IMPLEMENTASI ALGORITMA HORIZONTAL BIT ROTATION DALAM MENGAMANKAN INFORMASI

Disusun dan Diajukan Untuk Memenuhi Persyaratan Ujian Akhir
Memperoleh Gelar Sarjana Komputer Pada Fakultas Sains Dan Teknologi
Universitas Pembangunan Panca Budi

SKRIPSI

OLEH

NAMA	: MUHAMMAD NUR SITOMPUL
N.P.M	: 1514370424
PROGRAM STUDI	: SISTEM KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2020

ABSTRAK

MUHAMMAD NUR SITOMPUL

Implementasi Algoritma Horizontal Bit Rotation Dalam Mengamankan Informasi

2020

Untuk menjaga keamanan file-file penting biasanya digunakan teknik *enkripsi* agar kerahasiaan data tersebut terjamin, salah satunya dengan menggunakan algoritma kriptografi. Pada kriptografi klasik terdapat algoritma *Horizontal Bit Rotation*. ini mempunyai 7 putaran bit bilangan biner, rotasi maksimal adalah 7 putaran dan nilai minimal adalah 1 putaran. Algoritma ini berfungsi untuk rotation. Proses pengamanan pesan tersebut hanya berupa text yang dikirim, dan penerima harus memiliki kunci untuk membuka pesan asli. Dengan adanya *Horizontal Bit Rotation.* pesan teks yang muncul berupa hasil dari algoritma tersebut. Program yang dibahas menggunakan pemrograman *Visual Basic* 2010.

Kata Kunci : Bit Rotation, *Enkripsi*, Keamanan, *Visual Basic*.

DAFTAR ISI

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR ISTILAH

ASCII *ASCII* (*American Standard Code for Information Interchange*) atau kode Standar Amerika untuk Pertukaran Informasi. Merupakan suatu standar internasional dalam kode huruf dan lumeri seperti *Hex* dan *Unicode* tetapi *ASCII* lebih bersifat *universal*, contohnya 124 adalah untuk karakter "|".

UML *Unified Modeling Language (UML)* adalah bahasa spesifikasi standar yang dipergunakan untuk mendokumentasikan, menspesifikasikan dan membanngun perangkat lunak. *UML* merupakan metodologi dalam mengembangkan sistem berorientasi objek dan juga merupakan alat untuk mendukung pengembangan sistem.

BAB I

PENDAHULUAN

1.1 Latar belakang

Keamanan dan kerahasiaan data merupakan suatu aspek yang sangat penting dalam proses pertukaran pesan atau informasi. Suatu pesan yang sifatnya rahasia membutuhkan suatu sistem penyimpanan dan pengiriman data atau *file* agar tidak mudah terbaca dan diketahui semua orang. Ada berbagai macam cara untuk mengamankan data atau *file*, salah satunya adalah menggunakan metode kriptografi.

Saat ini kriptografi terbagi menjadi dua yaitu kriptografi klasik dan kriptografi modern. Pada kriptografi klasik terdapat algoritma *Horizontal Bit Rotation*. ini mempunyai 7 putaran bit bilangan biner. Algoritma ini berfungsi untuk rotation.

Proses pengamanan pesan tersebut hanya berupa text yang dikirim, dan penerima harus memiliki kunci untuk membuka pesan asli. Dengan adanya *Horizontal Bit Rotation.* pesan teks yang muncul berupa hasil dari algoritma tersebut. Saat ini, ilmu kriptografi semakin banyak digunakan dan mulai berubah menjadi kebutuhan. Dengan maraknya perkembangan ilmu dan teknologi, informasi-informasi penting pun tidak lagi hanya berada pada media tulis saja.

Berdasarkan latar belakang yang telah penulis uraikan di atas, maka penulis tertarik untuk memilih judul **"Implementasi Algoritma Horizontal Bit Rotation Dalam Mengamankan Informasi".**

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas dapat penulis simpulkan bahwa yang menjadi pokok permasalahan dalam pembahasan ini adalah sebagai berikut:

1. Bagaimana merancang sebuah keamanan untuk semua informasi ?
2. Bagaimana menerapkan metode *Algoritma Horizontal Bit Rotation* untuk mengamankan informasi ?

1.3 Batasan Masalah

Berdasarkan perumusan masalah diatas maka penulis melakukan pembatasan masalah yang akan dibahas sebagai berikut:

1. Nilai rotasi maksimal adalah 7 putaran dan nilai minimal adalah 1 putaran.
2. Program yang dibahas menggunakan pemrograman *Visual Basic Net* 2010.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian dengan Mengkonversi bilangan desimal ke bilangan biner ini yang ingin dicapai adalah sebagai berikut:

1. Merancang sistem aplikasi keamanan data dengan algoritma *Horizontal Bit Rotation*.
2. Memperkuat keamanan data sebuah file berisi informasi penting.

1.5 Manfaat Penelitian

Adapun manfaat dalam penelitian ini yang diperoleh dari penerapan dengan *algoritma Horizontal Bit Rotation* adalah sebagai berikut:

1. Kerahasiaan data yang dikirim dan diterima lebih aman.
2. Sebagai media pembelajaran dalam bidang keamanan informasi.

BAB II

LANDASAN TEORI

2.1 Keamanan Data

Seiring dengan kemajuan teknologi informasi maka sangat di perlukan sebuah keamanan data terhadap kerahasiaan informasi yang saling di pertukarkan melalui jaringan internet, apa lagi jika data tersebut dalam suatu jaringan komputer yang terhubung/terkoneksi dengan jaringan lain. Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima pesan. Selain itu data yang dibajak kemungkinan rusak atau hilang yang menimbulkan kerugian material yang besar (Angga & Desi, 2018).

2.1.1 Aspek Keamanan Data Secrecy

Berhubungan dengan akses membaca data dan informasi. Data dan informasi di dalam suatu sistem komputer hanya dapat diakses dan dibaca oleh orang yang berhak.

1. *Integrity*

   Berhubungan dengan akses merubah data dan informasi. Data dan informasi di dalam suatu sistem komputer hanya dapat diubah oleh orang yang berhak

2. *Availability*

   Berhubungan dengan ketersediaan data dan informasi. Data dan informasi yang berada dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak.

Ada 3 alasan kenapa keamanan data / data security itu penting. Yang pertama adalah mencegah potensi kerugian material. Yang kedua adalah mengurangi risiko penyalahgunaan data / informasi. Yang terakhir adalah memperkecil peluang tindakan kriminal.

Oleh karena itu, pengetahuan tentang keamanan / data security sudah menjadi kebutuhan. Hal itu karena semakin canggih teknologi yang dipakai, semakin banyak pula data / informasi yang diperlukan. Jadi, bukan sekadar *hardware* canggih saja ya. Didukung oleh perkembangan kriptografi, sekarang macam-macam data sangat bervariasi. Begitu juga cara untuk mengumpulkan data, sangat beragam.

2.2 Data

Data adalah istilah majemuk dari kata datum, berarti fakta atau bagian fakta yang mengandung arti, yang dihubungkan dengan kenyataan, simbol-simbol, gambar-gambar, kata-kata, angka-angka, huruf-huruf, yang menunjukkan suatu ide, objek, kondisi atau situasi dan sebagainya (Akim & Yani, 2014).

Dari segi Bahasa kata “data” ini diambil dari kata “datum” yang dalam Bahasa Romawi memiliki arti sebagai sesuatu yang diberikan. Oleh sebab itu itu

definisi sesungguhnya dari data ini ialah diberikan bukan memberikan, sebab apabila memberikan maka data itu sudah menjadi informasi yang baku serta juga diakui kebenarannya. Istilah data tersebut memang lebih banyak ditemui pada bidang komputer atau juga dalam lingkup sebuah penelitian.

Dalam bidang komputer sendiri anda pasti tidak asing dengan yang namanya database maupun juga software pengolah data. Sedangkan apabila dalam lingkup penelitian, sudah menjadi hal yang wajib bahwa tiap-tiap peneliti tersebut terlebih dahulu harus mencari data dengan melakukan observasi (pengamatan) sebelum dikaji secara lebih lanjut dan akhirnya akan diperoleh hasil penelitian. Hal tersebut juga sering dijumpai dalam bidang pendidikan ialah seperti pembuatan jurnal ataupun skripsi.

2.2.1 Fungsi Data

Setelah mengetahui pengertian dan definisi diatas mengenai data maka sudah terlihat jelas fungsi dari data itu sendiri. Mungkin istilah data tersebut lebih banyak didengar dalam bidang komputer ataupun juga penelitian namun pada dasarnya hampir di segala macam aspek kehidupan itu membutuhkan apa yang dinamakan data ini. Bagi para peneliti sebuah data itu dijadikan sebagai landasan utama dalam penelitiannya. Dalam penggunaan bidang komputer tersebut juga hampir selalu melibatkan suatu data yang kemudian diolah untuk dapat memecahkan masalah. Dengan melihat hal diatas maka bisa kita ambil kesimpulan bahwa data ini berfungsi

1. untuk membuat keputusan terbaik didalam memecahkan sebuah masalah,
2. dapat dijadikan juga sebagai dasar suatu perencanaan atau juga penelitian,
3. dijadikan sebagai acuan dalam tiap-tiap implementasi suatu kegiatan atau aktivitas dan terakhir
4. data ini juga dapat dijadikan sebagai bahan evaluasi.

Sebuah data itu dapat diibaratkan sebagai dasar dalam perencanaan atau riwayat segala tindakan yang sudah atau telah dilakukan. Inilah mengapa hampir didalam segala macam aspek kehidupan itu selalu melibatkan data.

2.2.2 Jenis – Jenis Data

Disebabkan data ini hampir ada di segala macam aspek kehidupan maka tidak mengherankan bahwa data ini dapat digolongkan atau dikelompokan menjadi beberapa jenis.

Terdapat banyak parameter pengelompokan data ini namun kebanyakan mungkin dikelompokkan dengan berdasarkan sifatnya, dengan berdasarkan sumber atau darimana data itu berasal, dengan berdasarkan waktu pengambilan dan masih banyak lagi. Nah untuk lebih jelasnya dibawah ini akan dijelaskan mengenai jenis data tersebut :

1. Berdasarkan sumbernya

Sebelumnya kita menyingung bahwa suatu data itu diperoleh dari cara memperoleh yang berbeda. Perbedaan sumber tersebut juga

dapat mengelompokkan data tersebut menjadi beberapa jenis yakni data primer dan juga data sekunder. Data primer atau data asli ini didapatkan dari sumber – sumber tertentu yang didapat sebagai objek penelitian. Data sekunder atau data tambahan ini sendiri biasanya diperoleh dari sumber – sumber terdahulu seperti contohnya seperti buku, jurnal dan lain – lain.

2. Berdasarkan sifat-sifatnya

Suatu data ini juga dapat dibedakan dengan berdasarkan sifat – sifatnya ialah data kualitatif dan juga data kuantitatif. Kedua jenis data tersebut juga sering digunakan dalam berbagai kesempatan penelitian yang pernah dilakukan sebelumnya Data kualitatif tersebut biasanya banyak dijumpai didalam berbentuk pernyataan verbal, gambar atau juga bahkan simbol. Data kuantitatif tersebut lebih mengarah kepada pernyataan dengan secara terbilang atau angka.

3. Berdasarkan waktu pengambilannya

Selanjutnya suatu data ini juga dapat dikelompokkan dengan berdasarkan waktu pengambilan atau pengumpulannya. Terdapat jenis data yang dikumpulkan dengan secara berkala dan juga data cross section. Data berkala ini dapat kita temukan dalam kegiatan atau aktivitas survey penduduk, data kebutuhan penduduk dalam setahun terakhir. Data cross section atau data yang terkumpul pada

waktu tertentu ini contohnya seperti data hasil ujian siswa yang diperoleh setelah ujian itu telah selesai dilaksanakan.

Sebenarnya apabila dibahas lebih dalam lagi masih terdapat banyak parameter – parameter pengelompokkan suatu data seperti dengan berdasarkan susunan, rasio serta masih banyak lagi namun ketiga parameter diatas inilah yang paling sering ditemui di masyarakat.

2.3 *Kriptografi*

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu *kriptografi*, terdapat dua buah proses yaitu melakukan *enkripsi* dan *dekripsi*. Pesan yang akan dienkripsi disebut sebagai *plaintext* (teks biasa). Algoritma yang dipakai untuk *mengenkripsi* dan *mendekripsi* sebuah *plaintext* melibatkan penggunaan suatu bentuk kunci. Pesan *plaintext* yang telah dienkripsi (atau dikodekan) dikenal sebagai *ciphertext* (teks sandi) (Fresly, Indah & Awang, 2015).

2.3.1 *Enkripsi*

Enkripsi (Encryption) adalah sebuah proses menjadikan pesan yang dapat dibaca (*plaintext*) menjadi pesan acak yang tidak dapat dibaca (*ciphertext*).

2.3.2 *Dekripsi*

Deskripsi merupakan proses kebalikan dari enkripsi dimana proses ini akan mengubah *ciphertext* menjadi *plaintext* dengan menggunakan algoritma "pembalik" dan *key* yang sama.

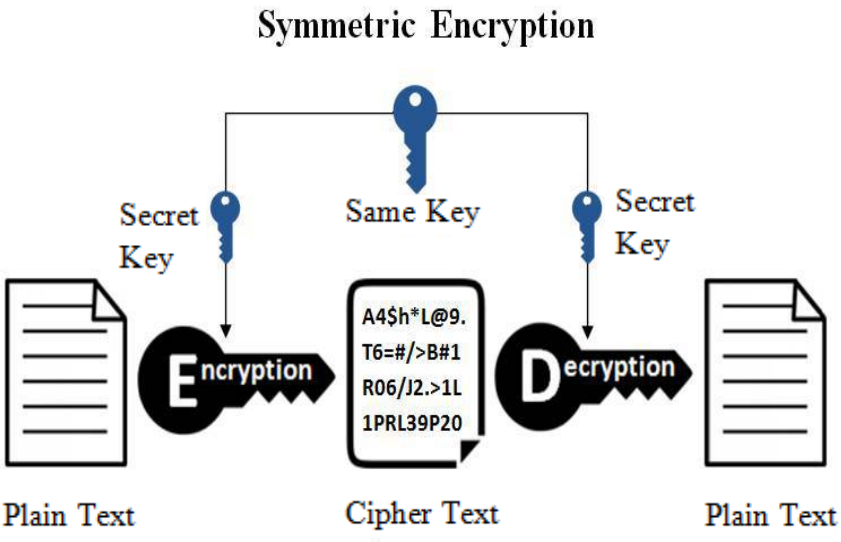
2.3.3 *Kunci (key)*

parameter yang digunakan untuk transformasi *enkripsi* dan *dekripsi*. Kunci biasanya berupa *string* atau deretan bilangan.

