PEMANFAATAN ALGORITMA *AES* DALAM PEMBUATAN SISTEM ENKRIPSI DAN DEKRIPSI DOKUMEN

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	**: T. ILHAMSYAH**
NPM	**: 1414370365**
PROGRAM STUDI	**: SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

ABSTRAK

T. ILHAMSYAH

PEMANFAATAN ALGORITMA *AES* DALAM PEMBUATAN SISTEM ENKRIPSI DAN DEKRIPSI DOKUMEN
2019

Tujuan dalam penelitian ini adalah untuk mengembangkan dan menerapkan aplikasi pengamanan dalam dunia digital serta dokumen yang bersifat rahasia. Penelitian ini ditujukan untuk pengguna dalam melakukan pengamanan dokumen digital yang telah memiliki banyak persoalan keamanan, diharapkan metode keamanan ini mampu di implementasikan di berbagai platfom. Metode yang digunakan adalah metode algorithma AES (*Advance Encyption Standard*) yang telah menjadi algorithma enkripsi standar Amerika sejak tahun 2001 menggantikan DES *(Data Encryption Standard)* yang sebelumnya digunakan jutaan pengguna dalam kurun waktu yang cukup lama. Pada tulisan ini, pembahasan dipusatkan pada *Algorithma Kriptografi Modern* dengan (AES) yang menggunakan bahasa pemrograman *Visual Basic* (*VB*). Pemrograman VB termasuk salah satu yang memiliki pengguna paling luas di dunia untuk saat ini. Dengan demikian, diharapkan tulisan ini membantu pembaca dalam memahami konsep dasar *kriptografi.*

Kata Kunci : *Advance Encryption Standard, Data Encryption Standard, Algorithma Kriptografi Modern, Visual Basic*

DAFTAR ISI

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Semakin pesatnya perkembangan teknologi membuat seluruh proses kehidupan manusia menjadi lebih gampang. Mulai dari berkomunikasi, bertukar pesan, dan bahkan memesan kendaraan melalui teknologi. Dengan pesatnya perkembangan teknologi pula, membuat seluruh proses perkembangan teknologi dikelilingi oleh data-data penting yang harus dijaga kerahasiaannya. Beberapa contoh teknologi yang sering digunakan dalam kehidupan sehari-hari yaitu mengirim email. *Email* merupakan suatu alat pengiriman pesan elektronik yang digunakan untuk mengirim pesan antara pengguna satu dengan lainnya. Dengan *email*, kita juga dapat berkirim dokumen seperti *PDF, DOC, XLS, PPT* dan bentuk dokumen lainnya.

Dengan berkembangnya teknologi dibidang komunikasi dan pengiriman pesan tersebut maka informasi tersebut harus memerlukan suatu keamanan dan kerahasiaan karena bisa saja informasi atau dokumen tersebut menyimpan hal rahasia atau menjadi dokumen berharga yang harus diawasi kerahasiaanya. Salah satu cara yang dapat digunakan untuk mengamankan informasi atau dokumen tersebut ialah dengan memanfaatkan sistem kriptografi.

Kriptografi merupakan suatu teknik yang digunakan untuk merubah suatu data yang dapat dipahami manusia ke bentuk yang tidak dapat dipahami oleh manusia.

pemakaian kriptografi dalam proses pengiriman informasi ataupun dokumen menjadi hal yang wajid disaat sekarang ini. Hal ini dianjurkan karena pemakaian kriptografi dapat menjadi suatu keamanan tambahan bagi proses pengiriman informasi dan dokumen tersebut.

Pada kriptografi, terdapat suatu sistem yang disebut enkripsi dan dekripsi. Enkripsi merupakan suatu proses mengubah data asli (*plaintext*) kedalam bentuk yang tidak dapat dibaca (*ciphertext*) dengan menggunakan suatu kunci. Sedangkan dekripsi merupakan suatu proses mengubah data yang sudah dalam bentuk terenkripsi (*ciphertext*) kedalam bentuk yang dapat dibaca kembali (*plaintext*) dengan menggunakan kunci. Untuk dapat melakukan suatu proses kriptografi, diperlukan algoritma dan kunci yang telah ditentukan oleh algoritma tersebut. dalam penulisan skripsi ini, penulis menggunakan algoritma *AES* untuk proses kriptografi yang akan digunakan dalam proses mengenkripsi dan mendekripsi data dokumen.

AES merupakan algoritma yang menggunakan kunci dan masukan dengan Panjang 128 bit. Namun untuk tingkat keamanan yang lebih tinggi, *AES* dapat menggunakan kunci 192 dan 256 bit. Setiap masukan 128 bit*plaintext* dimasukkan ke dalam *state* yang berbentuk bujur sangkar berukuran *4x4 byte*. State ini nantinya akan di-*XOR* dengan *key* dan selanjutnya diolah 10 kali dengan substitusi-transformasi *liniear-addkey*.

Untuk itulah penulis mengangkat judul "**PEMANFAATAN ALGORITMA *AES* DALAM PEMBUATAN SISTEM ENKRIPSI DAN DEKRIPSI DOKUMEN"**

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka rumusan masalah dalam penelitian ini adalah :

a. Bagaimana kriptografi dengan metode *AES* ini mampu melindungi dokumen terhadap ancaman yang mampu merusak kerahasiaan dokumen ?
b. Bagaimana merancang perangkat lunak pengamanan data teks dengan menggunakan metode kriptografi *AES*?

1.3 Batasan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka batasan masalah dalam penulisan ini adalah :

a. Program enkripsi dan dekripsi dokumen ini akan berbentuk *offline*.
b. Sistem ini nantinya hanya akan digunakan untuk mengenkripsi dan mendekripsi bentuk dokumen dengan karakter huruf, angka dan gambar dari apa saja diantaranya yaitu *(.doc, .docx, .xls, .ppt, pdf)*.
c. Sistem aplikasi akan menggunakan bahasa pemrograman *VB* sebagai bahasa pemroses enkripsi dan dekripsi dokumen.

1.4 Tujuan Penulisan

Berdasarkan latar belakang dan rumusan masalah yang telah dijelaskan diatas, berikut merupakan tujuan penelitian dari penulisan skripsi ini yaitu :

a. Untuk menerapkan algoritma kriptografi *AES* dalam mengamankan dokumen sehingga isi dari dokumen tersebut menjadi aman dan tidak dapat dipahami oleh sembarang orang.
b. Untuk membuat suatu sistem yang dapat mengenkripsi dan mendekrisi isi dokumen dengan menggunakan algoritma *AES* dalam proses pengamanannya.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini yaitu untuk menambah pengetahuan terhadap cara kerja kriptografi *AES* pada proses enkripsi dan dekripsi isi file dokumen dan sebagai bahan acuan bagi siapapun yang ingin melakukan penelitian lebih lanjut mengenai penerapan algoritma *AES* dalam pengamanan file.

1.6 Metode Penelitian

Metode penelitian yang tepat dan benar akan menentukan keberhasilan suatu penelitian. Melalui metode harus dengan jelas tergambar bagaimana penelitian ini dilaksanakan yang disusun dan tertata secara sistematis.

1.6.1 Metode Pengolahan Data

Untuk melengkapi penulisan skripsi ini, maka penulis melakukan beberapa metode penelitian antara lain :

1) Studi Pustaka

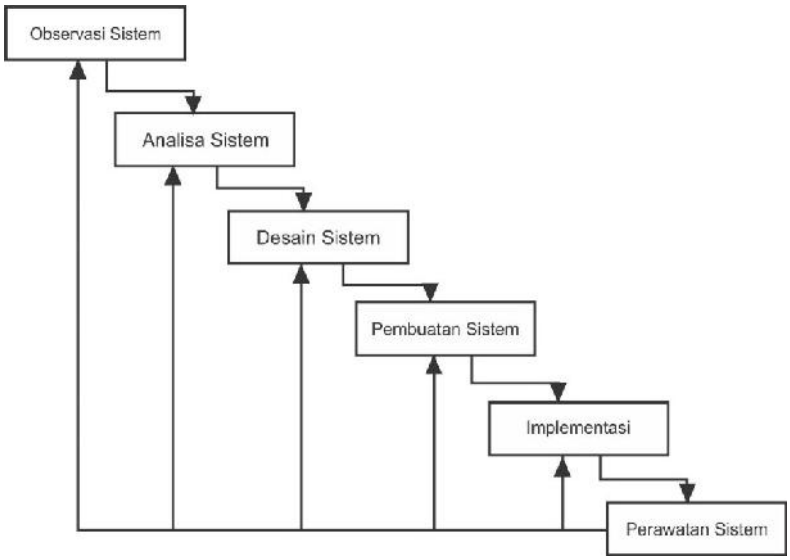
Mengumpulkan data dengan cara membaca dan mempelajari buku, jurnal ilmiah dan referensi mengenai judul yang diangkat.

