PENERAPAN ENKRIPSI DAN DEKRIPSI FILE MENGGUNAKAN ALGORITMA VIGENERE CIPHER

Disusun dan Diajukan untuk Memenuhi Persyaratan Ujian Akhir
Memperoleh Gelar Sarjana Komputer pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH :

NAMA : MAGDALENA RIKIANA BR BUTAR BUTAR

N.P.M : 1514370308

PROGRAM STUDI : SISTEM KOMPUTER

PROGRAM STUDI SISTEM KOMPUTER
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

ABSTRAK

MAGDALENA RIKIANA BR BUTAR BUTAR

“ PENERAPAN ENKRIPSI DAN DEKRIPSI FILE MENGGUNAKAN ALGORITMA VIGENERE CIPHER”

2019

Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses *enkripsi* maupun *dekripsi*.dan ilmu yang mempelajari cara pengamanan *file* atau data dengan tujuan mencegah dari orang lain yang ingin mengetahui isinya,dengan menggunakan kode-kode dan aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya. Salah satu yang harus benar-benar dijaga adalah pesan yang bersifat rahasia.Pesan adalah setiap pemberitahuan, kata, atau komunikasi baik lisan maupun tertulis, yang dikirimkan dari satu orang ke orang lain.Dalam tugas akhir ini akan disajikan perancangan aplikasi penerapan *enkripsi* dan *deskripsi file* dengan menggunakan algoritma *vigenere cipher* yang mana algoritma ini termasuk kedalam algoritma kriptografi klasik.merupakan salah satu metode yang dapat digunakan untuk meyandikan pesan dan yang memanfaatkan prinsip bujursangkar *vigenere* untuk melakukan enkripsi.Dari seluruh kombinasi yang ada,seluruhnya berhasil untuk proses *enkripsi* dan *dekripsi* guna mengembalikan *cipher text* menjadi *plaintext* yang asli.Setiap proses tersebut diimplementasikan dalam bahasa pemrograman *Microsoft visual basic.Net.*

Kata Kunci : *Kriptografi,Algoritma,Vigenere Cipher,Enkripsi,Dekripsi*

DAFTAR ISI

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan data dan informasi merupakan hal yang sangat penting di era informasi saat ini. Umumnya, setiap institusi memiliki dokumen-dokumen penting dan bersifat rahasia yang hanya boleh diakses oleh orang tertentu. Sistem informasi yang dikembangkan harus menjamin keamanan dan kerahasian dokumen-dokumen tersebut. Namun kendalanya bahwa media-media yang digunakan sering kali dapat disadap oleh pihak lain.Oleh karena itu terciptalah ilmu kriptografi.

Kriptografi merupakan teknik untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Pesan yang disamarkan (pesan asli) dinamakan *plainteks*,sedangkan pesan hasil penyamaran (teks tersandi) dinamakan *chiperteks*. Proses kriptografi terdiri atas *enkripsi* dan *dekripsi. Enkripsi* merupakan proses penyamaran dari *plainteks* ke *chiperteks* sedangkan *dekripsi* merupakan proses pembalikan dari *chiperteks* ke *plainteks*.Dan penulis ingin membuat keamanan pesan menggunakan metode algoritma *vigenere cipher*.dan proses pengamanan pesan tersebut hanya berupa text yang dikirim, dan penerima harus memiliki kunci untuk membuka pesan asli. Dengan adanya *vigenere* ini pesan teks yang muncul berupa hasil dari algoritma tersebut.Dan membuat suatu aplikasi penerapan algoritma *vigenere cipher* dengan

menggunakan sistem yang berbasiskan desktop. Aplikasi yang akan dirancang adalah sebagai penerapan algoritma *vigenere cipher* agar dapat memahami cara teknik enkripsi dan dekripsi *file* yang digunakan kepada pengguna awam dalam teknik manipulasi data tersebut.

Vigenere cipher merupakan metode kriptografi kunci simetris dengan model penggantian karakter atau *subtitusi*. Metode *vigenere cipher* menggunakan abjad sebagai kunci penyandian untuk melakukan penggantian atau subtitusi karakter pesan. Pemberian prosedur keamanan untuk memenuhi kebutuhan kemanan informasi berupa teks dapat dilakukan dengan menerapkan teknik kriptografi. Salah satunya dengan cara menerapkan *vigenere cipher* sebagai metode yang digunakan untuk proses enkripsi dan dekripsi *file.* Berdasarkan uraian diatas ,maka penulis tertarik untuk memilih judul **"Penerapan *Enkripsi* Dan *Dekripsi* File Menggunakan Algoritma *Vigenere Cipher*".**

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah penelitian di atas maka rumusan masalah adalah sebagai berikut :

1. Bagaimana merancang sebuah aplikasi *enkripsi* dan *dekripsi* file menggunakan algoritma *Vigenere Cipher* berbasis *desktop*?
2. Bagaimana proses penerapan *enkripsi* dan *dekripsi* menggunakan algoritma *Vigenere Cipher* pada *file*?

1.3 Batasan Masalah

Dalam perancangan aplikasi penelitian penulis membatasi masalah sebagai berikut :

1. Hanya membahas sampai pada proses penerapan *enkripsi* dan *dekripsi file*.
2. Hanya menggunakan metode *Vigenere Cipher*.
3. Bahasa pemograman yang digunakan adalah *Visual Basic.Net.*
4. Hanya menerapkan pada *file* dengan format *.txt.
5. Jumlah karakter kunci hanya sampai 255 sesuai dengan table ASCII.

1.4 Tujuan Penelitian

Tujuan penelitian yang ingin dicapai penulis dalam perancangan aplikasi penerapan algoritma *vigenere* ini adalah :

1. Untuk merancang sistem keamanan *file* dengan menggunakan algoritma *Vigenere Cipher*
2. Untuk membuat aplikasi *enkripsi* dan *dekripsi file* menggunakan algoritma *Vigenere Cipher.*

1.5 Manfaat Penelitian

Perancangan aplikasi penerapan algoritma *vigenere* ini bermanfaat bagi masyarakat luas antara lain :

1. Dengan menggunakan aplikasi ini seseorang dapat menjaga keamanan data dan informasi agar pihak yang tidak berwenang tidak dapat memecahkan data yang telah dienkripsi, sehingga keamanan dan kerahasiaaan data dapat terjaga.
2. Untuk menjaga dan mengamankan pertukaran data dan informasi menjadi aman.
3. Untuk dapat digunakan dalam proses kerahasian data agar suatu informasi tidak takut diketahuin oleh orang lain .dan data tersebut dapat terjaga dengan menggunakan algoritma *Vigenere Cipher*.

BAB II

LANDASAN TEORI

2.1 Aplikasi

Menurut Ninuk Wiliani dan Syadid Zambi (2017) “Aplikasi adalah program siap pakai yang dapat digunakan untuk menjalankan printah-printah dari pengguna aplikasi tersebut dengan tujuan mendapatkan hasil yang lebih akurat sesuai dengan pembuatan aplikasi tersebut”,Secara umum aplikasi dapat diartikan sebagai suatu program berbentuk perangkat lunak yang dilakukan oleh manusia.Menurut kamus besar bahasa Indonesia “Aplikasi adalah penerapan dari rancang sistem untuk mengolah data yang menggunakan aturan atau ketentuan bahasa pemrograman tertentu”.

Aplikasi berasal dari kata *application* yaitu bentuk benda dari kata kerja *to apply* yang dalam bahasa Indonesia berarti pengolah.secara istilah,aplikasi komputer adalah suatu sub kelas perangkat lunak komputer yang menggunakan kemampuan komputer langsung untuk melakukan suatu tugas yang diinginkan pemakai.

2.2 Kriptografi

Menurut Fresly Nandar Pabokory (2015) “Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya”.Kriptografi merupakan ilmu menulis pesan rahasia dengan tujuan menyembunyikan makna pesan tersebut.

Dari pernyataan diatas dapat disimpulkan bahwa kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan data atau informasi dengan cara menyembunyikan pesan asli agar tidak dapat dilihat dan dibaca oleh pihak yang tidak memiliki wewenang dalam informasi data tersebut.

Proses yang dilakukan untuk mengubah *plaintext* menjadi *ciphertext* disebut enkripsi *(encryption),*sedangkan proses untuk mengubah *ciphertext* kembali ke *plaintext* disebut (*decryption).*Di dalam kriptografi kita akan sering menemukan berbagai istilah atau *terminology.*Beberapa istilah yang harus diketahui yaitu :

1. Pesan, *Plainteks,* dan *Cipherteks*

   Pesan *(message)* merupakan data atau informasi yang dapat dibaca dan dimengerti maknanya.nama lain untuk pesan adalah *(plaintext)* atau teks jelas *(cleartext).*

2. Pengirim dan Penerima

   Komunikasi data melibatkan pertukaran pesan antara dua entitas,Pengirim merupakan entitas yang mengirim pesan kepada entitas lainnya,Penerima *(receiver)* adalah entitas yang menerima pesan.

3. *Enkripsi* dan *dekripsi*

   Proses menyandikan plainteks menjadi *cipherteks* disebut *enkripsi (encryption)* atau *enciphering*.Sedangkan proses mengembalikan cipherteks menjadi plainteks semula disebut dekripsi *(decryption)* atau *deciphering*.

4. *Cipher* dan kunci

   Algoritma kriptogarfi disebut juga *cipher,* yaitu aturan untuk *enkripsi* dan *dekripsi,*.Beberapa *cipher* memerlukan algoritma yang berbeda untuk *enkripsi* dan dekripsi.Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen-elemen *plainteks* dan himpunan yang berisi *cipherteks*. *Enkripsi* dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara dua himpunan tersebut.

2.2.1 Dasar Kriptografi

Kriptografi Merupakan ilmu mempelajari mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseoran agar data atau pesan tetap aman saat dikirimkan atau dari pengirim ke penerima tanpa mengalami gangguan dari pihak-pihak ketiga.Prinsip-prinsip yang mendasari kriptografi yakni:

1. *Secrecy (kerahasiaan),*“adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci

rahasia untuk membuka maupun menghapus informasi yang telah disandi".

2. Authentication,"adalah pengenalan identifikasi informasi dan pengenalan dari kesatuan sistem maupun informasi itu sendiri.Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri yang dimana informasi yang dikirimkan harus diautentifikasi keaslianya, isi datanya, dan waktunya".
3. Hak Akses terhadap suatu "file atau fasilitas lain dalam sebuah sistem pemrosesan informasi masih dalam area lain dimana gagasan kriptografi telah diterapkan".

2.2.2 Tujuan Kriptografi

Kriptografi bertujuan untuk layanan keamanan yang memiliki beberapa aspek keamanan yang memiliki beberapa aspek keamanan, antara lain sebagai berikut :

1. Confidelity (kerahasiaan)

   Merupakan layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak-pihak lain (kecuali pihak pengirim dan pihak penerima/pihak-pihak yang memiliki ijin).Umumnya hal ini dilakukan dengan cara membuat suatu algoritma dengan matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan sulit untuk dipahami.

2. Data integrity (keutuhan data)

   Merupakan layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).

3. Authentication (keotentikan)

   Merupakan layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.