Dengan menggunakan kunci K, maka fungsi *enkripsi* dan *dekripsi* dapat ditulis sebagai skema diperlihatkan pada Gambar berikut:

1. Algoritma Sandi Kunci Simetris

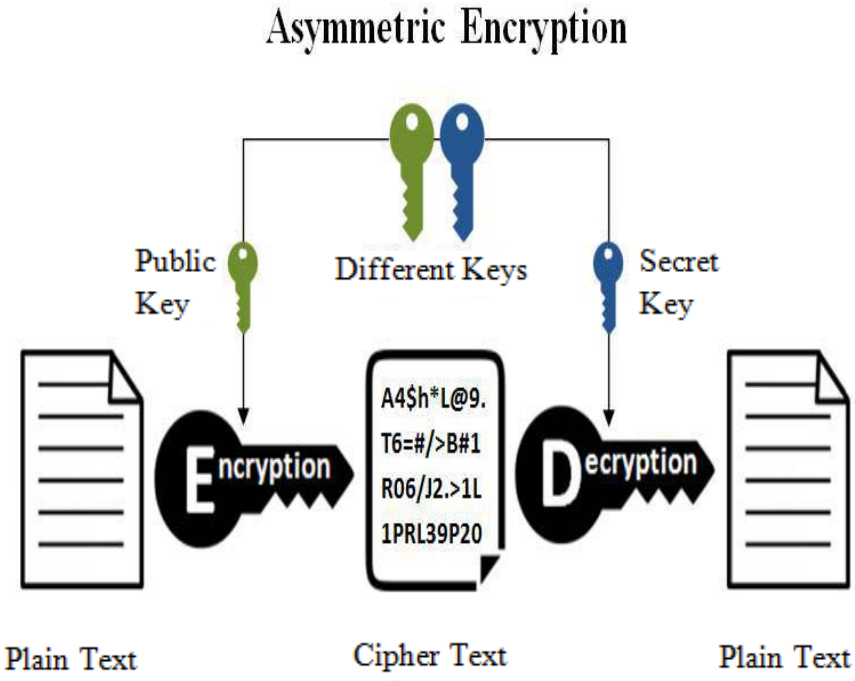
   Skema algoritma sandi akan disebut kunci simetris apabila untuk setiap proses enkripsi maupun dekripsi data secara keseluruhan digunakan kunci yang sama.



Sumber : JTsiskom (2015)

2. Algoritma Sandi Kunci Asimetris

Skema ini adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Skema ini disebut juga sebagai sistem kriptografi kunci publik karena kunci untuk enkripsi dibuat untuk diketahui oleh umum (public key) atau dapat diketahui siapa saja, tapi untuk proses dekripsinya hanya dapat dilakukan oleh yang berwenang yang memiliki kunci rahasia untuk mendekripsinya, disebut private key.



Gambar 2.2 Kunci Asimetris

Sumber : JTsiskom (2015)

Dalam penerapannya, Kriptografi memiliki tujuan untuk memberi layanan keamanan antara lain: kerahasiaan (*confidentiality*), integritas data (*data integrity*), otentikasi (*authentication*), dan penyangkalan(*non-repudiation*).

1. Kerahasiaan (*confidentiality*) mengacu pada layanan perlindungan informasi agar tidak dapat dibaca oleh pihak-pihak yang tidak berhak. Pihak yang tidak diinginkan, yang disebut musuh harus tidak dapat mengakses materi komunikasi.
2. Integritas data (*data integrity*) merupakan layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama masa pengiriman.
3. Otentikasi (*authentication*) ialah pelayanan yang berkaitan dengan pengidentifikasian, baik dari hal kebenaran pihak-pihak yang melakukan komunikasi (*user authentication*) maupun keaslian pesan (*data origin authentication*). Kedua belah pihak yang melakukan komunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan.
4. Penyangkalan (*Non-repudiation*) merupakan sebuah pembuktian penerima bahwa pengirim memang yang mengirim pesan, dan pembuktian pengirim bahwa penerima memang yang menerima pesan.

2.4 Enkripsi

Enkripsi (encryption) merupakan proses yang dilakukan untuk meyandikan plaintext sehingga menjadi ciphertext (Akim & Yani, 2014).

Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan

integritas dan autentikasi dari sebuah pesan. Contohnya, Message Authentication Code (MAC) atau digital signature. Penggunaan yang lain yaitu untuk melindungi dari analisis jaringan komputer.

2.4.1 Manfaat Enkripsi

1. Beberapa manfaat yang bisa didapatkan dari enkripsi ini adalah :
2. Kerahasiaan suatu informasi terjamin
3. Menyediakan authentication dan perlindungan integritas pada algoritma checksum/hash
4. Menanggulangi penyadapan telepon dan email
5. Untuk digital signature. Digital signature adalah menambahkan suatu baris statemen pada suatu elektronik copy dan mengenkripsi statemen tersebut dengan kunci yang kita miliki dan hanya pihak yang memiliki kunci dekripsinya saja yang bisa membukanya.
6. Untuk digital cash

2.4.2 Kerugian Enkripsi

Penyalahgunaan dan kerugian dari enkripsi adalah:

1. Penyandian rencana teroris
2. Penyembunyian record criminal oleh seorang penjahat
3. Pesan tidak bisa dibaca bila penerima pesan lupa atau kehilangan kunci (decryptor).

2.5 Dekripsi

Dekripsi (decryption) merupakan proses yang dilakukan untuk memperoleh kembali plaintext dari ciphertext (Akim & Yani, 2014).

Secara etimologis kata "dekripsi" diadaptasi dari bahasa latin *"describere"* yang artinya menggambarkan atau memberikan penjelasan mengenai suatu hal. Sehingga pengertian dekripsi adalah suatu bentuk karangan yang melukiskan sesuatu sesuai dengan keadaan yang sebenarnya, sehingga pembaca seolah-olah dapat melihat, mendengar, dan merasakan apa yang digambarkan penulis.

2.5.1 Ciri-Ciri Teks Dekripsi

Terdapat unsur-unsur teks dekripsi yang khas, meliputi ciri dan karakteristik teks dekripsi seperti gaya bahasa dan isinya. Berikut merupakan unsur dan ciri-ciri teks dekripsi selengkapnya.

1. Menggambarkan suatu objek seperti benda, tempat atau suasana tertentu.
2. Melibatkan panca indera seperti penglihatan, pendengaran, pengecapan, penciuman dan perabaan.
3. Mengungkapkan ciri-ciri fisik dan sifat objek seperti ukuran, bentuk, warna dan sifat objek.
4. menjelaskan objek dengan jelas, detail dan terperinci.
5. Menggunakan kata-kata atau frasa yang bermakna kata sifat atau keadaan.

2.5.2 Jenis-Jenis Teks Dekripsi

Terdapat beberapa macam-macam teks dekripsi jika dilihat dari isi teksnya. Berikut adalah jenis-jenis teks dekripsi dan pengertiannya lengkap.

1. **Teks dekripsi subjektif**

   Pengertian teks dekripsi subjektif adalah teks dekripsi yang dalam penggambaran objeknya berdasarkan atas kesan yang dimiliki oleh penulis paragraf tersebut.

2. **Teks dekripsi spatial**

   Pengertian teks dekripsi spatial adalah teks dekripsi dimana objek yang dijelaskan hanya berupa benda, tempat, ruang dan lain sebagainya.

3. **Teks dekripsi objektif**

   Pengertian teks dekripsi objektif adalah jenis teks dekripsi dimana penjelasan mengenai objek digambarkan apa adanya berdasarkan keadaan objek yang sebenarnya, tanpa ada tambahan opini dari penulis.

2.5.3 Struktur Teks Dekripsi

Secara umum terdapat 3 struktur teks dekripsi yang meliputi identifikasi, klasifikasi serta bagian dekripsi atau bagian inti. Berikut adalah 3 struktur teks dekripsi dan pengertiannya.

1. Identifikasi

   Pengertian identifikasi pada teks deskripsi adalah bagian yang berisikan penentuan dari identitas seseorang, benda, atau objek lainnya.

2. Klasifikasi

   Pengertian klasifikasi pada teks deskripsi adalah unsur penyusun yang bersistem dalam suatu kelompok menurut kaidah atau standar yang sebelumnya sudah ditetapkan.

3. Bagian Deskripsi

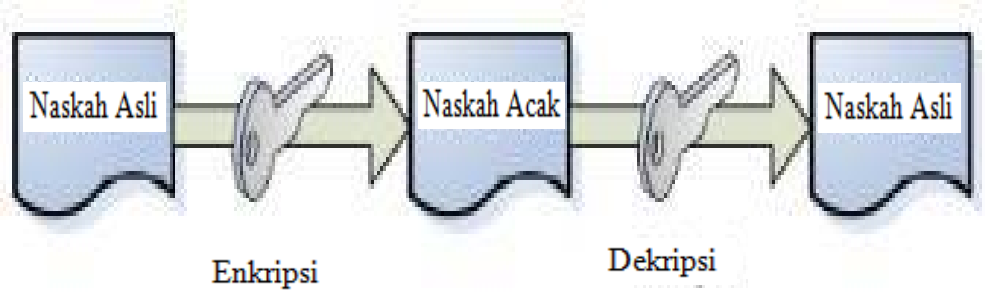
   Pengertian bagian deskripsi atau bagian inti pada paragraf deskripsi adalah bagian yang berisikan gambaran atau pemaparan tentang suatu objek atau topik yang dibahas.

2.6 Kriptografi Klasik

Kriptografi klasik merupakan kriptografi yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. Kriptografi ini melakukan pengacakan huruf pada kata terang / plaintext. Kriptografi ini hanya melakukan pengacakan pada huruf A – Z, dan sangatlah tidak disarankan untuk mengamankan informasi-informasi penting karena dapat dipecahkan dalam waktu singkat.

Algoritma kriptografi klasik memiliki ciri diantaranya berbasis karakter dan menggunakan kunci simetri. Dalam kriptografi klasik, teknik enkripsi yang

digunakan adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi (M. Miftakul, 2016).



Gambar 2.3 Proses enkripsi dan deskripsi
Sumber : M. Miftakul (2016)

Biarpun telah ditinggalkan, kriptografi klasik tetap dapat ditemui disetiap pelajaran kriptografi sebagai pengantar kriptografi modern.

Kriptogarfi klasik memiliki beberapa ciri :

1. Berbasis karakter
2. Menggunakan pena dan kertas saja, belum ada computer
3. Termasuk ke dalam kriptografi kunci simetris.

Tiga alasan mempelajari algoritma klasik :

1. Memahami konsep dasar kriptografi
2. Dasar algoritma kriptografi modern
3. Memahami kelemahan sistem kode

Pada dasarnya, algoritma kriptografi klasik dapat dikelompokkan ke dalam dua macam cipher, yaitu :

1. Cipher substitusi (substitution cipher)

   Di dalam cipher substitusi setiap unit plainteks diganti dengan satu unit cipherteks. Satu “unit” di isini berarti satu huruf, pasanga huruf,

atau dikelompokkan lebih dari dua huruf. Algoritma substitusi tertua yang diketahui adalah Caesar cipher yang digunakan oleh kaisar Romawi , Julius Caesar (sehingga dinamakan juga casear cipher), untuk mengirimakan pesan yang dikirimkan kepada gubernurnya.

metode substitusi, yang dibagi lagi menjadi 2 yaitu:

a. monoalphabetic , setiap huruf pesan disubstitusi oleh satu huruf kunci
b. polyalphabetic , setiap huruf pesan disubstitusi oleh beberapa huruf kunci dengan pola tertentu.

2. Cipher transposisi (transposition cipher)

Pada cipher transposisi, huruf-huruf di dalam plainteks tetap saja, hanya saja urutannya diubah. Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (scrambling) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karkater tersebut.

Metode substitusi adalah metode enkripsi dengan mengganti tiap-tiap huruf pesan dengan kunci tertentu menjadi huruf lain. Contohnya adalah Caesar Cipher (monoalphabetic) dan Viginere Cipher (polyalphabetic).

Metode transposisi adalah metode enkripsi dengan memindahkan posisi tiap-tiap huruf pesan dengan pola tertentu. Contohnya adalah Blocking Cipher dan Permutation.

2.7 Pemrograman

Pemrograman adalah proses menulis, menguji dan memperbaiki (*debug*), dan memelihara *kode* yang membangun suatu program komputer. *Kode* ini ditulis dalam berbagai bahasa pemrograman. Tujuan dari pemrograman adalah untuk memuat suatu program yang dapat melakukan suatu perhitungan atau 'pekerjaan' sesuai dengan keinginan si pemrogram. Untuk melakukan pemrograman, diperlukan keterampilan dalam *algoritma*, *logika*, bahasa *pemrograman*, dan pada banyak kasus, pengetahuan-pengetahuan lain seperti matematika.

Pemrograman adalah suatu seni dalam menggunakan satu atau lebih *algoritma* yang saling berhubungan dengan menggunakan suatu bahasa pemrograman tertentu sehingga menjadi suatu program komputer. Bahasa pemrograman yang berbeda mendukung gaya pemrograman yang berbeda pula. Gaya pemrograman ini biasa disebut *paradigma* pemrograman.

Apakah memprogram perangkat *lunak* lebih merupakan seni, ilmu, atau *teknik* telah lama diperdebatkan. Pemrogram yang baik biasanya meng*kombinasi*kan ketiga hal tersebut, agar dapat menciptakan program yang *efisien*, baik dari sisi saat dijalankan (*run time*) atau memori yang digunakan.
Menurut tingkat kedekatannya dengan mesin komputer, bahasa pemrograman terdiri dari :

1. Bahasa mesin, yang memberikan perintah ke komputer dengan menggunakan kode bahasa biner, misalnya 01100101100110.
2. Bahasa tingkat rendah, atau dikenal sebagai bahasa assembly (bah.Inggris Assembly), yang memberikan perintah ke komputer dengan menggunakan kode pendek (kode mnemonic), misalnya [kode_mesin | MOV], SUB, CMP,JMP,JGE,JL,LOOP,dll. Inggris Intermediate, yang merupakan bahasa komputer yang menggunakan campuran instruksi dalam kata-kata bahasa manusia lihat contoh di bawah Bahasa Tingkat Tinggi dan instruksi yang bersifat simbolik, misalnya, {,},?, <<, >> , &&, ||, dll.
3. Bahasa tingkat tinggi, yang merupakan bahasa komputer yang menggunakan instruksi berasal dari unsur kata-kata bahasa manusia, misalnya, mulai, akhir, jika, sementara, dan, atau, dll Komputer dapat memahami compiler bahasa manusia atau penerjemah program yang dibutuhkan.

Kebanyakan bahasa pemrograman diklasifikasikan sebagai High Level Languages, hanya bahasa C yang digolongkan sebagai Menengah dan Majelis Bahasa yang merupakan Rendah Bahasa.

2.8 Desktop

Aplikasi Desktop adalah suatu *aplikasi* yang mampu beroperasi secara *offline*, tetapi kita harus meng*instal*nya sendiri pada laptop atau komputer.

2.8.1 Keunggulan Dekstop

1. Dapat berjalan dengan *independen,* tanpa perlu menggunakan *browser.*
2. Tidak perlu *koneksi internet*, karena semua *file* yang diperlukan untuk menjalankan *aplikasi*nya sudah ter*install* sebelumnya.
3. Dapat dengan mudah me*modifikasi settingan*nya.
4. Prosesnya lebih cepat.