2) Observasi

Dalam membuat program, penulis melakukan observasi terhadap tampilan, sistem, cara kerja dan alur kerja dari beberapa program yang telah menggunakan algoritma *AES* dalam proses pengamanan data.

1.6.2 Metode Perancangan Sistem

Dalam proses pembuatan program ini, penulis menggunakan metode *Waterfall* yang meliputi beberapa proses, antara lain :



Gambar 1.1 *Waterfall*

Berikut merupakan penjelasan dari alur *Waterfall* pada gambar 1 :

1) Observasi Sistem

Tahapan pertama dari pembuatan program ini yaitu penulis mengobservasi terhadap sistem yang sudah menggunakan algoritma *AES* dalam teknologi pengamanan datanya.

Penulis mengobservasi mengenai tempilan, cara kerja dari program tersebut dan juga bagaimana mereka memproses data menggunakan algoritma *AES*.

2) Analisa Sistem

Tahapan kedua yang perlu dilakukan yaitu menganalisa sistem dari yang sudah ada. Penulis menganalisa cara kerja, alur proses dan tampilan.

3) Desain Sistem

Setelah penulis mengobservasi dan menganalisa, penulis mendesain sistem enkripsi dan dekripsi algoritma *AES* dengan menggunakan *VB*.

4) Pembuatan Sistem

Langkah selanjutnya adalah pembuatan sistem, pada tahap ini penulis membuat sistem dengan menggunakan bahasa pemrograman *VB*.

5) Implementasi

Langkah selanjutnya adalah implementasi sistem, dimana pada tahap ini penulis menguji dan mengeksekusi sistem yang telah dibuat.

6) Perawatan Sistem

Tahap terakhir yaitu perawatan sistem, dimana pada proses ini penulis menganalisa kesalahan atau *error* yang muncul pada program serta melakukan perbaikan terhadap *error* yang ada.

1.7 Sistematika Penulisan

Sistematika penulisan pada skripsi ini meliputi :

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian dan metode penelitian.

BAB II LANDASAN TEORI

Bab ini berisi tentang teori-teori yang mendasari permasalah yang dibahas yaitu mengenai algoritma AES, kriptografi, dan teori-teori lainnya yang mendukung penulisan skripsi.

BAB III ANALISA DAN PERANCANGAN SISTEM

Bab ini akan menjelaskan tentang Analisa sistem dan penjabaran mengenai rancangan program dan proses pembuatan.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini berisi tentang penjelasan dari hasil program yang telah dibuat yang meliputi desain dan pengujian dari program yang dibangun.

BAB V PENUTUP

Bab ini berisi tentang kesimpulan dari program yang telah dibuat dan saran terhadap sistem yang telah ada maupun sistem yang telah dibuat.

BAB II

LANDASAN TEORI

2.1 Konsep Dasar Sistem

Sistem merupakan pendekatan prosedur komponen, dengan pendekatan prosedur sistem dapat didefinisikan sebagai kumpulan dari prosedur-prosedur untuk membentuk suatu kesatuan dan tujuan tertentu.

Menurut Romney dan Steinbart (2015:3) “sistem adalah suatu rangkaian yang terdiri dari dua atau lebih komponen yang saling berhubungan dan saling berinteraksi satu dengan yang lain untuk mencapai tujuan dimana sistem biasanya terbagi dalam sub sistem yang lebih kecil yang mendukung sistem yang lebih besar”.

Menurut Gelinas dan Dull (2012:11), “Sistem merupakan seperangkat elemen yang saling bergantung yang bersama-sama mencapai tujuan tertentu. Dimana sistem harus memiliki organisasi, hubungan timbal balik, integrasi dan tujuan pokok”. Sedangkan menurut Mulyadi (2016:4) “Sistem adalah suatu jaringan prosedur yang dibuat menurut pola yang terpadu untuk melaksanakan kegiatan pokok perusahaan”.

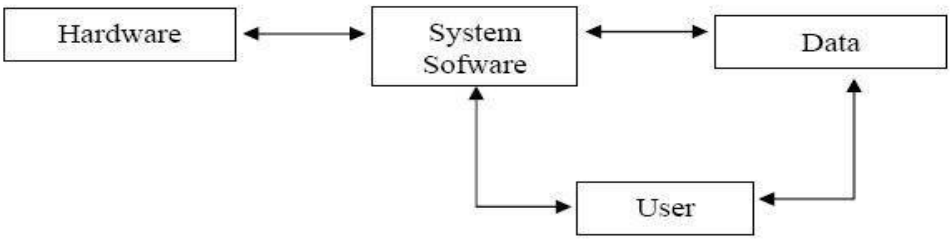
Berdasarkan pengertian dan referensi diatas dapat disimpulkan bahwa sistem merupakan gabungan elemen yang saling berkaitan dan berhubungan yang bersama-sama mencapai suatu tujuan tertentu dalam proses yang teratur yangdapatmendukung sistem yang lebih besar dan saling memiliki ketergantungan untuk mencapai tujuan tertentu.

2.2 Konsep Dasar Sistem Informasi

Telah diketahui bahwa informasi merupakan hal yang sangat penting di dalam mendukung pengambilan keputusan. Informasi dapat diperoleh dari sistem informasi (*Information system*) atau disebut juga dengan *processing system* atau *information processing system* atau *information generating system*. Sisteminformasi didefinisikan oleh Robert A. Leitch dan K. Roscoe Davis (JOG[7]) sebagai berikut:

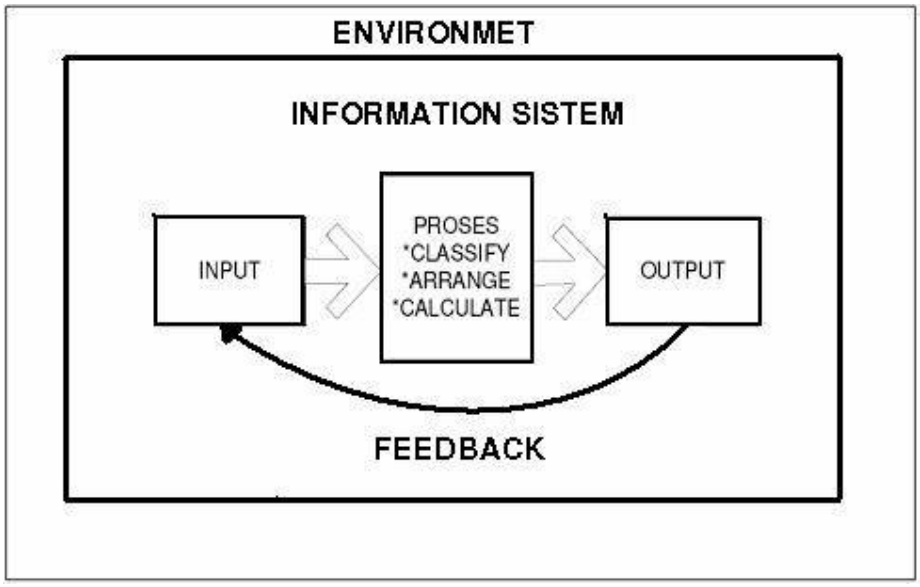
> *"Sistem informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan yang diperlukan".*

Sistem informasi sendiri memiliki sejumlah komponen tertentu. Seperti yang dikemukakan oleh Robert dan Donald Symanzky (JOG[7]), bahwa sistem informasi terdiri dari beberapa komponen yang berbeda yaitu, manusia, data, *hardware*, dan *software*. Sebagai suatu sistem, setiap komponen tersebutberinteraksi satu dengan lainnya membentuk satu kesatuan untuk mencapai sasarannya.



Gambar 2.1 Komponen Sistem Informasi

Ada tiga aktifitas pada sistem informasi untuk menghasilkan informasi pada suatu organisasi yang diperlukan untuk membuat suatu keputusan, pengkontrolan, analisis masalah-masalah dan membuat produk baru atau layanan. Aktifitas itu adalah input, proses dan output (BLA[15]).



Gambar 2.2 Aktifitas Sistem Informasi

INPUT : Menangkap atau pengumpulkan data mentah (*raw data*) di dalam organisasi atau dari luar organisasi (*environment*/lingkungan).

PROSES : Menterjemahkan data input ke dalam bentuk yang lebih berarti.

OUTPUT: Mengirim informasi yang telah diproses kepada manusia dan aktivitasnya.

Sistem informasi juga memerlukan *feedback* yang dihasilkan dari output, yang dikembalikan dan digunakan oleh elemen organisasi untuk membantu mereka, mengevaluasi atau menyempurnakan inputan yang akan dimasukkan.

2.3 Pengembangan Sistem

Informasi merupakan sumber daya yang sangat penting bagi organisasi, dengan sistem informasi berbasis komputer dapat mempermudah dalam pengolahan data sehingga informasi yang dihasilkan lebih cepat dan lebih baik daripada informasi yang dihasilkan sistem informasi yang dikelola secara manual.

