APLIKASI ENKRIPSI DAN DEKRIPSI PLANTEXT BERBASIS DEKSTOP DENGAN MENGGUNAKAN METODE ZIG ZAG 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	:	**MUHAMMAD NUGROHO**
NPM	:	**1514370156**
PROGRAM STUDI	:	**SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

ABSTRAK

MUHAMMAD NUGROHO
Aplikasi Enkripsi dan Dekripsi Plantext Berbasis Dekstop dengan Menggunakan Metode Zig Zag Cipher
2019

Keamanan data merupakan aspek yang sangat penting dalam berkomunikasi dengan menggunakan perangkat komunikasi seperti komputer, smartphone, dan lain lain. Kerahasiaan data harus terjaga dari pihak yang tidak berwenang karena banyak sekali terjadi penyadaan melalui handphone maupun komputer sehingga informasi yang ingin disampaikan ke penerima tersadap oleh pihak yang tidak berwenang, agar data atau informasi aman dari penyadap maka menggunakan kriptografi. Kriptografi adalah ilmu yang dengan kerahasiaan informasi data, pada sistem ini menggunakan kriptografi dengan menggunakan metode zig zag cipher untuk mengamankan planteks. Ini bertujuan untuk menjaga privasi pengguna agar lebih aman dan juga melindungi planteks serta memberi rasa aman kepada pengguna. Hasil dari penelitian ini adalah pada saat enkripsi semua karakter bisa dimasukan termasuk itu spasi. Penggunaan pada saat mengenkripsi tidak ada batasan untuk panjang planteks. Kesimpulannya adalah aplikasi ini dibuat dengan sederhana agar mudah digunakan untuk pengguna menggunakannya, dan aplikasi ini dapat melindungi planteks yang ingin dikirim ke penerima.

Kata Kunci: keamanan, komunikasi, kriptografi, *Zig Zag Cipher*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT, yang telah memberikan rahmat hidayah dan karunia-Nya sehingga penulis masih diberikan kesehatan sehingga akhirnya dapat menyelesaikan skripsi ini dengan baik

Skripsi disusun berdasarkan hasil penelitian yang sudah dilakukan dengan judul: "**Aplikasi Enkripsi dan Dekripsi Plantext Berbasis Dekstop dengan Menggunakan Metode Zig Zag Cipher**".

Dalam kesampatan ini penulis mengucapkan banyak terima kasih yang sebesar besarnya kepada banyak pihak yang telah membantu penulisa dalam penyelesaian penyusunan skripsi ini.

Penulis ingin mengucapkan terima kasih kepada :

1. Orang tua saya yang telah mendoakan saya dan mensuport saya.
2. Bapak Dr. Isa Indrawan, S.E., M.M., selaku Rektor Universitas Pembangunan Panca Budi Medan.
3. Bapak Ir. Bhakti Alamsyah, M.T., Ph.D. selaku Rektor I Universitas Pembangunan Panca Budi Medan.
4. Bapak Hamdani, S.T., M.T., selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
5. Bapak Eko Hariyanto, S.Kom, M.Kom.. selaku Ketua Program Studi Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
6. Bapak Andysah Putera Utama Siahaan, S.Kom., M.Kom., selaku Dosen Pembimbing I atas bimbingan saran dan pengarahannya sehingga penulisan skripsi ini dapat diselesaikan.
7. Bapak Dian Kurnia, S.Kom., M.Kom., Selaku Dosen Pebimbing II atas bimbingan saran dan pengarahannya sehingga penulisan skripsi ini dapat diselesaikan.
8. Teman-teman yang sudah memberikan motivasi untuk kelancaran skripsi ini.

Penulis mengucapkan terima kasih secara tulus dan ikhlas dan juga penulis juga menyadari bahwa penyusunan skripsi ini Belum sempurna baik dalam penulisan maupun isi, hal ini dikarenakan keterbatasan kemampuan penulis. Oleh karena itu, penulis megharapkan kritik dan saran yang sifatnya membangun dari pembaca agar di jadikan pembelajaran sebagai penyempurna skripsi ini.

Medan, 03 Februari 2020
Penulis

Muhammad Nugroho
151437015

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan Data merupakan aspek yang sangat penting dalam berkomunikasi dengan menggunakan perangkat komunikasi seperti komputer, telpon seluler, smartphone, dan lain lain. kerahasiaan data atau informasi harus terjaga dari pihak yang tidak berwenang hingga data atau informasi tersebut terkirim kepada penerima yang semestinya, alat komunikasi yang banyak digunakan adalah smartphone, apalagi jika pengirimannya dilakukan menggunakan jaringan publik itu membuat data yang kita kirim sangat mudah untuk disadap dan diketahui oleh orang lain. Salah satu cara untuk mengamankan data yakni menggunakan sistem kriptografi

Kriptografi adalah ilmu yang berdasarkan teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan autentikasi entitas. Ada empat tujuan utama dari kriptografi. Kerahasiaan (*confidentiality*) di mana kriptografi digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah disandi. Kerahasiaan dijaga dengan melakukan enkripsi (penyandian). Keutuhan (*integrity*) yang 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. Otentikasi (*authentication*) adalah kemampuan penerima pesan

untuk memastikan pesan tersebut asli. Seorang penyusup seharusnya tidak bisa menyamar sebagai orang lain. Anti penyangkalan (*non-repudiation*) adalah dimana pengirim pesan tidak bisa menyangkal bahwa dia telah mengirim pesan Secara umum tujuan dari kriptografi adalah mengolah informasi dengan algoritma tertentu supaya pesan tidak dapat dibaca. Proses yang dilakukan untuk mengamankan sebuah pesan (*plaintext*) menjadi pesan yang tersembunyi (*ciphertext*) disebut dengan enkripsi (*encryption*).

Pada proses enkripsi dan dekripsi memerlukan kunci, pada sistem ini kriptografi dibagi menjadi dua macam, yaitu kriptografi simetri dan kriptografi asimetri. Antara kedua sistem kriptografi ini ada perbedaannya yakni dalam segi kunci yang digunakan untuk mengenkripsi dan mendekrispsikan pesan. Pada sistem kriptografi simetri kunci yang digunakan untuk enkripsi dan dekripsi pesan itu sama. Dan untuk sistem kriptografi asimetri menggunakan kunci yang berbeda pada saat mengenkripsi dan mendekripsinya. Pada sistem kriptografi simetri mempunyai kelemahan pada kunci, yakni pengirim dan penerima harus menjaga kerahasiaan kuncinya agar tidak ada yang mengetahuinya. Dan untuk sistem kriptografi asimetri kunci pada saat enkripsi tidak perlu dijaga kerahasiaannya karena berupa kunci publik, dan untuk kunci dekripsi yang harus dijaga kerahasiaannya dari orang lain, yang boleh mengetahuinya hanya penerimanya saja.

Berdasarkan kejadian yang sering terjadi tersebut, maka dibutuhkan suatu aplikasi pengamanan isi pesan yang akan dikirim. Pengamanan pada pesan ini dilakukan dengan cara menyamarkan isi yang ada didalam pesan tersebut dengan

menggunakan algoritma kriptografi supaya yang dapat membaca pesan tersebut hanya orang yang berhak saja. Metode yang digunakan disini adalah zig zag *cipher* dari algoritma kriptografi, sistem ini menggunakan kunci simtetris. Metode Zig Zag *Cipher* merupakan salah satu algoritma kriptografi klasik dengan teknik transposisi. Teknik transposisi menggunakan permutasi karakter, yang mana dengan menggunakan teknik ini pesan yang asli tidak dapat dibaca kecuali orang yang memiliki kunci untuk menggembalikan pesan tersebut ke bentuk semula.

1.2 Rumusan Masalah

Adapun rumusan masalah dalam skripsi ini adalah sebagai berikut:

1. Bagaimana membuat aplikasi enkripsi dan dekripsi Planteks berbasis dekstop dengan metode zigzag *cipher*?
2. Bagaimana cara menjalankan aplikasi enkripsi dan dekripsi Planteks berbasis dekstop dengan metode zigzag *cipher*?

1.3 Batasan Masalah

Adapun batasan masalah didalam skripsi ini adalah

1. Aplikasi ini hanya ditujukan untuk komputer bersistem operasi windows.
2. Metode kriptografi yang digunakan adalah Zig Zag Cipher.
3. Hanya karakter yang bisa di inputkan diaplikasi ini.

1.4 Tujuan Penelitian

Adapun tujuan penelitian ini adalah.

1. Membuat aplikasi pengamanan data pada planteks dengan metode zig zag *cipher*.
2. Untuk menjaga perivasi pengguna agar lebih aman.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah.

1. Pesan yang dikirim hanya bisa dibaca oleh orang yang barhak saja.
2. Melindingi data dan memberikan rasa aman kepada pengguna dalam mengirim pesan.

BAB II

LANDASAN TEORI

2.1 Keamanan Data

Menurut Stiawan masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu informasi. Secara umum keamanan komputer mencakup beberapa aspek (Nugroho, 2016), yaitu :

1. *Privacy / Confidentiality Privacy* lebih kearah data - data yang sifatnya rahasia, sedangkan confidentiality berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu.
2. *Integrity* Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seizin pemilik informasi. Informasi yang diterima harus sesuai dan sama persis seperti saat informasi dikirimkan. Jika terdapat perbedaan antara informasi atau data yang dikirim dengan yang diterima maka aspek integrity tidak tercapai.
3. *Authenticity* Aspek ini berhubungan dengan metode atau cara untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betulbetul orang yang dimaksud.
4. *Availability* Aspek ini behubungan dengan ketersediaan data dan informasi. Data dan informasi yang berbeda dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak.

5. *Access* Control Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data, mekanisme authentication dan juga privacy. Access control seringkali dilakukan dengan menggunakan kombinasi user id/password atau dengan menggunakan mekanisme lain.

2.2 Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani: ”*cryptos*” artinya ”*secret*” (rahasia), sedangkan ”graphein” artinya ”writing” (tulisan), Jadi, kriptografi berarti ”*secret writing*” (tulisan rahasia). Menurut Rinaldi Munir (2006) Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi sepertikerahasiaan, integritas data, serta otentikasi (Easttom, 2015; Hasugian, 2017).

Pengertian Kriptografi dalam kamus bahasa Inggris Oxford adalah sebagai berikut : “ Sebuah teknik rahasia dalam penulisan, dengan karakter khusus, dengan mengguanakan huruf dan karakter di luar bentuk aslinya, atau dengan metode-metode lain yang hanya dapat dipahami oleh pihak-pihak yang memproses kunci, juga semua hal yang ditulis dengan cara seperti ini.” Jadi, secara umun kriptografi diartikan sebagai seni menulis atau memecahkan cipher (Zelviana, Efendi, & Dedy, 2012).

Definisi yang digunakan di dalam buku menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.

Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata . Namun saat ini kriptografi lebih dari sekadar *privacy*, tetapi juga untuk tujuan data *integrity*, *authentication*, dan *non-repudation*. Dalam melakukan pengamanan dengan ilmu kriptografi adapun komponen pendukung system kriptografi:

1. Pesan (*message*) adalah data atau informasi yang dapat dibaca atau dimengerti maknanya. Nama lainnya untuk pesan adalah plainteks (*plaintext*) atau teks jelas (*clear text*).
2. Pengirim (*sender*) adalah entitas yang melakukan pengiriman pesan kepada entitas lainnya.
3. Kunci (*cipher*)/*Secret Key* adalah aturan atau fungsi matematika yang digunakan untuk melakukan proses enkripsi dan dekripsi pada plaintext dan ciphertext.
4. *Ciphertext* adalah keluaran algoritma enkripsi. *Cipehertext* dapat dianggap sebagai pesan dalam bentuk tersembunyi. Algoritma enkripsi yang baik akan menghasilkan *ciphertext* yang terlihat teracak. Untuk selanjutnya digunakan istilah teks sandi sebagai padana kata ciphertext.
5. Enkripsi adalah mekanisme yang dilakukan untuk merubah plaintext menjadi *ciphertext*.
6. Dekripsi adalah mekanisme yang dilakukan untuk merubah ciphertext menjadi *plaintext.*

7. Penerima (*receiver*) adalah entitas yang menerima pesan dari pengirim/entitas yang berhak atas pesan yang dikirim

2.2.1 Tujuan Kriptografi

Tujuan dari kriptografi adalah untuk tidak menyembunyikan keberadaan pesan , melainkan untuk menyembunyikan maknanya (Hondro, 2015).

Aspek keamanan yang diberikan kriptografi selain menyandikan pesan juga menyediakan beberapa aspek keamanan. Berikut aspek keamanan kriptografi:

1. Kerahasiaan (*confidentiality*), adalah layanan yang digunakan untuk menjaga isi pesan dari siapapun yang tidak berhak membacanya. Layanan ini direalisasikan dengan cara menyandikan pesan menjadi bentuk yang tidak dapat dimengerti. Misalnya pesan “Harap datang pukul 8” disandikan menjadi “TrxC#45motypetre!%”.
2. Integritas data (*data integrity*), adalah layanan yang menjamin bahwa pesan masih asli / utuh atau belum pernah dimanipulasi selama pengiriman. Layanan ini direalisasikan dengan menggunakan tanda-tanda digital (digital signature). Pesan yang telah ditandatangani menyiratkan bahwa pesan yang dikirim adalah asli.
3. Otentifikasi (*authenification*), adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentification atau entity authentification*) maupun

mengidentifikasi kebenaran sumber pesan (*data origin authentification*). Layanan ini direalisasikan dengan menggunakan digital signature.