2.8.2 Kekurangan Dekstop

1. Apabila akan menjalankan *aplikasi*, harus di*instal* terlebih dahulu di komputer.
2. Bermasalah dengan *lisensi*. Hal ini membutuhkan *lisensi* yang banyak pada setiap computer
3. *Aplikasi* tidak dapat dibuka di computer lain, jika belum di*install*
4. Biasanya memerlukan *hardware* dengan *spesifikasi* tinggi.

2.9 Informasi

Informasi adalah data yang telah diolah menjadi bentuk yang memiliki arti bagi sipenerima dan bermanfaat bagi pengambilan keputusan saat ini atau mendatang. Secara umum Informasi adalah hasil pemrosesan data yang diperoleh dari setiap elemen sistem menjadi bentuk yang mudah dipahami dan merupakan pengetahuan yang relevan dan berguna. Adapun fungsi-fungsi informasi adalah sebagai berikut:

1. Untuk meningkatkan pengetahuan bagi si pemakai.
2. Untuk mengurangi ketidak pastian dalam proses pengambilan keputusan pemakai.
3. Menggambarkan keadaan yang sebenarnya dari sesuatu hal.Informasi yang berkualitas harus akurat, tepat dan *relevan*.

Sumber dari informasi adalah data. Data adalah kenyataan yang menggambarkan suatu kejadian-kejadian dan kesatuan nyata. Data merupakan bentuk yang masih mentah, belum dapat bercerita banyak sehingga perlu diolah lebih lanjut. Data diolah melalui suatu metode untuk menghasilkan informasi. Data dapat berbentuk simbol-simbol semacam huruf, angka, bentuk suara, sinyal, gambar, dan sebagainya.

2.10 Flowchart

Flowchart merupakan penyajian yang sistematis tentang proses dan logika dari kegiatan penanganan informasi atau penggambaran secara grafik dari langkah-langkah dan urut-urutan prosedur dari suatu program. Bagan alir (*flowchart*) adalah bagan (*chart*) yang menunjukkan alir (*flow*) di dalam program atau prosedur sistem secara logika (Muslim & Ali, 2013).

2.10.1 Jenis Jenis Flowchart / Bagan Alir

Dalam flowchart terdapat beberapa jenis-jenis, Berikut ini adalah penjelasan dari jenis-jenis flowchart :

1. System Flowchart

System flowchart dapat didefinisikan sebagai bagan yang menunjukkan arus pekerjaan secara keseluruhan dari sistem. Bagan ini menjelaskan urut-urutan dari prosedur-prosedur yang ada di dalam sistem. Bagan alir sistem menunjukkan apa yang dikerjakan di sistem.

2. Document Flowchart

Bagan alir dokumen (*document flowchart*) atau disebut juga bagan alir formulir (*form flowchart*) atau *paperwork flowchart* merupakan bagan alir yang menunjukkan arus dari laporan dan formulir termasuk tembusan-tembusannya.

3. Schematic Flowchart

Bagan alir skematik (*schematic flowchart*) merupakan bagan alir yang mirip dengan bagan alir sistem, yaitu untuk menggambarkan prosedur di dalam sistem. Perbedaannya adalah, bagan alir skematik selain menggunakan simbol-simbol bagan alir sistem, juga menggunakan gambar-gambar komputer dan peralatan lainnya yang digunakan. Maksud penggunaan gambar-gambar ini adalah untuk memudahkan komunikasi kepada orang yang kurang paham dengan simbol-simbol bagan alir. Penggunaan gambar-gambar ini memudahkan untuk dipahami, tetapi sulit dan lama menggambarnya.

4. Program Flowchart

Bagan alir program (*program flowchart*) merupakan bagan yang menjelaskan secara rinci langkah-langkah dari proses program. Bagan alir program dibuat dari derivikasi bagan alir sistem. Bagan alir program dapat terdiri dari dua macam, yaitu bagan alir logika program (*program logic flowchart*) dan bagan alir program komputer terinci (*detailed computer program flowchart*). Bagan alir logika program digunakan untuk menggambarkan tiap-tiap langkah di dalam program komputer secara logika. Bagan alat- logika program ini dipersiapkan oleh analis sistem. Gambar berikut menunjukkan bagan alir logika program. Bagan alir program komputer terinci (*detailed computer program flow-chart*) digunakan untuk menggambarkan instruksi-instruksi program komputer secara terinci. Bagan alir ini dipersiapkan oleh pemrogram.

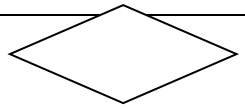
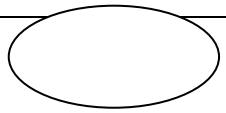
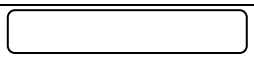
5. Process Flowchart

Bagan alir proses (process flowchart) merupakan bagan alir yang banyak digunakan di teknik industri. Bagan alir ini juga berguna bagi analis sistem untuk menggambarkan proses dalam suatu prosedur.

2.10.2 Simbol - Simbol Flowchart / Bagan Alir

Dalam flowchart terdapat beberapa jenis-jenis, Berikut ini adalah tabel simbol-simbol flowchart :

Tabel 2.1 Simbol-Simbol *Flowchart*

SIMBOL	**FUNGSI**
	Permulaan sub program
	Perbandingan, pernyataan, penyeleksian data yang memberikan pilihan untuk langkah selanjutnya
	Penghubung bagian-bagian flowchart yang berada pada satu halaman
	Penghubung bagianbagian flowchart yang berada pada halaman berbeda
	Permulaan/akhir program
	Arah aliran program
	Proses inisialisasi/pemberian harga awal
	Proses penghitung/ proses pengolahan dat
	Proses input/output data

Sumber : Santoso (2017)

2.11 Unified Modeling Language (UML)

Unified Modeling Language (UML) adalah bahasa spesifikasi standar yang dipergunakan untuk mendokumentasikan, menspesifikasikan dan membanngun perangkat lunak. *UML* merupakan metodologi dalam mengembangkan sistem berorientasi objek dan juga merupakan alat untuk mendukung pengembangan sistem.

UML sendiri juga memberikan standar penulisan sebuah sistem *blue print*, yang meliputi konsep bisnis proses, penulisan kelas-kelas dalam bahasa program yang spesifik, skema *database*, dan komponenkomponen yang diperlukan dalam sistem software (Suendri, 2018).

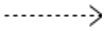
Tujuan *UML* adalah untuk menyediakan arsitek sistem, insinyur perangkat lunak, dan pengembang perangkat lunak dengan alat untuk analisis, perancangan, dan implementasi sistem berbasis softwarenya serta untuk pemodelan bisnis dan sejenisnya, proses (Hendro Purwoko, 2017).

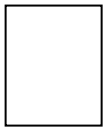
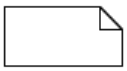
2.11.1 Use Case Diagram

Menggambarkan *external view* dari sistem yang akan kita buat modelnya, Model *use case* dapat dijabarkan dalam diagram *use case*, tetapi perlu diingat, diagram tidak indetik dengan model karena model lebih luas dari diagram. *Use case* harus mampu mengambarkan urutan aktor yang menghasilkan nilai terukur. Dengan menggunakan model ini diharapkan pengembangan piranti lunak dapat memenuhi semua kebutuhan pengguna dengan lengkap dan tepat, termasuk faktor-faktor seperti *scalability*, *robustnees*, *security*, dan sebagainya. Untuk

melakukan pemodelan sistem perangkat lunak secara visual digunakan UML (*Unified Modelling Language*) yang digambarkan secara elektronik lewat sarana perangkat lunak *Rational Rose*.

Tabel 2.2 Simbol *Use Case Diagram*

NO	GAMBAR	NAMA	KETERANGAN
1		*Actor*	Menspesifikasikan himpunan 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		*Generalization*	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.
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

Sumber : Gellysa Urva (2015)

2.11.2 *Activity* Diagram

Menunjukkan aktivitas sistem dalam bentuk kumpulan aksi-aksi, bagaimana masing-masing aksi tersebut dimulai, keputusan yang mungkin terjadi hingga berakhirnya aksi. *Activity* diagram juga dapat menggambarkan proses lebih dari satu aksi salam waktu bersamaan. "Diagram *activity* adalah aktifitas-aktifitas, objek, *state*, *transisi state* dan *event*. Dengan kata lain kegiatan diagram alur kerja menggambarkan perilaku sistem untuk aktivitas".

Tabel 2.3 Activity Diagram

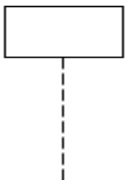
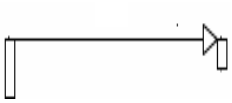
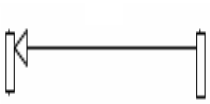
NO	GAMBAR	NAMA	KETERANGAN
1		*Actifity*	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain
2		*Action*	State dari sistem yang mencerminkan eksekusi dari suatu aksi
3		*Initial Node*	Bagaimana objek dibentuk atau diawali.
4		*Actifity Final Node*	Bagaimana objek dibentuk dan dihancurkan
5		*Fork Node*	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran

Sumber : Gellysa Urva (2015)

2.11.3 *Sequence* Diagram

Secara mudahnya *sequence diagram* adalah gambaran tahap demi tahap, termasuk kronologi (urutan) perubahan secara logis yang seharusnya dilakukan untuk menghasilkan sesuatu sesuai dengan *use case diagram*.

Tabel 2.4 Simbol *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

Sumber : Gellysa Urva (2015)

2.12 Algoritma

Algoritma adalah metode efektif yang diekspresikan sebagai rangkaian terbatas. Algoritma juga merupakan kumpulan perintah untuk menyelesaikan suatu masalah. Perintahperintah ini dapat diterjemahkan secara bertahap dari awal hingga akhir. Masalah tersebut dapat berupa apa saja, dengan syarat untuk setiap

permasalahan memiliki kriteria kondisi awal yang harus dipenuhi sebelum menjalankan sebuah algoritma. Algoritma juga memiliki pengulangan proses (iterasi), dan juga memiliki keputusan hingga keputusan selesai (Gun, 2017).

Dalam matematika dan ilmu komputer, algoritma adalah urutan atau langkah-langkah untuk penghitungan atau untuk menyelesaikan suatu masalah yang ditulis secara berurutan. Sehingga, algoritma pemrograman adalah urutan atau langkah-langkah untuk menyelesaikan masalah pemrograman komputer.

Dalam pemrograman, hal yang penting untuk dipahami adalah logika kita dalam berpikir bagaimana cara untuk memecahkan masalah pemrograman yang akan dibuat. Sebagai contoh, banyak permasalahan matematika yang mudah jika diselesaikan secara tertulis, tetapi cukup sulit jika kita terjemahkan ke dalam pemrograman. Dalam hal ini, algoritma dan logika pemrograman akan sangat penting dalam pemecahan masalah.

Berikut ini bentuk dasar algoritma:

1. Algoritma Sekuensial (*Sequence Algorithm*)
2. Algoritma Perulangan (*Looping Algorithm*)
3. Algoritma Percabangan atau Bersyarat (*Conditional Algorithm*)

Algoritma memiliki lima ciri utama yang saling berhubungan satu dengan lainnya. Menurut Donald E. Knuth, dapun kriteria algoritma adalah sebagai berikut:

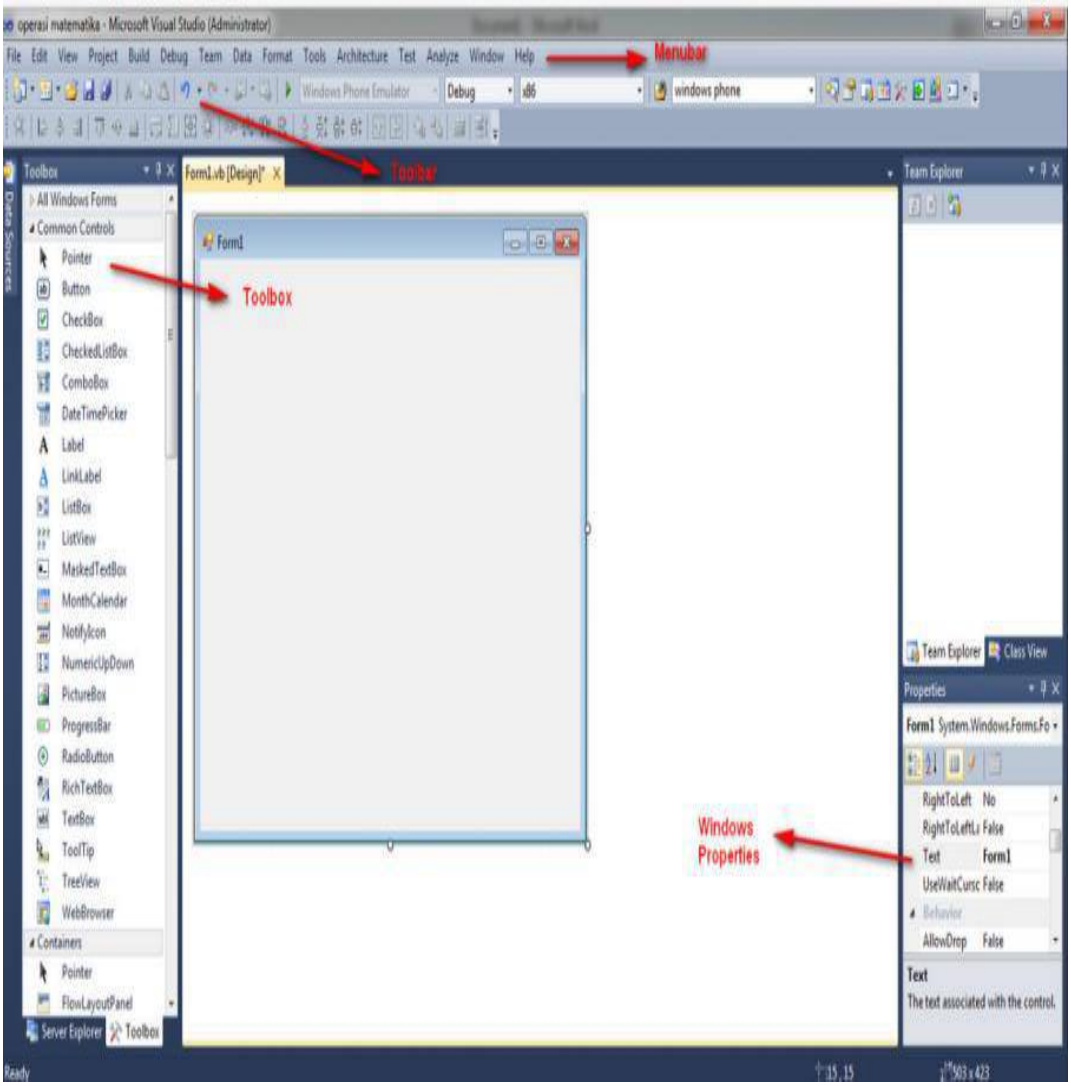
1. **Ada Input**, yaitu permasalahan yang dihadapi dan akan dicarikan solusinya. Algoritma memiliki nol atau lebih input (masukan).
2. **Ada Proses**, yaitu rencana atau langkah-langkah yang harus dilakukan untuk mencapai tujuan akhir.