Pengembangan sistem (*system development*) dapat berarti menyusun sistem yang baru untuk menggantikan sistem yang lama secara keseluruhan atau memperbaiki sistem yang telah ada. Sistem yang lama perlu diganti atau diperbaiki disebabkan karena beberapa hal, yaitu :

1. Adanya permasalahan-permasalahan (*Problems)* yang timbul di dalam sistem lama. Permasalahan-permasalahan yang timbul dapat berupa :
   a. Ketidakberesan

      Ketidakberesan dalam sistem yang lama menyebabkan sistem yang lama tidak dapat beroperasi sesuai dengan yang diharapkan. Ketidak beresan ini dapat berupa :

1) Kecurangan-kecurangan yang disengaja yang menyebabkan tidak amannya harta kekayaan perusahaan dan kebenaran dari data menjadi tidak terjamin.
2) Kesalahan-kesalahan yang tidak disengaja yang juga dapat menyebabkan kebenaran dari data tidak terjamin.
3) Tidak efisiennya operasi.
4) Tidak ditaatinya kebijaksanaan manajemen yang telah ditetapkan.

b. Pertumbuhan Organisasi

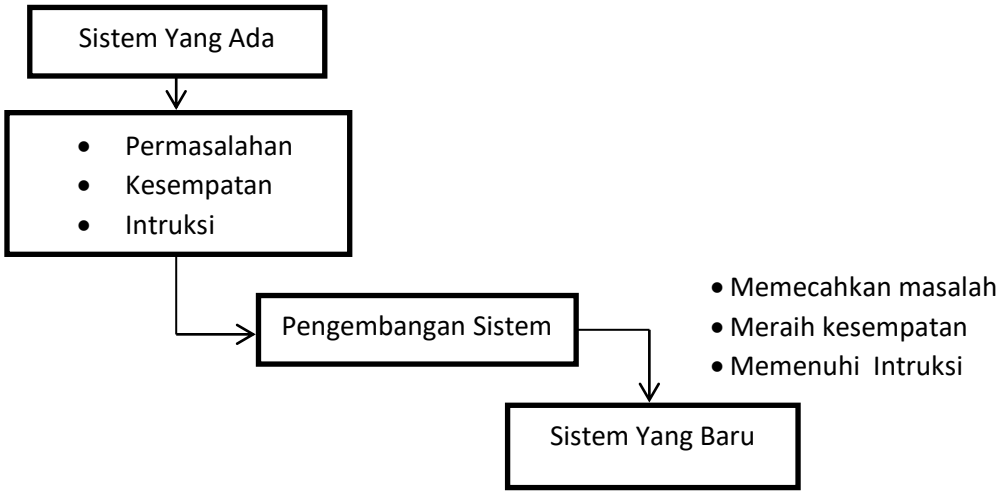
Pertumbuhan organisasi menyebabkan harus disusunnya sistem yang baru. Pertumbuhan organisasi diantaranya adalah kebutuhan informasi yang semakin luas, *volume* pengolahan data semakin meningkat, perubahan prinsip akuntansi yang baru. Karena adanya perubahan ini menyebabkan sistem yang lama tidak efektif lagi, sehingga sistem yang lama sudah tidak dapat memenuhi lagi kebutuhan informasi yang dibutuhkan manajemen.

2. Untuk meraih kesempatan-kesempatan (*Opportunities*)

Teknologi informasi telah berkembang dengan cepatnya. Organisasi mulai merasakan bahwa teknologi informasi ini perlu digunakan untuk meningkatkan penyediaan informasi sehingga dapat mendukung dalam pengambilan keputusan. Kecepatan informasi atau efisiensi waktu sangat menentukan berhasil atau tidaknya strategi dan rencana yang telah disusun untuk meraih kesempatan-kesempatan yang ada.

3. Adanya intruksi-intruksi (*Directives*)

   Pengembangan sistem yang baru dapat juga terjadi karena adanya intruksi-intruksi dari atas pimpinan ataupun dari luar organisasi, seperti misalnya peraturan pemerintah.



Gambar 2.3 Pengembangan Sistem

2.4 Siklus Hidup Pengembangan Sistem

Proses pengembangan sistem melewati beberapa tahapan-tahapan, mulai dari sistem itu direncanakan sampai dengan sistem itu diterapkan, dioperasikan dan dipelihara. Bila operasi sistem yang sudah dikembangkan masih timbul kembali permasalahan-permasalahan kritis serta tidak dapat diatasi dalam tahap pemeliharaan sistem, maka perlu dikembangkan kembali suatu sistem untuk mengatasinya dan proses ini kembali ke tahap yang pertama. Siklus ini disebut dengan siklus hidup sistem (*system life cycle*).

Ide dari *system life cycle* adalah sederhana dan masuk akal. Di *system lifecycle*, tiap-tiap bagian dari perkembangan sistem dibagi menjadi beberapa tahapankerja. Tiap-tiap tahapan ini mempunyai karakteristik tersendiri.

Menurut KUL[16], SDLC berfungsi untuk menggambarkan tahapan-tahapan utama dalam mengembangkan suatu sistem informasi. Kegiatan-kegiatan utama dalam SDLC dapat digolongkan menjadi tiga bagian, yaitu penelitian, pengembangan sistem, dan manajemen sistem. Ketiga bagian tersebut secara lebih rinci dapat dijelaskan seperti berikut :

1. Penelitian

   Kegiatan ini merupakan tahapan paling awal dalam siklus hidup sistem, tahapan perencanaan sistem termsuk dalam kegiatan ini. Sebelum suatu sistem dikembangkan, maka perlu direncanakan terlebih dahulu secara cermat. Perencanaan sistem (*system planning*) ini menyangkut estimasi dari kebutuhan-kebutuhan fisik, tenaga kerja, dan dana yang dibutuhkan untuk mendukung pengembangan sistem serta untuk mendukung operasinya setelah diterapkan.

2. Pengembangan Sistem

   Secara garis besar kegiatan ini dapat dibagi menjadi tiga bagian, setiap kegiatan dalam pengembangan sistem ini dapat dijelaskan melalui tujuan (*purpose*) dan hasil kegiatannya (*deliverable*).

a. Analisis

   Dalam tahapan ini, sistem yang ada dianalisis untuk :

1. Membuat keputusan apabila sistem yang ada mempunyai masalah atau tidak berfungsi secara baik dan hasil analisisnya digunakan sebagai dasar untuk memperbaiki sistem.
2. Mengetahui ruang lingkup pekerjaan yang akan ditangani.
3. Memahami sistem yang ada/berjalan.
4. Mengidentifikasi masalah dan mencari solusinya

Kegiatan dilakukan dalam tahap analisis ini adalah :

a) *Problem detection,* mendeteksi masalah-masalah pada sistemapabila sistem makin berkurang manfaatnya.
b) *Initial investigation,* memeriksa sistem yang sedang berjalandengan memfokuskan pada bagian-bagian yang mengalami masalah.
c) *Requirement analysis,* mengetahui kebutuhan sistem sesuaidengan harapan *user*, penerapan sistem yang baru akan menimbulkan perbedaan antara sistem yang lama dengan sistem yang ideal (berbasis komputer).
d) *Generation of system alternatives,* mencari perbedaan antaraalternatif sistem yang baru dalam upaya penggantian sistem yang lama.
e) *Selection of proper system,* membandingkan alternatif-alternatifsistem dengan mengunakan suatu metode, memilih alternatif sistem yang paling baik, dan merancangnya untuk *user*.

b. Desain

Tahap ini memiliki tujuan untuk mendesain sistem yang baru yang dapat mengatasi permasalahan-permasalahan yang muncul dipilih dari alternatif

pemilihan sistem yang terbaik. Kegiatan yang dilakukan pada tahapan ini adalah :

1. *Input design*, merancang bentuk-bentuk inputan baik yangberupa dokumen atau dilayar/antarmuka pengguna (*userinterface*).
2. *Output design*, merancang tampilan-tampilan untuk outputdari sistem, termasuk dokumen serta antarmuka pengguna (*user interface*).
3. *File design*, merancang bentuk *file/basisdata* yangdibutuhkan dalam suatu sistem informasi.

c. Implementasi

1. Melakukan spesifikasi dari konsep yang ada untuk penerapan sistem informasi yang dibangun.
2. Mengimplementasikan sistem yang baru.
3. Menjamin bahwa sistem yang baru dapat berjalan secara optimal.

Kegiatan-kegiatan yang dilakukan dalam tahap implementasi ini adalah :

a) *Programming & Testing*, membuat program berdasarkanacuan dari hasil analisis, dan mengetes keseluruhan program untuk memastikan semua fungsi/modul-modul program dapat berfungsi secara benar.
b) *Training*, melakukan pelatihan-pelatihan terhadap *user* atauoperator-operator yang akan menggunakan sistem.
c) *Change over*, mengganti sistem yang lama dengan sistemyang baru.