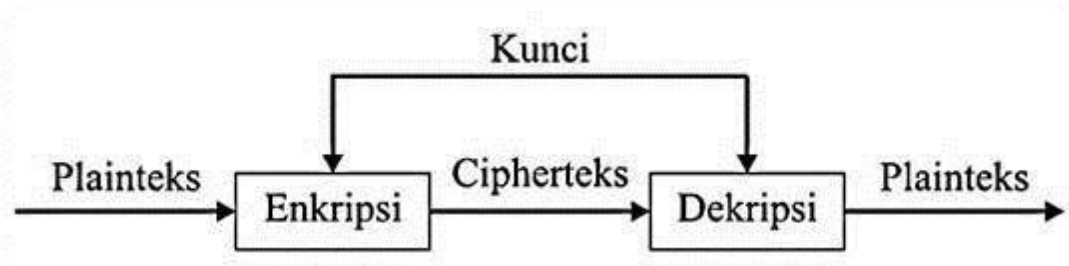
4. Non-repudiation (anti-penyangkalan)

   Merupakan layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

2.3 Enkripsi Dan Dekripsi

Menurut Hafid Rosianto (2017) "*Enkripsi* adalah sebuah proses yang melakukan perubahan sebuah kode dari yang biasa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca)". *Enkripsi* dapat diartikan sebagai kode atau *cipher*. Sebuah sistem pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk mengganti kata dari informasi atau yang merupakan bagian dari informasi yang dikirim.Sebuah *cipher* menggunakan suatu algoritma yang dapat mengkode semua aliran data (*stream*) dan *bit* dari sebuah pesan menjadi *cryptogram* yang tidak dimengerti (*unnitelligible).*

Dekripsi merupakan algoritma atau cara yang dapat digunakan untuk membaca informasi yang telah dienkripsi untuk kembali dapat dibaca. Dengan kata lain dekripsi merupakan proses membalikkan hasil yang diberikan dari proses *enkripsi* ke dalam bentuk awal sebelum dienkrip.



Gambar 2.1 Proses Enkripsi dan Dekripsi

Sumber : Fresly Nandar Pabokory (2015)

Ada beberapa elemen dari enkripsi yang akan dijabarkan di bawah ini:

1. Algoritma dari *Enkripsi* dan *Dekripsi*

Algoritma dari *enkripsi* merupakan fungsi yang digunakan untuk melakukan enkripsi dan dekripsi. Algoritma yang digunakan menentukan keakuratan dari enkripsi, dan ini biasanya dibuktikan dengan basis matematika. Berdasarkan cara memproses teks (*plaintext*), *cipher* dapat dikategorikan menjadi dua jenis:*block cipher* dan *stream cipher*.*Block cipher* bekerja dan dengan memproses data secara *blok*, dan dimana beberapa karakter digabungkan menjadi satu blok.Dengan setiap proses satu blok akan menghasilkan keluaran satu blok juga.sementara itu stream cipher bekerja memproses masukkan (karakter atau data) secara terus menerus dan menghasilkan data pada saat yang bersamaan.

2. Kunci yang digunakan dan panjang kunci

Kekuatan dari penyandian bergantung kepada kunci yang digunakan. Untuk itu, kunci yang lemah tersebut tidak boleh digunakan. Selain itu, panjang kunci yang biasanya ukuran dalam *bit*, juga menentukan kekuatan dari enkripsi.Maka kunci yang lebih panjang biasanya lebih aman dari kunci yang pendek.Semakin panjang sebuah kunci,maka semakin besar *keyspace* yang akan dijalani.

2.4 File

Menurut Fresly Nandar Pabokory (2015) "*File* adalah entitas dari data yang disimpan didalam sistem *file* yang dapat diakses dan diatur pengguna.sebuah file memiliki nama yang unik dalam direktori dimana ia berada.Alamat direkrtori dimana suatu berkas ditempatkan diistilahkan dengan path.sebuah *file* berisi aliran data (atau data stream) yang berisi sekumpulan data yang saling berkaitan serta artribut berkas yang disebut dengan properties yang berisi informasi mengenai *file* yang bersangkutan seperti informasi mengenai kapan sebuah berkas dibuat.

2.5 Kode ASCII

Kode American Standard Code for Information Interchange (ASCII) "Merupakan standar internasional yang selalu digunakan dalam pengkodean huruf dan simbol-simbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal". Dalam kriptografi, kode ASCII ini merupakan bit yang akan mewakili teks asli yang kemudian dienkripsi untuk mendapatkan teks kode dalam bentuk urutan bit.

2.6 Algoritma Kriptografi

Menurut Hafid Rosianto (2017) "Algoritma dalam kriptografi merupakan sekumpulan aturan (fungsi matematis yang digunakan) untuk proses *enkrip*si dan proses *deskripsi"*.Konsep matematis yang mendasari algoritma adalah relasi antara himpunan, yaitu relasi antara himpunan yang berisi elemen-elemen *ciphertext*. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara kedua himpunan tersebut.

E(P) = C ……...….....(1)

Dan fungsi *dekripsi* memetakan himpunan C ke himpunan P

D(C) = P …….…….....(2)

Karena fungsi dekripsi D mengembalikan himpunan C menjadi himpunan P asal, maka algoritma kriptografi harus memenuhi persamaan

D(E(P)) = P …….……..(3)

Tingkat keamanan suatu *algoritma* kriptografi seringkali diukur dari kuantitas proses yang dilakukan dalam suatu fungsi, baik itu fungsi *enkrip*si

maupun fungsi *deskripsi*. Proses tersebut juga dapat dihubungkan dengan sumber data yang dibutuhkan, Menunjukkan semakin kuat *algoritma* kriptografi tersebut.

2.7 Jenis Jenis Kriptografi

2.7.1 Kriptografi Klasik

Kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum komputer ditemukan dan kriptografi ini rata-rata masih menggunakan kunci simetris dan menyandikan pesan dengan teknik subtitusi atau transposisi. Kriptografi ini hanya melakukan pengacakan pada huruf A-Z, dan sangatlah tidak disarankan untuk mengamankaninformasi-informasi penting karena dapat dipecahkan dalam waktu singkat. Biarpun telah ditinggalkan, kriptografi klasik tetap dapat ditemui disetiap pelajaran kriptografi sebagai pengantar kriptografi modern (Hartini & Primaini, 2013)".

2.7.2 Kriptografi Modern

Menurut Hafid Rosianto (2017) "Kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik.Kriptografi modern terdapat berbagai macam algoritma yang untuk mengamankan informasi yang dikirim melalui jaringan komputer". Algoritma kriptografi modern :

1. Algoritma Simetris

Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya.Algoritma kriprografi simetris sering disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma

satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu. Pada umumnya yang termasuk ke dalam kriptografi simetris ini beroperasi dalam mode blok (*block cipher*), yaitu setiap kali proses *enkripsi* atau *dekripsi* dilakukan terhadap satu blok data (yang berukuran tertentu), atau beroperasi dalam mode aliran (*stream cipher*), yaitu setiap kali *enkripsi* atau *dekripsi* dilakukan terhadap satu bit atau satu *byt*e data.

2. Algoritma Asimetris

Algoritma *asimetris "*adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi deskripsi". Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsi suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia itu, yang dalam hal ini kunci rahasia untuk melakukan pembongkaran terhadap kode yang dikirim untuknya.

2.8 Vigenere Cipher

Priyono (2016) Vigenere Cipher "adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso.nama *vigenere* sendiri diambil dari seorang yang bernama *blaise de vigenere*.Vigenere cipher termasuk dalam cipher abjad majemuk (*Polyalphabetic Substituyion Cipher*)".*Vigenere Cipher* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf pada kata kunci.Karakter huruf yang yang digunakan pada *vigenere cipher* yaitu A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z.

Dan dengan angka 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23, 24,25.Panjang kunci tersebut bisa lebih pendek ataupun sama dengan *plaintext*, maka kunci tersebut akan diulang secara periodik hingga panjang kunci tersebut sama dengan panjang *plaintext*nya. Tabel yang digunakan merupakan tabel 26 huruf alfabetik *standart*, yang dimulai dari A sampai Z.

Enkripsi (penyandian) dan dekripsi dengan sandi *Vigenere cipher* juga dapat dituliskan secara matematis, dengan menggunakan penjumlahan dan operasi modulus. Berikut ini rumus enkripsi dan dekripsi Vi*genere Cipher* :

Enkripsi : Ci$\rightarrow$(Pi + Ki) Mod 26 …….……(1)

Dekripsi : Pi$\rightarrow$(Ci - Ki) Mod 26 …….....…….……(2)

Keterangan :

Ci : Ciphertext

Pi : Plaintext

Ki : Kunci

Mod : Modulus

N : Banyak Karakter

Tabel 1.1 Tabel *Substitusi* Algoritma *Vigenere Cipher*

Plaintext: **PANCABUDI**

Kunci: **MAGDALENA**

Contoh Tabel Substitusi Algoritma *Vigenere Cipher*

Dengan metode pertukaran angka dengan huruf di atas, diperoleh bahwa teks asli (PANCABUDI) memiliki kode angka (15,0,13,2,0,1,20,3,8), sedangkan kode angka untuk teks kunci (MAGDALENA) yaitu (12,0,6,3,0,11,4,14,0). Setelah dilakukan perhitungan, maka dihasilkan kode angka ciphertext (1,0,19,5,0,12,24,17,8). Jika diterjemahkan kembali menjadi huruf sesuai urutan awal, maka menjadi huruf BATFAMYRI.

Sedangkan teknik lain untuk melakukan proses enkripsi dengan metode *vigenere cipher* yaitu menggunakan *tabula recta* (disebut juga bujur sangkar *vigenere*).Kolom paling kiri dari bujur sangkar menyatakan huruf-huruf kunci, sedangkan baris paling atas menyatakan huruf-huruf atau plaintext.yang mana jumlah pergeseran huruf plaintext ditentukan nilai numerik huruf kunci tersebut (yaitu, a=0, b=1, c=2,…….,z=25).

Gambar 2.2 Tabula Recta (bujur sangkar) Algoritma *Vigenere Cipher*

Sumber : Gede Angga Pradipta (2016)

Bujur sangkar vigenere digunakan untuk memperoleh ciphertert dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek dari pada panjang plaintext, maka kunci diulang penggunaannya (sistem periodik). Bila panjang atau ukuran kunci adalah merupakan m,maka periodenya dikatakan m.Sebagai contoh,jika plaintext adalah **UNIVERSITAS PANCABUDI** dan kunci adalah **Magdalena,** maka penggunaan kunci secara periodik sebagai berikut.

Plaintext : UNIVERSITAS PANCABUDI

Kunci : Magdalena

"Untuk mendapatkan hasil dari *ciphertext* dari teks dan kunci di atas,maka untuk huruf *plaintext* pertama adalah U, dan ditarik garis vertikal dari huruf U dan ditarik garis mendatar dari huruf M, perpotongannya adalah pada kotak yang berisi huruf g".

Dengan cara yang sama, ditarik garis *vertikal* dari huruf N dan ditarik garis mendatar pada huruf a, perpotongannya adalah pada kotak yang juga berisi berisi huruf N. hasil enkripsi seluruhnya adalah sebagai berikut.