4. Nirpenyangkalan (*non-repudiation*), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.2.2 Jenis Kriptografi Berdasarkan Perkembangan

Berdasarkan perkembangan dari tahun ke tahun sejak pertama kali kriptografi ditemukan, ada dua jenis algoritma kriptografi (Harahap, 2016), yaitu :

1. Kriptografi Klasik Algoritma kriptografi yang termasuk ke dalam jenis kriptografi klasik ini digunakan pada masa sebelum berlakunya komputarisasi dengan komputer, algoritma kriptografi ini rata-rata masih menggunakan kunci simetris dan menyandikan pesan dengan teknik subtitusi atau transposisi.
2. Kriptografi Modern Algoritma kriptografi yang termasuk ke dalam jenis kriptografi modern ini memiliki tingkat kesulitan yang lebih tinggi dan kompleks serta menggunakan pengetahuan matematika dalam penerapan kuncinya. Pada kriptografi modern, kunci yang digunakan untuk menyandikan pesan sudah berupa kunci asimetris.

2.2.3 Jenis Kunci Pada Kriptografi

Menurut Dony Arius Berdasarkan kunci yang digunakan dalam proses kriptografi, maka algoritma kunci kriptografi dibagi menjadi (Hondro, 2015):

1. Algoritma Simetri Algoritma ini sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi dan dekripsi. Bila mengirim pesan dengan menggunakan algoritma simetri, penerima pesan harus mengetahui kunci yang digunakan agar bisa si penerima mampu mendekripsikan pesan yang dikirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Algoritma yang menggunakan kunci simetris misalnya DES, Kode Rivest's IDEA, AES, OTP, A5 dan lainlain.
2. Algoritma Asimetri Algorima asimetri sering juga disebut dengan algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian yaitu kunci umum (*public key*) yang bias diketahui oleh umum dan kunci rahasia (*private key*) yaitu kunci yang dirahasiakan dan hanya boleh diketahui oleh satu orang saja.
3. Fungsi Hash Fungsi hash sering disebut dengan fungsi has satu arah (*one way function*), *message digest*, *fingerprint*, fungsi kompersi dan *Message Authentication Code* (MAC) yang merupakan suatu fungsi matematika yang mengambil masukan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap.

2.2.4 Jenis Algoritma Kriptografi

Berdasarkan jenis kunci, algoritma kriptografi dikelompokan menjadi dua bagian, yaitu : algoritma simetris (algoritma kunci privat) dan algoritma asimetris (algoritma kunci public) (Zelviana et al., 2012).

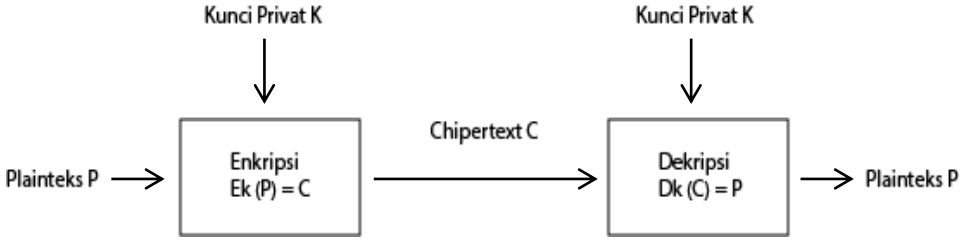
1. Algoritma Simetris

Algoritma simetris adalah salah satu jrnis kunci pada algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Istilah lain untuk kriptografi kunci simetri adalah kriptografi kunci privat (*private-key cryptography*). Sistem kriptografi kunci-simetri diasumsikan sebagai pengirim dan penerima pesan yang sudah berbagi kunci yang sama sebelum bertukar pesan. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kuncinya.

Kriptografi simetri adalah jenis kriptografi yang diketahui masuk ke dalam catatan sejarah hingga tahun 1976. Semua algoritma kriptografi klasik termasuk ke dalam sistem kriptografi simetri. Salah satu kelebihan pada algoritma simetris yaitu proses enkripsi dan deskripsinya jauh lebih cepat dibandingkan dengan algoritma asimetris. Sedangkan kelemahannya yaitu pada permasalahan distribusi kunci (*key distribution*).

Seperti yang telah dibahas sebelumnya, proses enkripsi dan deskripsi pada kriptografi simetri menggunakan kunci yang sama. Sehingga timbul persoalan untuk menjaga kerahasian kunci. Contohnya pada saat pengiriman kunci dilakukan melalui media yang tidak aman seperti internet. Jika kunci ini hilang atau sudah diketahui oleh orang yang tidak berhak, maka kriptosistem ini dinyatakan tidak aman lagi. Kelemahan lain adalah masalah efisiensi jumlah

kunci. Jika terdapat n user, maka diperlukan n(n-1)/2 kunci, sehingga untuk jumlah user yang sangat banyak, sistem ini tidak efisien lagi



Gambar 2.1 Algoritma Simetris

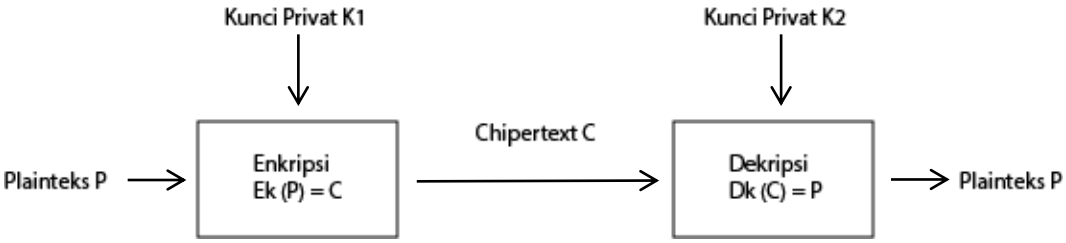
2. Algoritma Asimetris

Algoritma asimetris atau dapat disebut juga dengan algoritma kunci public, didesain sebaik mungkin sehingga kunci yang digunakan untuk enkripsi berbeda dengan kunci dekripsinya. Dimana kunci untuk enkripsi tidak rahasia (diumumkan ke publik), sementara kunci dekripsinya bersifat rahasia (hanya diketahui oleh penerima pesan).

Pada kriptografi asimetris, setiap orang yang akan berkomunikasi harus mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Pengirim pesan akan mengenkripsi pesan menggunakan kunci publik si penerima pesan dan hanya penerima pesan yang dapat mendekripsi pesan tersebut karena hanya ia yang mengetahui kunci privatnya sendiri. Kriptografi kunci-publik dapat dianalogikan seperti kotak surat yang terkunci dan memiliki lubang untuk memasukkan surat. Setiap orang dapat memasukkan surat ke dalam kotak surat tersebut, tetapi hanya pemilik kotak yang dapat membuka kotak dan membaca surat di dalamnya karena ia yang memiliki kunci. Sistem ini memiliki dua keuntungan. Yang pertama yaitu,

tidak ada kebutuhan untuk mendistribusikan kunci privat sebagaimana pada sistem kriptografi simetri. Kunci publik dapat dikirim ke penerima pesan melalui saluran yang sama dengan saluran yang digunakan untuk mengirim pesan. Saluran untuk mengirim pesan umumnya tidak aman.

Kedua, jumlah kunci yang digunakan untuk berkomunikasi secara rahasia dengan banyak orang tidak perlu sebanyak jumlah orang tersebut, cukup membuat dua buah kunci, yaitu kunci publik bagi para koresponden untuk mengenkripsi pesan, dan kunci privat untuk mendekripsi pesan. Berbeda dengan kriptografi kunci-simetris yang membuat kunci sebanyak jumlah pihak yang diajak berkorespondensi. Meski masih terbilang baru (sejak 1976), kriptografi kunci-publik mempunyai kontribusi yang luar biasa dibandingkan dengan sistem kriptografi simetri. Kontribusi yang paling penting adalah tanda-tangan digital pada pesan untuk memberikan aspek keamanan otentikasi, integritas data, dan nirpenyangkalan. Tanda-tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci yang digunakan. Pengirim pesan mengenkripsi pesan (yang sudah diringkas) dengan kunci privatnya, hasil enkripsi inilah yang dinamakan tanda-tangan digital. Tanda-tangan digital dilekatkan (embed) pada pesan asli. Penerima pesan memverifikasi tanda-tangan digital dengan menggunaklan kunci publik.



Gambar 2.2 Algoritma Asimetris

2.3 Algoritma Zig Zag Cipher

Menurut Dony Ariyus, Metode Zig Zag Cipher merupakan salah satu algoritma kriptografi klasik dengan teknik transposisi. Teknik transposisi menggunakan permutasi karakter, yang mana dengan menggunakan teknik ini pesan yang asli tidak dapat dibaca kecuali orang yang memiliki kunci untuk menggembalikan pesan tersebut ke bentuk semula (Hondro, 2015).

Metode Transposisi adalah metode yang enkripsi dengan menyusun plaintext pada matriks secara baris, lalu dari hasil susunan tersebut menghasilkan sebuah ciphertext dengan mengambil rangkaian karakter secara kolom. Metode Transposisi juga disebut metode permutasi.

Teknik yang diterapkan pada metode zig zag cipher adalah teknik transposisi cipher enkripsi dan dekripsi pesan dengan cara mengubah urutan huruf huruf yang ada di dalam *plaintext* (pesan yang belum dienkripsi) menjadi *ciphertext* dengan cara tertentu agar isi pesan tersebut tidak dimengerti kecuali oleh orang-orang tertentu. Pada dasarnya prinsip pengubahan pesan mirip dengan anagram seperti kata “melepas” diubah menjadi “saeeplm”, tapi tentu saja transposisi cipher mempunyai rumus atau kunci tertentu yang diperlukan agar pesan bisa dimengerti.

Transposisi cipher kolum atau diterapkan individual, lebih mudah untuk *cryptanalyze*. Zig zag yang terapkan dengan menggabungkan tiap pola zig zag dan columnar transposisi untuk menghasilkan *ciphertext* yang lebih sulit untuk *cryptanalyze.* Transposisi zig zag dapat dilakukan berturut-turut dengan cara membentuk bari atau kolom yang diatur dalam format matriks. Jika zig zag yang transposisi dilakukan baris, maka pesan dibaca dalam model zig zag berdasarkan angka dalam kunci. Jika digit di kuncinya adalah i, maka pesan dibaca sebagai berikut urutan posisi matrix :

(i, 1) (i +1, 2) (i, 3) (i +1, 4) (i, 5)

Jika transposisi sama dilakukan kolom bijaksana, maka pesan dibaca

(1, i) (2, i +1) (3, i) (4, i +1) (5, i)

Setelah transposisi diproses dengan kunci pada enkripsi simetris cipher, kunci yang sama digunakan untuk dekripsi. Jika j yang digit di kuncinya adalah i, maka baris teks cipher adalah

(i, 1) (i +1, 2) (i, 3) (i +1, 4) (i, 5)

Menurut Siahaan Metode enkripsi *Rail Fence* adalah salah satu bentuk cipher transposisi yang sederhana yang diinspirasi dari model *Polybius square*. *Polybius square* adalah menyusun huruf sebagai matriks 5x5 dan mengkodekan huruf A sebagai 1-1, huruf B sebagai 1-2 dan seterusnya. Setiap karakter pada *Polybius square* diganti dengan indeks cell matriks tanpa menggunakan kunci khusus dan hanya merubah posisi sehingga teks tidak terbaca. Berbeda dengan *Polybius square*, metode *Rail Fence* menyusun teks secara zig-zag yang model

matriksnya diketahui oleh pengirim dan penerima pesan (Latifah, Ambo, & Kurnia, 2017).

Studi oleh Singh dkk (2012) menyebutkan bahwa teknik *Rail Fence* adalah menuliskan *plaintext* dalam urutan diagonal dan membacanya sebagai urutan baris sehingga terbentuk *ciphertext*. Contohnya jika ingin mengenkripsi HALO APA KABAR maka spasi dihilangkan kemudian disusun diagonal membentuk pola zig-zag. Misal ingin dibuat dengan kedalaman (jumlah baris) 3, maka hasil perubahan susunannya adalah sebagai berikut :

H				A				A			
	A		O		P		K		B		R
		L				A				A	

Hasil cipher text : HAA AOPKBR LAA .

2.4 Aplikasi

Aplikasi berasal dari kata *application* yang artinya penerapan, lamaran, penggunaan. Secara istilah aplikasi adalah program siap pakai yang direka untuk melaksanakan suatu fungsi bagi pengguna atau aplikasi yang lain dan dapat digunakan oleh sasaran yang dituju.

Istilah aplikasi berasal dari bahasa inggris "*application*" yang berarti penerapan, lamaran ataupun penggunaan. Sedangkan secara istilah, pengertian aplikasi adalah suatu program yang siap untuk digunakan yang dibuat untuk melaksanakan suatu fungsi bagi pengguna jasa aplikasi serta pengguna aplikasi

lain yang dapat digunakan oleh suatu sasaran yang akan dituju. Menurut kamus komputer eksekutif, aplikasi mempunyai arti yaitu pemecahan masalah yang menggunakan salah satu tehnik pemerosesan data aplikasi yang biasanya berpacu pada sebuah komputansi yang diinginkan atau diharapkan maupun pemerosesan data yang diharapkan.

Menurut Suprianto Aplikasi adalah program yang memiliki aktivitas pemerosesan perintah yang diperlukan untuk melaksanakan permintaan pengguna dengan tujuan tertentu. Sedangkan menurut janner (2006 : 22) aplikasi adalah program atau sekelompok program yang dirancang untuk digunakan oleh pengguna akhir (*end user*) (Ali Subhan Afrizal, 2014).

Menurut Nugroho B Perangkat lunak aplikasi adalah suatu subkelas perangkat lunak komputer yang memanfaatkan kemampuan komputer langsung untuk melakukan tugas yang diinginkan pengguna. Contoh utama perangkat lunak aplikasi adalah pengolah kata, lembar kerja, dan pemutar media (Fricles Ariwisanto Sianturi, 2013).

2.5 Sistem Informasi

3.5.1 Sistem

Pengertian dari system adalah sebagai proses sekumpulan elemen yang berhubungan satu dengan yang lain secara fungsional. Agar suatu system terlaksana diperlukan data yang relavan, akurat, tepat guna dan tepat waktu yang memungkinkan pihak manajemen pihak manajemen dapat mengambil suatu keputusan yang tepat.