2.5 Pengertian Informasi

Tidak mudah untuk mendefinisikan konsep informasi karena istilah yang satu ini mempunyai banyak aspek, ciri dan manfaat yang satu dengan yang lainnya terkadang sangat berbeda. Informasi merupakan data yang berasal dari fakta lalu membuat pengetahuan yang didapatkan dari pembelajaran, pengalaman ataupun intruksi dan selanjutnya dilakukan pengolahan (proses) untuk menjadi bentuk yang berguna atau bermanfaat bagi si penerima atau pemakainya.

Menurut krismiaji (2015:14), "Informasi adalah data yang telah diorganisasi dan telah memiliki kegunaan dan manfaat". Hal serupa juga disampaikan oleh Romney dan steinbart (2015:4) : "Informasi adalah data yang telah dikelola dan diproses untuk memberikan arti dan memperbaiki proses pengambilan keputusan keputusan. Sebagaimana perannya, pengguna membuat keputusan yang lebih baik sebagai kuantitas dari peningkatan informasi".

Berdasarkan beberapa pengertian diatas dapat disimpulkan bahwa pengertian informasi adalah data yang di olah dari hasil kesaksian atau rekaman peristiwa atau data. Data itu sendiri adalah kenyataan yang menggambarkan suatu kejadian, sedangkan kejadian itu merupakan peristiwa yang terjadi pada waktu tertentu dan berasal dari fakta yang telah diolah menjadi bentuk yang berguna dan berarti bagi pemakainya dan dapat memberikan ilmu pengetahuan kepada seorang yang menggunakannya serta mempermudah dalam proses mengambil keputusan.

2.6 Pengertian Data

Ladjamudin (2013:8), “Data adalah deskripsi dari sesuatu dan kejadianyang kita hadapi (*the description of things and events that we face*). Sementaradata bisnis *(business data*) dedefinisikan sebagai deskripsi organisasi tentangsuatu (*resources*) dan kejadian (*transactions*) yang terjadi (*business data is anorganization’s description of things (resources) and events (transactions) that itface*).

Ibrahim (2015:182), “Data dalam penelitian ini adalah segala bentuk fakta,data dan informasi yang digali dari subjek penelitian.Dari pengertian diatas, dapat disimpulkan bahwa data merupakan kumpulan fakta mengenai suatu benda, peristiwa atau kegiatan yang disimpan atau dicatat.

2.7 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani dimana *crypto* artinya “*secret*” (rahasia) dan *graphein* artinya “*writing*” (tulisan). Jadi, kata kriptografi adalah “*secret writing*” (tulisan rahasia).

Kriptografi ialah ilmu yang berfokus pada cara memproteksi data menggunakan teknik enkripsi, dekripsi dan proses lain yang berhubungan. Matematika merupakan hal yang penting dalam dunia kriptografi, karena hanya dengan pengetahuan matematis dapat dikembangkan prosedur yang dibutuhkan untuk mengenkripsi data secara aman. Hal penting lainnya adalah komputer. Komputer menjalankan prosedur enkripsi dan dekripsi.

Ide utama dari sebuah sistem kriptografi adalah untuk menyamarkan informasi rahasia dengan cara yang tidak dipahami oleh pihak yang tidak berhak. Dua kegunaan umum kriptografi adalah untuk menyimpan data secara aman di komputer dan untuk mengirimkan data melalui saluran yang tidak aman seperti *internet*. Faktanya adalah bahwa pesan yang terenkripsi tidak mencegah pihak lain untuk mengakses pesan tersebut, tetapi dapat dipastikan bahwa pihak lain tidak dapat mengerti apa yang mereka lihat.

Setiap orang mempunyai cara-cara yang sangat unik untuk merahasiakan pesan. Cara-cara unik tersebut tentu saja sangat berbeda-beda pada setiap pelaku kriptografi. Setiap cara menulis pesan rahasia, pesan tersebut mempunyai nilai estetika tersendiri sehingga kriptografi berkembang menjadi sebuah seni merahasiakan pesan.

Dalam menjaga kerahasian data, kriptografi memakai teknik enkripsi dalam mengirimkan data asli (*plaintext*). Setelah melalui proses enkripsi, *plaintext* tersebut berubah ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. Proses untuk mengembalikan *ciphertext* menjadi *plaintext* disebut dengan proses dekripsi. Untuk melakukan proses dekripsi diperlukan adanya suatu kunci rahasia.

Dalam kriptografi ini ada 4 tujuan dasar ilmu kriptografi yang merupakan aspek-aspek keamanan informasi sebagai berikut :

a. Kerahasian adalah layanan yang digunakan untuk menjaga isi dari data tersebut agar tidak dapat tidak dapat dibaca oleh siapapun atau pihak-pihak yang tidak berhak.

b. Integritas Data merupakan layanan yang menjamin data masih asli/utuh selama pengiriman.

c. Otentikasi Data adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber data (*origin authentication*).

d. Nirpenyangkalan (*Non-repudiation*) adalah merupakan suatu usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi yang telah mengirimkan/ membuat.

Di dalam kriptografi kita akan sering menemukan berbagai istilah atau *terminology* yang penting yang harus diketahui. Beberapa istilah yang harus diketahui yaitu sebagai berikut :

a. Pesan, *Plaintext* dan *Ciphertext*

Pesan adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Pesan asli disebut *plaintext*. Agar pesan tidak bisa dimengerti maknanya oleh pihak yang tidak berwewenang, maka pesan perlu disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan bersandi adalah *Ciphertext*.

b. Pengirim dan Penerima

Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirimkan pesan kepada lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan. Entitas

disini dapat berupa orang, mesin (komputer), kartu kredit, kartu atm dan lain-lainnya.

c. Enkripsi dan Dekripsi

Kriptografi mempunyai dua bagian yang penting yaitu, enkripsi dan dekripsi. Enkripsi adalah proses penyandian dari pesan yang asli (*plaintext*) menjadi pesan yang tidak dapat diartikan seperti pesan aslinya (*ciphertext*) dengan menggunakan aturan tertentu. Sedangkan dekripsi merupakan kebalikannya yaitu mengubah pesan yang sedang sudah disandikan menjadi pesan aslinya.

d. Cipher dan Kunci

Algoritma kriptografi disebut juga *cipher* yaitu aturan *enchipering* dan *dechipering* atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Keamanan algoritma kriptografi sering diukur dari banyaknya kerja (*work*) yang dibutuhkan untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan. Kunci merupakan parameter yang digunakan untuk transformasi *enciphering* dan *dechipering*. Kunci biasanya berupa string atau deretan bilangan.

e. Sistem Kriptografi

Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Sistem kriptografi (cryptosystem) terdiri dari algoritma kriptografi, semua *plaintext*, *ciphertext*, dan kunci.

f. Penyadap (*eavesdropper*)

Penyadap adalah orang yang mencoba menangkap pesan selama ditransmisikan. Tujuan penyadap adalah untuk memperoleh informasi sebanyak-banyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan tujuan memecahkan *ciphertext* menjadi *plaintext*.

g. Kriptanalisis dan kriptologi

Kriptanalisis (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan pelaku tersebut adalah kriptanalisis. Jika seorang kriptografer (*cryptographer)* mentransformasikan *plaintext* menjadi *ciphertext* dengan suatu algoritma dan kunci, maka sebaliknya seorang kriptanalis akan berusaha untuk memecahkan *ciphertext* tersebut untuk menemukan *plaintext* atau kunci.

Kriptografi juga memiliki 3 fungsi dasar yaitu :

a. Enkripsi merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirim agar terjaga kerahasiannya. Pesan asli disebut *plaintext,* yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan *cipher* atau kode dengan menggunakan algoritma yang mengkodekan data yang kita inginkan.

b. Dekripsi merupakan kebalikan dari proses enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks asli), disebut dengan dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi.

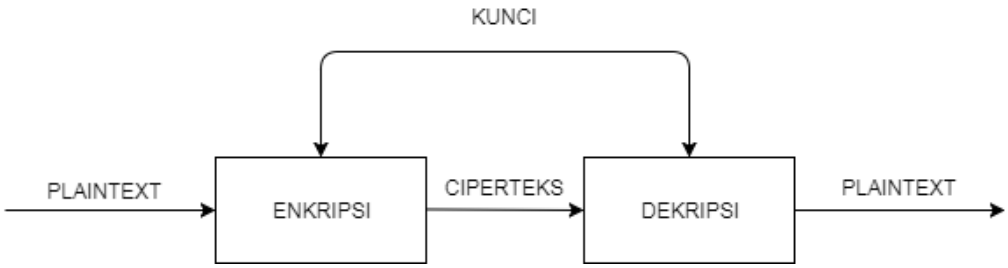
c. Kunci adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian yaitu, kunci rahasia (*private key*) dan kunci umum (*public key*).