Plaintext : UNIVERSITAS PANCABUDI

Kunci : magdalenama gdalenama

Ciphertext : GNOYECWVTMS VDNNEOUPI

2.9 Bahasa Pemograman

Menurut Jusuf Wahyudi (2013) Bahasa pemrograman adalah perintah-perintah atau instruksi yang dimengerti oleh komputer untuk melakukan tugas tertentu".Bahasa pemrograman merupakan sebuah instruksi untuk memerintah komputer agar bisa menjalankan fungsi tertentu, namun hanya instruksi standar saja.Bahasa pemrograman juga memiliki perhimpunan dari aturan sintaks dan semantik yang tugasnya untuk mendefinisikan program komputer.Bahasa pemrograman komputer yang kita kenal antara lain adalah *Java, Visual Basic, C++, C, PHP*, dan bahasa pemrograman lainnya. Namun kebutuhan bahasa pemegraman ini harus disesuaikan dengan fungsi dan perangkat yang menggunakannya.Menurut generasi bahasa pemrograman digolongkan menjadi 4 generasi, yaitu:

1. Generasi pertama : *machine language*
2. Generasi kedua : *assembly language*: *Assembler*
3. Generasi ketiga: *high level programming language*, contoh: C dan *Pascal*
4. Generasi keempat : *4 GL (fourth-generation language)*, contoh: *SQL*
5. Generasi kelima : *Programming Language Based Object Oriented & Web Development*

Secara umum bahasa pemrograman dibagi menjadi 4 kelompok, yaitu :

1. *Object Oriented Language* : Seperti bahasa *Visual C, Delphi, Visual dBase, Visual FoxPro.*
2. *Low Level Language* : Bahasa *Assembly.*

3. *Middle Level Language* : Bahasa *C.*
4. *High Level Language* :*Bahasa Basic* dan *Pascal.*

Menurut dari tingkat kedekatannya dengan mesin komputer,bahasa pemrograman terdiri dari sebagai berikut:

a. Bahasa Mesin, yaitu untuk memberikan perintah kepada komputer dengan memakai kode bahasa biner,contohnya adalah 01100101100110.
b. Bahasa Tingkat Rendah, atau dikenal dengan istilah bahasa rakitan (bah.Inggris *Assembly*), yaitu memberikan perintah kepada komputer dengan memakai kode-kode singkat (kode *mnemonic*), contohnya *MOV, SUB, CMP, JMP, JGE, JL, LOOP*, dsb.
c. Bahasa Tingkat Menengah, yaitu bahasa komputer yang memakai campuran instruksi dengan kata-kata bahasa manusia (lihat contoh Bahasa Tingkat Tinggi di bawah) dan instruksi yang bersifat simbolik, contohnya {, }, ?, <<, >>, &&.
d. Bahasa Tingkat Tinggi, yaitu bahasa yang merupakan komputer yang memakai instruksi yang berasal dari unsur kata-kata bahasa manusia, contohnya adalah : *begin, end, if, for, while, and, or, dsb.*

Fungsi dari bahasa pemrograman adalah untuk memerintahkan sebuah komputer agar dapat mengolah data yang sesuai dengan di inginkan. *Output* dari bahasa pemrograman ini dapat berupa aplikasi ataupun program khusus.

2.10 *Microsoft Visual Studio*

Menurut Ninuk Wiliani (2017)" *Microsoft Visual Studio* merupakan sebuah perangkat lunak lengkap (*suite*) yang dapat digunakan untuk melakukan pengembangan aplikasi".Baik itu aplikasi bisnis,aplikasi personal,ataupun komponen komponen aplikasi dalam bentuk aplikasi *console*, aplikasi *Windows,* ataupun aplikasi *Web.Visual Studio* mencakup compiler dan kompiler yang dimasukkan ke dalam paket *Visual Studio* antara lain adalah *Visual C++, Visual C#, Visual Basic, Visual Basic.NET, Visual InterDev, Visual J++, Visual J#, Visual FoxPro, dan Visual SourceSafe Microsoft Visual Studio* dapat digunakan untuk mengembangkan aplikasi dalam *native code* (bahasa mesin yang berjalan di *Windows*.

Visual studio dapat digunakan untuk membuat sebuah aplikasi yang berbasis desktop yang merupakan *platform* windows,namun juga dapat dijalankan dalam bentuk *Microsift Intermediate Language.Net Framework*. Selain itu *Visual Studio* juga dapat digunakan untuk membuat sebuah aplikasi yang dapat dijalankan di *windows mobile* yang juga berjalan diatas.*Net Compact Framework.*

2.11 *Visual Basic* 2010

Menurut Ninuk Wiliani (2017) "*Visual Studio* 2010 pada dasarnya adalah sebuah bahasa pemrograman komputer".Dimana pengertian dari bahasa pemrograman itu adalah perintah-perintah atau instruksi yang dimengerti oleh komputer untuk melakukan tugas-tugas tertentu. *Visual Studio* 2010 yang sering disebut dengan *VB.Net* 2010, yaitu sebagai bahasa pemrograman sebagai sarana (tool) untuk menghasilkan program-progam aplikasi berbasiskan windows. *Visual basic* merupakan sebuah bahasa pemrograman yang berpusat pada object (*Object Oriented Programming*) digunakan dalam pembuatan aplikasi *Windows* yang berbasis *Graphical User Interface*, hal ini menjadikan *Visual Basic* menjadi bahasa pemrograman yang wajib diketahui dan dikuasai oleh setiap programmer. Beberapa karakteristik obyek tidak dapat dilakukan oleh *Visual Basic* misalnya seperti *Inheritance* tidak bisa *module* dan *Polymorphism* secara terbatas bisa dilakukan dengan deklarasi class module yang mempunyai *Interface* tertentu.

Adapun beberapa kemampuan atau beberapa manfaat dari *Visual Studio* 2010 diantaranya :

1. Untuk membuat program aplikasi berbasiskan windows.
2. Untuk membuat objek-objek pembantu program seperti,misalnya : aplikasi Internet .
3. Untuk menguji program (*debugging*) yang menghasilkan program berakhiran *EXE* yang bersifat executable atau juga dapat langsung dijalankan.

Visual Studio 2010 “merupakan bahasa yang dapat cukup mudah untuk dipelajari. Bagi programmer pemula yang baru ingin belajar program, lingkungan *Visual Studio* dapat membantu membuat program dalam sekejap mata. Sedang bagi programer tingkat lanjut, kemampuan yang besar dapat digunakan untuk membuat programprogram yang kompleks, misalnya lingkungan net-working atau client server”.*Bahasa Visual Studio* cukup sederhana dan menggunakan kata-kata bahasa *Inggris* yang umum digunakan.dan di dalam *Visual Basic* semuanya sudah disediakan dengan pilihan-pilihan yang tinggal diambil sesuai dengan kebutuhan. Selain itu, sarana pengembangannya yang bersifat visual memudahkan kita untuk mengembangkan aplikasi berbasiskan Windows.

Adapun kelebihan dan kekurangan dari *Visual Basic*ini yaitu :

1. Kelebihan *Visual Basic*
    a. *VB.Net* menyediakan fasilitas *Real Time Background Compiler* yaitu sebagai penanganan dalam error atau bug.
    b. Lebih cepat dalam pembuatan aplikasi berbasis desktop
    c. Menyediakan untuk *developer* pemrograman data akses *ActiveX Data Object (ADO).*
2. Kelemahan Visual Basic
    a. Untuk versi *VB.Net 2010* dengan seterusnya tidak mempunyai Komponen *Crystal Report* karena sudah terpisah.
    b. Harus *ada Net framework* agar aplikasi bisa berjalan

c. Tidak mempunyai database sendiri.

d. Memerlukan kapasitas yang besar untuk instalasi *VB.Net.*

2.12 *Flowchart*

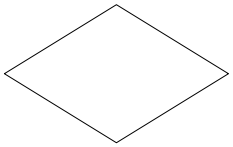
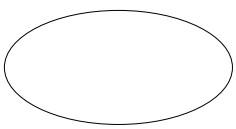
Menurut Mohamad Natsir (2017) *Flow chart* atau *diagram* alir "adalah sebuah diagram dengan simbol-simbol grafis yang menyatakan aliran algoritma atau proses yang menampilkan langkah-langkah yang disimbolkan dalam bentuk kotak,dan beserta urutannya dengan menghubungkan masing-masing langkah tersebut dengan menggunakan tanda panah. Diagram ini juga bisa memberi solusi selangkah demi selangkah untuk penyelesaian masalah yang ada di dalam proses atau algoritma tersebut".

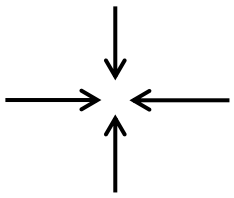
Flow chart digunakan dalam merancang dan mendokumentasikan proses yang kompleks atau program.Seperti jenis lain *diagram*, mereka membantu memvisualisasikan apa yang terjadi dan dengan demikian membantu pengunjung untuk memahami proses, dan mungkin juga menemukan kelemahan, kemacetan, dan ketidakjelasan lain di dalamnya. Ada berbagai jenis diagram alur yang masing-masing memiliki repertoire kotak sendiri dan ketentuan notasinya. Dua jenis yang paling umum dari kotak di *flow chart* adalah :

1. Langkah pengolahan, biasanya disebut aktivitas, dan dilambangkan sebagai persegi panjang.
2. Keputusan, biasanya dilambangkan sebagai belah ketupat.

Flowchart memberikan solusi langkah demi langkah dari sebuah masalah yang ingin dipecahkan. Kegunaan *flowchart* adalah untuk menganalisis, merancang, mendokumentasikan serta mengelola suatu proses atau program di berbagai bidang. Sebuah proses atau *action* direpresentasikan dalammm sebuah kotak, dan tanda panah yang menghubungkan kotak-kotak ini mewakili aliranm atau arah aliran data. Berikut ini adalah simbol-simbol *flowchart* yang sering digunakan beserta deskripsinya:

Tabel 2.2 Simbol-Simbol *Flowchat*

No	**Simbol *Flowchart***	**Fungsinya**
1		*Terminal* atau *Start*, berfungsi untuk memulai dan mengakhiri alur program.
2		*Process*, adalah untuk mengolah dan mengubah data yang ada didalam komputer.
3		*Decision*, digunakan untuk menentukan operasi perbandingan logika ketika masuk pada alur program.
4		*Input* dan *Output*, adalah simbol yang digunakan untuk memasukan data yang biasanya berupa *username* dan *password*, dimana hasil dari proses.
5		*Connector*, adalah menentukan hubungan arus proses program yang berjalan dalam halaman yang sama.

6		*Arrow Flow*, adalah untuk menunjukkan alur proses program yang terdiri dari, alur atas ke bawah, kanan ke kiri dan juga sebaliknya.
7		*Document*, adalah sebuah simbol untuk data atau informasi.

Sumber : Mohamad Natsir (2017)

2.13 Pengertian UML (Unified Modeling Language)

Menurut Winda Aprianti (2016) *Unified Modeling Language (UML)* adalah standarisasi bahasa pemodelan untuk membangun perangkat lunak yang dibangun dengan menggunakan teknik pemrograman berorientasi objek.Diagram diagram yang digunakan pada *UML* antara lain adalah *class diagram, object diagram, use case diagram, activity diagram,* dan *sequence diagram.*

UML adalah bahasa dengan spesifikasi standar yang dipergunakan untuk mendokumentasikan, menspesifikasikan dan membangun perangkat lunak.UML juga merupakan metodologi dalam mengembangkan sistem berorientasi objek dan juga Merupakan alat untuk mendukung pengembangan sistem.*UML* saat ini sangat banyak dipergunakan dalam dunia industri yang merupakan standar bahasa pemodalan umum. Berikut beberapa tujuan atau fungsi dari penggunaan *UML,* yang diantaranaya:

1. Dapat memberikan bahasa permodelan untuk *visual* kepada pengguna dari berbagai macam pemrograman maupun proses rekayasa.