Untuk menjelaskan arti system tersebut, ada beberapa pendapat ahli , seperti : menurut jogiyanto, system adalah kumpulan dari elemen-elemen yang berinteraksi untuk mencapai suatu tujuan tertentu (Ananta, 2015).

Menurut Darmawan mendefinisikan bahwa “sistem sebagai kumpulan atau grup dari bagian atau komponen apa pun baik fisik yang saling berhubungan satu sama lain dan bekerja sama secara harmonis untuk mencapai satu tujuan” (Kristania, 2017).

Menurut Sutabri Sebuah sistem mempunyai karakteristik atau sifat-sifat tertentu yang mencirikan bahwa hal tersebut bisa dikatakan sebagai suatu sistem yang terdiri dari :

1. Komponen Sistem (*Components*)
2. Batasan Sistem (*Boundary*)
3. Lingkungan luar sistem (*Environment*)
4. Penghubung Sistem (*Interface*)
5. Masukan Sistem (*Input*)
6. Keluaran Sistem (*Output*)
7. Pengolah Sistem (*Proces*)
8. Sasaran Sistem (*Objective*)

3.5.2 Informasi

Informasi adalah data yang diolah menjadi sebuah bentuk yang lebih berguna bagi penerimannya dan lebih bermanfaat bagi yang menerimannya sehingga dapat digunakan sebagai dasar pengambilan keputusan . secara

garis besarnya dapat dikatakan bahwa tidak ada suatu kegiatan yang tidak memerlukan informasi , baik bersifat pribadi maupun bersifat pribadi.

Menurut jogiyanto, informasi adalah data yang telah diolah menjadi bentuk yang lebih berarti dan berguna bagi penerimanya untuk mengambil keputusan masa kini maupun masa yang akan dating (Ananta, 2015).

Menurut Darmawan mengemukakan bahwa “Informasi merupakan hasil dari pengolahan data, akan tetapi tidak semua hasil dari pengolahan tersebut bisa menjadi informasi, hasil pengolahan data yang tidak memberikan makna atau arti serta tidak bermanfaat bagi seseorang bukanlah merupakan informasi bagi orang tersebut” (Kristania, 2017).

Sedangkan Menurut McLeod dalam Darmawan menyatakan suatu informasi yang berkualitas harus memiliki ciri-ciri :

1. Akurat
2. Tepat Waktu
3. Relevan
4. Lengkap

3.5.3 Sistem Informasi

Menurut Sutabri mengemukakan bahwa “Sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian yang mendukung fungsi operasi organisasi yang bersifat manajerial dengan kegiatan strategi dari suatu organisasi untuk dapat

menyediakan kepada pihak luar tertentu dengan laporan-laporan yang diperlukan".

Menurut Sutabri Sistem informasi terdiri dari komponenkomponen yang disebut dengan istilah blok bangunan (*building block*), yang terdiri dari blok masukan, blok model, blok keluaran, blok teknologi, blok basis data, dan blok kendali. Sebagai suatu sistem, keenam blok tesebut saling berinteraksi satu dengan yang lain membentuk satu kesatuan untuk mencapai sasaran (Kristania, 2017).

Menurut Robert A . Leitch Dan K .Roscoe davis , system informasi adalah suatu system didalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporanlaporan yang diperlukan (Ananta, 2015).

Sedangkan menurut john F. Nash dan Martin B Robert, system informasi merupakan kombinasi dari manusia, fasilitas atau alat teknologi, media prosedur dan pengendalian yang dimaksud menata jaringan komunikasi yang penting, pengolahan atas transaksi-transaksi tertentu dan rutin, membantu manajemen, pemakai intern dan ekstern serta menyediakan dasar pengambilan keputusan yang tepat . System informasi mempunyai beberapa komponen sebagai berikut:

1. Data/input
2. Proses/pengolahan
3. Informasi/output

3.6 Unified Modelling Language (UML)

Pengertian *Unified Modelling Language* (UML) merupakan salah satu bentuk language atau bahasa, mneurut pencetusnya UML didefinisikan sebagai bahasa visuai untuk menjelaskan, memberikan spesifikasi, merancang, membuat model, dan mendokumentasikan aspek aspek dari sebuah sistem.

UML disebut sebagai bahasa pemodelan bukan metode. Kebanyakan metode terdiri paling sedikit prinsip, bahasa pemodelan dan proses. Bahasa pemodelan (sebagian besar grafik) merupakan notasi dari metode yang digunakan untuk mendesain secara cepat. Menurut Rosa dan Shalahuddin UML (*Unified Modeling Language*) adalah salah satu standar bahasa visual yang banyak digunakan di dunia industri untuk mengidentifikasi requirement, membuat analisis & desain, serta menggambarkan arsitektur dalam pemrograman berorientasi objek. UML muncul karena adanya kebutuhan pemodelan visual untuk menspesifikasikan, menggambarkan, membangun, dan dokumentasi dari sistem perangkat lunak. UML hanya berfungsi untuk melakukan pemodelan, jadi penggunaan UML tidak terbatas pada metologi tertentu, meskipun pada kenyataannya UML paling banyak diguakan pada metodologi berorientasi objek (Pratama & Junianto, 2016).

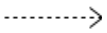
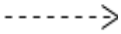
Perancangan sistem pada UML adalah sebagai berikut:

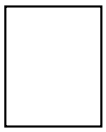
3.6.1 Use case Diagram

Use Case atau diagram use case merupakan pemodelan untuk kelakuan (*behavior*) sistem informasi yang akan dibuat. Use case mendeskripsikan sebuah interaksi antara satu atau lebih aktor dari dengan sistem informasi yang akan

dibuat. Secara kasar, use case digunakan untuk mengetahui fungsi apa saja yang ada di dalam sebuah sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi itu (Herpendi, 2016).

Tabel 2.1 Use Case Diagram

No	Gambar	Nama	Keterangan
1		*Actor*	Menspesifikasikan 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.
3		*Generalization*	Hubungan dimana objek anak berbagi perilaku dan struktur data dari objek yang ada diatasnya .
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.

6		*Association*	Apa yang menghubungkan antara objek satu dengan objek lainnya.
7		*System*	Menspesifikasikan paket yang menampilkan sistem secara terbatas.
8		*Use Case*	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu actor
9		*Collaboration*	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan prilaku yang lebih besar dari jumlah dan elemen-elemennya (sinergi).
10		*Note*	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi

3.6.2 Activity Diagram

Activity Diagram (Diagram Aktifitas) menggambarkan berbagai alir aktifitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir. Activity diagram juga dapat menggambarkan proses paralel yang mungkin terjadi pada beberapa eksekusi. Diagram Aktifitas merupakan state diagram khusus, di mana sebagian besar state adalah action dan sebagian besar transisi di-trigger oleh selesainya state sebelumnya (internal processing). Oleh karena itu Diagram AKtifitas tidak menggambarkan behaviour internal sebuah sistem (dan interaksi antar subsistem) secara eksak, tetapi lebih menggambarkan proses-proses dan jalurjalur aktivitas dari level atas secara umum. Menggambarkan proses bisnis dan urutan aktifitas dalam sebuah proses. Dipakai pada business modeling untuk memperlihatkan urutan aktifitas proses bisnis (Herpendi, 2016).

Tabel 2.2 Activity Diagram

No	Gambar	Nama	Keterangan
1		*Actifity*	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain
2		*Action*	State dari sistem yang mencerminkan eksekusi dari suatu aksi
3		*Initial Node*	Bagaimana objek dibentuk /diawali.

4		*Actifity Final Node*	Bagaimana objek dibentuk dan dihancurkan
5		*Fork Node*	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran

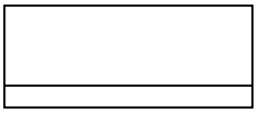
Sumber : Indrajani (2015 : 38).

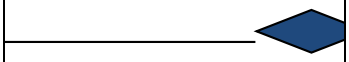
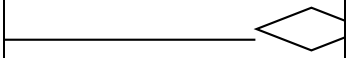
3.6.3 Class Diagram

Class Diagram menurut Munawar merupakan himpunan dari objek-objek yang sejenis. Sebuah objek memiliki keadaan sesaat (state) dan perilaku (behavior). State sebuah objek adalah kondisi objek tersebut yang dinyatakan dalam attribute. Sedangkan perilaku suatu objek mendefinisikan bagaimana sebuah objek bertindak dan memberikan (Pratama & Junianto, 2016).

Menurut Rosa dalam jurnal (Sari dan David) mengungkapkan : "Class diagram menggambarkan struktur sistem dari segi pendefinisian kelas-kelas yang akan dibuat untuk membangun sistem. Kelas memiliki apa yang disebut atribut dan metode atau operasi. Atribut merupakan variabel-variabel yang dimiliki oleh suatu kelas, sedangkan operasi atau metode adalah fungsi-fungsi yang dimiliki oleh suatu kelas." (Yunahar Heriyanto, 2018).

Tabel 2.3 Class Diagram

Simbol	Nama	Fungsi
	*Class*	Menggambarkan *Class* baru pada diagram.

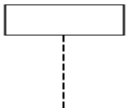
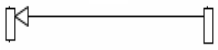
	Association	Menggambarkan relasi antar asosiasi
	*Composition*	Jika sebuah *class* tidak bisa berdiri sendiri dan harus merupakan bagian dari *class* yang lain, maka class tersebut memiliki relasi *Composition* terhadap *class* tempat dia bergantung tersebut.
	Depedency	Umumnya penggunaan *dependency* digunakan untuk menunjukkan operasi pada suatu *class* yang menggunakan *class* yang lain.
	*Aggregation*	*Aggregation* mengindikasikan keseluruhan bagian *relationship* dan biasanya disebut sebagai relasi.

3.6.4 Sequence Diagram

Menurut Nofriyadi Jurdam, “Sequence Diagram adalah tool yang sangat populer dalam pengembangan sistem informasi secara object-oriented untuk menampilkan interaksi antar objek.” Berdasarkan definisi tersebut, dapat disimpulkan bahwa Sequence Diagram adalah tool yang digunakan dalam pengembangan sistem(Yunahar Heriyanto, 2018).

Sequence diagram menggambarkan kelakuan objek pada use case dengan mendeskripsikan waktu hidup objek dan pesan yang dikirimkan dan diterima antar objek. Simbol-simbol yang digunakan dalam sequence diagram yaitu (Urva & Siregar, 2015) :

Tabel 2.4 Sequence Diagram

NO	GAMBAR	NAMA	KETERANGAN
1		*LifeLine*	Objek *entity*, antarmuka yang saling berinteraksi.
2		*Message*	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi.
3		*Message*	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi.

3.7 Dekstop

Desktop sebenarnya sebutan yang biasa digunakan sebagai pengganti dari komputer desktop. Komputer desktop adalah komputer pribadi yang ditujukan untuk penggunaan secara umum disuatu lokasi yang berlawanan dengan komputer portabel seperti NoteBook dan NetBook.

Komponen-komponen penyusun komputer desktop seperti monitor atau layar komputer, CPU, dan keyboard terpisah satu sama lain dan biasanya berukuran besar. Berbeda dengan komputer portabel yang komponen-komponennya disatukan dan berukuran kecil sehingga memudahkan untuk dibawa ke mana saja (Huda, 2013)

3.8 Visual Basic 2010

Microsoft Visual Studio adalah sebuah Integrated Development Environment buatan Microsoft Coroporation. Microsoft Visual Studio dapat digunakan untuk mengembangkan aplikasi dalam native code (dalam bentuk bahasa mesin yang berjalan di atas Windows) ataupun managed code (dalam bentuk Microsoft Intermediate Language di atas .NET Framework). Selain itu, Visual Studio juga dapat digunakan untuk mengembangkan aplikasi Silverlight, aplikasi Windows Mobile (yang berjalan di atas .NET Compact Framework). Visual Basic mencakup sebuah kode editor yang didukung oleh fitur intellisense atau yang disebut dengan code refactoring. Debugger telah terintegrasi bekerja pada level source level debugger dan level debugger mesin. Toll built in mencakup form desainer untuk membangun sebuah aplikasi GUI, web desainer, class desainer dan database schema desainer.

Menurut Edy Winarno Microsoft Visual Studio didukung bahasa pemrograman yang berbeda. Adapun bahasa pemrograman yang didukung oleh Visual Basic Studio adalah bahasa pemrograman C++, Visual Basic, Visual C#. Visual Studio juga dapat mendukung bahasa pemrograman lain seperti M, phyton

dan ruby yang semuanya itu terdapat pada pack extra yang terpisah dai visual studio (Putri & Azpar, 2016).

Pada awalnya BASIC (Beginner's Allpurpose Symbolic Instruction Code) adalah bahasa pemerogramanan yang merupakan awal dari bahasa pemrograman tingkat tinggi sesudahnya, yang berbasis DOS (Diskette Operating sistem). BASIC memiliki struktur bahasa yang sulit dan memiliki tampilan yang tidak menarik, dengan kemajuan teknologi maka diperlukan suatu aplikasi pemrograman yang bukan hanya cepat tapi juga menarik dan user friendly atau mudah digunakan. Maka Microsoft mengembangkan Visual Basic sebagai salah satu bahasa pemerograman tingkat tinggi berdasarkan dari bahasa pemerograman BASIC.

Visual Basic, membuat bahasa BASIC yang susah digunakan menjadi lebih mudah dengan orentasi grafis dan objek atau OPP (Objects Oriented Programming). Yang lebih mudah digunakan, cepat dengan wizard generator code, dan memungkinkan mendisain interface yang menarik dan mudah untuk digunakan user nantinya.

Visual Basic versi pertama di keluarkan tahun 1991, yang dikembangkan oleh Alan Cooper, yang melakukan pendekatan bahasa pemerograman dengan GUI (Graphic User Interface). Berikut sejarang Versi Visual Basic (Kanedi, 2013):

1. Visual Basic 1.0 di rilis pada May 1991 untuk sistem operasi Windows 3.0. pertama kali diperkenalkan di Atlanta.
2. Visual Basic 2.0, dirilis pada November 1992.