3. **Ada Output**, yaitu solusi atau tampilan akhir yang didapatkan dari suatu algoritma. Algoritma memiliki minimal satu output.
4. **Ada intruksi-intruksi yang jelas dan tidak ambigu**, yaitu instrukti yang jelas dalam algoritma sehingga tidak terjadi kesalahan dalam menghasilkan output.
5. **Ada tujuan akhir yang dicapai**, yaitu akhir dari program dimana program akan berhenti ketika tujuan akhir telah tercapai.

2.13 Visual Basic 2010

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 basic* adalah 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*. (Ninuk & Syadid, 2017).

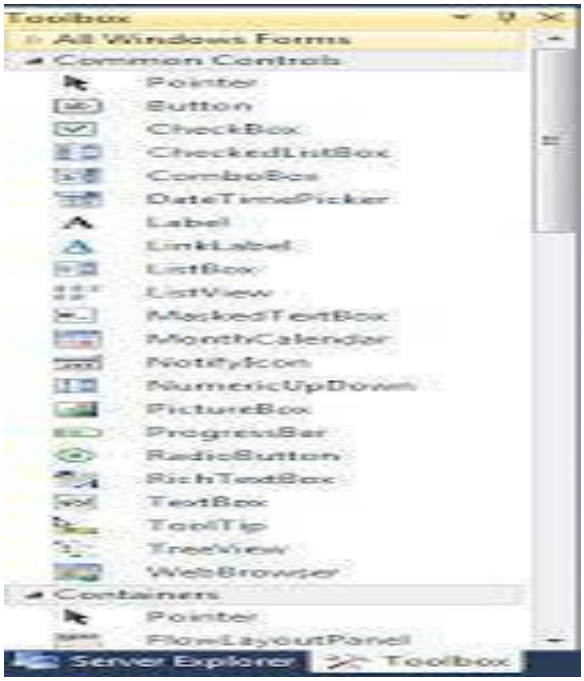
Toolbox ditempatkan disebelah kiri jendela kerja. Dibawah ini adalah *screenshot* tampilan *Visual Basic* 2010 :



Gambar 2.4 Tampilan VB 2010
Sumber : Indra (2013)

2.13.1 Toolbox

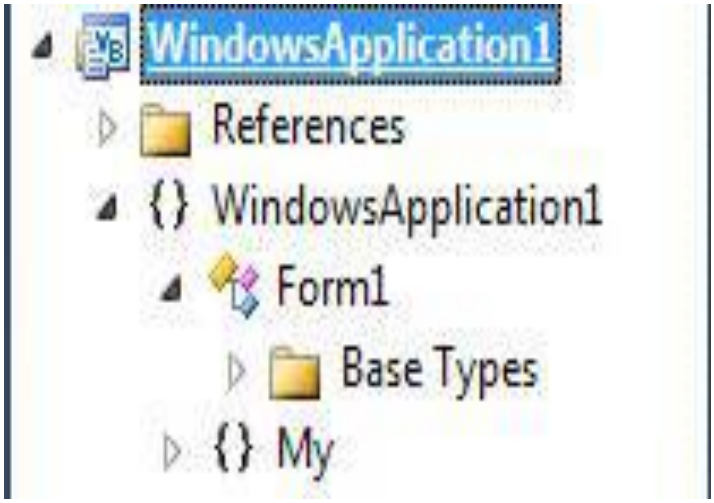
Toolbox merupakan komponen lingkungan kerja VB yang berisikan *tool-tool* untuk ditempatkan di *form*. Jika kita membuat sebuah aplikasi, maka komponen-komponen tersebut akan kita tempatkan di *form* dan menjadi komponen jendela program.



Gambar 2.5 Tampilan Toolbox
Sumber : Indra (2013)

2.13.2 Windows Project

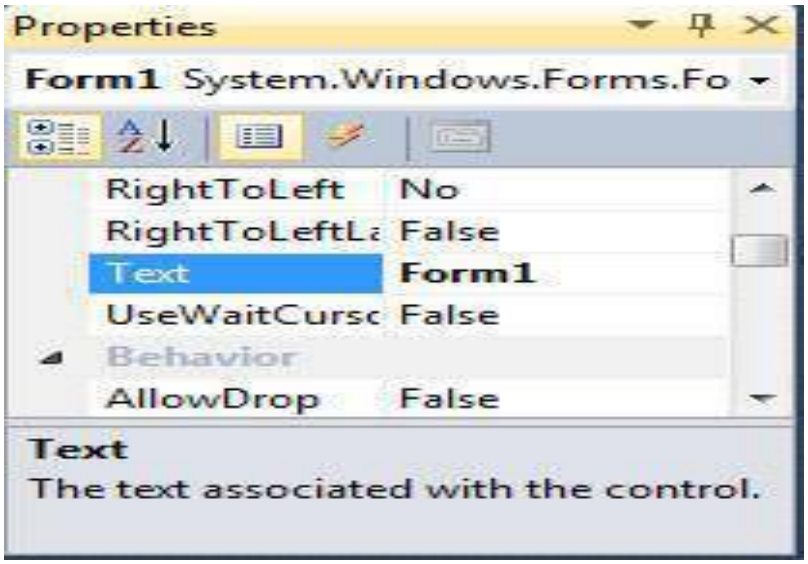
Window Project berfungsi untuk menampilkan daftar form dan modul yang terdapat di project aplikasi yang sedang dikerjakan.



Gambar 2.5 Tampilan *windows project*
Sumber : Indra (2013)

2.13.3 *Windows Properties*

Windows Properties berfungsi untuk menampilkan daftar properti dari sebuah komponen yang sedang aktif. Kita dapat mengubah properti dari sebuah komponen dengan cara mengaktifkan (mengklik/memilih) komponen tersebut, kemudian mengubah nilai propertinya di *Window Properties*.



Gambar 2.6 Tampilan *Windows properties*
Sumber : Indra (2013)

2.14 Tabel *ASCII*

ASCII (*American Standard Code for Information Interchange*) atau kode Standar Amerika untuk Pertukaran Informasi. Merupakan suatu standar internasional dalam kode huruf dan lumeri seperti *Hex* dan *Unicode* tetapi *ASCII* lebih bersifat *universal*, contohnya 124 adalah untuk karakter "|". Dalam *kriptografi*, kode *ASCII* ini merupakan urutan bit yang akan mewakili teks asli yang kemudian di*enkripsi* untuk mendapatkan teks kode dalam bentuk urutan bit.

ASCII memerlukan 8 bit untuk mendapatkan satu karakter dan blok kode mempunyai 64 bit untuk satu blok (Rizky & Muhammad, 2017).

Tabel 2.5 Tabel ASCII

ASCII control characters

DEC	HEX	Simbolo ASCII	
00	00h	NULL	(carácter nulo)
01	01h	SOH	(inicio encabezado)
02	02h	STX	(inicio texto)
03	03h	ETX	(fin de texto)
04	04h	EOT	(fin transmisión)
05	05h	ENQ	(enquiry)
06	06h	ACK	(acknowledgement)
07	07h	BEL	(timbre)
08	08h	BS	(retroceso)
09	09h	HT	(tab horizontal)
10	0Ah	LF	(salto de línea)
11	0Bh	VT	(tab vertical)
12	0Ch	FF	(form feed)
13	0Dh	CR	(retorno de carro)
14	0Eh	SO	(shift Out)
15	0Fh	SI	(shift In)
16	10h	DLE	(data link escape)
17	11h	DC1	(device control 1)
18	12h	DC2	(device control 2)
19	13h	DC3	(device control 3)
20	14h	DC4	(device control 4)
21	15h	NAK	(negative acknowle.)
22	16h	SYN	(synchronous idle)
23	17h	ETB	(end of trans. block)
24	18h	CAN	(cancel)
25	19h	EM	(end of medium)
26	1Ah	SUB	(substitute)
27	1Bh	ESC	(escape)
28	1Ch	FS	(file separator)
29	1Dh	GS	(group separator)
30	1Eh	RS	(record separator)
31	1Fh	US	(unit separator)
127	20h	DEL	(delete)

ASCII printable characters

DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo
32	20h	espacio	64	40h	@	96	60h	`
33	21h	!	65	41h	A	97	61h	a
34	22h	"	66	42h	B	98	62h	b
35	23h	#	67	43h	C	99	63h	c
36	24h	$	68	44h	D	100	64h	d
37	25h	%	69	45h	E	101	65h	e
38	26h	&	70	46h	F	102	66h	f
39	27h	'	71	47h	G	103	67h	g
40	28h	(	72	48h	H	104	68h	h
41	29h	)	73	49h	I	105	69h	i
42	2Ah	*	74	4Ah	J	106	6Ah	j
43	2Bh	+	75	4Bh	K	107	6Bh	k
44	2Ch	,	76	4Ch	L	108	6Ch	l
45	2Dh	-	77	4Dh	M	109	6Dh	m
46	2Eh	.	78	4Eh	N	110	6Eh	n
47	2Fh	/	79	4Fh	O	111	6Fh	o
48	30h	0	80	50h	P	112	70h	p
49	31h	1	81	51h	Q	113	71h	q
50	32h	2	82	52h	R	114	72h	r
51	33h	3	83	53h	S	115	73h	s
52	34h	4	84	54h	T	116	74h	t
53	35h	5	85	55h	U	117	75h	u
54	36h	6	86	56h	V	118	76h	v
55	37h	7	87	57h	W	119	77h	w
56	38h	8	88	58h	X	120	78h	x
57	39h	9	89	59h	Y	121	79h	y
58	3Ah	:	90	5Ah	Z	122	7Ah	z
59	3Bh	;	91	5Bh	[	123	7Bh	{
60	3Ch	<	92	5Ch	\	124	7Ch	|
61	3Dh	=	93	5Dh	]	125	7Dh	}
62	3Eh	>	94	5Eh	^	126	7Eh	~
63	3Fh	?	95	5Fh	_			

theASCIIcode.com.ar

Extended ASCII characters

DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo	DEC	HEX	Simbolo
128	80h	Ç	160	A0h	á	192	C0h	└	224	E0h	Ó
129	81h	ü	161	A1h	í	193	C1h	┴	225	E1h	ß
130	82h	é	162	A2h	ó	194	C2h	┬	226	E2h	Ô
131	83h	â	163	A3h	ú	195	C3h	├	227	E3h	Ò
132	84h	ä	164	A4h	ñ	196	C4h	─	228	E4h	õ
133	85h	à	165	A5h	Ñ	197	C5h	┼	229	E5h	Õ
134	86h	å	166	A6h	ª	198	C6h	ã	230	E6h	µ
135	87h	ç	167	A7h	º	199	C7h	Ã	231	E7h	þ
136	88h	ê	168	A8h	¿	200	C8h	╚	232	E8h	Þ
137	89h	ë	169	A9h	®	201	C9h	╔	233	E9h	Ú
138	8Ah	è	170	AAh	¬	202	CAh	╩	234	EAh	Û
139	8Bh	ï	171	ABh	½	203	CBh	╦	235	EBh	Ù
140	8Ch	î	172	ACh	¼	204	CCh	╠	236	ECh	ý
141	8Dh	ì	173	ADh	¡	205	CDh	═	237	EDh	Ý
142	8Eh	Ä	174	AEh	«	206	CEh	╬	238	EEh	¯
143	8Fh	Å	175	AFh	»	207	CFh	¤	239	EFh	´
144	90h	É	176	B0h	░	208	D0h	ð	240	F0h	
145	91h	æ	177	B1h	▒	209	D1h	Ð	241	F1h	±
146	92h	Æ	178	B2h	▓	210	D2h	Ê	242	F2h	‗
147	93h	ô	179	B3h	│	211	D3h	Ë	243	F3h	¾
148	94h	ò	180	B4h	┤	212	D4h	È	244	F4h	¶
149	95h	ò	181	B5h	Á	213	D5h	ı	245	F5h	§
150	96h	û	182	B6h	Â	214	D6h	Í	246	F6h	÷
151	97h	ù	183	B7h	À	215	D7h	Î	247	F7h	¸
152	98h	ÿ	184	B8h	©	216	D8h	Ï	248	F8h	°
153	99h	Ö	185	B9h	╣	217	D9h	┘	249	F9h	¨
154	9Ah	Ü	186	BAh	║	218	DAh	┌	250	FAh	·
155	9Bh	ø	187	BBh	╗	219	DBh	█	251	FBh	¹
156	9Ch	£	188	BCh	╝	220	DCh	▄	252	FCh	³
157	9Dh	Ø	189	BDh	¢	221	DDh	¦	253	FDh	²
158	9Eh	×	190	BEh	¥	222	DEh	Ì	254	FEh	■
159	9Fh	ƒ	191	BFh	┐	223	DFh	▀	255	FFh	

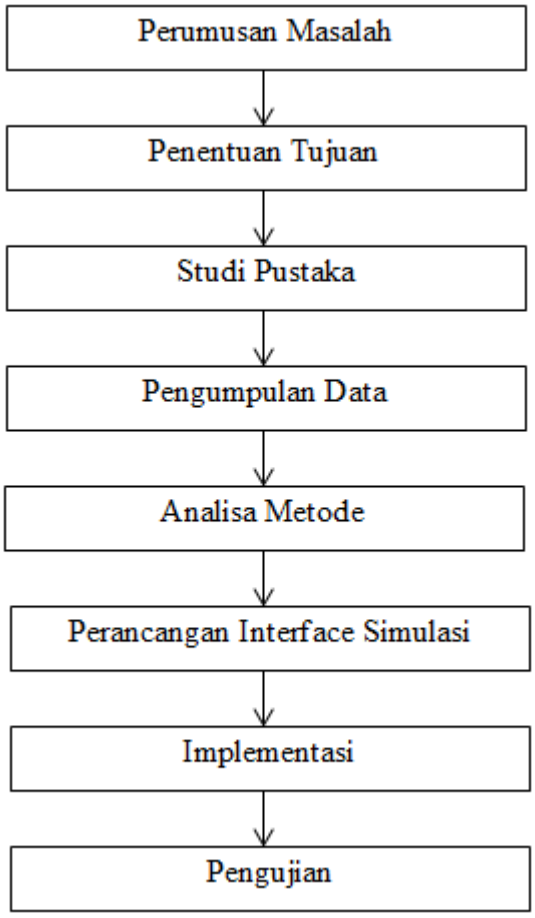
Sumber : Rizki (2014)

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Adapun tahapan penelitian yang dilakukan oleh penulis ini dengan judul implementasi algoritma *horizontal bit rotation* dalam mengamankan informasi adalah sebagai berikut :



3.2 Metode Pengumpulan Data

Pengumpulan data adalah pencarian terhadap sesuatu kerena ada perhatian dan keinginan terhadap hasil suatu aktivitas. Metode pengumpulan data dalam penulisan ini yaitu :

3.2.1 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 HBR

Pertukaran pesan rahasia dalam hal ini pesan rahasia berbentuk teks menggunakan kunci dengan metode *Horizontal* yaitu dengan proses *Horizontal*. Diagram dibawah adalah penggambaran bagaimana pertukaran pesan rahasia menggunakan proses *Horizontal*.

3.3.1 Proses Antarmuka HBR

Pada tahap ini penulis melakukan proses penginputan pesan rahasia berupa text dan kunci enkripsi dengan metode *Horizontal Bit Rotation* untuk proses enkripsi dan dekripsi.