2. Dapat menyatukan praktek-praktek terbaik yang ada dalam permodelan.
3. Dapat memberikan model yang siap untuk digunakan, merupakan bahasa permodelan *visual* yang ekspresif untuk mengembangkan sistem dan untuk saling menukar model secara mudah.
4. Dapat berguna sebagai *blue print*, sebab sangat lengkap dan detail dalam perancangannya yang nantinya akan diketahui informasi yang detail mengenai koding suatu program.
5. Dapat memodelkan sistem yang berkonsep berorientasi objek, jadi tidak hanya digunakan untuk memodelkan perangkat lunak *(software)* saja.
6. Dapat berguna untuk menciptakan suatu bahasa permodelan yang nantinya dapat dipergunakan oleh manusia maupun oleh mesin.

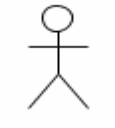
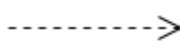
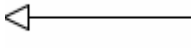
Sistem yang digunakan dalam perancangan berorientasi objek berbasiskan UML adalah sebagai berikut :

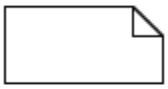
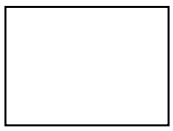
1. *Use Case Diagram*

Menurut Yunahar Heriyanto (2018) *Use Case Diagram* adalah sesuatu atau proses merepresentasikan hal-hal yang dapat dilakukan oleh aktor dalam menyelesaikan sebuah pekerjaan.*Diagram use case* merupakan pemodelan untuk kelakuan *(behavior)* sistem informasi yang akan dibuat.*Use case* merupakan sesuatu yang mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat. Secara kasar, *use*

case digunakan untuk mengetahui fungsi apa saja yang ada di dalam sebuah sistem dan siapa saja yang berhak menggunakan fungsi-fungsi tersebut..Berikut adalah simbol-simbol yang ada pada *diagram use case* :

Tabel 1.1 Simbol-Simbol *Use Case Diagram*

NO	Simbol	Deskripsi
1		Orang/Actor, proses himpuan peran yang pengguna mainkan ketika berinteraksi dengan *use case*.
2		Dependency, hubungan dimana perubahan yang terjadi pada suatu elemen mandiri *(independent)* akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri (*independent*).
3		Generalzation, hubungan dimana objek anak (*descendent*) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (*ancestor*).
4		Include, menspesifikasikan bahwa *use case* sumber secara *eksplisit*.
5		Extend, menspesifikasikan bahwa *use case* target, memperluas perilaku dari *use case* sumber pada suatu titik yang diberikan.

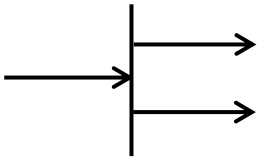
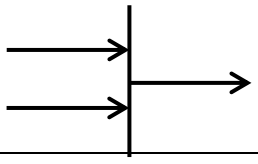
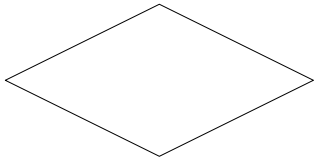
NO	Simbol	Deskripsi
6		Association, merupakan Apa yang menghubungkan antara objek satu dengan objek lainnya.
7		Collaboration, interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan prilaku yang lebih besar dari jumlah dan elemen-elemennya (sinergi).
8		*Use Case*, deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu aktor
9		*Note*, Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi
10		System, Menspesifikasikan paket yang menampilkan sistem secara terbatas.

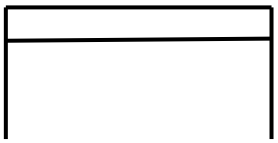
Sumber: Winda Aprianti (2016)

2. Diagram Aktifitas (*Activity Diagram*)

Activity diagram adalah "menggambarkan *workflow* (aliran kerja) atau dengan aktivitas dari sebuah sistem atau proses bisnis".Berikut simbol-simbol yang digunakan dalam *activity diagram* yaitu :

Tabel 2.4 Simbol *Activity Diagram*

Gambar	Keterangan
	*Start Point,* diletakkan pada pojok kiri atas dan merupakan awal aktivitas.
	*End Point,* akhir aktivitas
	*Activities,* menggambarkan suatu proses/kegiatan bisnis.
	*Fork/*percabangan digunakan untuk menunjukkan kegiatan yang dilakukan secara paralel atau untuk menggabungkan dua kegiatan paralel menjadi satu.
	*Join* (penggabungan) atau *rake,* digunakan untuk menunjukkan adanya dekomposisi.
	*Decision Points,* menggambarkan pilihan untuk pengambilan keputusan, *true* atau *false*.

	*Swimlane,* pembagian *activity diagram* untuk menunjukkan siapa melakukan apa

Sumber: Winda Aprianti (2016)

3. Diagram Kelas (*Class Diagram*)

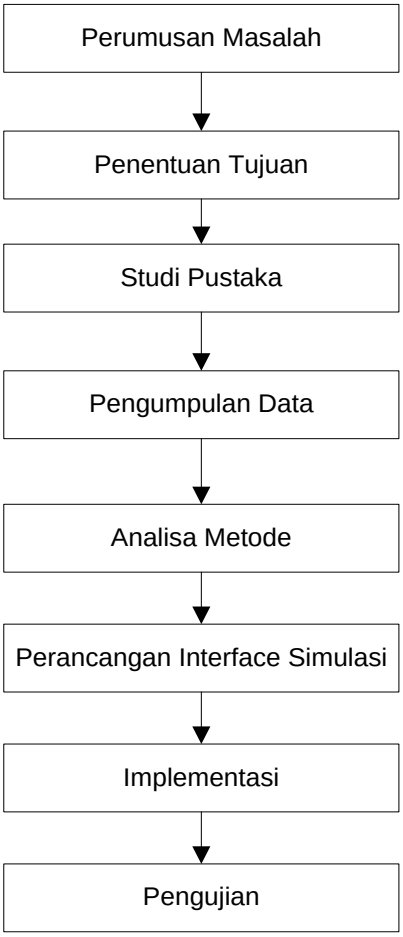
"Merupakan hubungan antar kelas dan penjelasan detail tiap-tiap kelas di dalam model desain dari suatu sistem, juga memperlihatkan aturan-aturan dan tanggung jawab entitas yang menentukan perilaku sistem. *Class Diagram,* juga menunjukkan sebuah kelas dan *constraint* yang berhubungan dengan objek yang dikoneksikan. *Class Diagram* secara khas meliputi : Kelas (*Class*), Relasi *Assosiations, Generalitation* dan *Aggregation,* attribut *(Attributes),* operasi *(operation/method)* dan *visibility,* tingkat akses objek eksternal kepada suatu operasi atau attribut. Hubungan antar kelas mempunyai keterangan yang disebut dengan *Multiplicity* atau *Cardinality"*.

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Adapun tahapan penelitian yang dilakukan oleh penulis ini dengan judul Pembuatan Aplikasi Penerapan *Enkripsi* Dan *Dekripsi File* Menggunakan Algoritma *Vigenere Cipher* adalah sebagai berikut:



Gambar 3.1 Tahapan Penelitian

3.2 Metode Pengumpulan Data

Pengumpulan data adalah pencarian terhadap susuatu kerena ada perhatian dan keinginan terhadap hasil suatu aktivitas. Metode pengumpulan data dalam penulisan ini dibagi menjadi 3, yaitu :

1. Pengamatan (*Observation*)

   Penulis melakukan pengamatan langsung pada setiap penggunan aplikasi chating yang sudah ada seperti WA,BBM dan Line untuk mengamati proses keamanan yang sudah dibuat sebelumnya.

2. Penelitian Kepustakaan (*Library Research*)

   Merupakan cara untuk mencari referensi dengan mengumpulkan bahan-bahan pustaka yang dilakukan di perpustakaan kampus, maupun perpustakaan umum, juga melakukan pencarian lewat internet, dengan mengunjungi situs-situs seperti *google Book online* yang dapat membantu pembahasan materi.

3.3 Analisis Sistem Sedang Berjalan

Visual basic 2010 akan menjadi sarana untuk menciptakan perangkat lunak ini. Pada analisa proses ini penggunaan digunakan sebagai metode yang didalamnya terdapat kombinasi dari algoritma *Vigenere Cipher*.Algoritma *Vigenere Cipher* digunakan oleh pengirim untuk mengenkripsi pesan yang akan dikirimkan.Perhitungan secara matematis dilakukan sebagai penggambaran proses yang akan terjadi pada metode ini yang didalamnya terdapat algoritma *Vigenere Cipher*. Berikut tahapannya :

1. Proses Enkripsi Pesan Asli oleh Pengirim

Tahap ini dilakukan dengan menggunakan Algoritma *Vigenere Cipher* yang akan digunakan untuk meng-*enkripsi* pesan asli (*plaintext)* pengirim.

Diketahui *Plaintex*t "PANCABUDI" dengan kunci "LENA".Maka untuk mendapatkan ciphertextnya harus menggunakan penghitungan seperti di bawah ini: Langkah pertama membuat tabel konversi *ASCII*.

Penerima memilih kata LENA sebagai kunci yang akan ia gunakan untuk melakukan proses enkripsi menggunakan *Algoritma Vigenere Cipher*, sehingga pada prosesnya kata PANCABUDI akan mengikuti banyak karakter ciphertext yang didapat.

Plaintext : PANCABUDI

Kunci : LENA

Selanjutnya akan di *enkripsi* dengan *Algoritma Vigenere Cipher* yaitu:

C = P + K mod 255

Dalam hal ini plaintext adalah ciphertext yang didapat.

C1 = P + L mod 255

= 80 + 76 mod 255

= 156

= œ

C2 = A + E mod 255

= 65 + 69 mod 255

= 134

= †

C3 = N + N mod 255

= 78 + 78 mod 255

= 156

= œ

C4 = C + A mod 255

= 67 + 65 mod 255

= 132

= „

C5 = A + L mod 255

= 65 + 76 mod 255

= 141

= spasi

C6 = B + E mod 255

= 66 + 69 mod 255

= 135

= ‡

C7 = U + N mod 255

= 85 + 78 mod 255

= 163

= £

C8 = D + A mod 255

= 68 + 65 mod 255

= 133

= …

C9 = I + L mod 255

= 73 + 76 mod 255

= 149

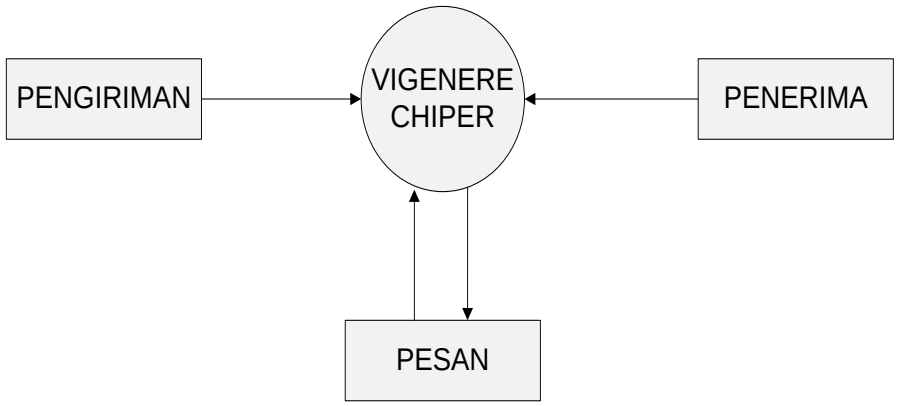
= •

Sehingga ciphertext kedua yang didapat adalah:

Ciphertext = œ † œ „ ‡ £ … •

3.4 Skema Pengiriman Pesan

Pertukaran data dalam hal ini pesan rahasia berbentuk teks dengan menggunakan metode tradisional yaitu dengan cara bertukar kata kunci tunggal. Diagram dibawah adalah penggambaran bagaimana pertukaran pesan rahasia menggunakan kunci tunggal terjadi. Pemberitahuan kata kunci dari pengirim ke penerima menggunakan media yang umum digunakan oleh banyak orang.