3. Visual Basic 3.0, di keluarkan pada tahun 1993, dalam versi ini mulai dimasukkan Jet Database Engine.
4. Visual Basic 4.0. Dikeluarkan pada Agustus 1995.
5. Visual Basic 5.0. Dirilis Febuari 1997 untuk versi windows 32 Bit. Dengan fitur ekspor impor dari VB4 ke VB5.
6. Visual Basic 6.0, di rilis pada tahun 1998 dan memperbaiki beberapa cakupan, termasuk kemampuan untuk membuat aplikasi berbasis Web.
7. Visual Basic .NET (VB 7.0). Dirilis pada tahun 2002.
8. Visual Basic .NET 2003 (VB 7.1) di rilis tahun 2003 merupakan pengembangan dan update dari VB .NET
9. Visual Basic 2005 (VB 8.0). Dirilis tahun 2005.
10. Saat ini Visual Basic 2010, di keluarkan pada tahun 2010 yang merupakan penambahan dan sekuel dari Visual basic 2007.

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Pada tahapan perancangan program dan mengenai tahapan yang akan dilakukan dalam penelitian ini akan dijelaskan secara jelas. Akan ada tahapan analisa, perancangan, permodelan sistem, dan perancangan tampilan antar muka.

3.2 Analisa Proses Zig Zag Cipher

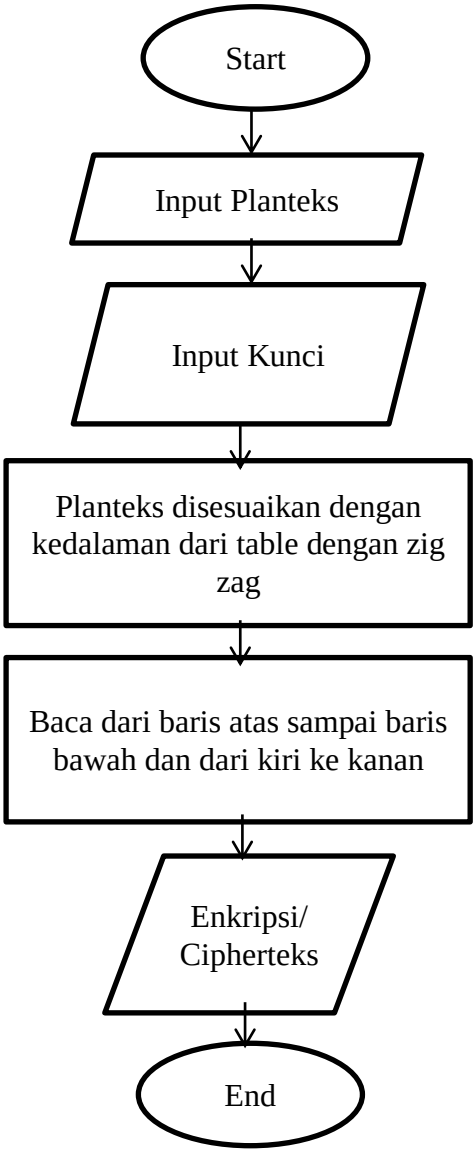
Zig Zag cipher akan bekerja dengan menggunakan tabel kolom dan baris. Pada metode ini, plaintext akan dibentangkan pada tabel tersebut. Karakter pertama akan diletakkan pada ujung kiri atas. Karakter selanjutkan akan diletakkan secara diagonal ke bawah hingga menemukan baris terakhir sesuai dengan kedalaman kunci. Pada saat baris terakhir sudah ditempati oleh karakter plaintext, maka karakter berikutnya akan diletakkan mengarah diagonal ke atas, yaitu kanan atas. Proses ini adalah proses pada saat mengenkripsi kalimat.

3.3 Perancangan Program

Pada Bagian ini akan dibuat perancangan sistem program yang akan dibuat dan akan dirancang sedemikian rupa agar menghasilkan sebuah program aplikasi yang mudah untuk dipahami dan juga mudah untuk digunakan, dan dapat juga menampilkan penjelasan dan keluaran yang jelas.

3.3.1 Flowchart Enkripsi

Bagian flowchart enkripsi akan menggambarkan dan menjelaskan cara mengenkripsi pada program atau sistem, berikut ini adalah flowchart enkripsi.



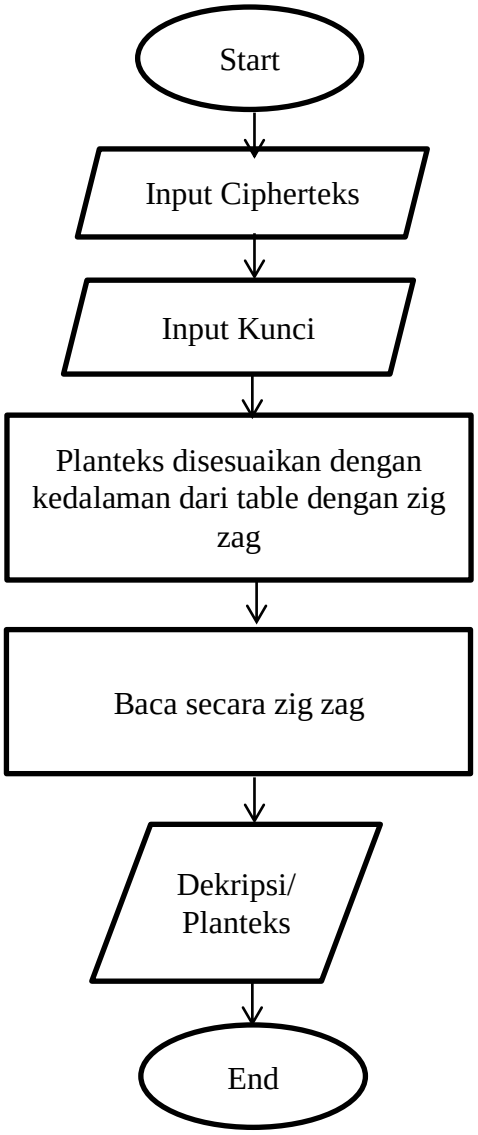
Gambar 3.1 Flowchart enkripsi

Gambar 3.1 menunjukkan alur pada saat mengenkripsi. gambar yang diatas menunjukan bahwa proses enkripsi dimulai dengan menginput planteks dan

juga kunci atau kedalaman, kemudian planteks akan disesuaikan dengan kunci ataupun kedalaman yang tadi diinputkan.

3.3.2 Flowchart Dekripsi

Flowchart dekripsi akan menjelaskan dan juga menggambarkan bagaimana proses program pada saat mengdekripsikan kalimat atau cipherteks.



Gambar 3.2 Flowchart dekripsi

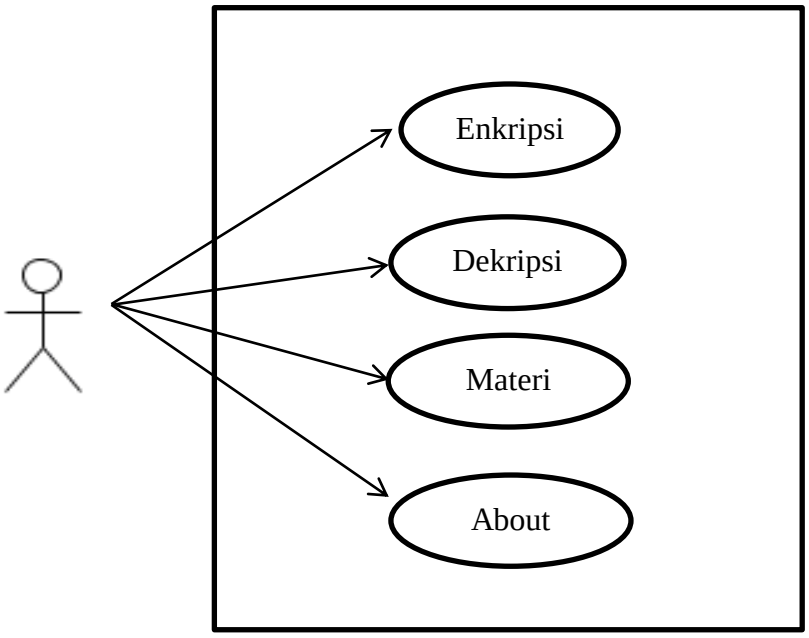
Gambar 3.2 menunjukkan alur pada saat mengdekripsi. gambar yang diatas menunjukan bahwa proses dekripsi dimulai dengan menginput Cipherteks yang didapat dan juga kunci yang sesuai dengan padasaat enkripsi, kemudian cipherteks akan disesuaikan dengan kunci yang sudah di tentukan dengan pengguna yang mengenkripsi.

3.4 Permodelan Sistem

Pada bagian ini akan menggunakan diagram UML (Unified Modelling Language) untuk menggambarkan atau menjelaskan bagaimana sistem akan berjalan atau juga sistem yang akan bekerja, intinya sistem yang berorientasi objek. Pada bagian ini diagram UML yang akan digunakan ialah Use Case Diagram, Activity Diagram, Class Diagram, dan juga Sequence Diagram.

3.4.1 Use Case Diagram

diagram use case ini menggambarkan sebuah aktifitas atau apa saja yang dapat dilakukan oleh pengguna mau itu yang ingin mengenkripsi, dan juga pengguna yang ingin mengdekripsi. Berikut ini adalah use case diagram yang menggambarkan aktivitas.

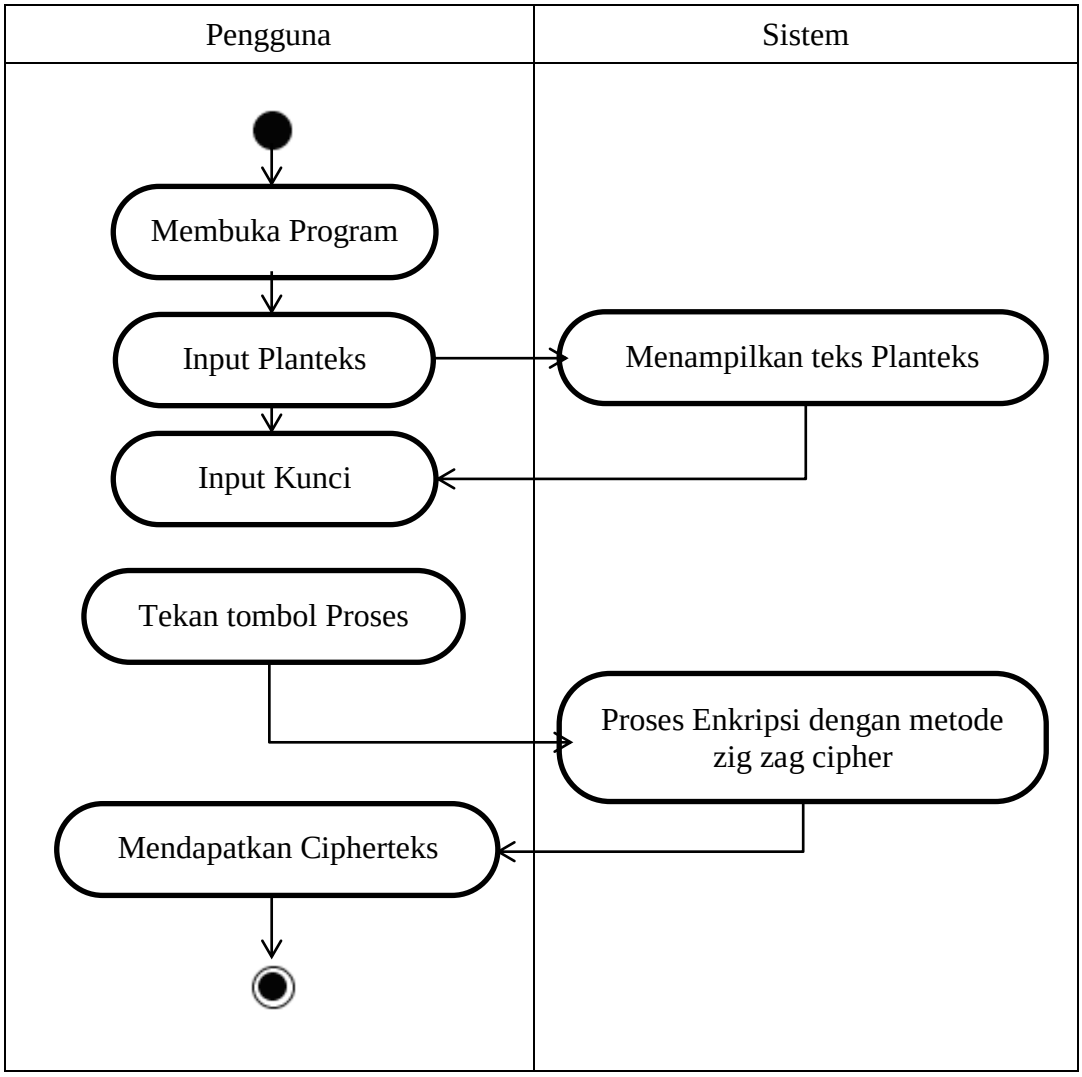


Gambar 3.3 Use-case diagram

Pada Gambar 3.3 menggambarkan sistem yang digunakan oleh pengguna. Pengguna dapat melakukan proses enkripsi, dekripsi, dan juga materi. Tergantung dari pengguna yang sebagai pengirim ataupun penerima

