT89C51***. Simposium Nasional RAPI XI FT UMS – 2012. ISSN : 1412-9612.

Pranata. A, Prayudha. J, & Sandika. T. 2017. ***Rancang Bangun Alat Pendeteksi Dehidrasi Dengan Metode Fuzzy Logic Berbasis Arduinon***. Jurnal SAINTIKOM Vol. 16, No. 3, September 2017.

Riskawati, Nurlina & Karim R. 2017. ***Alat Ukur dan Pengukuran***. Bahan Ajar Universitas Muhammadiyah Makasar. Fakultas Keguruan dan Ilmu Pendidikan.

Suraya, & Novianta. M.A. 2013. ***Prototipe Deteksi Gempa Menggunakan Metode Perambatan Gelombang Pada Sensor Getar Berbasis Mikrokontroler Dengan Informasi SMS Gateway***. Teknik Informatika Institut Sains & Teknologi AKPRIND Yogyakarta. 2013.

Syamsuar. S, Wibawa. N, & Makarim, H. 2011. ***Cara Kerja dan Penggunaan Motor Direct Current (DC) Pada Kapal Selam***. Penelitian Pusat Teknologi Industri dan Sistem Transportasi (BPPT). Volume 23, Nomor 5, Mei 2011

Wayahdi, M. R., Zarlis, M., & Putra, P. H. (2019, June). Initialization of the Nguyen-widrow and Kohonen Algorithm on the Backpropagation Method in the Classifying Process of

Temperature Data in Medan. In Journal of Physics: Conference Series (Vol. 1235, No. 1, p. 012031). IOP Publishing.

Winadi. R. 2007. ***Pembuatan Sensor Posisi Faraday Untuk Pendeteksi Dini Gempa Pada Gedung*.** Proyek Akhir, PENS-ITS, Surabaya, 2007.

The McGraw-Hill Companies, ***Resistors***. Topics Covered in Chapter 2. 2007.

TLT-8016 Basic Analog Circuits, ***Diodes and Diode Circuits***. Chapter 3. 2006.

Internet : www.ele.uri.edu/courses/ele432/spring08/LEDs.pdf

Internet : web.mit.edu/viz/EM/visualizations/coursenotes/modules/guide12.pdf

Internet : veronica.staff.gunadarma.ac.id/.../files/.../BAB+2+Transformator.pdf

Internet : https://components101.com/microcontrollers/atmega16-pinout-features-datasheet