Gambar 3.2 Skema Pengiriman Pesan

3.5 Kelemahan – kelemahan proses sistem yang sedang berjalan

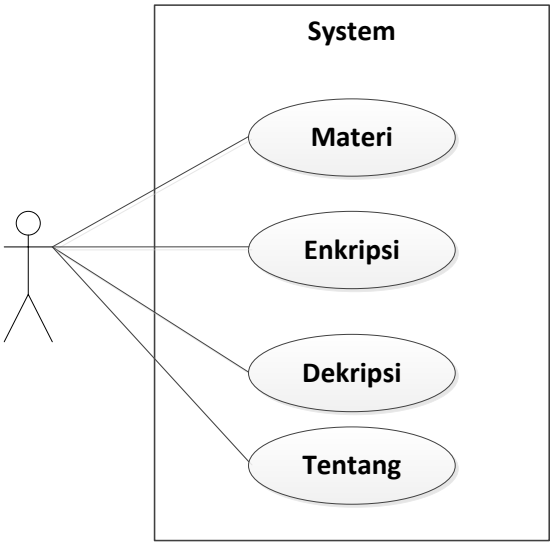
1. Penggunaan kata kunci tunggal berpotensi terjadinya salah pemahaman. Dalam hal ini kemungkinan penerima salah mengartikan kunci yang diberikan oleh pengirim adalah hal yang dapat terjadi.
2. Pemberitahuan atau pertukaran kata kunci yang dikirimkan oleh pengirim ke penerima memiliki potensi dapat diketahui oleh orang lain sehingga pesan rahasia dapat terbongkar.

3.6 Rancangan Penelitian

Perancangan merupakan proses mendapatkan informasi dari model dan menampilkannya secara grafik dengan menggunakan sebuah standar elemen grafik.Tujuan dari perancangan ini memungkinkan adanya komunikasi yang lebih berkualitas antara pengguna, pengembang penganalisis, tetster, manajer dan siapapun yang terlibat dalam proyek pengembangan sistem informasi.

1. Use Case Diagram

Berikut adalah *use case diagram* yang menggambarkan kegiatan.

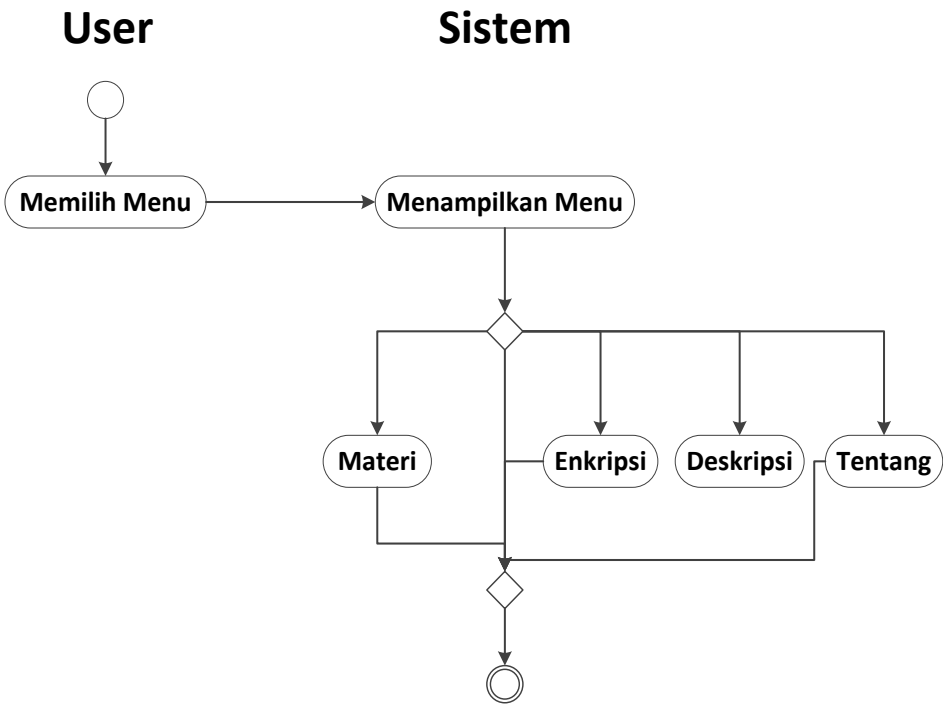


Gambar 3.3. *Use Case Diagram*

Keterangan : Dalam *use case* diagram di atas, *user/*pengguna sebagai *actor* yang mempunyai *use case* Materi, *Enkripsi*,*Dekripsi* dan Tentang.

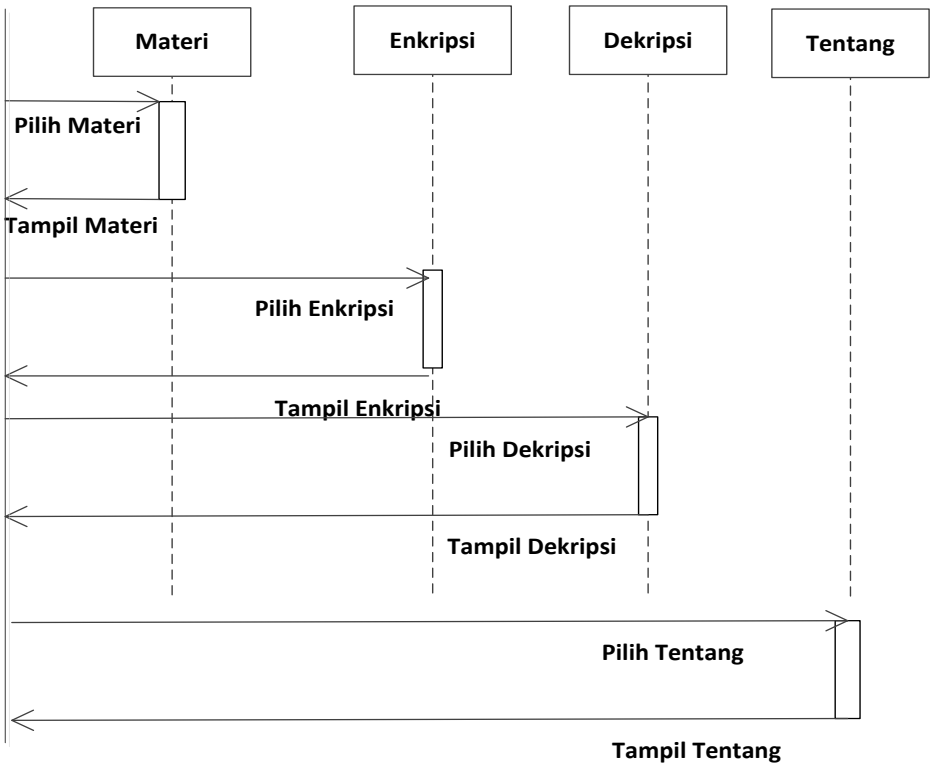
2. Activity Diagram

Activity diagram menggambarkan aktifitas-aktifitas yang terjadi dalam aplikasi dari aktivitas dimulai sampai aktivitas berhenti.



Gambar 3.4. *Activity Diagram*

3. Sequence Diagram



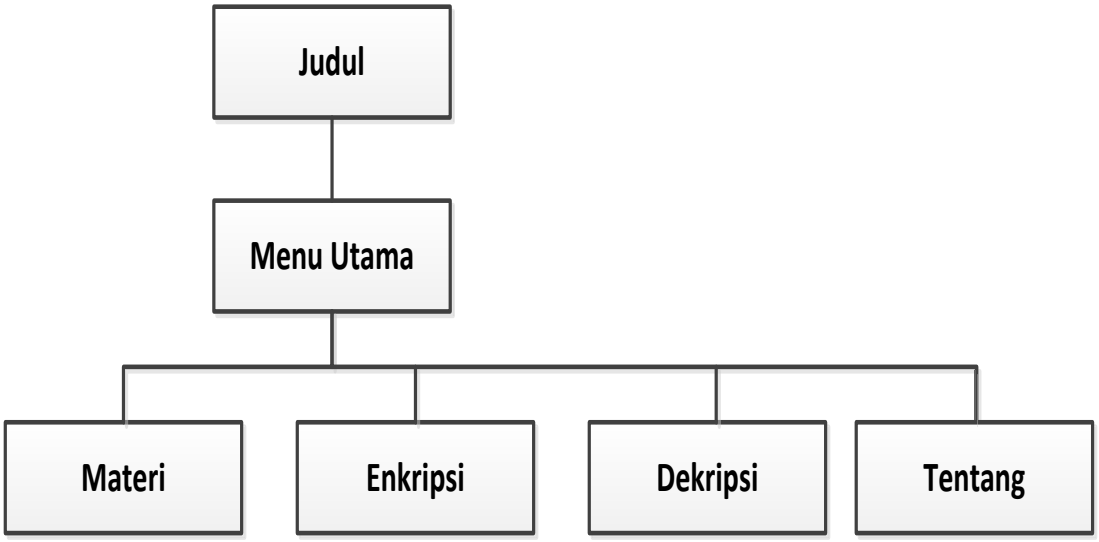
Gambar 3.5 *Sequence Diagram*

Keterangan Gambar :

1. Dalam *diagram* di atas menjelaskan bahwa *user* memilih materi kemudian Sistem menampilkan materi yang berkaitan dengan materi
2. *User* merequest *Enkripsi* kemudian Sistem menampilkan menu *Enkripsi*
3. *User* merequest *Dekripsi* kemudian Sistem menampilkan menu *Dekripsi*
4. *User* merequest *Menu* Tentang kemudian Sistem menampilkan *Form* Tentang.

3.7 Struktur Program

Struktur program mempresentasikan organisasi komponen program (modul) serta mengimplementasikann suatu hirarki kontrol. Hirearki kontrol tidak mengimplementasikan aspek prosedural dari perangkat lunak seperti urutan proses, kejadian atau urutan dari keputusan atau perulangan operasi.