3.4.2 Activity Diagram

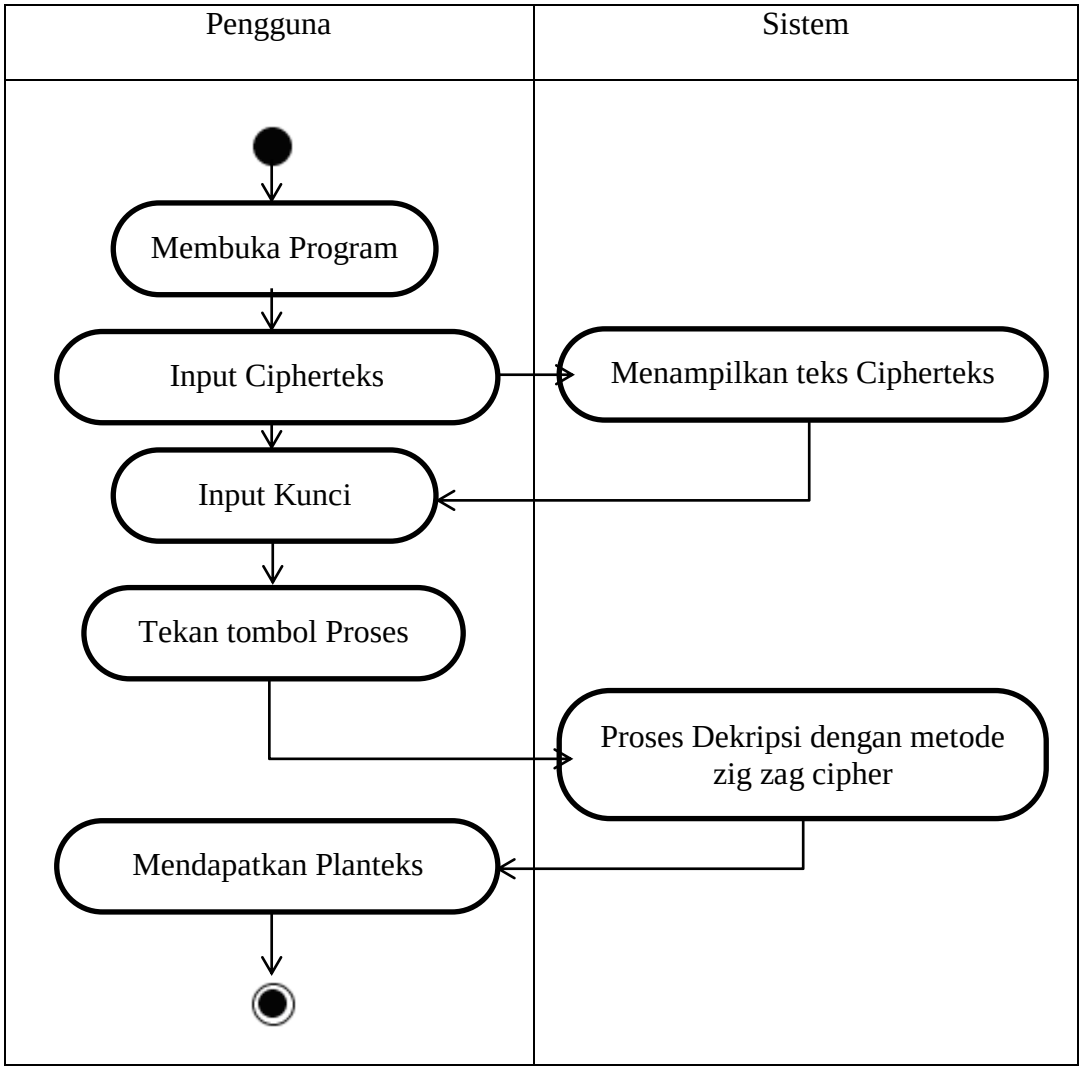
Activity diagram ini menggambarkan alur aktivitas pengguna jika mengenkripsi sebuah kalimat. aktivitas yang dibuat secara berurutan dan juga detail sesuai dengan intruksi. Gambar berikut ini adalah aktivitas pada saat mengenkripsi kalimat.



Gambar 3.4 Activity Diagram Enkripsi

Pada gambar 3.4 terdapat 2 kotak kotak yang kiri pada gambar menunjukan aktivitas yang dilakukan oleh pengguna yang ingin mengenkripsi. dan kalau kotak yang kanan menggambarkan respon yang diberikan sistem terhadap aktivitas yang dilakukan oleh pengguna pada sistem

Dan berikut ini adalah gambar yang menggambarkan alur aktivitas pengguna jika mengdekripsikan kalimat.

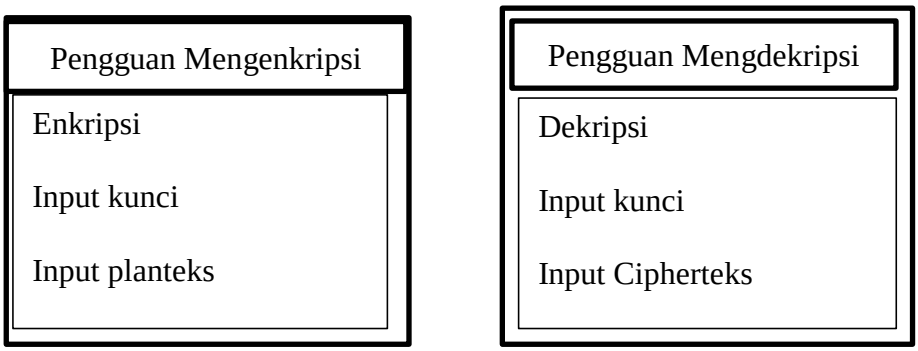


Gambar 3.5 Activity Diagram Dekripsi

Pada gambar 3.5 ini juga terdapat 2 kotak yang kiri adalah kotak yang menunjukan aktivitas yang dilakukan oleh pengguna dan kalau kotak yang kanan menunjukkan respo yang diberikan sistem terhadap pengguna.

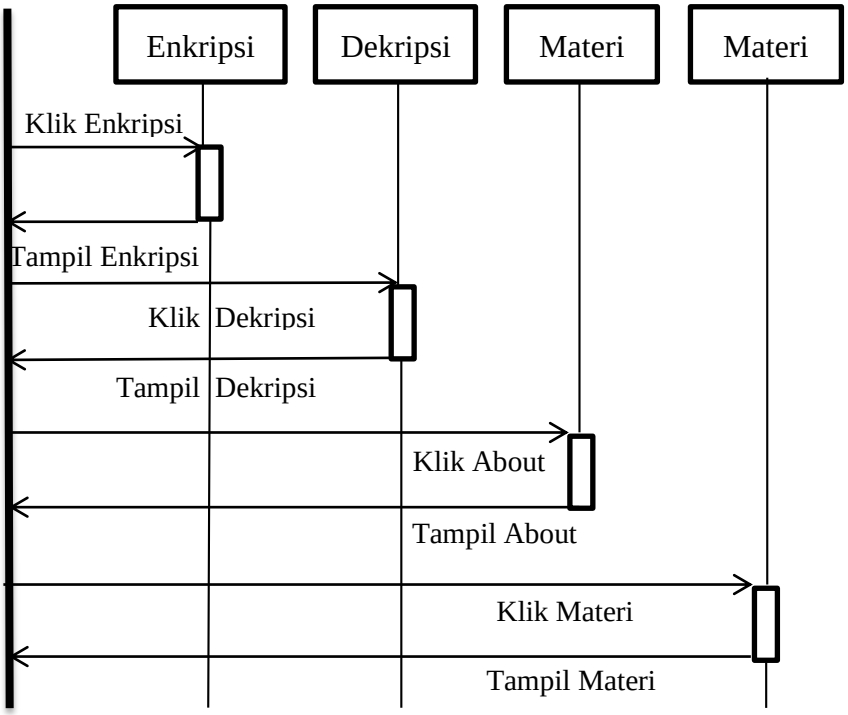
3.4.3 Class Diagram

Pada class diagram ini menggambarkan apa saja yang dapta dilakukan oleh pengguna, berikut adalah class diagramnya.



Gambar 3.6 Claas Diagram

3.4.4 Sequence Diagram



Gambar 3.7 Sequence Diagram

Pada Gambar 0.1 menjelaskan aktivitas pada saat menjalankan program dan juga bagaimana respon yang dilakukan oleh sistem. Berikut penjelasannya.

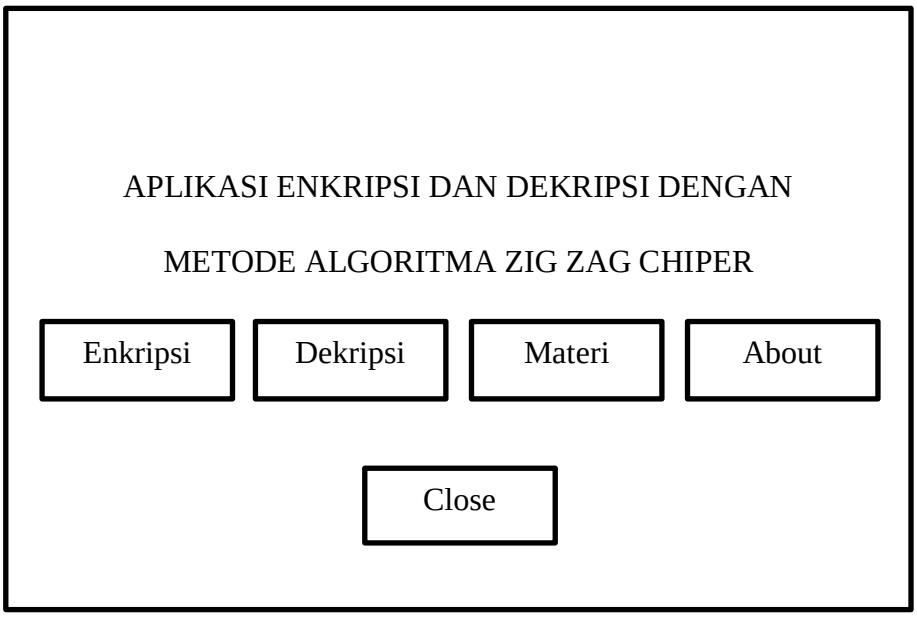
1. Pada saat pengguna meminta menu enkripsi maka sistem merespon dengan menampilkan menu enkripsi.
2. Pada saat pengguna meminta menu dekripsi maka sistem akan merespo dengan menampilkan menu dekripsi.
3. Dan pada saat pengguna meminta menu materi respon sistem akan langsung menampilkan menu materi.

3.5 Perancangan Tampilan Antar Muka

Perancangan tampilan antar muka ini akan menjelaskan tampilan dari program yang akan dibuat. Tampilan antar muka ini terbagi lagi menjadi beberapa bagian yakni tampilan menu, tampilan enkripsi, tampilan dekripsi, dan tampilan penjelasan. Berikut ini adalah penjelasan dan juga rancangan tampilan yang akan dibuat .

3.5.1 Perancangan Tampilan Utama

Pada bagian ini akan menjelaskan perancangaan tampilan menu utama. Pada tampilan menu utama ini terdapat beberapa tombol yakni tombol enkripsi, tombol dekripsi, tombol tentang, tombol close



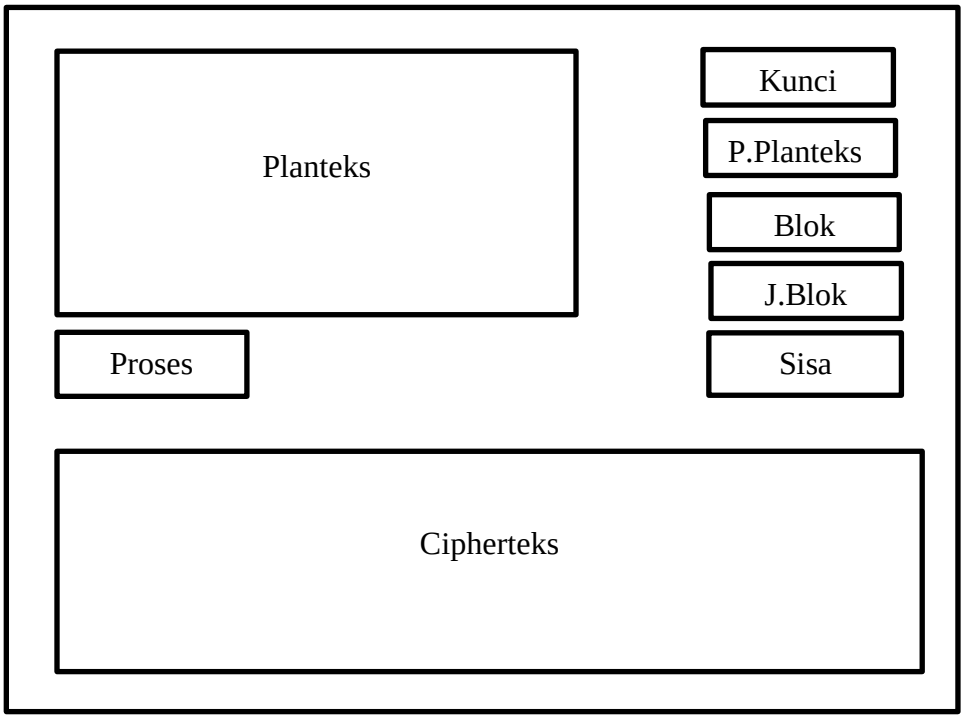
Gambar 3.8 Perancangan Tampilan Menu

Dari tampilan yang ada diatas terdapat 4 tombol yaitu Enkripsi, Dekripsi, Materi, dan Close. Berikut penjelasan dari tombol tombol yang ada ditampilan menu.

1. Tombol enkripsi berfungsi untuk menghubungkan atau menampilkan tampilan form enkripsi.
2. Tombol dekripsi berfungsi untuk menghubungkan atau menampilkan tampilan form dekripsi.
3. Tombol materi berfungsi untuk menghubungkan atau menampilkan tampilan dari materi yang digunakan.
4. Tombol close berfungsi untuk menutup program.