2.8 Algoritma Kriptografi

Algoritma kriptografi atau sering disebut dengan *cipher* adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi (Schneier, 2015). Algoritma kriptografi ada dua macam, diantaranya yaitu :

2.8.1 Algoritma Simetris

Algortima simetris atau disebut juga algoritma konvensional adalah algoritma yang menggunakan kunci yang sama pada proses enkripsi dan dekripsi. Algoritma ini mengharuskan pengirim dan penerima menyetujui satu kunci tertentu sebelum dapat berkomunikasi secara aman. Keamanan algoritma simtri tergantung pada rahasia kunci. Pemecahan kunci berarti memungkinkan setiap orang dapat mengenkripsi dan mendekripsi pesan dengan mudah.

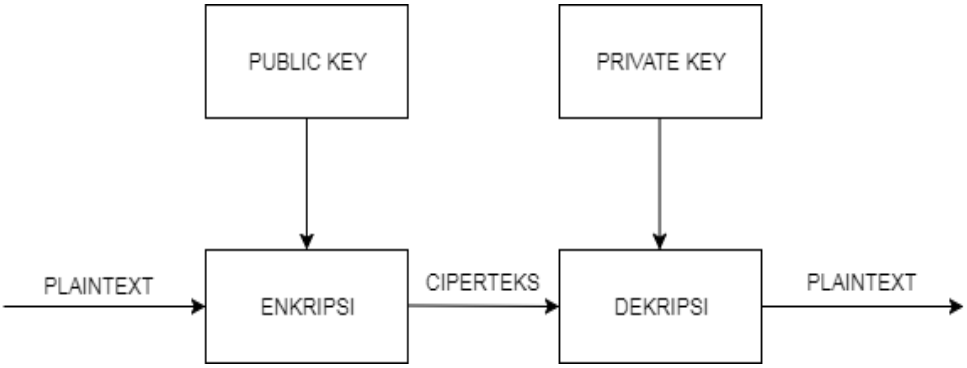


Gambar 2.4 Algoritma Kriptografi Simetris

(Sumber: Basri, (2016))

2.8.2 Algoritma Asimetris

Algoritma asimetris merupakan algoritma kriptografi yang salah satukuncinya digunakan untuk proses enkripsi dan satu lagi digunakan untuk proses dekripsi. Semua orang yang mendapatkan kunci *public* dapat menggunakannya untuk mengenkripsi pesan, sedangkan hanya pengirim dan penerima sajalah yang dapat mendekrip pesan tersebut karena memegang kunci *private*.



Gambar 2.5 Algoritma Kriptografi Asimetris

(Sumber : Basri, (2016))

2.9 Enkripsi dan Dekripsi

Enkripsi merupakan sebuah metode penyandian sebuah pesan atau informasi menjadi sebuah teks yang tidak dapat dibaca. Enkripsi berkaitan erat dengan kriptografi, yang merupakan sebuah metode untuk mengamankan sebuah pesan hingga tidak dapat dibaca oleh pihak ketiga. Enkripsi dapat dibagi menjadi dua proses enkripsi yang berbeda yaitu *Block Cipher* dan*Stream Cipher* (Ferguson dkk, 2015).

Dekripsi yaitu kebalikan dari proses enkripsi yaitu proses konversi data yang sudah dienkripsi (*ciphertext*) kembali menjadi data aslinya (*Original Plaintext*) sehingga dapat dibaca atau dimengerti kembali.Pesan yang akan dienkripsi disebut plaintext yang dimisalkan *plaintext* (P), proses enkripsi dimisalkan enkripsi (E), proses dekripsi dimisalkan dekripsi (D), dan pesan yang sudah dienkripsi disebut *ciphertext* yang dimisalkan *ciphertext* (C)(Ferguson dkk, 2015).

2.10 Model-Model Enkripsi

Dalam membahas model-model enkripsi beserta algoritma yang akan dipakai untuk setiap enkripsi ada 2 hal penting yang harus dijabarkan, yaitu enkripsi dengan kunci pribadi dan enkripsi dengan kunci *public* (Ferguson dkk, 2015).

2.10.1 Enkripsi Kunci Pribadi

Enkripsi dapat dilakukan jika si pengirim dan si penerima telahsepakat untuk menggunakan metode enkripsi atau kunci enkripsi tertentu.Metode enkripsi atau kuncinya ini harus dijaga ketat supaya tidak ada pihak luar yang mengetahuinya. Kesepakatan cara enkripsi atau kunci dalamenkripsi ini bisa dicapai lewat jalur komunikasi lain yang lebih aman,misalnya dengan bertemu langsung.

Cara enkripsi dengan kesepakatan atau kunci enkripsi di atas dikenal dengan istilah enkripsi dengan kunci pribadi, karena cara enkripsi atau kunci yang hanya boleh diketahui oleh dua pribadiyang berkomunikasi tersebut. Cara enkripsi inilah yang umum digunakanpada saat ini baik untuk kalangan pemerintah maupun kalangan bisnis.

Cara enkripsi ini juga dikategorikan sebagai kriptografi simetris, karena dua belah pihak mengetahui kunci yang sama. Selain masalah komunikasi awal untuk penyampaian kunci, cara enkripsi ini juga mempunyai kelemahan yang lain.Kelemahan ini timbul jika terdapat banyak orang yang ingin salingberkomunikasi. Karena setiap pasangan harus menghafal banyak kunci danharus menggunakannya secara tepat. Sebab, jika tidak, maka si penerima tidakbisa mengartikannya.

2.10.2 Enkripsi Dengan Kunci Public

Cara enkripsi ini mempunyai banyak kelebihan, salah satunya adalah tiap orang hanya perlu memiliki satu set kunci, tanpa peduli berapa banyak orang yang akan diajak berkomunikasi. Jadi, jika ada n set kunci saja. Selain itu, cara enkripsi ini tidak membutuhkan saluran yang aman untuk pengiriman kunci, sebab kunci yang dikirimkan ini harus diketahui oleh public.

Cara enkripsi sangat praktis sehingga masyarakat umum pun dapat dengan mudahmemakainya. Cara kerja enkripsi ini secara singkat dapat diterangkan sebagai berikut. Setiap orang yang menggunakan enkripsi ini harus mempunyai duabuah kunci, satu disebut kunci rahasia yang hanya boleh diketahui oleh dirinya sendiri dan yang lain disebutkunci public yang disebarkan ke oranglain. Kedua kunci ini dibuat secara acakdengan menggunakan rumus matematika tertentu.

Jadi, kedua kunci ini berkaitan erat secara matematika. Jika si A hendak mengirim pesan kepada si B, si A perlu mengenkrip pesanitu dengan kunci public milik si B. Pesan si A yang telah dienkrip dengan menggunakan kunci public si B

hanya bisa dibuka dengan kunci public itu sendiri. Si B wajib untuk menjamin keamanan kunci rahasianya. Karena kunci rahasia ini tidak perlu diketahui pihak si pengirim berita,kunci ini tidak akan pernah dikirim lewat jalur umum. Hal ini membuat caraini jauh lebih aman daripada enkripsi dengan kunci pribadi.

Misalkan si C dapat mengirim ke B dengan menggunakan kunci public si B yang sama. Walaupun mengetahui kunci public si B, pesan yang telah dienkripsi dengan itusangat sulit untuk dibuka. Cara enkripsi ini dikategorikan dalam kriptografi asimetris, karena kunci yang dipakai untuk mengenkrip dan untuk membukaenkrip adalah dengan menggunakan dua kunci yang berbeda (WahanaKomputer, dkk, 2014:94).

2.11 *Advance Encryption Standard (AES)*

*AES (Advanced Encryption Standard)*merupakan algoritma *Rijndael* yang telahmemenangkan sayembara terbuka yang dilakukan oleh *NIST(National Institute of Standard and Technology).* Sayembara ini dilakukan untuk menemukan algoritma baru untuk menggantikan algoritma *DES (Data Encryption Standard)* yang dirasa sudah tidak aman lagi (Munir, 2013). *NIST* memberikan spesifikasi *AES* yaitu harus memiliki panjang blok 128 bit dan mampu mendukung panjang kunci 128, 192, dan 256. Setelah melalui beberapa tahapan seleksi, akhirnya *NIST* memilih sistem penyandian *Rijndael* yang dikembangkan oleh *Joan Daemen* dan *Vincent Rijment* sebagai sistem penyandian *AES* pada tahun 2000.

Pemilihan *Rijndael* sebagai pemenang sayembara tersebut berdasarkan pada kriteria berikut ini:

1. Keamanan

   Sistem penyandian harus tahan terhadap serangan analisis sandi selain serangan secara *brute force*.