Gambar 3.6 *Struktur Navigasi Enkripsi*

3.7 Rancangan Tampilan

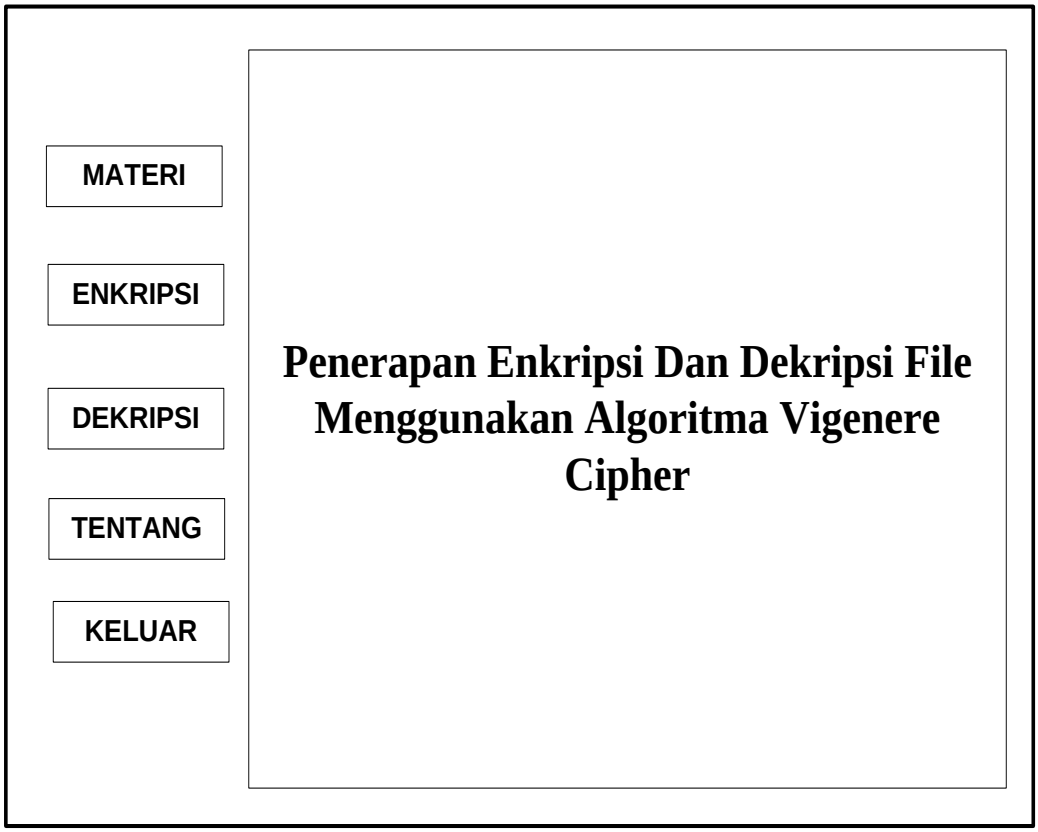
1. Rancangan Halaman Judul

Halaman judul merupakan halaman yang pertama muncul pada saat program dijalankan Pada rancangan di atas akan menampilkan judul yang kemudian akan pindah ke *form* menu utama dengan menggunakan timer.

Gambar 3.7 Rancangan Halaman Judul

2. Rancangan Halaman Menu Utama

Form ini berisi tombol-tombol seperti menu Materi, *Enkripsi*, *Deskips*i, tentang, dan Keluar.



Gambar 3.8 Rancangan Halaman Menu Utama

Pada tampilan di atas terdapat 5 tombol yaitu Materi, Enkripsi, Dekripsi, Tentang dan keluar.

a. Tombol Materi berfungsi untuk menghubungkan pengguna ke form materi.

b. Tombol *Enkripsi* berfungsi untuk menghubungkan pengguna ke *form Enkripsi*.

c. Tombol *Dekripsi* berfungsi untuk menampilkan form *Dekripsi*.

d. Tombol Tentang berfungsi untuk menghubungkan pengguna ke *form* tentang.

e. Tombol Keluar berfungsi untuk keluar dari program.

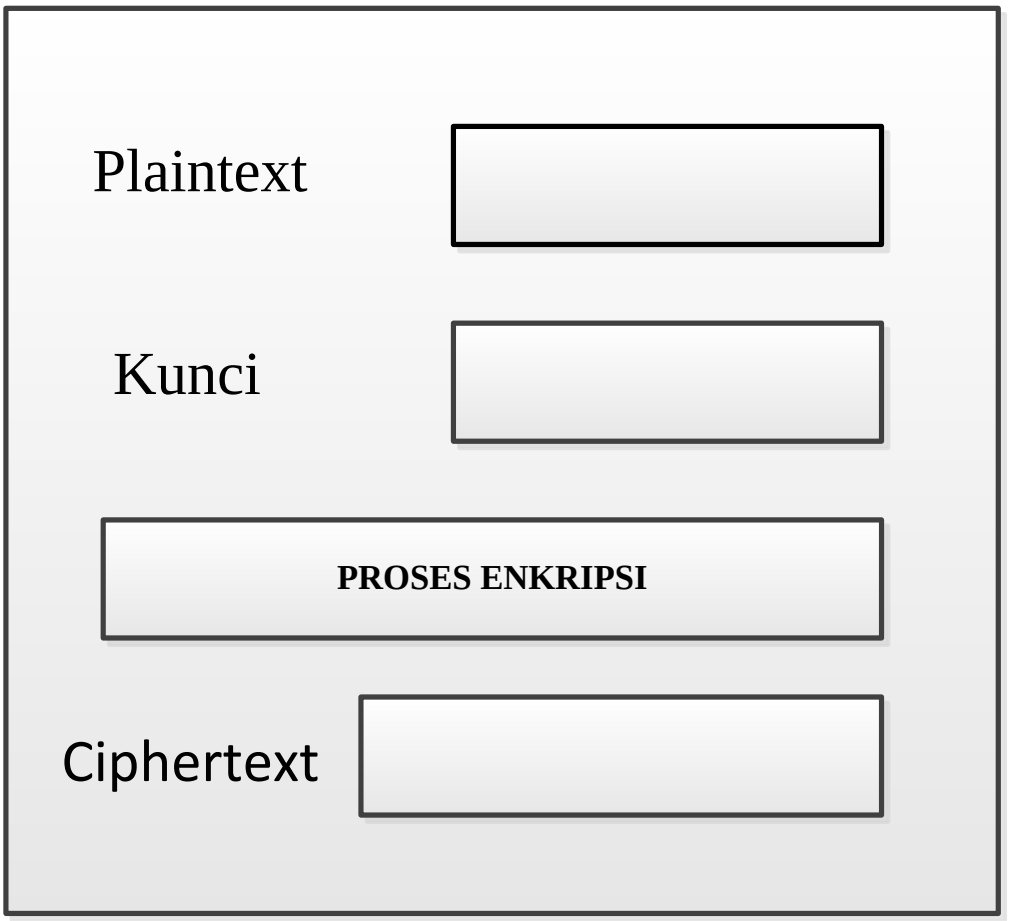
3. Rancangan Halaman Materi

Form ini digunakan untuk menjelaskan cara kerja penyandian, dimulai dari plaintext kemudian kunci yang dikonversikan dalam bentuk angka. Setelah itu dilakukan proses penjumlahan dan jika hasil penjumlahan maka akan dikurangi 6 lalu hasilnya akan dikembalikan lagi ke dalam bentuk huruf.

Gambar 3.9 Rancangan Halaman Materi

4. Rancangan Halaman Enkripsi

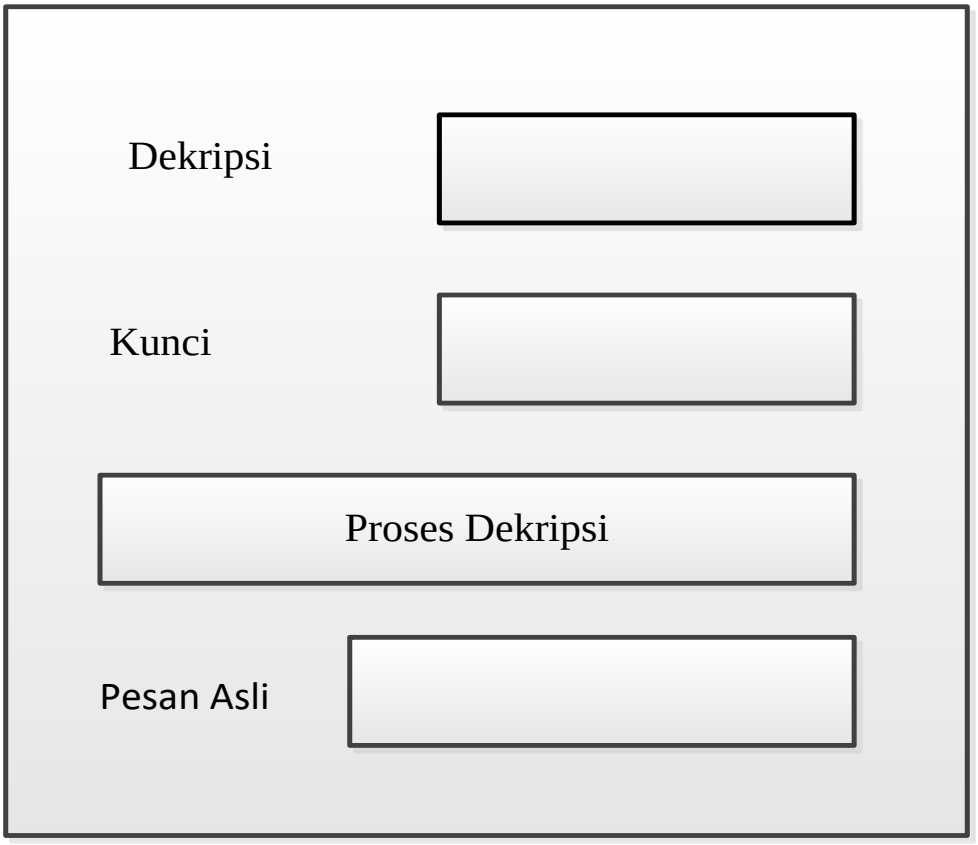
Berisi penjelasan mengenai Enkripsi. Pengguna memasukkan tulisan asli atau *plaintext* ke dalam tombol masukan *plaintext* kemudian dimasukkan juga kunci. Setelah itu, ditekan tombol Proses *Enkripsi* yang kemudian akan menampilkan ciphertext atau tulisan yang telah disandikan.



Gambar 3.10 Rancangan Halaman *Enkripsi*

5. Rancangan Halaman Dekripsi

Berisi penjelasan mengenai dekripsi. Pengguna memasukkan tulisan asli atau *plaintext* ke dalam tombol masukan *plaintext* kemudian dimasukkan juga kunci. Setelah itu, ditekan tombol Proses deskrisi yang kemudian akan menampilkan ciphertext atau tulisan yang telah disandikan.



Gambar 3.11 Rancangan Halaman *Dekripsi*

Pada gambar di atas terdapat kotak input Dekripsi berfungsi untuk memasukkan tulisan yang telah disandikan.Kemudian terdapat tombol Proses Dekripsi untuk mengembalikan ke pesan asli jika kunci yang dimasukkan sama dengan kunci pada saat penggunaan *plaintext.*

BAB IV

HASIL DAN PEMBAHASAN

4.1 Implementasi Sistem

4.1.1 Spesifikasi Sistem

Analisis kebutuhan sistem merupakan analisis yang dibutuhkan untuk menentukan spesifikasi kebutuhan sistem.Spesifikasi merupakan elemen atau komponen-komponen apa saja yang dibutuhkan untuk sistem yang akan dibangun sampai dengan sistem tersebut diimplementasikan.Analisis kebutuhan ini juga menentukan spesifikasi masukkan yan diperlukan sistem, keluaran yang akan dihasilkan sistem dan proses yang dibutuhkan untuk mengolah masukkan sehingga menghasilkan suatu keluaran yang diinginkan.