3.5.2 Perancangan Tampilan Enkripsi

Pada perancangan tampilan enkripsi terdapat tombol dan juga ada inputan. Berikut adalah rancangan tampilan enkripsi



Gambar 3.9 Perancangan Tampilan Enkripsi

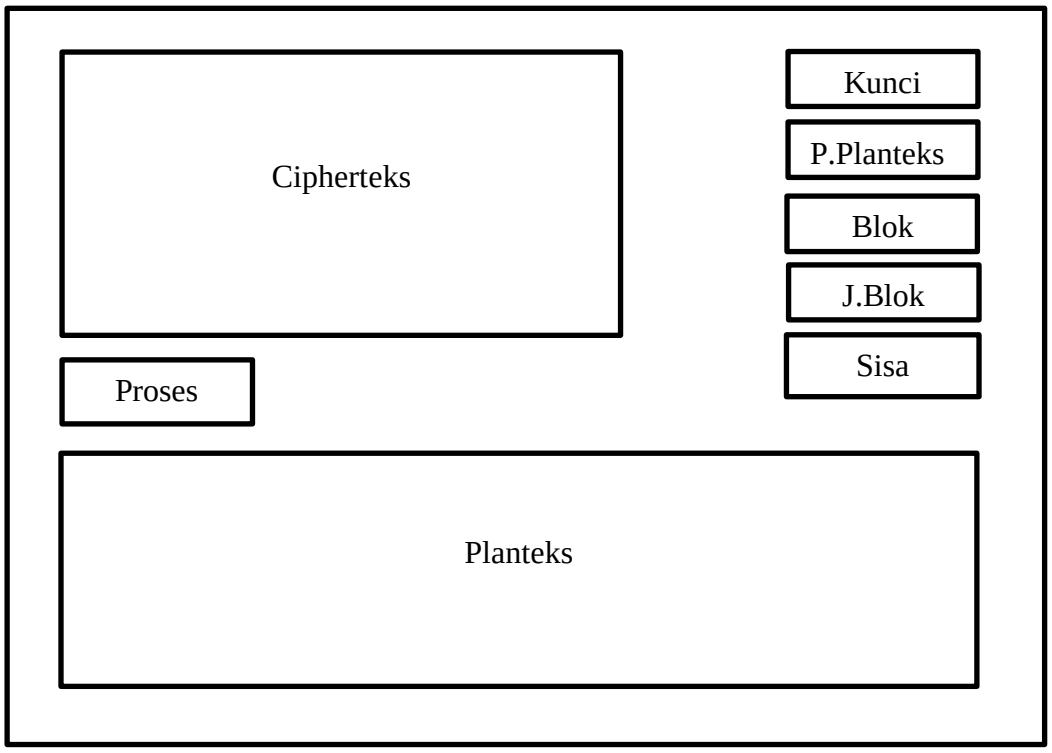
Dari tampilan yang ada diatas ada palnteks, kedalaman, panjanga planteks, blok, jumlah blok, sisa, tombol proses, dan juga hasil. Dari beberapa bagian yang ada pada gambar yang termasuk bagian inputan hanya bagian planteks dan juga kedalaman. Berikut ini adalah penjelasan dari tiap tiap bagian yaitu.

1. Planteks adalah bagian tempat untuk penginputan kalimat yang ingin di enkripsi.
2. Kedalaman atau kunci adalah bagian untuk penentuan dari hitungan yang digunakan, ini juga termasuk juga kunci bagian ini juga inputan.
3. Panjang Planteks adalah tampilan yang dimana akan muncul jumlah karakter yang kita masukkan diinputan planteks.
4. Blok adalah jumlah karakter dengan kunci secara penuh.
5. Jumlah Blok adalah total blok dari panjang planteks

6. Sisa adalah penambahan karakter dari blok yang tidak penuh
7. Tombol proses adalah tombol untuk memproses yang sudah kita input planteks dan kedalaman.
8. Hasil adalah bagian yang akan menampilkan hasil yang sudah diproses.

3.5.3 Perancangan Tampilan Dekripsi

Pada perancangan tampilan dekripsi ini menjelaskan tampilan program untuk mendekripsikan kalimat yang terenkripsi. Pada bagian ini tampilannya tidak berbeda dengan pada saat kita mengenkripsi, tampilannya sebagai berikut.



Gambar 3.10 Perancangan Tampilan Dekripsi

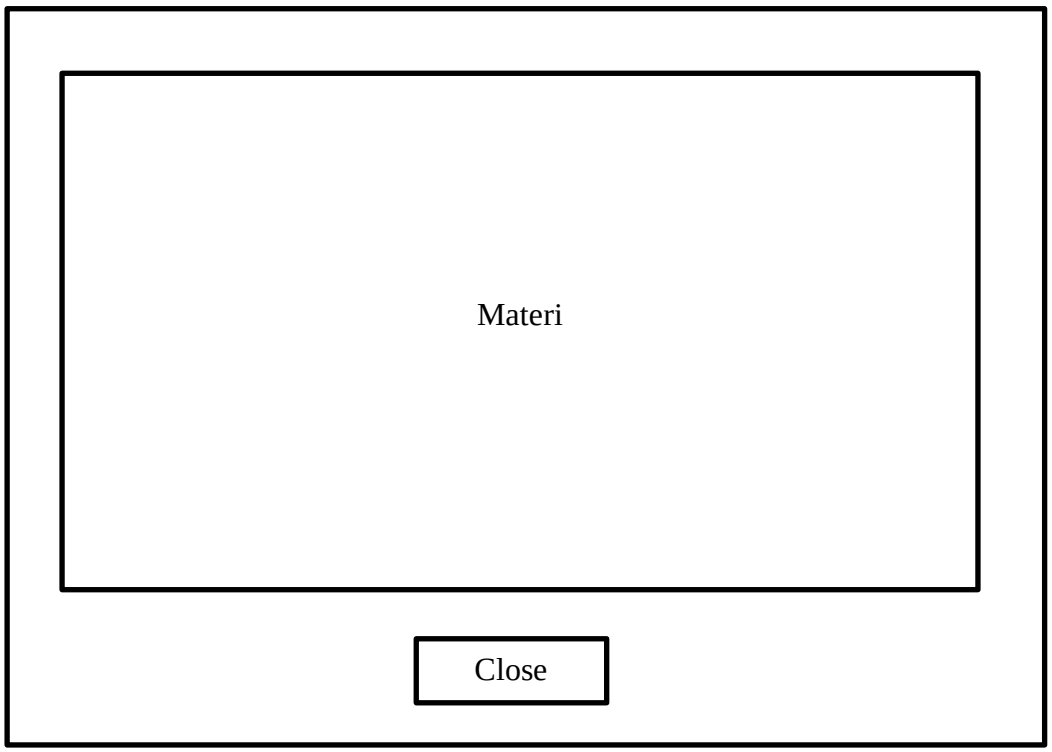
Dari tampilan yang diatas secara tampilan tidak berbeda dengan yang untuk mengenkripsi kalimat berikut adalah penjelasan dari tiap tiap bagian yang ada di tampilan yakni.

1. Cipherteks adalah bagian tempat untuk penginputan kalimat yang ingin di deskripsikan.
2. Kedalaman adalah bagian untuk penentuan dari hitungan yang digunakan, ini juga termasuk juga kunci bagian ini juga inputan, ini harus sesuai dengan kunci pada saat mengenkripsi.
3. Panjang Planteks adalah tampilan yang dimana akan muncul jumlah karakter yang kita masukkan diinputan planteks.
4. Blok adalah jumlah karakter dengan kunci secara penuh.
5. Jumlah Blok adalah total blok dari panjang planteks.
6. Sisa adalah penambahan karakter dari blok yang tidak penuh.
7. Tombol proses adalah tombol untuk memproses yang sudah kita input planteks dan kedalaman.
8. Planteks adalah bagian yang akan menampilkan hasil yang sudah didekripsi.

3.5.4 Perancangan Tampilan Materi

Pada bagian perancangan tampilan materi ini, akan menampilkan materi dari algoritma yang akan diguanakan pada aplikasi ini. Dan juga menjelaskan bagaimana kerja kriptografi yang digunakan yakni algoritma zig zag cipher. Pada tampilan ini hanya menjelaskan sedikit dan juga skema dari algoritma zig zag cipher.

Pada bagian ini tidak terdapat banyak tombol hanya tombol close yang terdapat dibawah dan juga tidak ada bagian untuk penginputan pada bagian ini.. Pada bagian ini hanya berisi penjelasan saja, berikut adalah tampilan untuk materi, berikut ini adalah rancangan tampilan dari aplikasinya.

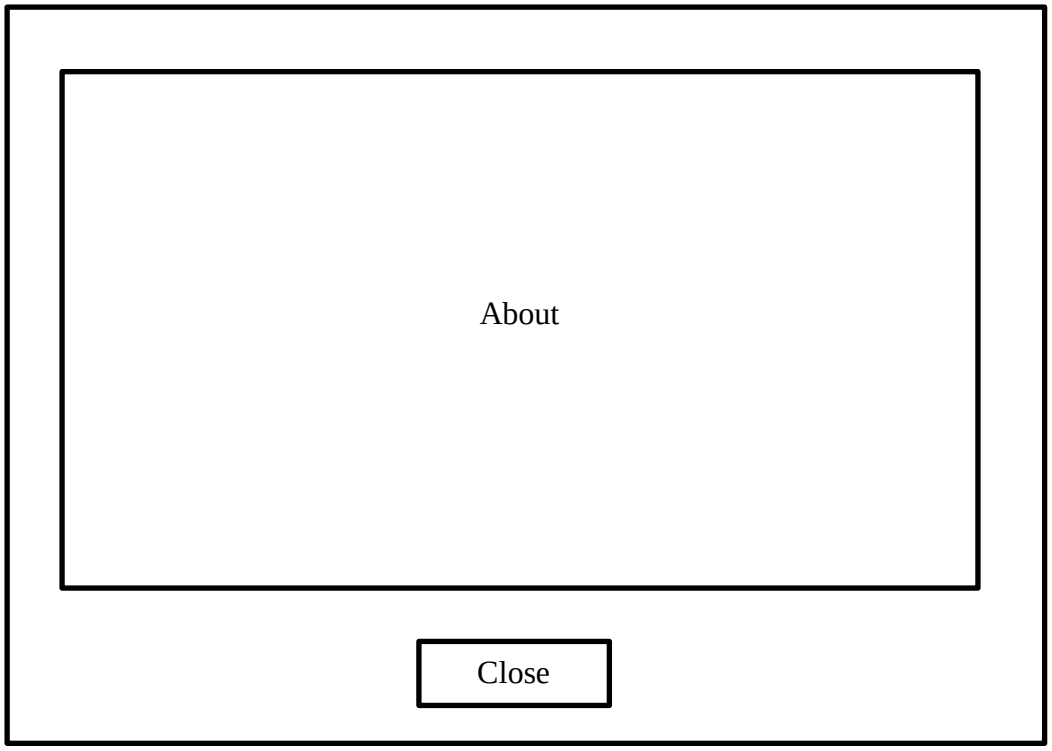


Gambar 3.11 Perancangan Tampilan Materi

3.5.5 Perancangan Tampilan About

Perancangan tampilan About ini menampilkan form atau tampilan yang berisi tentang profil mahasiswa yang membuat. Dan juga didalamnya terdapat judul skripsi yang dibuat oleh penulis dan juga maksud dari pembuatan dari aplikasi tersebut, beserta nama dan nomor mahasiswa dari penulis.

Dari rancangan tampilan yang akan dibuat pada bagian ini tidak terdapat banyak tombol yang ada hanya tombol close yang berguna untuk menutup tampilan about ini. Dan juga tidak ada bagian untuk penginputan pada tampilan ini, berikut ini adalah rancangan tampilan dari aplikasinya.



Gambar 3.12 Perancangan Tampilan About

BAB IV

HASIL PEMBAHASAN

4.1 Impelmentasi Sistem

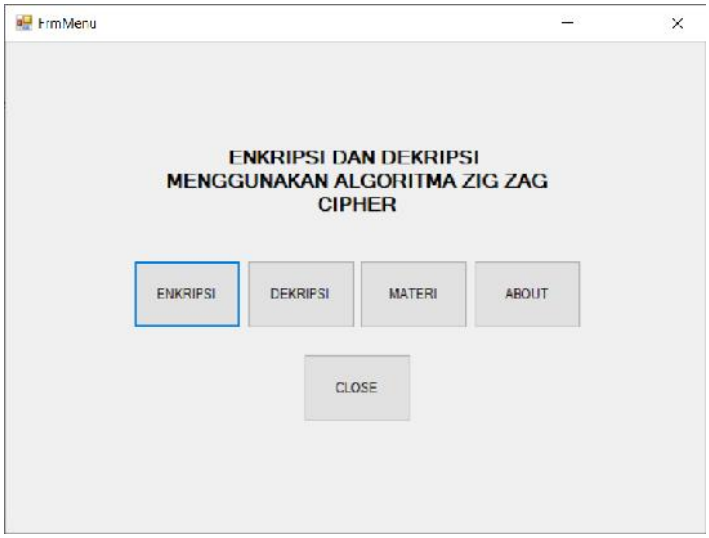
Pada tahapan implementasi sistem ini merupakan tahapan yang dimana aplikasi atau program yang telah dirancang akan dijalankan. Tahapan ini akan menunjukkan bagaimana setiap proses dari aplikasi atau program yang dirancang, apakah mampu berjalan dengan baik dan mempu memberikan hasil yang diinginkan. Perancangan aplikasi atau program menggunakan Microsoft Visual Studio 2010. Program akan ditampilkan dalam bentuk form yang akan menjadi tampilan untuk pengguna untuk melakukan proses implementasi.

4.2 Pengujian Tampilan Sistem

Pengujian tampilan sistem ini akan mencoba semua tampilan yang ada diaplikasi yang dibuat, apakah sesuai dengan yang diinginkan atau dirancang. Pada bagian ini akan dicoba satu persatu tampilannya sebagai berikut ini.

4.2.1 Tampilan Utama

Tampilan Utama merupakan tampilan yang pertama kali ketika aplikasi dijalankan. Ada beberapa tombol yaitu tombol enkripsi, tombol dekripsi, tombol materi, tombol about, dan juga tombol close. Berikut adalah tampilan awal dari aplikasi.