3.3.2 Proses Enkrispi

Pada saat penginputan pesan text dan kunci, program akan memproses enkripsi dari plaintext menjadi chipertext.

3.3.3 Proses Dekripsi

Bila program sudah menampilkan chipertext maka selanjutkan proses deskripsi dimana dari chipertext akan kembali menjadi plaintext (kembali ke pesan awal) dan form di bawah akan menampilkan hasil akhir dari proses enkripsi dan dekripsi.

3.4 Rancangan Penelitian

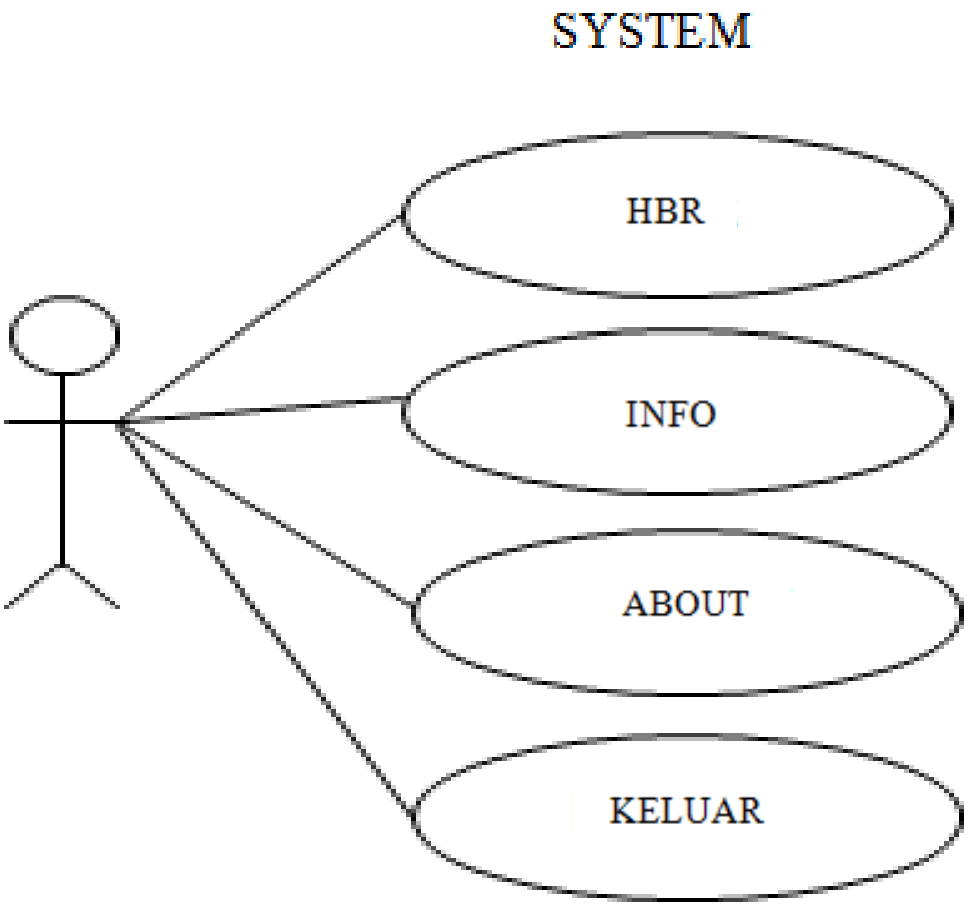
Analisis kebutuhan sistem merupakan analisis yang dibutuhkan untuk menentukan spesifikasi kebutuhan sistem. Spesifikasi ini juga meliputi elemen atau komponen – komponen apa saja yang dibutuhkan untuk sistem yang akan dibangun sampai dengan sistem tersebut diimplementasikan. Analisis kebutuhan ini juga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

3.4.1 Perancangan UML

Perancangan atau pemodelan berorientasi objek merupakan proses mendapatkan informasi dari model dan menampilkannya secara grafik dengan menggunakan sebuah standar elemen grafik.

3.4.1.1 *Use case Diagram*

Berikut adalah *use case diagram* yang menggambarkan kegiatan.



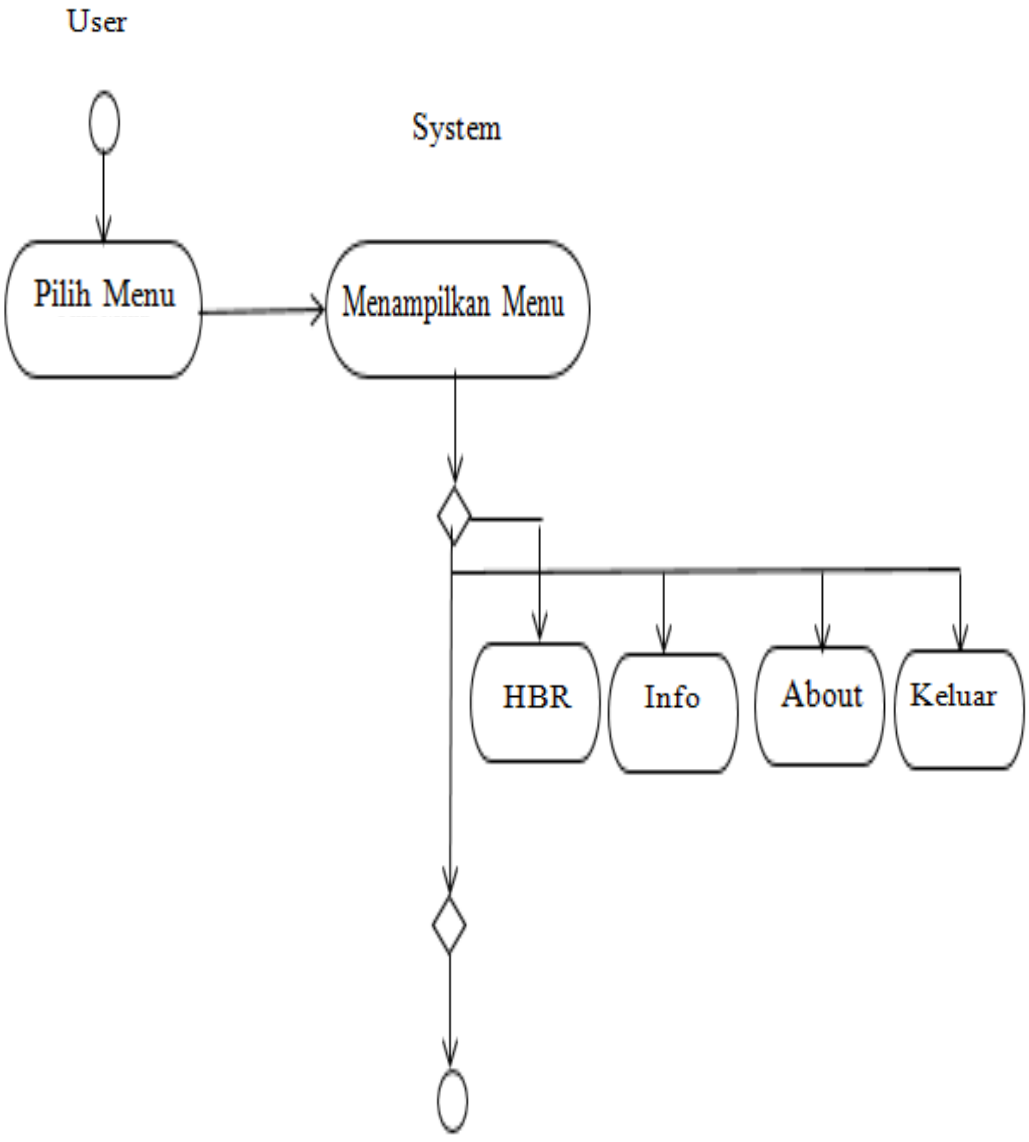
Gambar 3.2 *Use Case Diagram HBR*

Keterangan :

Dalam *use case diagram* di atas, user/pengguna sebagai actor yang mempunyai *use case* HBR, Info, About dan Keluar.

3.4.1.2 *Activity Diagram*

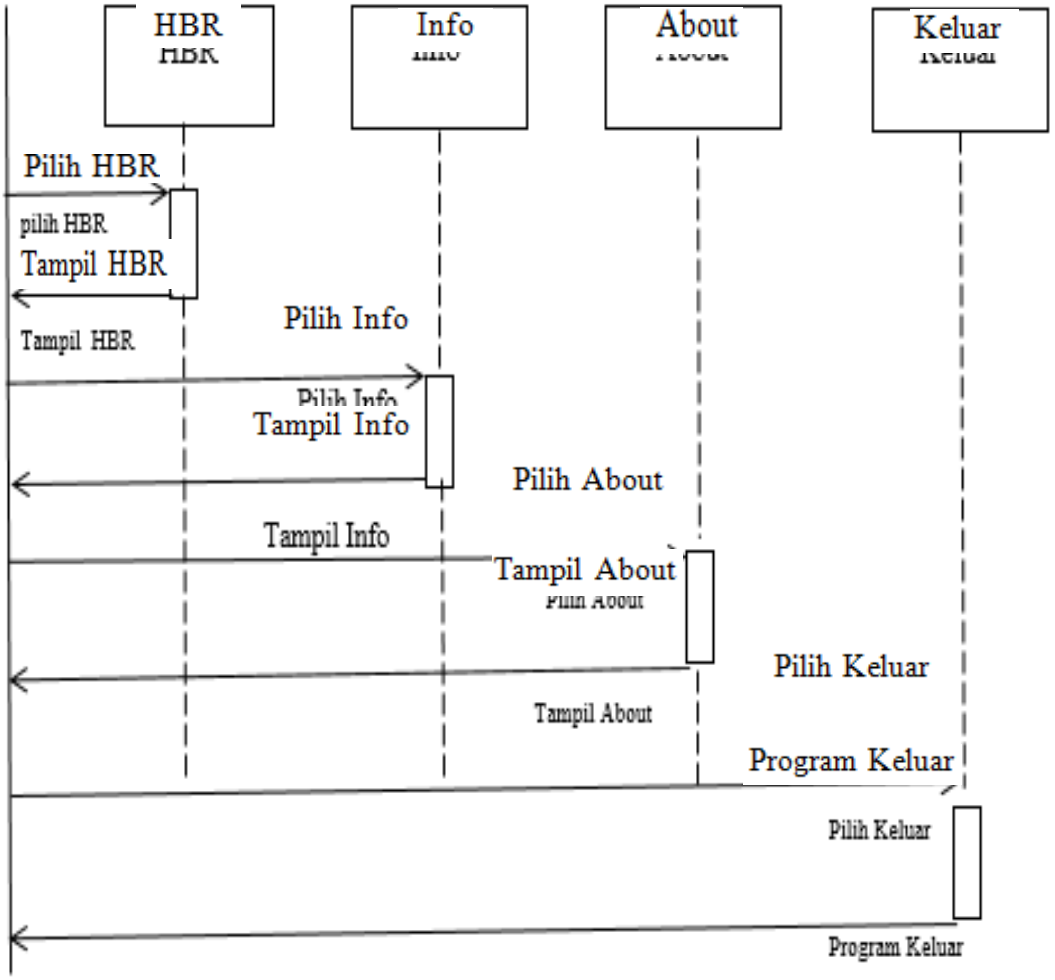
Activity diagram menggambarkan aktifitas-aktifitas yang terjadi dalam aplikasi dari aktivitas dimulai sampai aktivitas berhenti.



Gambar 3.3 *Activity Diagram HBR*

3.4.1.3 *Sequence Diagram*

Sequence Diagram menggambarkan tahap-tahap proses berjalannya program sesuai dengan *Use Case*.



Gambar 3.4 *Sequence Diagram HBR*

Keterangan :

1. Dalam diagram di atas menjelaskan bahwa bila *user* memilih menu HBR kemudian sistem menampilkan program untuk proses enkripsi dan deskripsi.

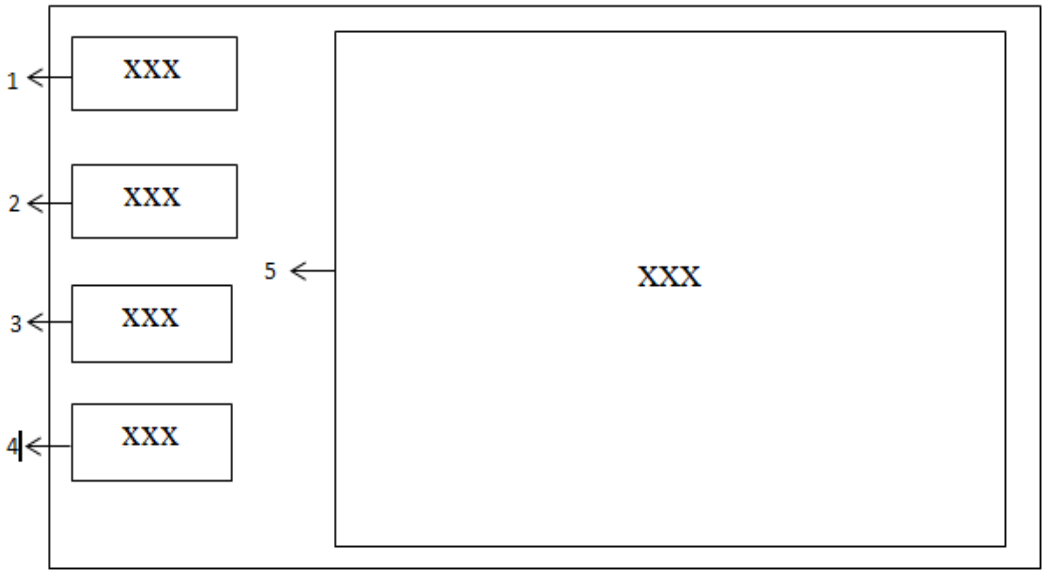
2. *User merequest* info kemudian sistem menampilkan informasi mengenai algoritma Horizontal Bit Rotation.
3. *User merequest* about kemudian sistem menampilkan data pribadi penulis.
4. *User merequest* menu keluar kemudian sistem akan keluar dari program.

3.4.2 Perancangan Antarmuka

Perancangan ini dibuat sebelum program yang asli berhasil di buat, agar dapat mempermudah dalam hal mendesain program.

3.4.2.1 Rancangan Halaman Menu

Halaman menu merupakan halaman yang pertama muncul pada saat program dijalankan.