1. Analisis Perangkat Keras (Hardware)

Perangkat keras minimum yang digunakan untuk membangun Sistem Informasi Penjualan ini adalah

a. Processor Berkecepatan 3.0 Ghz

b. RAM 4 Gb

c. Hardisk minimal 10 Gb untuk menyimpan data

d. LAN Card

e. Keyboard dan Mouse

f. Monitor 20 inch.

2. Analisis Perangkat Lunak (Software)

Untuk mendukung dalam penyimpanan informasi, dibutuhkan suatu fasilitas yang memadai. Yaitu berupa perangkat lunak (software) yang dirancang untuk memudahkan dalam pembangunan dan menjalankan sisten nantinya. Adapun perangkat lunak yang digunakan adalah sebagai berikut :

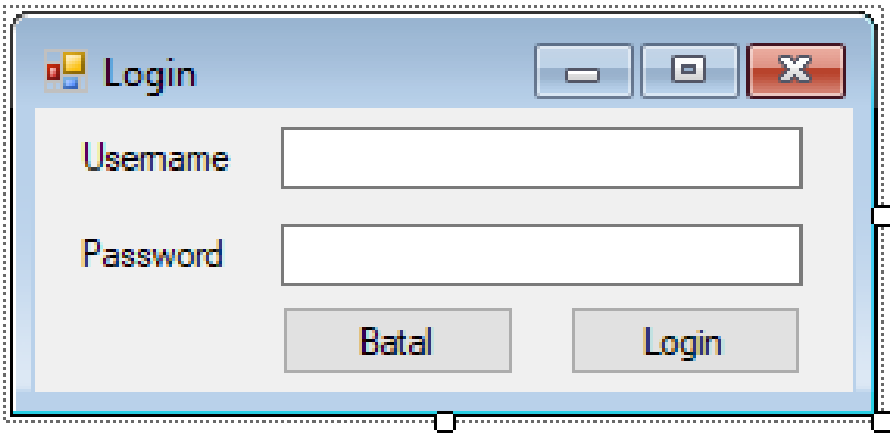
a. Microsoft Windows 10 , Windows 10 sebagai sistem operasi

b. Visual Studio 2010, Sebagai Perancangan Program Aplikasi.

4.1.2 Hasil Rancangan Sistem

1. Tampilan Menu *Login*

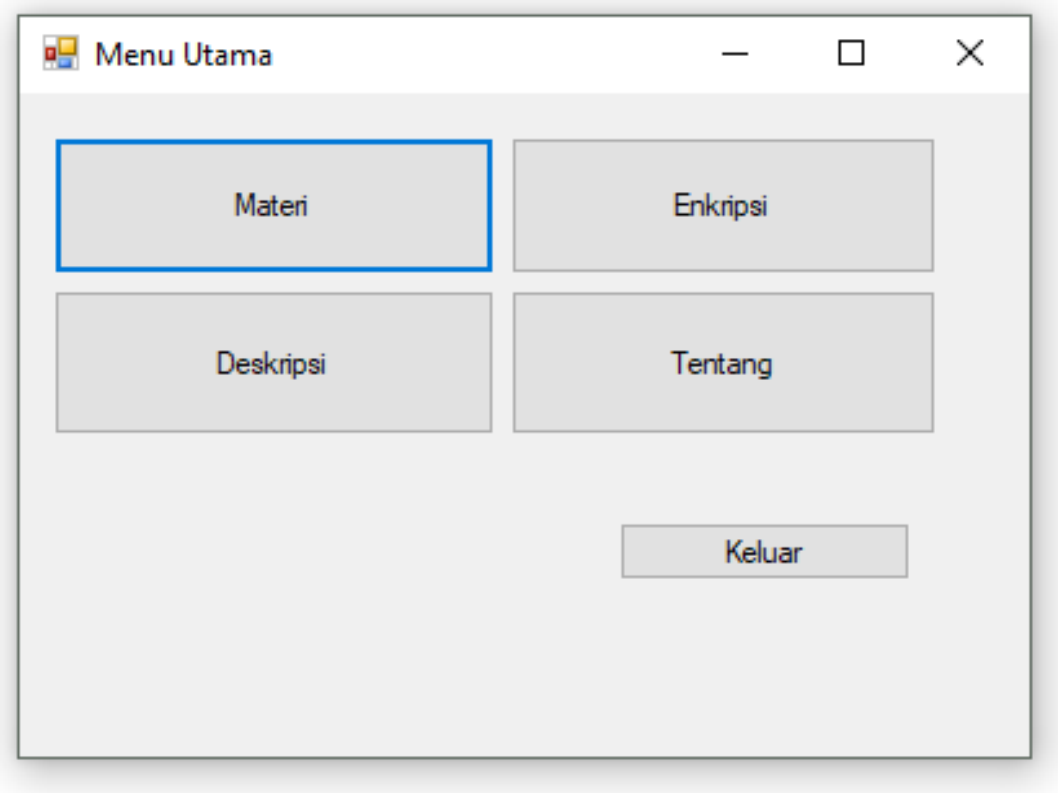
Rancangan Tampilan *Login* adalah tampilan awal sebelum masuk ke aplikasi. Halaman ini berfungsi untuk memberikan hak akses bagi seorang user sebelum menggunakan aplikasi. Adapun fungsi dari tombol yang ada pada menu *Login* yaitu Tombol *Login* berfungsi untuk memverifikasi data valid untuk melanjutkan ke menu selanjutnya.Berikut tampilan Menu *Login* dapat dilihat pada gambar dibawah ini :



Gambar 4.1 Tampilan Menu *Login*

2. Tampilan Menu Utama

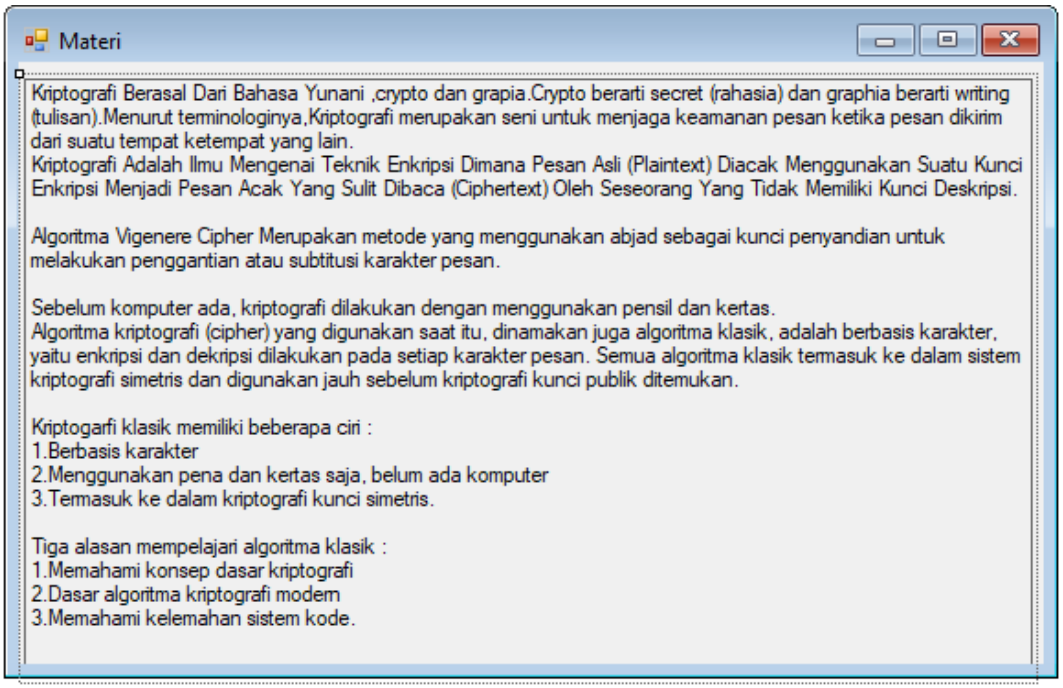
Tampilan Menu Utama merupakan tampilan yang pertama muncul saat program dijalankan. Di dalam menu utama terdapat menu seperti Materi, *Enkripsi*, *Deskripsi* dan Tentang:



Gambar 4.2 Tampilan Menu Utama

3. Tampilan Materi

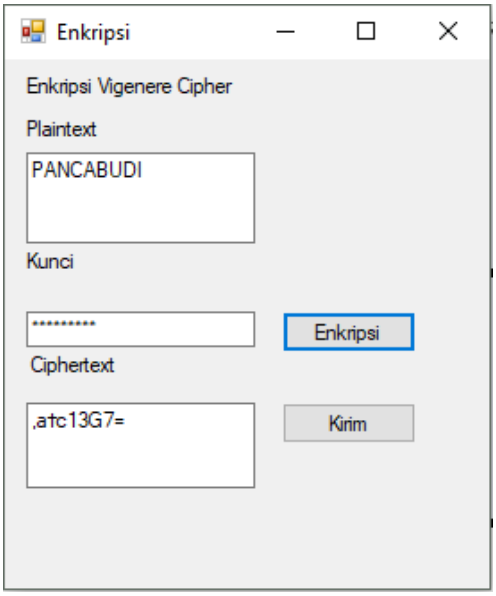
Tampilan Materi terdapat sub menu yaitu sejarah singkat dari kriptografi.



Gambar 4.3 Tampilan Materi

4. Tampilan Menu Enkripsi

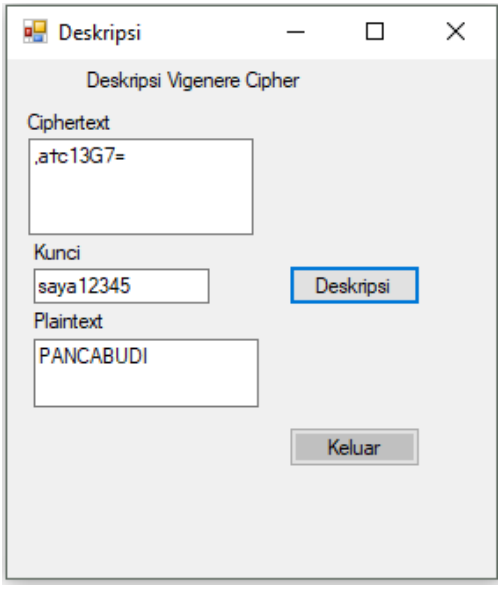
Tampilan enkripsi berfungsi untuk menggantikan tulisan asli menjadi tulisan yang disandikan dengan menggunakan algoritma Vigenere Cipher. Untuk mengkonversikan tulisan tersebut, dibutuhkan kunci agar ciphertext tidak mudah untuk dibuka:



Gambar 4.4 Tampilan Menu Enkripsi

5. Tampilan Menu Deskripsi

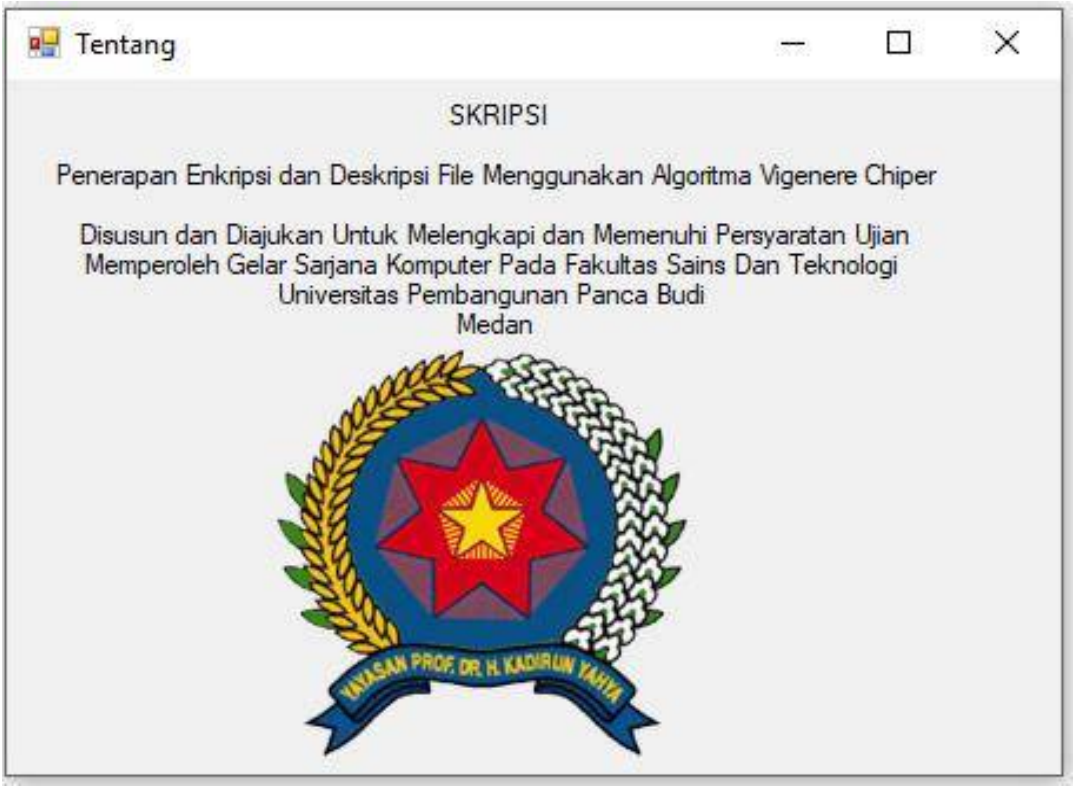
Tampilan Deskripsi menampilkan tulisan dikembalikan ke dalam bentuk semula menggunakan kunci.:



Gambar 4.5 Tampilan Data Alternatif

6. Tampilan Menu Tentang

Tampilan Tentang menampilkan tentang versi program serta profil pembuat program:



Gambar 4.6 Tampilan Menu Tentang

4.2 Pengujian Black Box

Untuk dapat menggunakan aplikasi ini dengan baik, dibutuhkan seperangkat komputer dengan spesifikasi minimal.Black Box pengujian merupakan metode pengujian perangkat lunak yang menguji fungsionalitas aplikasi yang bertentangan dengan struktur internal atau kerja.Metode uji ini dapat diterapkan pada semua tingkat pengujian perangkat lunak : unit, integrasi, fungsional, sistem dan penerimaan.

Tabel 4.1. Tabel Pengujian Black Box

No	Rancangan Proses	Hasil Yang Diharapkan	Hasil	Keterangan
1	Menu Utama Interaktif dan Mudah Digunakan	Halaman Index (Awal)	Sesuai	-
2	Proses Data Enkripsi	Halaman Enkripsi	Sesuai	-
3	Proses Data Deskripsi	Halaman Deskripsi	Sesuai	-
4	Menu Tentang	Halaman Tentang	Sesuai	-

4.3 Kelebihan dan Kekurangan Sistem

Adapun kelebihan dan kekurangan dari aplikasi *vigenere chiper* ini adalah sebagai berikut:

a. Kelebihan Sistem

1. Dapat mengenkripsi tulisan dengan algoritma *Vigenere Cipher* dengan cepat
2. Menghindari dari kesalahan saat mengenkripsi tulisan

b. Kekurangan Sistem

1. Tidak dapat dijalankan dalam jaringan pada computer.
2. Tidak dapat menampilkan enkripsi dengan algoritma selain *Vigenere Cipher.*

BAB V
PENUTUP

5.1 Simpulan

Berdasarkan pembahasan dalam Penerapan Kriptografi *Vigenere Chiper*, maka dapat diambil kesimpulan sebagai berikut :

1. Perangkat lunak ini dirancang untuk menampilkan simulasi pengamanan aplikasi menggunakan kriptografi.
2. Penggunaan Algoritma *Vigenere* memiliki manfaat bagi pengguna aplikasi.
3. Pengamanan aplikasi menggunkan kriptografi dengan algoritma *vigenere chiper* ini sangat berguna dikarenakan proses enkripsi dan deskripsinya sulit untuk ditebak dan di bobol.

5.2 Saran

Adapun saran-saran yang dapat dilakukan penelitian ataupun pengembangan selanjutnya adalah sebagai berikut:

1. Perangkat lunak ini dapat dikembangkan dengan menggunakan kombinasi metode-metode lain.
2. Perangkat lunak ini dapat dikembangkan dan terhubung ke jaringan sehingga dapat dijalankan di lebih dari satu komputer.
3. Perangkat lunak ini dapat dikembangkan menggunakan algoritma-algoritma lain yang lebih kompleks.

DAFTAR PUSTAKA

Andrian, Yudhi, and Purwa Hasan Putra. "Analisis Penambahan Momentum Pada Proses Prediksi Curah Hujan Kota Medan Menggunakan Metode Backpropagation Neural Network." Seminar Nasional Informatika (SNIf). Vol. 1. No. 1. 2017.

Aryza, S., Irwanto, M., Lubis, Z., Siahaan, A. P. U., Rahim, R., & Furqan, M. (2018). A Novelty Design Of Minimization Of Electrical Losses In A Vector Controlled Induction Machine Drive. In IOP Conference Series: Materials Science and Engineering (Vol. 300, No. 1, p. 012067). IOP Publishing.

Dalam Pengamanan Pesan Teks. Jurnal Riset Komputer (JURIKOM). Volume :

Fachri, Barany. Aplikasi Perbaikan Citra Efek Noise Salt & Papper Menggunakan Metode Contraharmonic Mean Filter. In: Seminar Nasional Royal (Senar). 2018. P. 87-92.

Fresly Nandar Pabokory, Indah Fitri Astuti & Awang Harsa Kridalaksana.(2015).Implementasi Kriptografi Pengamanan Data Pada Pesan Teks,Isi File Dokumen,Dan File Dokumen Menggunakan Algoritma AES. Jurnal Informatika Mulawarman. Vol. 10 No. 1.22-23.

Ginting, G., Fadlina, M., Siahaan, A. P. U., & Rahim, R. (2017). Technical approach of TOPSIS in decision making. Int. J. Recent Trends Eng. Res, 3(8), 58-64.

Hafid Rosianto.(2017).Implementasi Algoritma Des Berbasis Blowfish Untuk Enkripsi Dan Dekripsi Data. Jurnal Teknik Elektro.Volume 06 Nomor 02.121-128.

Hafni, Layla, And Rismawati Rismawati. "Analisis Faktor-Faktor Internal Yang Mempengaruhi Nilai Perusahaan Pada Perusahaan Manufaktur Yang Terdaftar Di Bei 2011-2015." Bilancia: Jurnal Ilmiah Akuntansi 1.3 (2017): 371-382.

Hamdi, Muhammad Nurul, Evi Nurjanah, And Latifah Safitri Handayani. "Community Development Based Onibnu Khaldun Thought, Sebuah Interpretasi Program Pemberdayaan Umkm Di Bank Zakat El-Zawa." El Muhasaba: Jurnal Akuntansi (E-Journal) 5.2 (2014): 158-180.

https://docobook.com/instruksi-bahasa-pemrograman-yang.html
https://ejournal.istn.ac.id/rekayasainformasi/article/view/17/15
https://fmipa.unmul.ac.id/files/docs/20-31%20Jurnal%20Fresly.pdf
https://www.academia.edu/21896432/Jurnal_Enkripsi_Dekripsi_Blowfish
https://www.academia.edu/35598877/PB_caesar_cipher_

Indra Permana, Aminuddin "Sistem Pakar Mendeteksi Hama Dan Penyakit Tanaman Kelapa Sawit Pada Pt. Moeis Kebun Sipare-Pare Kabupaten Batubara." (2013).

Jurnal Media Infotama, Vol.9, No.2.65.

Jusuf Wahyudi.(2013).Instruksi Bahasa Pemrograman ADT Pada virus Dan Loop Batch.

Mayasari, Nova. "Comparison of Support Vector Machine and Decision Tree in Predicting On-Time Graduation (Case Study: Universitas Pembangunan Panca Budi)." Int. J. Recent Trends Eng. Res 2.12 (2016): 140-151.

Mohamad Natsir.(2017). Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java. Jurnal Format Volume 6 Nomor 1.95. http://publikasi.mercubuana.ac.id/index.php/format/article/download/1532/1209

Ninuk Wiliani & Syadid Zambi.(2017).Rancang Bangun Aplikasi Kasir Tiket Nonton Bola Bareng Pada X Dengan Visual Basic 2010 Dan Mysql.Jurnal Rekayasa Informasi, Vol. 6. No.2,78.

Permana, A. I., and Z. Tulus. "Combination of One Time Pad Cryptography Algorithm with Generate Random Keys and Vigenere Cipher with EM2B KEY." (2020).

Permana, Aminuddin Indra. "Kombinasi Algoritma Kriptografi One Time Pad dengan Generate Random Keys dan Vigenere Cipher dengan Kunci EM2B." (2019).

Priyono.(2016). Penerapan Algoritma Caesar Cipher Dan Algoritma Vigenere Cipher

Puspita, Khairani, and Purwa Hasan Putra. "Penerapan Metode Simple Additive Weighting (SAW) Dalam Menentukan Pendirian Lokasi Gramedia Di Sumatera Utara." Seminar Nasional Teknologi Informasi Dan Multimedia, ISSN. 2015.

Putera, A., Siahaan, U., & Rahim, R. (2016). Dynamic key matrix of hill cipher using genetic algorithm. Int. J. Secur. Its Appl, 10(8), 173-180.

Rizal, Chairul. "Pengaruh Varietas dan Pupuk Petroganik Terhadap Pertumbuhan, Produksi dan Viabilitas Benih Jagung (Zea mays L.)." ETD Unsyiah (2013).

Syahputra, Rizki, And Hafni Hafni. "Analisis Kinerja Jaringan Switching Clos Tanpa Buffer." Journal Of Science And Social Research 1.2 (2018): 109-115.

Wahyuni, Sri. "Implementasi Rapidminer Dalam Menganalisa Data Mahasiswa Drop Out." Jurnal Abdi Ilmu 10.2 (2018): 1899-1902.

Yunahar Heriyanto.(2018).Perancangan sistem informasi rental mobil berbasis web pad apt.apm rent car. Jurnal Intra-Tech. Volume 2, No.2 Oktober 2018.67-68. https://www.researchgate.net/publication/315963831_Pembuatan_Sistem_Informasi_Rental_Mobil_dengan_Menggunakan_Java_dan_Mysql