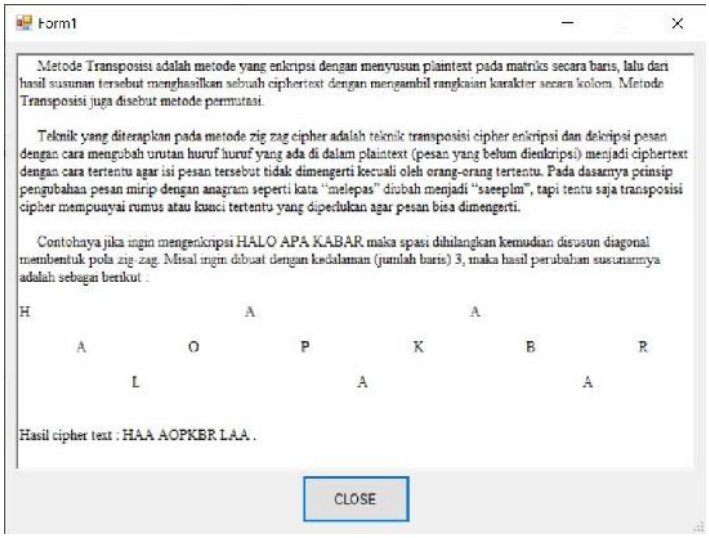


Gambar 4.1 Tampilan Utama

Pada tampilan ini pengguna dapat memilih untuk membuka beberapa menu tampilan yang lain, contohnya tombol enkripsi yang mengarahkan pengguna pada tampilan yang berguna untuk mengenkripsi kalimat. Tombol dekripsi yang akan mengarahkan pengguna pada tampilan yang berguna untuk mendekripsi kalimat. Tombol materi yang akan mengarahkan pengguna pada tampilan materi yang menjelaskan gimana kerja dari aplikasi tersebut. Tombol *about* yang akan menjelaskan ke pengguna tentang aplikasi. Dan tombol *close* yang akan menutup aplikasi.

4.2.2 Tampilan Materi

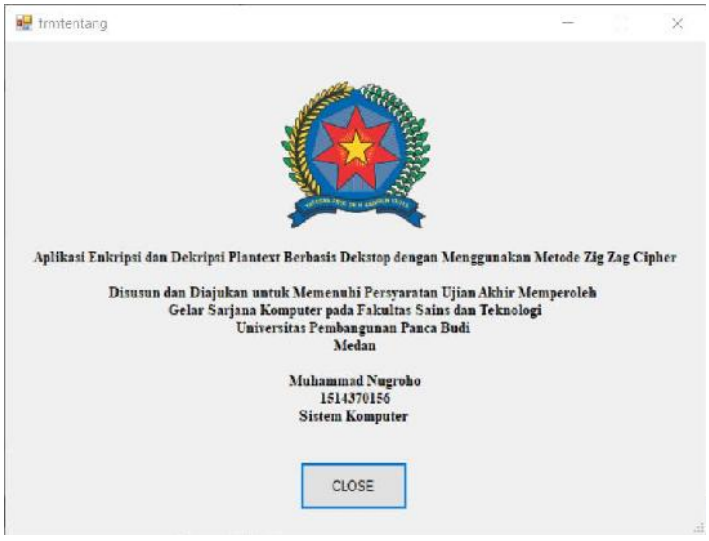
Pada tampilan materi disini akan menjelaskan isi tentang materi yang dijalankan. Pada halaman ini akan dijelaskan algoritma zig zag cipher, berikut ini adalah tampilannya.



Gambar 4.2 Tampilan Materi

4.2.3 Tampilan Tentang / About

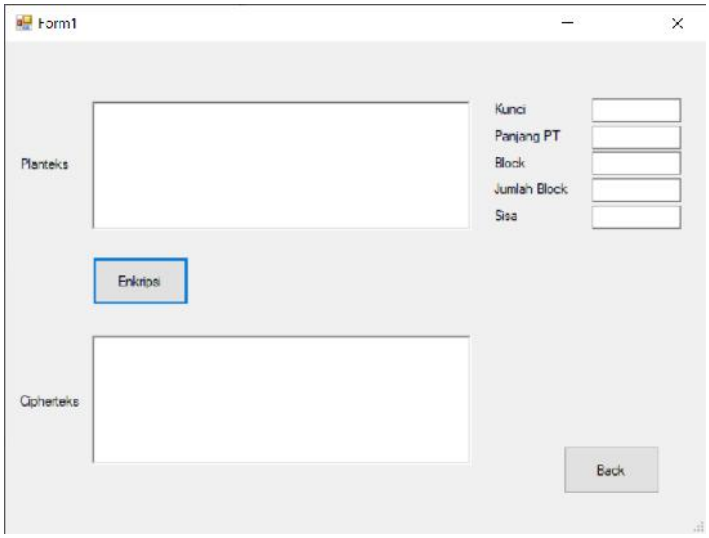
Pada tampilan ini akan menampilkan halaman atau form yang berisi profil dari aplikasi ini. Didalamnya berisi judul dari aplikasi, dan maksud tujuan pembuatan aplikasi ini. Dan beserta nama dan nomor mahasiswa penulisnya.



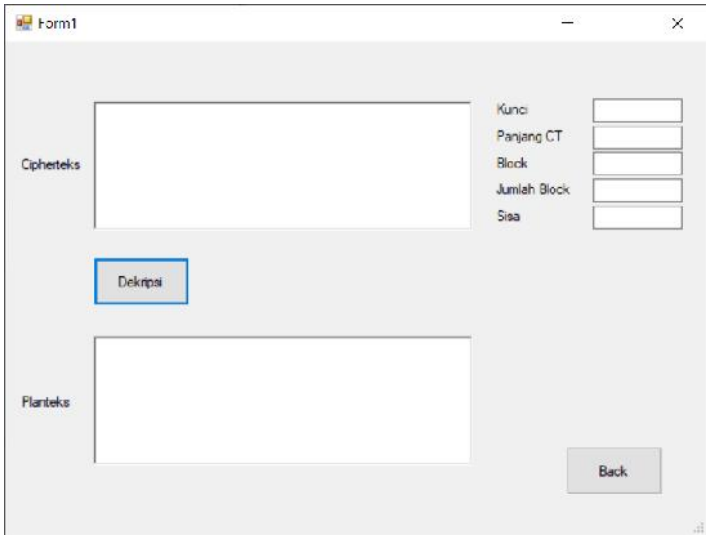
Gambar 4.3 Tampilan About

4.2.4 Tampilan Enkripsi dan Dekripsi

Tampilan enkripsi dan dekripsi ini adalah tampilan pada saat pengguna mengenkripsi dan juga mendekripsi kalimat. Pada tampilan enkripsi dan dekripsi berikut ini tidak jauh berbeda agar pengguna mudah memahaminya.



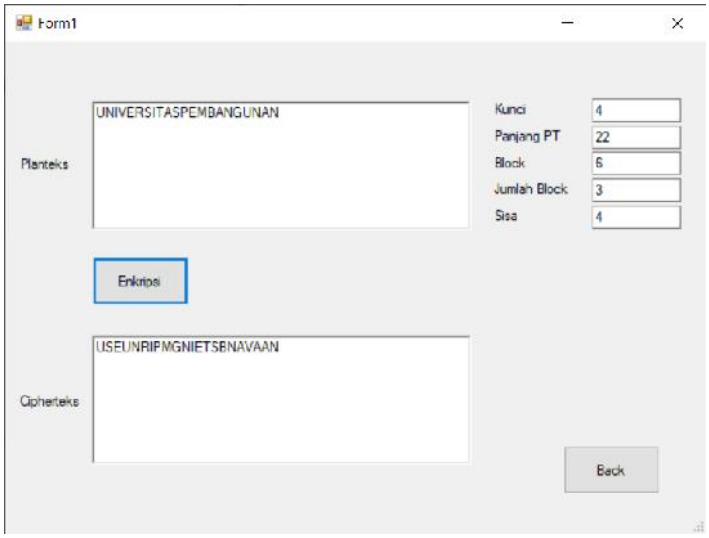
Gambar 4.4 Tampilan Enkripsi



Gambar 4.5 Tampilan Dekripsi

4.3 Pengujian Sistem

Pada tahapan pengujian sistem ini akan dilakukan pengujian, apakah sistem yang sudah dirancang berjalan dengan baik dan juga sesuai dengan yang diinginkan. Pengujian dilakukan dengan memasukan kalimat atau *plantext*, selanjutnya pengguna juga harus memasukan kedalaman, kedalaman ini berfungsi sebagai kunci juga. Setelah itu akan diproses oleh aplikasi, apakah aplikasi dapat memberikan hasil yang sesuai dengan yang diinginkan. Proses yang dilakukan oleh aplikasi adalah mengenkripsi dan juga mendekripsikan kalimat dan juga kata dengan menggunakan metode algoritma Zig Zag Cipher. Antara pengguna yanng mengenkripsi dengan pengguna yang mendekripsi harus menggunakan kunci atau kedalaman yang sama, yang sudah disepakati sebelumnya Berikut ini adalah pengujian sistem pada saat mengenkripsi.



Gambar 4.6 Pegujian Sistem Pertama

Dari gambar diatas, kalimat yang ingin dienkripsi adalah UNIVERSITAS PEMBANGUNAN disini saya membuat tanpa spasi dan dengan kedalaman atau kunci 4. Berikut ini adalah proses enkripsinya.

Panjang	22
Kunci	4

	1	2	3	4	5	6	7	8	9	10	11	12
B1	U						S					
B2		N				R		I				P
B3			I		E				T		S	
B4				V						A		

	13	14	15	16	17	18	19	20	21	22
B1	E						U			
B2		M				G		N		
B3			B		N				A	
B4				A						N

Dari penjelasan yang ada diatas panjang dai kalimat adalah 22 karakter dan kuncinya 4, kunci 4 dilihat dari banyaknya baris seperti yang diatas.

Blok	6
Jumlah Blok	3

Blok 1

U					
	N				R
		I		E	
			V		

Blok 2

S					
	I				P
		T		S	
			A		

Blok 3

E					
	M				G
		B		N	
			A		

Sisa 4

U			
	N		
		A	
			N

Jumlah Karakter Pada Baris

B1	3	1	4
B2	6	1	7
B3	6	1	7
B4	3	1	4

Karakter Setiap Baris

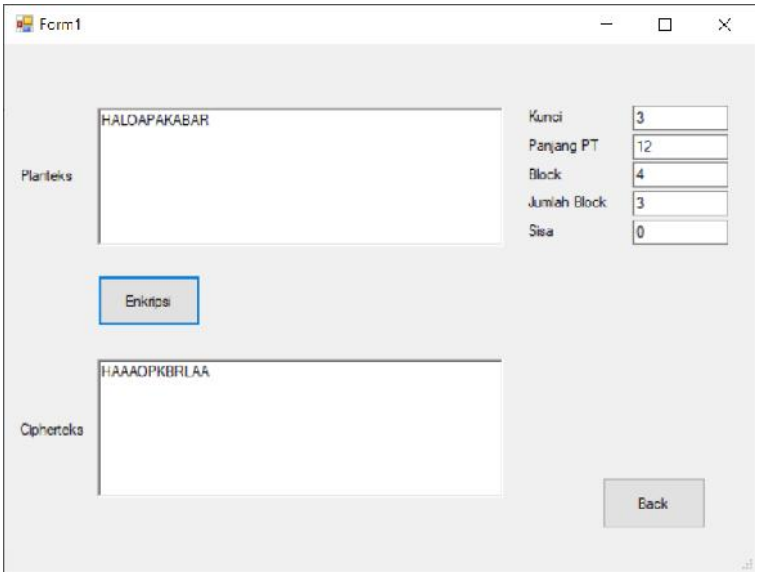
B1	U	S	E	U			
B2	N	R	I	P	M	G	N
B3	I	E	T	S	B	N	A
B4	V	A	A	N			

Ciphertext USEUNRIPMGNIETSBNAVAAN

U	S	E	U	N	R	I	P	M	G	N
B1				B2						

I	E	T	S	B	N	A	V	A	A	N
B3							B4			

Berikut ini adalah pengujian sisitem yang ke 2 kalimat yang akan digunakan adalah HALOAPAKABAR dan tanpa spasi. Dengan kedalaman 3, pengujian sistem seperti dibawah ini.



Gambar 4.7 Pengujian Sistem Ke 2

Panjang 12

Kunci 3

	1	2	3	4	5	6	7	8	9	10	11	12
B1	H				A				A			
B2		A		O		P		K		B		R
B3			L				A				A	

Blok 4

Jumlah Blok 3

Blok 1

H			
	A		O
		L	

Blok 2

A			
	P		K
		A	

Blok 3

A			
	B		R
		A	

Jumlah Karakter Pada Baris

B1	3
B2	6
B3	3

Karakter Setiap Baris

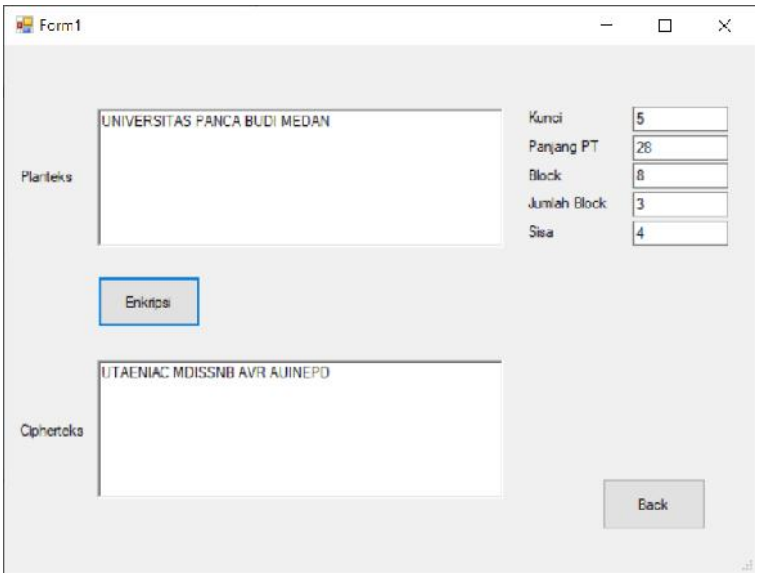
B1	H	A	A			

B2	A	O	P	K	B	R
B3	L	A	A			

Ciphertext HAAAOPKBRLAA

H	A	A	A	O	P	K	B	R	L	A	A
B1			B2						B3		

Berikut ini adalah pengujian ke tiga yang digunakan pada pengujian ini adalah kalimat UNIVERSITAS PANCA BUDI. Pada saat pengujian satu dan dua tidak memakai spasi tapi pada pengujian yang ke tiga akan menggunakan spasi berikut adalah contoh dan penjelasannya.