2. Biaya

   Sistem penyandian harus memiliki biaya komputasi dan memori yang efisien sehingga dapat diimplementasikan secara perangkat keras maupun perangkat lunak.

3. Karakteristik algoritma dan implementasi

   Sistem penyandian harus bersifat terbuka, fleksibel, dan sederhana.

Penyandian *AES* menggunakan proses yang berulang yang disebut dengan ronde. Jumlah ronde yang digunakan oleh *AES* tergantung dengan panjang kunci yang digunakan. Setiap ronde membutuhkan kunci ronde dan masukan dari ronde berikutnya. Kunci ronde dibangkitkan berdasarkan kunci yang diberikan. Berikut merupakan tabel relasi antara jumlah ronde dan panjang kunci. (Sadikin, 2013)

Tabel 2.1 Relasi Jumlah Ronde dan Kunci (Sadikin, 2013)

Panjang Kunci *AES* (bit)	**Jumlah Ronde (Nr)**
128	10
192	12
256	14

Algoritma *AES* mempunyai tiga parameter yaitu:

1. Plainteks, *array* yang berukuran 16 *byte*, yang berisi data masukan.

2. Cipherteks, *array* yang berukuran 16 *byte*, yang berisi hasil enkripsi.
3. Kunci, *array* yang berukuran 16 *byte*, yang berisi kunci *cipher*.

AES memiliki panjang blok 128 bit. Kunci *AES* dapat memiliki Panjang kunci bit 128, 192, dan 256 bit. Selain itu *AES* menggunakan 5 unit ukuran data : bit, *byte*, *word*, blok, dan state. Bit merupakan satuan data terkecil, yaitu nilai digit sistem biner. Sedangkan *byte* berukuran 8 bit, *word* berukuran 4 *byte* (32 bit), blok berukuran 16 *byte* (128 bit). Sedangkan state adalah blok yang ditata sebagai matriks *byte* berukuran 4x4 (Sadikin, 2013).

2.12 Bahasa Pemrograman

(Wikipedia, 2018) Bahasa pemrograman, atau sering diistilahkan juga dengan bahasa komputer atau bahasa pemrograman komputer, adalah instruksi standar untuk memerintah komputer.Bahasa pemrograman ini merupakan suatu himpunan dari aturan sintaksis dan semantik yang dipakai untuk mendefinisikan program komputer. Bahasa ini memungkinkan seorang *programmer* dapat menentukan secara persis data mana yang akan diolah oleh komputer, bagaimana data ini akan disimpan/diteruskan, dan jenis langkah apa secara persis yang akan diambil dalam berbagai situasi.

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

a. Bahasa Mesin, yaitu memberikan perintah kepada komputer dengan memakai kode bahasa biner, contohnya 01100101100110.

b. Bahasa Tingkat Rendah, atau dikenal dengan istilah bahasa rakitan (bah.Inggris *Assembly*), yaitu memberikan perintah kepada komputer dengan memakai kode-kode singkat (kode *mnemonic*), contohnya *MOV, SUB, CMP, JMP, JGE, JL, LOOP,* dsb.
c. Bahasa Tingkat Menengah, yaitu bahasa komputer yang memakai campuran instruksi dalam kata-kata bahasa manusia (lihat contoh Bahasa Tingkat Tinggi di bawah) dan instruksi yang bersifat simbolik, contohnya {, }, ?, <<, >>, &&, ||, dsb.
d. Bahasa Tingkat Tinggi, yaitu bahasa komputer yang memakai instruksi berasal dari unsur kata-kata bahasa manusia, contohnya *begin, end, if, for, while, and, or, dsb.* Komputer dapat mengerti bahasa manusia itu diperlukan program *compiler* atau *interpreter.*

Sebagian besar bahasa pemrograman digolongkan sebagai Bahasa Tingkat Tinggi, hanya bahasa *C* yang digolongkan sebagai Bahasa Tingkat Menengah dan *Assembly* yang merupakan Bahasa Tingkat Rendah.

Bahasa Pemrograman (*programming language*) adalah sebuah instruksi standar untuk memerintah komputer agar menjalankan fungsi tertentu. Bahasa pemrograman ini merupakan suatu himpunan dari aturan sintaksis dan semantik yang dipakai untuk mendefinisikan program komputer. Bahasa ini memungkinkan seorang *programmer* dapat menentukan secara persis data mana yang akan diolah oleh komputer, bagaimana data ini akan disimpan/diteruskan, dan jenis langkah apa secara persis yang akan diambil dalam berbagai situasi.

Fungsi bahasa pemrograman yaitu memerintah komputer untuk mengolah data sesuai dengan alur berpikir yang kita inginkan. Keluaran dari bahasa pemrograman tersebut berupa program atau aplikasi. Contohnya adalah program yang digunakan oleh kasir di mal-mal atau swalayan, penggunaan lampu lalu lintas di jalan raya.

Bahasa Pemrograman yang kita kenal ada banyak sekali di belahan dunia, tentang ilmu komputer dan teknologi dewasa ini. Perkembangannya mengikuti tingginya inovasi yang dilakukan dalam dunia teknologi. Contoh bahasa pemrograman yang kita kenal antara lain adalah untuk membuat aplikasi *game*, antivirus, *web*, dan teknologi lainnya.Bahasa pemrograman komputer yang kita kenal antara lain adalah *Java, Visual Basic, C++, C, Cobol, PHP, .NET*, dan ratusan bahasa lainnya. Namun tentu saja kebutuhan bahasa ini harus disesuaikan dengan fungsi dan perangkat yang menggunakannya.

Secara umum bahasa pemrograman terbagi menjadi 4 kelompok, yaitu :

a. *Object Oriented Language (Java, PHP, Javascript, C++)*
b. *High Level Language* (seperti *Pascal* dan *Basic*)
c. *Middle Level Language* (seperti bahasa *C*)
d. *Low Level Language* (seperti bahasa *Assembly*)

Sedangkan menurut tingkatannya, bahasa pemrograman memiliki 3 jenis tingkatan yaitu :

1. Bahasa tingkat tinggi :Bahasa pemrograman masuk tingkat ini karena bahasa tersebut mendekati bahasa manusia. Contohnya bahasa *Basic, Visual Basic, Pascal, Java, PHP.*

2. Bahasa tingkat menengah :Disebut tingkat menengah karena bisa masuk ke dalam bahasa tingkat tinggi maupun rendah. Contohnya bahasa *C*.
3. Bahasa tingkat rendah :Bahasa pemrograman masuk tingkat ini karena bahasanya masih jauh dari bahasa manusia. Contohnya bahasa *Assembly*.

2.13 Visual Basic

(Repository.usu.ac.id, 2018)Visual basic adalah bahasa pemprograman windows yang berbasis grafis (GUIGraphical User Interface). Sifat bahasa pemprogramanya adalah eventdriven, artinya program akan terjadi jika ada respon dari pemaka berupa event/kejadian tertentu (tombol diklik, mouse ditekan dan lain-lain). Saat event terjadi maka kode yang berhubungan dengan event akan dijalankan. Dalam Visual Basic, pembuatan aplikasi dimulai dengan memperkirakan kebutuhan, merancang tampilan dan selanjutnya diikuti dengan pembuatan kode untuk program tersebut.

2.14 Proses Pembuatan Suatu Program

(Wikipedia, 2018) Proses pembuatan program yaitu kita menulis kode sumber pada teks editor misalnya notepad kemudian mengubahnya menjadi bahasa mesin yang bisa dieksekusi oleh *CPU*. Proses pengubahan kode sumber (*source code*) menjadi bahasa mesin (*machine language*) ini terdiri dari dua macam yaitu kompilasi dan interpretasi.

2.14.1 Kompilasi

Dalam proses kompilasi semua kode sumber dibaca terlebih dahulu dan jika idak ada kesalahan dalam menulis program maka akan dibentuk kode mesinnya sehingga program bisa dijalankan. Program yang melakukan tugas ini disebut *Compiler*. Program hasil kompilasi akan berbentuk *executable*. Program bisa langsung dijalankan tanpa harus memiliki *Compiler* di komputer yang menjalankan program tersebut. Bahasa yang menggunakan teknik kompilasi misalnya bahasa *C, C++, Pascal, Assembly* dan masih banyak lagi.

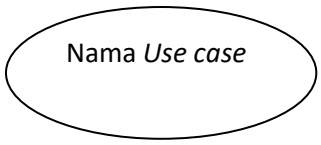
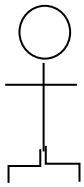
2.14.2 Interpretasi

Bahasa yang menggunakan teknik interpretasi akan membaca kode sumber perbaris dan dieksekusi perbaris. Jika ditemukan kesalahan dalam penulisan program maka di baris kesalahan itulah program akan dihentikan. Program yang melakukan tugas ini disebut *Interpreter*. Pada teknik interpretasi tidak ada akan dihasilkan program *standalone*, artinya untuk menjalankan program kita harusmempunyai kode sumbernya sekaligus *interpreter* program tersebut.Bahasa yangmenggunakan teknik interpretasi misalnya bahasa *Perl, Python, Ruby, Java* dan masih banyak lagi.