Gambar 3.5 Rancangan Halaman Judul

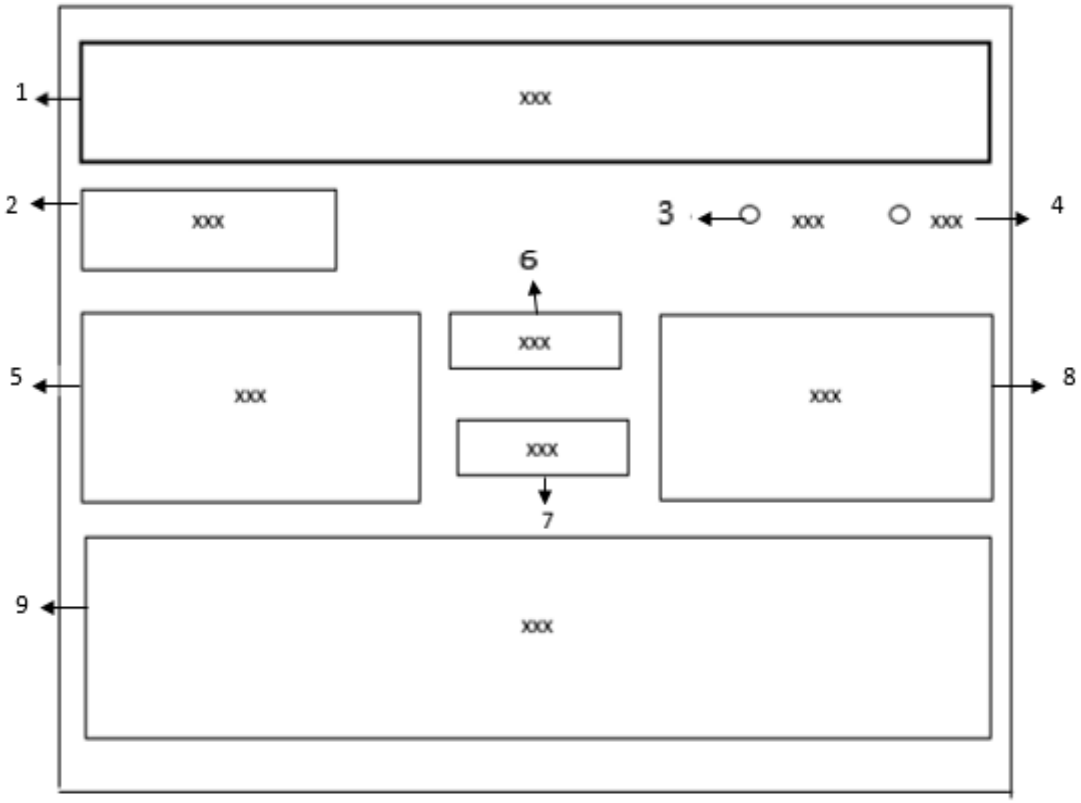
Pada tampilan di atas terdapat 4 tombol yaitu HBR, Info, *About* dan keluar.

Keterangan:

1. Berfungsi untuk menjalankan proses *enkripsi* dan *deskripsi*
2. Berfungsi untuk menampilakan keterangan mengenai *Algoritma Horizontal Bit Rotation.*
3. Berfungsi untuk menampilkan tentang data pribadi penulis.
4. Berfungsi untuk mengelurkan aktifitas program.
5. Berfungsi untuk menampilkan judul.

3.4.2.2 Rancangan Proses HBR

Form ini berisi proses *enkripsi* dan *deskripsi.*

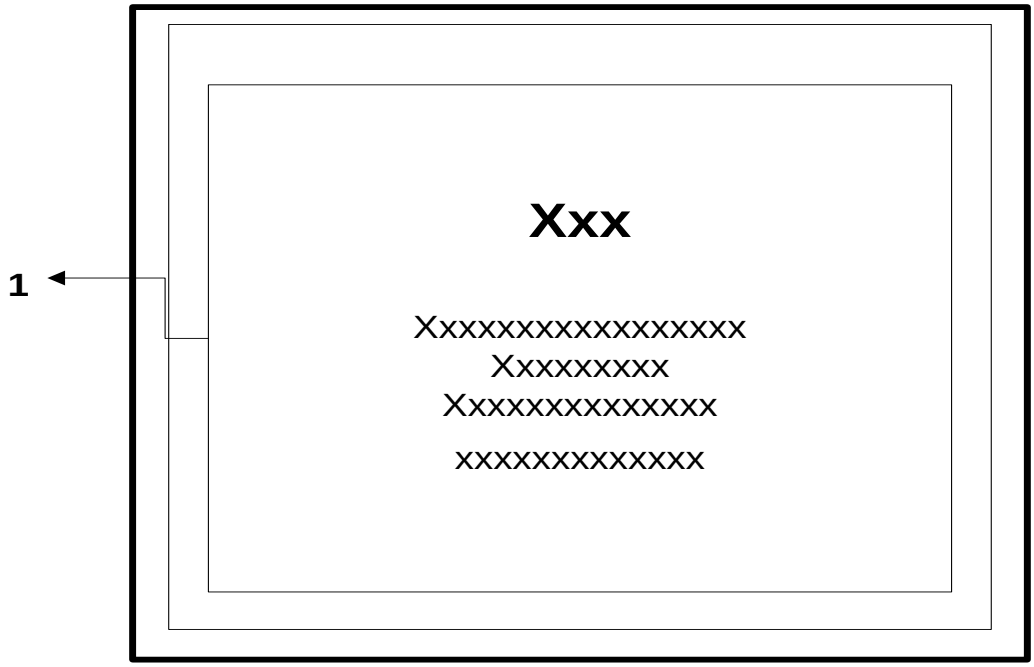


Gambar 3.6 Rancangan Proses HBR

Keterangan :

1. Palintext : Kolom pesan asli sebelum di *enkripsi*
2. Kunci : Kolom kunci (key)
3. Arah : untuk menentukan perputaran kunci
4. *Ciphertext* : kolom untuk menampilkan hasil *enkripsi*
5. *Enkripsi* : button untuk melakukan proses *enkripsi*
6. *Deskripsi* : button untuk melakukan proses *deskripsi*
7. *Plaintext* : digunakan untuk menampilkan pesan hasil *deskripsi*
8. *Log* : kolom untuk menampilkan penghitungan hasil *enkripsi* dan *deskripsi*

3.4.2.3 Rancangan Halaman Info



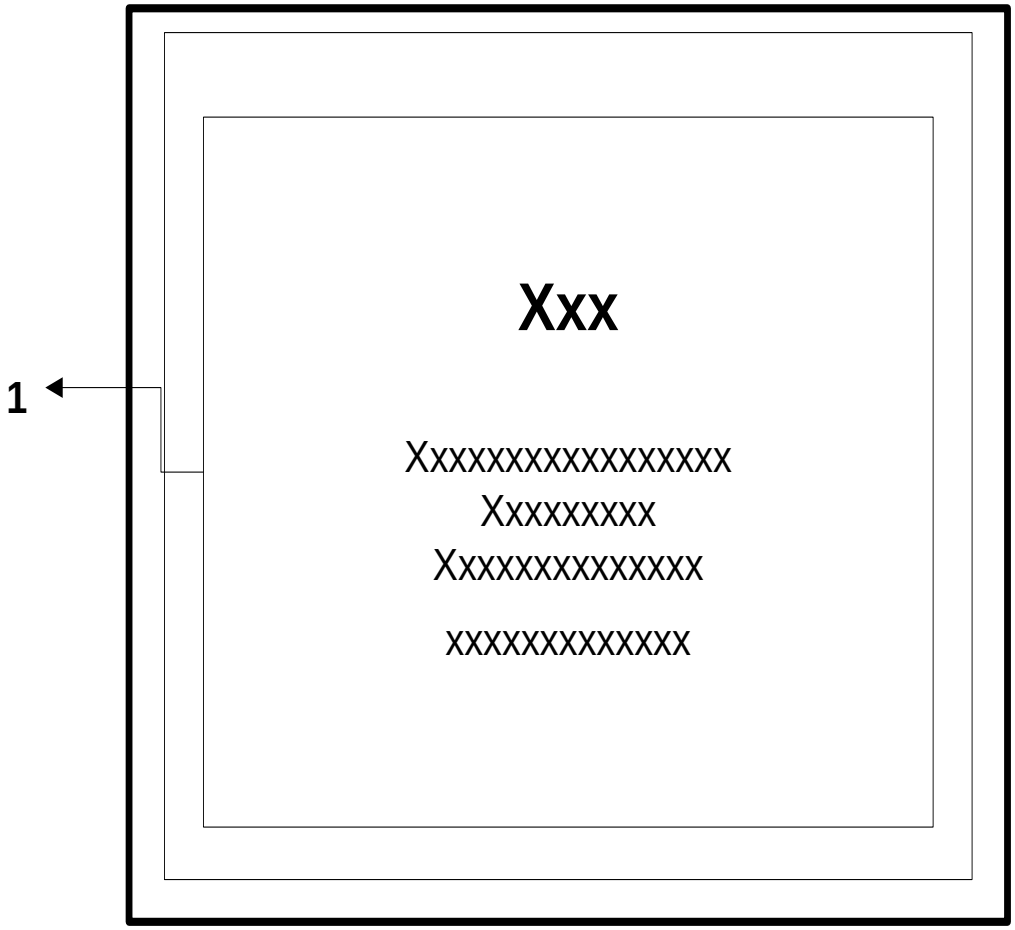
Gambar 3.7 Rancangan Halaman Info

Keterangan:

Halaman info menampilkan penjelasan mengenai *Horizontal Bit Rotation.*

3.4.2.4 Rancangan Halaman *About*

Berisi penjelasan mengenai data pribadi penulis.



Gambar 3.8 Rancangan Halaman *about*

Keterangan:

1. Berfungsi untuk menampilkan data pribadi penulis

BAB IV

HASIL DAN PEMBAHASAN

4.1 Kebutuhan Spesifikasi *Minimum Hardware* dan *Software*

Dalam membuat program ini di butuhkan *hardware* dan *software* yang dapat membantu dalam menyelesaikan program tersebut :

4.1.1 Perangkat Keras (*Hardware*)

Perangkat keras minimum yang digunakan untuk membangun keamanan dengan menggunakan algoritma horizontal bit rotation ini adalah

1. Processor
2. RAM 2 Gb
3. *Keyboard* dan *Mouse*
4. Monitor atau Laptop

4.1.2 Analisis Perangkat Lunak (*Software*)

Untuk mendukung membangun 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 :

1. *Microsoft Visual Studio* 2010

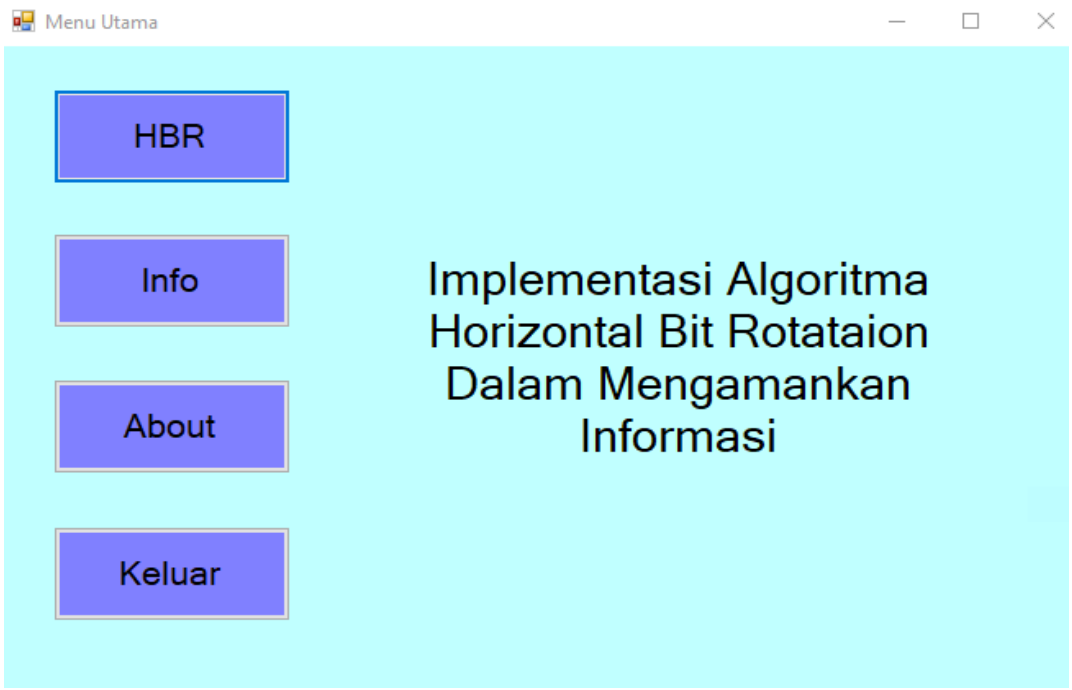
4.2 Pengujian Aplikasi dan Pembahasan

4.2.1 Implementasi Sistem

Tahap implementasi merupakan lanjutan dari tahap perancangan sistem. Pada tahap ini dilakukan implementasi sistem ke dalam bahasa pemrograman berdasarkan hasil analisa dan perancangan sistem. Pada tahap implementasi ini digunakan perangkat lunak dan perangkat keras, sehingga sistem yang dibangun dapat diselesaikan dengan baik.

4.2.1.1 Tampilan Halaman Menu

Halaman ini merupakan halaman yang muncul pertama sekali pada saat sistem dijalankan. Tampilan halaman menu yang dapat dilihat pada gambar berikut :



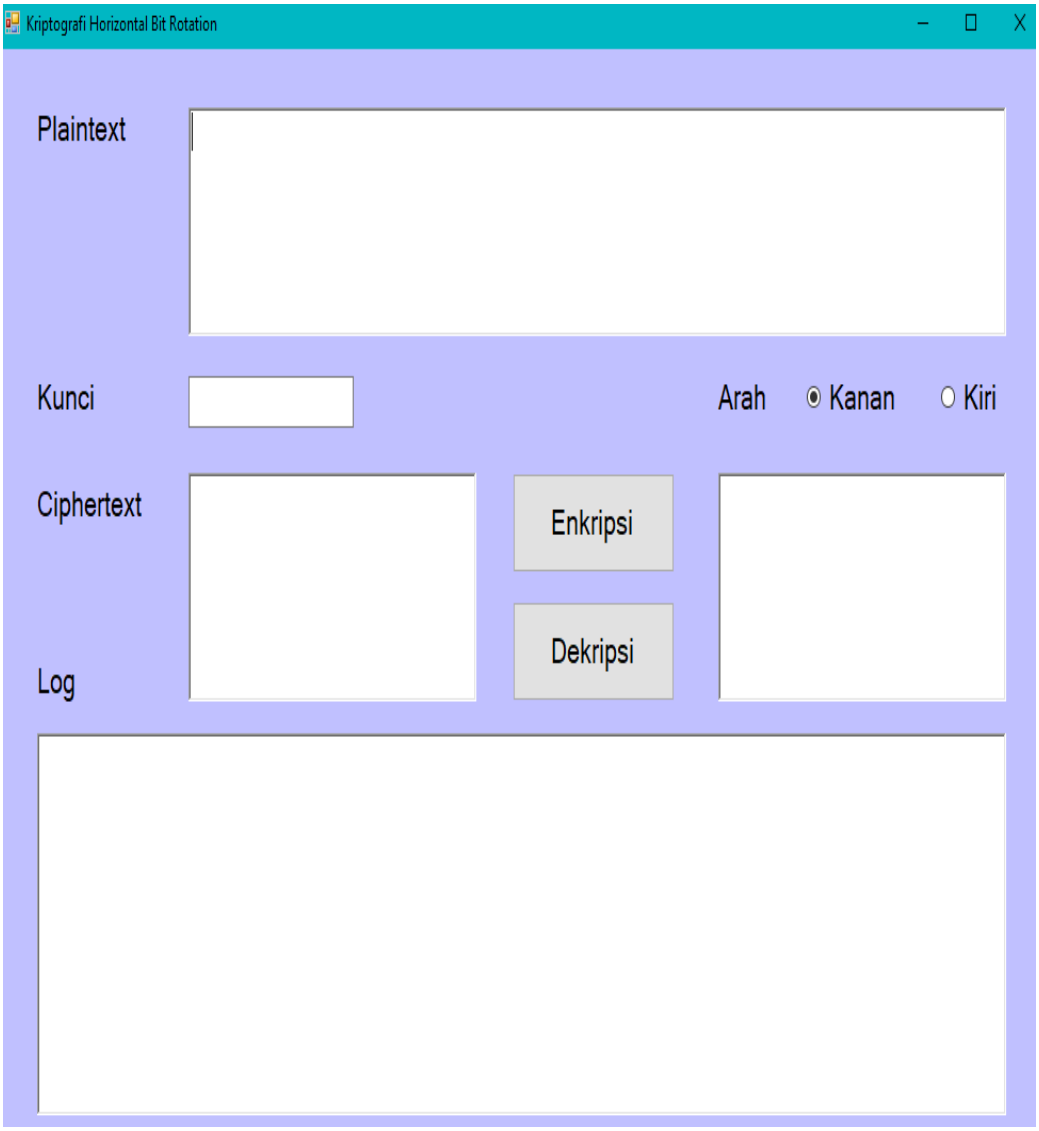
Gambar 4.1 Tampilan Halaman menu

Berikut adalah proses tambilan menu:

Pada saat program dijalankan akan tampil halaman menu yang terdapat beberapa pilihan button yang memiliki fungsi yang berbeda.