Gambar 4.8 Pengujian Sistem Ke 3

Panjang 28
Kunci 5

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
B1	U								T					
B2		N						I		A				
B3			I				S				S			
B4				V		R								A
B5					E								P	

	15	16	17	18	19	20	21	22	23	24	25	26	27	28
B1			A								E			
B2		C								M		D		
B3	N				B								A	
B4						U		I						N
B5							D							

Blok 8
Jumlah Blok 3

Blok 1

U							
	N						I
		I				S	
			V		R		
				E			

Blok 2

T							
	A						C
		S				N	
					A		
				P			

Blok 3

A							
							M
		B					
			U		I		
				D			

Sisa 4

E			
	D		
		A	
			N

Jumlah Karakter Pada Baris

B1	3	1	4
B2	6	1	7
B3	6	1	7
B4	6	1	7
B5	3		3

Karakter Setiap Baris

B1	U	T	A	E			
B2	N	I	A	C		M	D
B3	I	S	S	N	B		A
B4	V	R		A	U	I	N
B5	E	P	D				

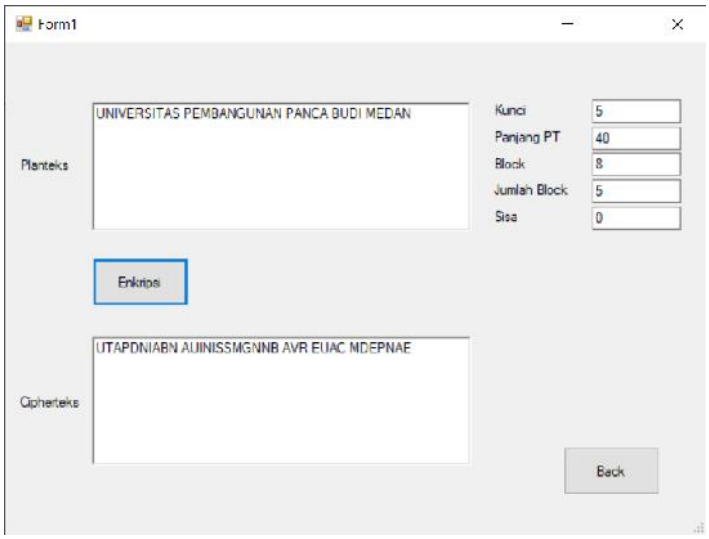
Ciphertext UTAENIAC MDISSNB AVR AUINEPD

U	T	A	E	N	I	A	C		M	D
B1				B2						

I	S	S	N	B		A
B3						

V	R		A	U	I	N	E	P	D
B4							B5		

Berikut ini adalah pengujian ke empat plantext yang akan digunakan adalah UNIVERSITAS PEMBANGUNAN PANCA BUDI MEDAN. Dengan menggunakan kunci 5 berikut adalah pengujiannya dan penjelasannya.



Gambar 4.9 Pengujian Sistem Ke 4

Panjang	40		1	2	3	4	5	6	7	8	9	10
Kunci	5	B1	U								T	
		B2		N						I		A
		B3			I				S			
		B4				V		R				
		B5					E					

	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
B1							A								P
B2						B		N							
B3	S				M				G				N		
B4				E						U		A			
B5			P								N				

	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
B1								D							
B2	A						U		I						N
B3		N				B								A	
B4			C								M		D		
B5				A								E			

Blok 8

Jumlah Blok 5

Blok 1

U							
	N						I
		I				S	
			V		R		
				E			

Blok 2

T							
	A						B
		S				M	
					E		
				P			

Blok 3

A							
	N						
		G				N	
			U		A		
				N			

Blok 4

P							

	A						U
		N				B	
			C				
				A			

Blok 5

D							
	I						N
						A	
			M		D		
				E			

Jumlah Karakter Pada Baris

B1 5
B2 10
B3 10
B4 10
B5 5

Karakter Setiap Baris

B1	U	T	A	P	D					
B2	N	I	A	B	N		A	U	I	N
B3	I	S	S	M	G	N	N	B		A
B4	V	R		E	U	A	C		M	D
B5	E	P	N	A	E					

Ciphertext UTAPDNIABN AUINISSMGNNB AVR EUAC MDEPNAE

U	T	A	P	D	N	I	A	B	N		A	U	I	N
B1					B2									

I	S	S	M	G	N	N	B		A
B3									

V	R		E	U	A	C		M	D	E	P	N	A	E
B4										B5				

BAB V

PENUTUP

5.1 Kesimpulan

Kesimpulan dari penelitian dan percobaan yang sudah dilakukan terhadap aplikasi enkripsi dan dekripsi tersebut. Maka dapat diambil kesimpulan sebagai berikut :

1. Aplikasi ini dapat melindungi keamanan dalam melakukan komunikasi atau juga dalam bertukar informasi.
2. Aplikasi ini dapat memberikan rasa aman kepada pengguna aplikasi ini.
3. Aplikasi ini dibuat dengan sederhana, agar pengguna dapat dengan mudah menggunakannya.

5.2 Saran

Saran dari penelitian dan percobaan yang sudah dilakukan, saran yang dapat penulis sampaikan sebagai berikut :

1. Aplikasi ini kedepannya dapat dikembangkan lagi dengan dikombinasikan menggunakan metode metode algoritma yang lain.
2. Untuk pengembangan aplikasi ini bisa juga berbasis web dan lain-lain.
3. Dari aplikasi yang buat bisa dikembangkan lagi dalam segi keamanannya atau kuncinya digandakan.

DAFTAR PUSTAKA

Ali Subhan Afrizal. (2014). Rancang Bangun Aplikasi Dekstop Kamus Indonesia, Inggris Dan Arab Menggunakan Netbeans Dan Mysql. *Jurnal Teknik Informatika Politeknik Sekayu (TIPS)*, *1*(1), 1–9.

Ananta, D. (2015). Perancangan Aplikasi Penjualan Barang Berbasis Desktop. *Perancangan Aplikasi Penjualan Barang Berbasis Desktop Pada Cv. Metro Rantauprapat*, *1*(3), 9–12.

Barus, S., Sitorus, V. M., Napitupulu, D., Mesran, M., & Supiyandi, S. (2018). Sistem Pendukung Keputusan Pengangkatan Guru Tetap Menerapkan Metode Weight Aggregated Sum Product Assesment (WASPAS). Jurnal Media Informatika Budidarma, 2(2).

Batubara, Supina. "Analisis perbandingan metode fuzzy mamdani dan fuzzy sugeno untuk penentuan kualitas cor beton instan." IT Journal Research and Development 2.1 (2017): 1-11.

Batubara, Supina, Sri Wahyuni, and Eko Hariyanto. "Penerapan Metode Certainty Factor Pada Sistem Pakar Diagnosa Penyakit Dalam." Seminar Nasional Royal (SENAR). Vol. 1. No. 1. 2018.

Easttom, C. (2015). *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. New York: McGraw-Hill.

Fachri, B. (2018, September). APLIKASI PERBAIKAN CITRA EFEK NOISE SALT & PAPPER MENGGUNAKAN METODE CONTRAHARMONIC MEAN FILTER. In Seminar Nasional Royal (SENAR) (Vol. 1, No. 1, pp. 87-92).

Fachri, B. (2018). Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif. Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika), 3, 98-102.

Fricles Ariwisanto Sianturi. (2013). Perancangan Aplikasi Pengamanan Data Dengan Kriptografi Advanced Encryption Standard (AES). *Pelita Informatika Budi Darma*, *4*(1), 42–46. Retrieved from http://ejurnal.stmik- budidarma.ac.id/index.php/pelita/article/view/208

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.

Harahap, M. K. (2016). Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher Dan One Time Pad. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, *1*(1), 61–64. https://doi.org/10.30743/infotekjar.v1i1.43

Hasugian, A. H. (2017). *Implementasi Algoritma Hill Cipher*. (August 2013),115–122.

Herpendi. (2016). Aplikasi Pengelolaan Nilai Akademik Mahasiswa dan DPNA (Daftar Peserta dan Nilai Akhir) Herpendi. *Faks*, *2*(1), 2460–173.

Hondro, R. K. (2015). *Aplikasi Enkripsi Dan Dekripsi Sms Dengan Algoritma*. Huda, S. (2013). *SISTEM INFORMASI KEUANGAN BERBASIS DESKTOP DENGAN JAVA STANDARD EDITION & MySQL DI SEKOLAH TINGGI TEKNOLOGI NURUL JADID PAITON PROBOLINGGO*. (09011188), 26.

Kanedi, at al. (2013). TATA KELOLA PERPUSTAKAAN MENGGUNAKAN BAHASA PEMROGRAMAN VISUAL BASIC 6.0 (Studi Kasus Pada Sekolah Menengah Pertama Negeri 3 Seluma) Indra. *Jurnal Media Infotama*, *214*(1).

Khairul, K., IlhamiArsyah, U., Wijaya, R. F., & Utomo, R. B. (2018, September). IMPLEMENTASI AUGMENTED REALITY SEBAGAI MEDIA PROMOSI PENJUALAN RUMAH. In Seminar Nasional Royal (SENAR) (Vol. 1, No. 1, pp. 429-434).

Kristania, Y. M. (2017). Sistem Informasi Pelatihan Mobil Pada Citra Indotech Jaya Purwokerto Berbasis Desktop. *Khatulistiwa Informatika*, *V*(1), 64–71.

Kurniawan, H. (2018). Pengenalan Struktur Baru untuk Web Mining dan Personalisasi Halaman Web. Jurnal Teknik dan Informatika, 5(2), 13-19.

Latifah, R., Ambo, S. N., & Kurnia, S. I. (2017). *Karakter Khusus*. (November),1–2.

Nugroho, at al. (2016). Aplikasi Keamanan Email Menggunakan Algoritma Rc4. *Jurnal SAINTIKOM*, *15*(ISSN : 1978-6603), 81–88. Retrieved from https://lppm.trigunadharma.ac.id/public/fileJurnal/hpO91 Jurnal Nurcahyo.pdf

Pratama, Y. A., & Junianto, E. (2016). Sistem Pakar Diagnosa Penyakit Ginjal Dan Saluran Kemih Dengan Metode Breadth First Search. *Jurnal Informatika*, *2*(1). https://doi.org/10.31311/ji.v2i1.69

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.

Putri, N. E., & Azpar, S. (2016). Sistem Informasi Pengolahan Data Pendidikan Anak Usia Dini (PAUD) Terpadu Amalia Syukra Padang Nency Extise Putri1, , Supriandi Azpar2 1,2STMIK INDONESIA PADANG e-mail: n_cyland@yahoo.co.id ABSTRAK. *Sistem Informasi Pengolahan Data Pendidikan Anak Usia Dini (PAUD) Terpadu Amalia Syukra Padang*, 203–212.

Rahim, R., Aryza, S., Wibowo, P., Harahap, A. K. Z., Suleman, A. R., Sihombing, E. E., ... & Agustina, I. (2018). Prototype file transfer protocol application for LAN and Wi-Fi communication. Int. J. Eng. Technol., 7(2.13), 345-347.

Rahim, R., Supiyandi, S., Siahaan, A. P. U., Listyorini, T., Utomo, A. P., Triyanto, W. A., ... & Khairunnisa, K. (2018, June). TOPSIS Method Application for Decision Support System in Internal Control for Selecting Best Employees. In Journal of Physics: Conference Series (Vol. 1028, No. 1, p. 012052). IOP Publishing.

Rossanty, Y., Aryza, S., Nasution, M. D. T. P., & Siahaan, A. P. U. (2018). Design Service of QFC And SPC Methods in the Process Performance Potential Gain and Customers Value in a Company. Int. J. Civ. Eng. Technol, 9(6), 820-829.

Sari, R. D., Supiyandi, A. P. U., Siahaan, M. M., & Ginting, R. B. (2017). A Review of IP and MAC Address Filtering in Wireless Network Security. Int. J. Sci. Res. Sci. Technol, 3(6), 470-473.

Siahaan, A. P. U., Ikhwan, A., & Aryza, S. (2018). A Novelty of Data Mining for Promoting Education based on FP-Growth Algorithm.

Sidik, A. P. (2018). Algoritma RSA dan Elgamal sebagai Algoritma Tambahan untuk Mengatasi Kelemahan Algoritma One Time Pad pada Skema Three Pass Protocol.

Sitorus, Z. (2018). Kebutuhan Web Service untuk Sinkronisasi Data Antar Sistem Informasi dalam Universitas. Jurnal Teknik dan Informatika, 5(2), 87-90.

Tasril, V. (2018). Sistem Pendukung Keputusan Pemilihan Penerimaan Beasiswa Berprestasi Menggunakan Metode Elimination Et Choix Traduisant La Realite. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 100-109.

Urva, G., & Siregar, H. F. (2015). *Pemodelan UML E- Marketing Minyak Goreng*. (9), 92–101.

Yunahar Heriyanto. (2018). Perancangan Sistem Informasi Rental Mobil Berbasis Web Pada PT.APM Rent Car. *Jurnal Intra-Tech*, *2*(2), 64–77.

Zelviana, A., Efendi, S., & Dedy, A. (2012). Perancangan Aplikasi Pembelajaran Kriptografi Kunci Publik ElGamal Untuk Mahasiswa. *Jurnal Dunia Teknologi Informasi*, *1*(1), 56–62.