2.15 *Use Case* Diagram

Use case merupakan pendeskripsian sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat. Secara kasar, *use case* digunakan untuk mengetahui fungsi apasaja yang ada dalam sebuah sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi itu (Rosa & Shalahuddin, 2013).

Tabel 2.2 Tabel *Use Case* Diagram

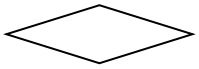
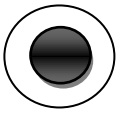
Simbol	Deskripsi
Use case 	Fungsionalisasi yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau aktor, biasanya dinyatakan dengan menggunakan kata kerja di awal frase nama *use case.*
Aktor  Nama aktor	Orang, proses atau sistem yang lain yang berinteraksi dengan sistem informasi yang akan dibuat diluar sistem yang akan dibuat itu sendiri. Jadi walaupun *symbol* dari aktor adalah gambar orang, tetapi aktor belum tentu menggunakan orang; biasanya dinyatakan menggunakan kata benda di awal frase nama actor
Asosiasi / *Association* ————————	Komunikasi antara aktor dan *use case* yang berpartisipasi pada *use case* atau *usecase* memiliki interaksi dengan actor
Ekstensi / *Extend* <<extend>> ——→	Kelakuan yang hanya berjalan dibawah kondisi tertentu seperti menggerakkan *handphone*.
Generalisasi ——→	Elemen yang menjadi spesialisasi elemen lain
Include <<include>> ——→	Kelakuan yang harus terpenuhi agar suatu *event* dapat terjadi

(Sumber : Rosa A.S dan M. Shalahudin, 2014:162)

2.16 *Activity Diagram*

Rosa dan M. Shalahudin (2014:161), "Diagram aktivitas atau *activitydiagram* menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sebuah sistem atau proses bisnis atau menu yang ada pada perangkat lunak. Yang perlu di perhatikan disini adalah bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas yang dapat dilakukan oleh sistem.

Tabel 2.3 Simbol-Simbol *Activity Diagram*

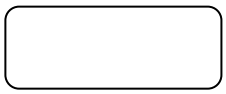
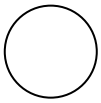
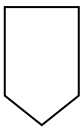
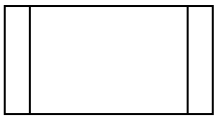
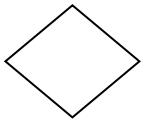
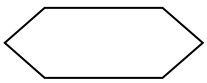
Simbol	Deskripsi
Status awal 	Status awal aktivitas sistem, sebuah diagram aktivitas memiliki sebuah status awal.
Aktivitas 	Aktivitas yang dilakukan sistem, aktivitas biasanya diawali dengan kata kerja.
Percabangan / *decision* 	Asosiasi percabangan dimana jika ada aktivitas pilihan lebih dari satu.
Penggabungan / Join 	Asosiasi penggabungan dimana lebih dari satu aktivitas digabungkan menjadi satu.
Status Akhir 	Status akhir yang dilakukan sistem, sebuah diagram aktivitas memiliki sebuah status akhir.

(Sumber : Rosa A.S dan M. Shalahudin, 2014:162)

2.17 *Flowchart*

Indrajani (2015:36), "*Flowchart* adalah penggambaran secara grafik dari langkah-langkah dan urutan prosedur suatu program."Indrajani (2015:38), menjelaskan simbol-simbol dalam *Flowchart* adalah :

Tabel 2.4 *Flowchart*

Simbol	Maksud	Simbol	Maksud
	Terminal (*START, END*)		Titik sambungan pada halaman yang sama
	*Input / Output (READ, WRITE)*		Tititk konektor yang berada pada halaman lain
	Proses		*Call* (Memanggil subprogram)
	*Decision (YES, NO)*		Dokumen
	*Display*		*Stored Data*
	Alur proses		*Preparation* (Pemberi nilai awal suatu variabel)

(Sumber : Rosa A.S dan M. Shalahudin, 2014:162)

BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Implementasi Sistem

Tahap implementasi sistem merupakan tahap dimana aplikasi yang telah dirancang dijalankan. Tahap ini menunjukkan apakah setiap proses dapat berjalan dengan baik dan mampu memberikan hasil yang diharapkan. Proses perancangan aplikasi menggunakan *visual basic NET 2010* ditampilkan dalam bentuk form-form yang menjadi sarana bagi pengguna untuk melakukan proses implementasi.

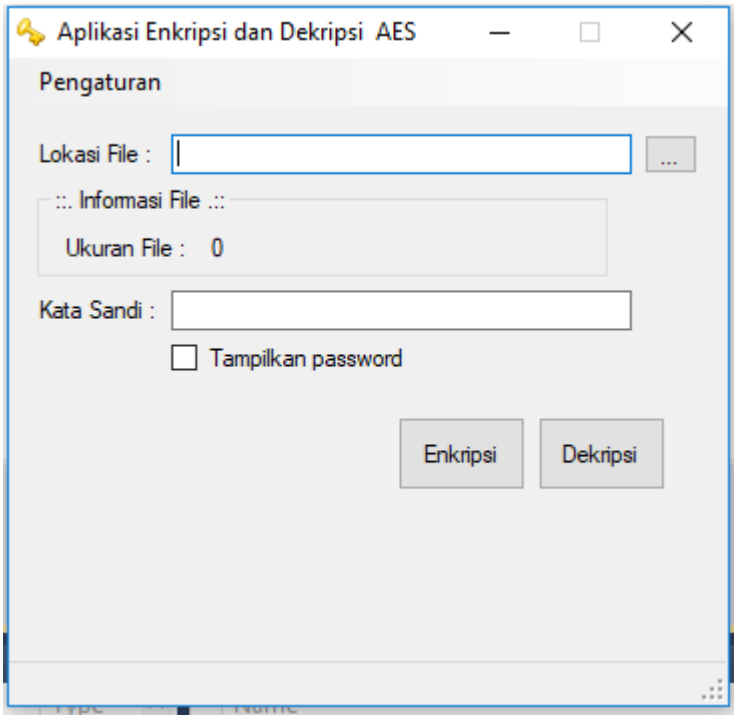
4.2 Pengujian Sistem

Pengujian sistem dilakukan untuk menunjukkan apakah sistem yang telah dirancang dapat berjalan sesuai harapan. Selain itu tujuan pengujian adalah untuk dapat menemukan kesalahan fungsi pada aplikasi yang dibangun dan memperbaikinya.

Pengujian dilakukan dengan memasukkan karakter atau hurufdari file berformat .txt selanjutnya diproses oleh aplikasi siapakah aplikasi tersebut dapat memberikan hasil yang sesuai. Proses yang akan dilakukan pengujian dalam aplikasi ini adalah simulasi pengiriman pesan dengan menggunakan metode algoritma AES antara pengirim kepada penerima dengan kunci yang dimiliki masing-masing pihak tanpa perlu bertukar kunci tunggal hingga pada akhirnya pesan asli yang dikirimkan oleh pengirim dapat dibaca oleh penerima .

4.2.1 Tampilan Awal/ Home

Tampilan pada gambar dibawah merupakan tampilan awal ketika aplikasi dijalankan. Pada form ini pengguna dapat memilih untuk membuka beberapa form lainnya seperti tombol tentang yang akan mengarahkan pengguna menuju form yang menjelaskan profil aplikasi ini, tombol materidan tombol pengaturan yang akan mengarahkan pengguna ke form yang menjelaskan tata cara penggunaan dari aplikasi ini.



Gambar 4.1 Tampilan Awal/ *Home*

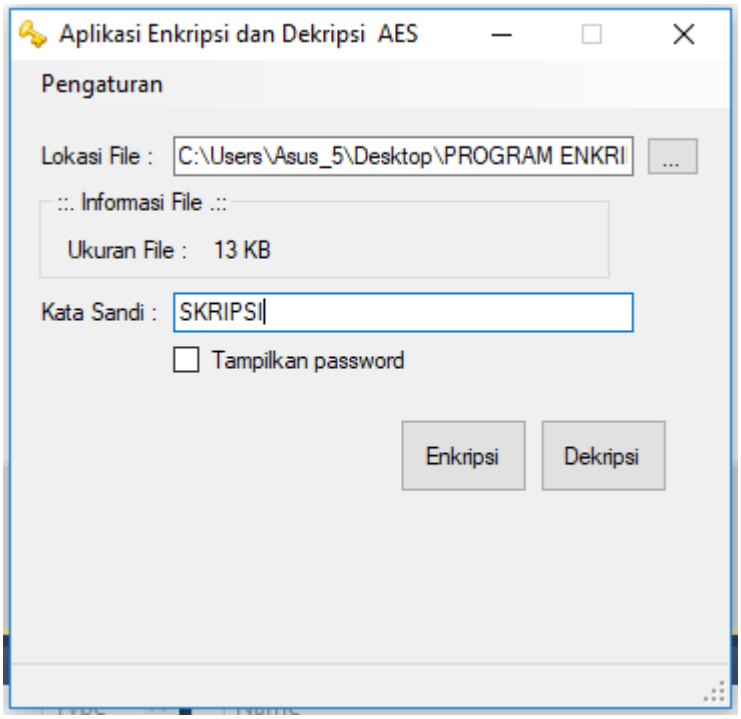
4.2.2 Tampilan Aturan Penggunaan Aplikasi

Tampilan aturan penggunaan aplikasi merupakan tampilan halaman atau form yang berisi tentang tata cara penggunaan aplikasi yang dijalankan. Padahal aman tersebut di jelaskan apa - apa saja yang menjadi kewajiban bagi pengirim dan penerima saat menjalankan simulasi algoritma AES.