4.2.1.2 Tampilan Halaman HBR

Halaman ini merupakan halaman yang muncul pada saat button HBR di klik. Tampilan halaman HBR dapat dilihat pada gambar berikut :



Gambar 4.2 Tampilan HBR

Berikut adalah proses dari enkripsi dan deskripsi :

Enkripsi

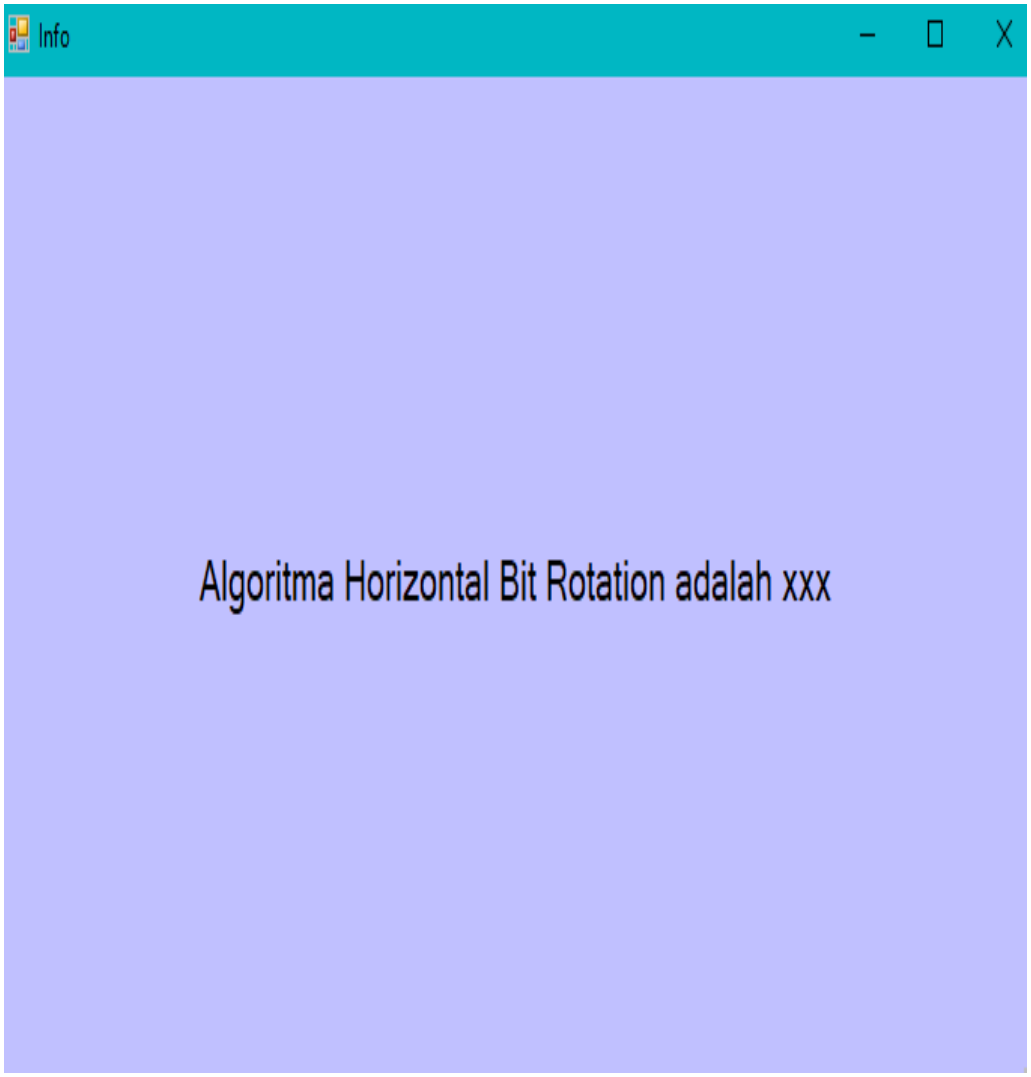
1. Pada saat ingin memulai mengenkripsi pesan, pada bagian plaintext harus ditulis isi pesan yang ingin di enkripsi
2. Lalu letakkan kunci pada kolom kunci
3. Pada bagian arah dapat dipilih kanan atau kiri untuk proses kunci
4. Maka akan muncul proses hasil pesan yang telah di ekripsi pada kolom plaintext
5. Hasil dari perhitungan ekripsi akan muncul kolom log

Deskripsi

1. Jika ingin mendeskripsikan pesan maka masukkan kunci pada kolom kunci sesuai lalu pilih arah kanan atau kiri
2. Lalu klik button deskripsi
3. Maka hasil deskripsi akan muncul pesan seperti semula pada kolom plaintext.
4. Hasil dari perhitungan deskripsi akan muncul kolom log

4.2.1.3 Tampilan Halaman Info

Ketika button info di klik maka akan muncul tentang Algoritma Horizontal Bit Rotation seperti pada gambar berikut :



Gambar 4.3 Tampilan Info

4.2.1.4 Tampilan Halaman About

Ketika Button about di klik maka akan muncul tampilan form yang menjelaskan sedikit keterangan tentang si penulis seperti pada gambar berikut :

Gambar 4.4 *Tampilan about*

4.3 Pengujian Sistem

Perangkat lunak adalah elemen kritis dari jaminan kualitas perangkat lunak dan merepresentasikan kajian pokok dari spesifikasi, perancangan, dan pengkodean. Pengujian yang digunakan untuk menguji perhitungan *enkripsi* dan *dekripsi* menggunakan algoritma *Horizontal bit rotation.*

4.3.1 Enkripsi

Bagian ini akan dilakukan pengujian yang berisi kalimat “saya muhammad nur sitompul, kuliah di universitas pembangunan panca budi” dengan *key* “4” dan arah “kanan”.

Hasil perhitungan dapat dilihat pada kalkulasi berikut ini:

PT[0] = s = 115 = 01110011--ROT 4-->	CT[0] = 00110111 = 55	= 7
PT[1] = a = 97 = 01100001--ROT 4-->	CT[1] = 00010110 = 22	= _
PT[2] = y = 121 = 01111001--ROT 4-->	CT[2] = 10010111 = 151	= —
PT[3] = a = 97 = 01100001--ROT 4-->	CT[3] = 00010110 = 22	= _
PT[4] = = 32 = 00100000--ROT 4-->	CT[4] = 00000010 = 2	= _
PT[5] = m = 109 = 01101101--ROT 4-->	CT[5] = 11010110 = 214	= Ö
PT[6] = u = 117 = 01110101--ROT 4-->	CT[6] = 01010111 = 87	= W
PT[7] = h = 104 = 01101000--ROT 4-->	CT[7] = 10000110 = 134	= †
PT[8] = a = 97 = 01100001--ROT 4-->	CT[8] = 00010110 = 22	= _
PT[9] = m = 109 = 01101101--ROT 4-->	CT[9] = 11010110 = 214	= Ö
PT[10] = m = 109 = 01101101--ROT 4-->	CT[10] = 11010110 = 214	= Ö
PT[11] = a = 97 = 01100001--ROT 4-->	CT[11] = 00010110 = 22	= _
PT[12] = d = 100 = 01100100--ROT 4-->	CT[12] = 01000110 = 70	= F
PT[13] = = 32 = 00100000--ROT 4-->	CT[13] = 00000010 = 2	= _
PT[14] = n = 110 = 01101110--ROT 4-->	CT[14] = 11100110 = 230	= æ
PT[15] = u = 117 = 01110101--ROT 4-->	CT[15] = 01010111 = 87	= W
PT[16] = r = 114 = 01110010--ROT 4-->	CT[16] = 00100111 = 39	= '
PT[17] = = 32 = 00100000--ROT 4-->	CT[17] = 00000010 = 2	= _
PT[18] = s = 115 = 01110011--ROT 4-->	CT[18] = 00110111 = 55	= 7
PT[19] = i = 105 = 01101001--ROT 4-->	CT[19] = 10010110 = 150	= –
PT[20] = t = 116 = 01110100--ROT 4-->	CT[20] = 01000111 = 71	= G
PT[21] = o = 111 = 01101111--ROT 4-->	CT[21] = 11110110 = 246	= ö
PT[22] = m = 109 = 01101101--ROT 4-->	CT[22] = 11010110 = 214	= Ö
PT[23] = p = 112 = 01110000--ROT 4-->	CT[23] = 00000111 = 7	= _

PT[24] = u = 117 = 01110101--ROT 4--> CT[24] = 01010111 = 87 = W

PT[25] = l = 108 = 01101100--ROT 4--> CT[25] = 11000110 = 198 = Æ

PT[26] = , = 44 = 00101100--ROT 4--> CT[26] = 11000010 = 194 = Â

PT[27] = = 32 = 00100000--ROT 4--> CT[27] = 00000010 = 2 = _

PT[28] = k = 107 = 01101011--ROT 4--> CT[28] = 10110110 = 182 = ¶

PT[29] = u = 117 = 01110101--ROT 4--> CT[29] = 01010111 = 87 = W

PT[30] = l = 108 = 01101100--ROT 4--> CT[30] = 11000110 = 198 = Æ

PT[31] = i = 105 = 01101001--ROT 4--> CT[31] = 10010110 = 150 = –

PT[32] = a = 97 = 01100001--ROT 4--> CT[32] = 00010110 = 22 = _

PT[33] = h = 104 = 01101000--ROT 4--> CT[33] = 10000110 = 134 = †

PT[34] = = 32 = 00100000--ROT 4--> CT[34] = 00000010 = 2 = _

PT[35] = d = 100 = 01100100--ROT 4--> CT[35] = 01000110 = 70 = F

PT[36] = i = 105 = 01101001--ROT 4--> CT[36] = 10010110 = 150 = –

PT[37] = = 32 = 00100000--ROT 4--> CT[37] = 00000010 = 2 = _

PT[38] = u = 117 = 01110101--ROT 4--> CT[38] = 01010111 = 87 = W

PT[39] = n = 110 = 01101110--ROT 4--> CT[39] = 11100110 = 230 = æ

PT[40] = i = 105 = 01101001--ROT 4--> CT[40] = 10010110 = 150 = –

PT[41] = v = 118 = 01110110--ROT 4--> CT[41] = 01100111 = 103 = g

PT[42] = e = 101 = 01100101--ROT 4--> CT[42] = 01010110 = 86 = V

PT[43] = r = 114 = 01110010--ROT 4--> CT[43] = 00100111 = 39 = '

PT[44] = s = 115 = 01110011--ROT 4--> CT[44] = 00110111 = 55 = 7

PT[45] = i = 105 = 01101001--ROT 4--> CT[45] = 10010110 = 150 = –

PT[46] = t = 116 = 01110100--ROT 4--> CT[46] = 01000111 = 71 = G

PT[47] = a = 97 = 01100001--ROT 4--> CT[47] = 00010110 = 22 = _

PT[48] = s = 115 = 01110011--ROT 4--> CT[48] = 00110111 = 55 = 7

PT[49] = = 32 = 00100000--ROT 4--> CT[49] = 00000010 = 2 = _

PT[50] = p = 112 = 01110000--ROT 4--> CT[50] = 00000111 = 7 = _

PT[51] = e = 101 = 01100101--ROT 4--> CT[51] = 01010110 = 86 = V

PT[52] = m = 109 = 01101101--ROT 4--> CT[52] = 11010110 = 214 = Ö

PT[53] = b = 98 = 01100010--ROT 4--> CT[53] = 00100110 = 38 = &

PT[54] = a = 97 = 01100001--ROT 4--> CT[54] = 00010110 = 22 = _

PT[55] = n = 110 = 01101110--ROT 4--> CT[55] = 11100110 = 230 = æ

PT[56] = g = 103 = 01100111--ROT 4--> CT[56] = 01110110 = 118 = v

PT[57] = u = 117 = 01110101--ROT 4--> CT[57] = 01010111 = 87 = W

PT[58] = n = 110 = 01101110--ROT 4--> CT[58] = 11100110 = 230 = æ

PT[59] = a = 97 = 01100001--ROT 4--> CT[59] = 00010110 = 22 = _

PT[60] = n = 110 = 01101110--ROT 4--> CT[60] = 11100110 = 230 = æ

PT[61] = = 32 = 00100000--ROT 4--> CT[61] = 00000010 = 2 = _

PT[62] = p = 112 = 01110000--ROT 4--> CT[62] = 00000111 = 7 = _

PT[63] = a = 97 = 01100001--ROT 4--> CT[63] = 00010110 = 22 = _

PT[64] = n = 110 = 01101110--ROT 4--> CT[64] = 11100110 = 230 = æ

PT[65] = c = 99 = 01100011--ROT 4--> CT[65] = 00110110 = 54 = 6

PT[66] = a = 97 = 01100001--ROT 4--> CT[66] = 00010110 = 22 = _

PT[67] = = 32 = 00100000--ROT 4--> CT[67] = 00000010 = 2 = _

PT[68] = b = 98 = 01100010--ROT 4--> CT[68] = 00100110 = 38 = &

PT[69] = u = 117 = 01110101--ROT 4--> CT[69] = 01010111 = 87 = W

PT[70] = d = 100 = 01100100--ROT 4--> CT[70] = 01000110 = 70 = F

PT[71] = i = 105 = 01101001--ROT 4--> CT[71] = 10010110 = 150 = ─

Hasil pesan dari enkripsi yaitu: “7_—__ÖW†_ÖÖ_F_æW'_7–
GöÖ_WÆÂ_¶WÆ–_†_F–_Wæ–gV'7–G_7__VÖ&_ævWæ_æ___æ6__&WF─”

4.3.2 Dekripsi

Bagian ini akan dilakukan pengembalian hasil *enkripsi* menjadi *plaintext* awal.

Hasil perhitungan dapat dilihat pada kalkulasi berikut ini:

CT[0] = 7 = 55 = 00110111--ROT 4--> PT[0] = 01110011 = 115 = s

CT[1] = _ = 22 = 00010110--ROT 4--> PT[1] = 01100001 = 97 = a

CT[2] = — = 151 = 10010111--ROT 4--> PT[2] = 01111001 = 121 = y

CT[3] = _ = 22 = 00010110--ROT 4--> PT[3] = 01100001 = 97 = a

CT[4] = _ = 2 = 00000010--ROT 4--> PT[4] = 00100000 = 32 =

CT[5] = Ö = 214 = 11010110--ROT 4--> PT[5] = 01101101 = 109 = m

CT[6] = W = 87 = 01010111--ROT 4--> PT[6] = 01110101 = 117 = u

CT[7] = † = 134 = 10000110--ROT 4--> PT[7] = 01101000 = 104 = h

CT[8] = _ = 22 = 00010110--ROT 4--> PT[8] = 01100001 = 97 = a

CT[9] = Ö = 214 = 11010110--ROT 4--> PT[9] = 01101101 = 109 = m

CT[10] = Ö = 214 = 11010110--ROT 4--> PT[10] = 01101101 = 109 = m

CT[11] = _ = 22 = 00010110--ROT 4--> PT[11] = 01100001 = 97 = a

CT[12] = F = 70 = 01000110--ROT 4--> PT[12] = 01100100 = 100 = d

CT[13] = _ = 2 = 00000010--ROT 4--> PT[13] = 00100000 = 32 =

CT[14] = æ = 230 = 11100110--ROT 4--> PT[14] = 01101110 = 110 = n

CT[15] = W = 87 = 01010111--ROT 4--> PT[15] = 01110101 = 117 = u

CT[16] = ' = 39 = 00100111--ROT 4--> PT[16] = 01110010 = 114 = r

CT[17] = _ = 2 = 00000010--ROT 4--> PT[17] = 00100000 = 32 =

CT[18] = 7 = 55 = 00110111--ROT 4--> PT[18] = 01110011 = 115 = s

CT[19] = – = 150 = 10010110--ROT 4--> PT[19] = 01101001 = 105 = i

CT[20] = G = 71 = 01000111--ROT 4--> PT[20] = 01110100 = 116 = t

CT[21] = ö = 246 = 11110110--ROT 4--> PT[21] = 01101111 = 111 = o

CT[22] = Ö = 214 = 11010110--ROT 4--> PT[22] = 01101101 = 109 = m

CT[23] = _ = 7 = 00000111--ROT 4--> PT[23] = 01110000 = 112 = p

CT[24] = W = 87 = 01010111--ROT 4--> PT[24] = 01110101 = 117 = u

CT[25] = Æ = 198 = 11000110--ROT 4--> PT[25] = 01101100 = 108 = l

CT[26] = Â = 194 = 11000010--ROT 4--> PT[26] = 00101100 = 44 = ,

CT[27] = _ = 2 = 00000010--ROT 4--> PT[27] = 00100000 = 32 =

CT[28] = ¶ = 182 = 10110110--ROT 4--> PT[28] = 01101011 = 107 = k

CT[29] = W = 87 = 01010111--ROT 4--> PT[29] = 01110101 = 117 = u

CT[30] = Æ = 198 = 11000110--ROT 4--> PT[30] = 01101100 = 108 = l

CT[31] = – = 150 = 10010110--ROT 4--> PT[31] = 01101001 = 105 = i

CT[32] = _ = 22 = 00010110--ROT 4--> PT[32] = 01100001 = 97 = a

CT[33] = † = 134 = 10000110--ROT 4--> PT[33] = 01101000 = 104 = h

CT[34] = _ = 2 = 00000010--ROT 4--> PT[34] = 00100000 = 32 =

CT[35] = F = 70 = 01000110--ROT 4--> PT[35] = 01100100 = 100 = d

CT[36] = – = 150 = 10010110--ROT 4--> PT[36] = 01101001 = 105 = i

CT[37] = _ = 2 = 00000010--ROT 4--> PT[37] = 00100000 = 32 =

CT[38] = W = 87 = 01010111--ROT 4--> PT[38] = 01110101 = 117 = u

CT[39] = æ = 230 = 11100110--ROT 4--> PT[39] = 01101110 = 110 = n

CT[40] = – = 150 = 10010110--ROT 4--> PT[40] = 01101001 = 105 = i

CT[41] = g = 103 = 01100111--ROT 4--> PT[41] = 01110110 = 118 = v

CT[42] = V = 86 = 01010110--ROT 4--> PT[42] = 01100101 = 101 = e

CT[43] = ' = 39 = 00100111--ROT 4--> PT[43] = 01110010 = 114 = r

CT[44] = 7 = 55 = 00110111--ROT 4--> PT[44] = 01110011 = 115 = s

CT[45] = – = 150 = 10010110--ROT 4--> PT[45] = 01101001 = 105 = i

CT[46] = G = 71 = 01000111--ROT 4--> PT[46] = 01110100 = 116 = t

CT[47] = _ = 22 = 00010110--ROT 4--> PT[47] = 01100001 = 97 = a

CT[48] = 7 = 55 = 00110111--ROT 4--> PT[48] = 01110011 = 115 = s

CT[49] = _ = 2 = 00000010--ROT 4--> PT[49] = 00100000 = 32 =

CT[50] = _ = 7 = 00000111--ROT 4--> PT[50] = 01110000 = 112 = p

CT[51] = V = 86 = 01010110--ROT 4--> PT[51] = 01100101 = 101 = e

CT[52] = Ö = 214 = 11010110--ROT 4--> PT[52] = 01101101 = 109 = m

CT[53] = & = 38 = 00100110--ROT 4--> PT[53] = 01100010 = 98 = b

CT[54] = _ = 22 = 00010110--ROT 4--> PT[54] = 01100001 = 97 = a

CT[55] = æ = 230 = 11100110--ROT 4--> PT[55] = 01101110 = 110 = n

CT[56] = v = 118 = 01110110--ROT 4--> PT[56] = 01100111 = 103 = g

CT[57] = W = 87 = 01010111--ROT 4--> PT[57] = 01110101 = 117 = u

CT[58] = æ = 230 = 11100110--ROT 4--> PT[58]= 01101110 = 110 = n

CT[59] = _ = 22 = 00010110--ROT 4--> PT[59] = 01100001 = 97 = a

CT[60] = æ = 230 = 11100110--ROT 4--> PT[60] = 01101110 = 110 = n

CT[61] = _ = 2 = 00000010--ROT 4--> PT[61] = 00100000 = 32 =

CT[62] = _ = 7 = 00000111--ROT 4--> PT[62] = 01110000 = 112 = p

CT[63] = _ = 22 = 00010110--ROT 4--> PT[63] = 01100001 = 97 = a

CT[64] = æ = 230 = 11100110--ROT 4--> PT[64] = 01101110 = 110 = n

CT[65] = 6 = 54 = 00110110--ROT 4--> PT[65] = 01100011 = 99 = c

CT[66] = _ = 22 = 00010110--ROT 4--> PT[66] = 01100001 = 97 = a

CT[67] = _ = 2 = 00000010--ROT 4--> PT[67] = 00100000 = 32 =

CT[68] = & = 38 = 00100110--ROT 4--> PT[68] = 01100010 = 98 = b

CT[69] = W = 87 = 01010111--ROT 4--> PT[69] = 01110101 = 117 = u

CT[70] = F = 70 = 01000110--ROT 4--> PT[70] = 01100100 = 100 = d

CT[71] = – = 150 = 10010110--ROT 4--> PT[71] = 01101001 = 105 = i

Hasil *dekripsi* kembali seperti awal yaitu “saya muhammad nur sitompul, kuliah di universitas pembangunan panca budi”.

4.4 Pengujian Aplikasi

Pengujian aplikasi perlu di lakukan untuk mengetahui bahwa aplikasi tersebut berjalan sesuai keinganan atau tidak.

Tabel 4.1 Pengujian Program

No	Pengjian forum	Pengujian Botton	Hasil
1.	Halaman Menu	HBR	☑ Berhasil ☐ Tidak
		Info	☑ Berhasil ☐ Tidak
		Abaout	☑ Berhasil ☐ Tidak
		Keluar	☑ Berhasil ☐ Tidak

2.	HBR	Arah	☑ Berhasil ☐ Tidak
		Enkripsi	☑ Berhasil ☐ Tidak
		Deskripsi	☑ Berhasil ☐ Tidak
3.	Info		☑ Berhasil ☐ Tidak
4.	About		☑ Berhasil ☐ Tidak
5	Keluar		☑ Berhasil ☐ Tidak

BAB V

PENUTUP

5.1 Kesimpulan

Setelah keseluruhan proses dilakukan, yaitu dari perancangan hingga pengujian perangkat lunak, maka dapat diambil kesimpulan sebagai berikut:

1. *Algoritma Horizontal Bit Rotation* dilakukan dengan menambahkan kunci kepada pesan asli sehinggsa pesan rahasia didapatkan.
2. Pada *Algoritma Horizontal Bit Rotation* terdapat dua pilihan arah untuk proses enkripsi dan deskripsi
3. Setelah dilakukan pengujian pada pesan, sulit untuk membaca hasil dari *Algoritma Horizontal Bit Rotation*.
4. Isi pesan yang terlalu banyak tidak mempengaruhi Kecepatan waktu proses enkripsi dan deskripsi

5.2 Saran

Adapun saran-saran yang dapat penulis berikan untuk pengembangan dan perbaikan sistem ini adalah sebagai berikut :

1. Penelitian ini dapat dikembangkan lagi dengan menambahkan proses kunci seperti menambahkan secara vertikal
2. Penelitian ini agar dapat dikembangkan lagi dengan menambahkan proses simpan pada hasil enkripsi dan deskripsi agar lebih memudahkan dalam melihat pesan yang telah di enkripsi dan deskripsi

DAFTAR PUSTAKA

Akim Manaor Hara Pardede, ST., M.Kom, Yani Maulita,S.Kom., M.Kom. (2014). Perancangan Perangkat Lunak Enkripsi Dan Deskripsi File Dengan Metode Transposisi Kolom. Jurnal Kaputama. 8 (1). 28-35. Diakses dari https://www.researchgate.net.

Angga Aditya Permana, Desi Nurnaningsih. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma *Advanced Encyption Standard (Aes)*. Teknik Informatika. 11 (2). 177-186. Diakses dari http://journal.uinjkt.ac.id.

Fachri, barany, agus perdana windarto, and ikhsan parinduri. "penerapan backpropagation dan analisis sensitivitas pada prediksi indikator terpenting perusahaan listrik." jepin (jurnal edukasi dan penelitian informatika) 5.2 (2019): 202-208.

Fachri, b., windarto, a. P., & parinduri, i. (2019). Penerapan backpropagation dan analisis sensitivitas pada prediksi indikator terpenting perusahaan listrik. Jepin (jurnal edukasi dan penelitian informatika), 5(2), 202-208.

Fachri, barany; windarto, agus perdana; parinduri, ikhsan. Penerapan backpropagation dan analisis sensitivitas pada prediksi indikator terpenting perusahaan listrik. Jepin (jurnal edukasi dan penelitian informatika), 2019, 5.2: 202-208

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 *Advanced EncryptionStandard*. Informatika Mulawarman. 10 (1). 20-31. Diakses dari http://e-journals.unmul.ac.id.

Hamdi, nurul. "model penyiraman otomatis pada tanaman cabe rawit berbasis programmable logic control." jurnal ilmiah core it: community research information technology 7.2 (2019)

Kiki Yulansari, Sukadi. (2013). Sistem Informasi Pengolahan Data Iuran Badan Pembantu Penyelenggaraan Pendidikan Sekolah Menengah Kejuruan Negeri 2 Donorojo. Seruni - Seminar Riset Unggulan Nasional Informatika dan Komputer FTI UNSA. 2 (1). 5-13. Diakses dari https://ijns.org.

M. Miftakul Amin. (2016). Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks. Jurnal Pseudocode. III (2). 129-136. Diakses dari https://media.neliti.com.

Muslim Setyo Rejeki, Ali Tarmuji. (2013). Membangun Aplikasi Autogenerate Script Ke Flowchart Untuk Mendukung Business Process Reengineering. Sarjana Teknik Informatika. 1 (2). 448-456. Diakses dari https://www.neliti.com.

Ninuk Wiliani, Syadid Zambi. (2017). Rancang Bangun Aplikasi Kasir Tiket Nonton Bola Bareng Pada X Kasir Di Suatu Lokasi X Dengan Visual Basic 2010 Dan Mysql. Rekayasa Informasi. 6 (2). 77-83. Diakses dari https://ejournal.istn.ac.id.

Permana, aminuddin indra. "kombinasi algoritma kriptografi one time pad dengan generate random keys dan vigenere cipher dengan kunci em2b." (2019).

Putra, randi rian. "sistem informasi web pariwisata hutan mangrove di kelurahan belawan sicanang kecamatan medan belawan sebagai media promosi." jurnal ilmiah core it: community research information technology 7.2 (2019).

Putra, randi rian, et al. "decision support system in selecting additional employees using multi-factor evaluation process method." (2019).

Putra, randi rian. "implementasi metode backpropagation jaringan saraf tiruan dalam memprediksi pola pengunjung terhadap transaksi." jurti (jurnal teknologi informasi) 3.1 (2019): 16-20.

Rizqi Sukma Kharisma, Muhammad Aziz Fatchu Rachman. (2017) Pembuatan Aplikasi Notes Menggunakan Algoritma Kriptografi Polyalphabetic Substitution Cipher Kombinasi Kode Ascii Dan Operasi Xor Berbasis Android. Teknologi Informasi. XII (35). 1-7. Diakses dari https://jti.respati.ac.id.

Saputra, muhammad juanda, and nurul hamdi. "rancang bangun aplikasi sejarah kebudayaan aceh berbasis android studi kasus dinas kebudayaan dan pariwisata aceh." journal of informatics and computer science 5.2 (2019): 147-157

Sidik, a. P., efendi, s., & suherman, s. (2019, june). Improving one-time pad algorithm on shamir's three-pass protocol scheme by using rsa and elgamal algorithms. In journal of physics: conference series (vol. 1235, no. 1, p. 012007). Iop publishing.

Sitepu, n. B., zarlis, m., efendi, s., & dhany, h. W. (2019, august). Analysis of decision tree and smooth support vector machine methods on data mining. In journal of physics: conference series (vol. 1255, no. 1, p. 012067). Iop publishing.

Suendri. (2018). Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem Informasi Remunerasi Dosen Dengan Database Oracle (Studi Kasus: UIN Sumatera Utara Medan). Ilmu Komputer dan Informatika. 3 (1). 1-9. Diakses dari https://jurnal.uinsu.ac.id.

Tasril, v., wijaya, r. F., & widya, r. (2019). Aplikasi pintar belajar bimbingan dan konseling untuk siswa sma berbasis macromedia flash. Jurnal informasi komputer logika, 1(3).