Gambar 4.2 Tampilan Aturan Penggunaan Aplikasi

4.2.3 Tampilan Halaman Utama Algoritma AES

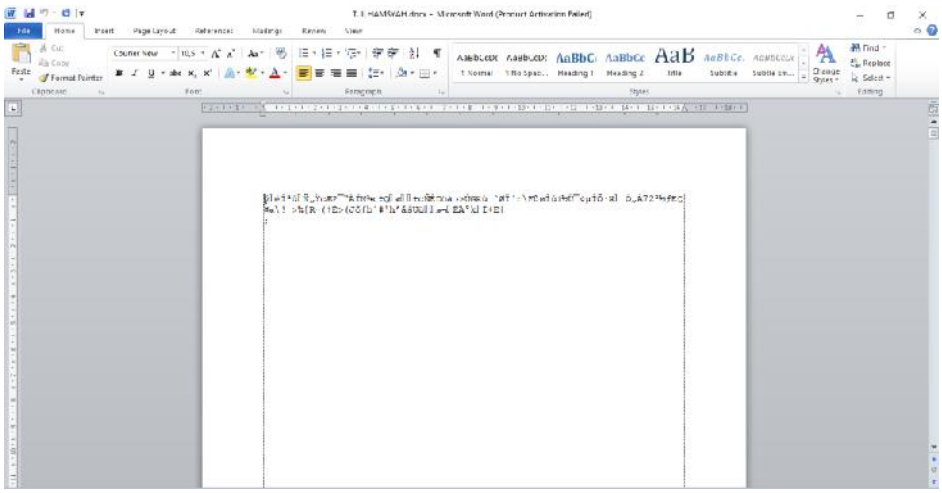
Tampilan berikut merupakan tampilan utama pada aplikasi ini. Algoritma AES merupakan protokol yang menjamin tidak adanya pertukaran kunci antara pihak-pihak yang melakukan enkripsi dan dekripsi. Kedua belah pihak menggunakan kunci mereka masing–masing untuk mengenkripsi pesan dan kemudian untuk mendekripsi pesan tanpa perlu mengetahui kunci yang lainnya.



Gambar 4.3 Tampilan Halaman Utama Algoritma AES

4.2.4 Tampilan Hasil Algoritma AES

Tampilan berikut ini merupakan tampilan hasil file yang di enkripsi menggunakan algoritma AES:



Gambar 4.4 Tampilan Hasil Algoritma AES

BAB V

PENUTUP

5.1 Kesimpulan

Secara keseluruhan perancangan dan pembuatan aplikasi enkripsi dan dekripsi yang menggunakan metode kriptograpi *Advanced Encryption Standard* (AES) ini dapat diambil kesimpulannya sebagai berikut :

1. Penerapan kriptograpi dengan metode *Advanced Encryption Standard* (AES) ini mampu mengubah data asli (*plaintext*) menjadi data rahasia (*chipertext*).
2. Penerapan algorithma AES pada aplikasi keamanan data ini mengubah data yang ingin diamankan (*plaintext),* kemudian dilakukan dengan proses enkripsi dan dekripsi, proses enkripsi dilakukan dengan 4 langkah proses, langkah yang pertama adalah *AddRoundkey,* melakukan *XOR* antara *plaintext* dengan *chiperkey,* langkah kedua ialah *subbyte (substitusi byte)* dengan menggunakan tabel substitusi (S.BOX), langkah ketiga adalah *ShiftRows* adalah proses mengacak data masing-masing kolom *array* stat, kemudian langkah ke empat yaitu *Mixcolumn*s, mengacak data di masing – masing kolom *array state* dengan menggunakan rumus dan begitu juga dalam melakukan dekripsi.
3. Aplikasi ataupun metode yang digunakan mampu menjadi rekomendasi dalam perlidungan data diberbagai kepentingan digital.

5.2 Saran

Saran – saran yang berguna untuk pengembangan lebih lanjut terhadap program aplikasi ini sebagai berikut :

1. Menciptakan pengembangan keamanan data untuk skala yang lebih luas pada aplikasi ini.
2. Tampilan yang *frendly* dan tambahan fitur bisa menjadi pilihan dalam pengembangan aplikasi.
3. Menciptakan versi yang berbeda dalam setiap kebutuhan pengguna untuk meningkatkan kinerja aplikasi dari setiap kebutuhan.

DAFTAR PUSTAKA

A.S, Rosa & M. Salahuddin, 2013. *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek.* Bandung: Informatika.

A.S. Rosa & M. Salahuddin, 2014. *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*. Bandung: Informatika.

Abdullor, Rohi, 2015. *Web Programming is Easy*. Jakarta: PT Elex Media Komputindo.

Anwar, Syaiful & Fahrizal Irawan, 2017. *Rancang Bangun Sistem Informasi Pengajuan Pengadaan Suku Cadang Mobil Pada PT. Andalan Chrisdeco Berbasis Web.* Jurnal Pilar Nusa Mandiri. Jakarta Selatan: Program Studi Manajemen Informatika, AMIK BSI Jakarta.

Badawi, A. (2018). Evaluasi Pengaruh Modifikasi Three Pass Protocol Terhadap Transmisi Kunci Enkripsi.

Balantai Timur. Jurnal TEKNOIF. Padang: Dosen Sekolah Tinggi Manajemen Informatika Komputer, STMIK Jayanusa Padang.

Basri, 2016. *Kriptografi Simetris dan Asimetris Dalam Perspektif Keamanan Data dan Kompleksitas Komputasi*. Sulawesi Barat: Universitas Al Asyariah Mandar.

Dhany, H. W., Izhari, F., Fahmi, H., Tulus, M., & Sutarman, M. (2017, October). Encryption and decryption using password based encryption, MD5, and DES. In International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017) (pp. 278-283). Atlantis Press.

Fachri, Barany. "Aplikasi Perbaikan Citra Efek Noise Salt & Papper Menggunakan Metode Contraharmonic Mean Filter." Seminar Nasional Royal (Senar). Vol. 1. No. 1. 2018.

Fuad, R. N., & Winata, H. N. (2017). Aplikasi Keamanan File Audio Wav (Waveform) Dengan Terapan Algoritma Rsa. Infotekjar: Jurnal Nasional Informatika Dan Teknologi Jaringan, 1(2), 113-119.

Gellinas, U. J. & Dull, R. B, 2012. *Accounting Information Systems, 9th ed*. USA:

Harison & Ahmad Syarif, 2016. *Sistem Informasi Geografis Sarana Kabupaten Pasaman Barat*. Jurnal TEKNOIF. Padang: Institut Teknologi Padang.

Hariyanto, E., Lubis, S. A., & Sitorus, Z. (2017). Perancangan prototipe helm pengukur kualitas udara. KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), 1(1).

Hendini, Ade, 2016. *Pemodelan UML, Sistem Informasi Monitoring Penjualan dan Stok Barang (Studi Kasus: Distro Zhezha Pontianak)*. Jurnal Khatulistiwa Informatika. Pontianak: Program Studi Manajemen Informatika, AMIK BSI Pontianak.

Hendrawan, J. (2018). Rancang Bangun Aplikasi Mobile Learning Tuntunan Shalat. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 44-59.

Ibrahim, 2015. *Metode Penelitian Kualitatif*. Bandung: Alfabeta.

Indrajani, 2015. *Database Design Case Study All In One*. Jakarta: PT Elex Media Komputindo.

Iqbal, M., Siahaan, A. P. U., Purba, N. E., & Purwanto, D. (2017). Prim's Algorithm for Optimizing Fiber Optic Trajectory Planning. Int. J. Sci. Res. Sci. Technol, 3(6), 504-509.

Iswandy, Eka, 2015. *Sistem Penunjang Keputusan Untuk Menentukan Penerimaan Dana Santunan Sosial Anak Nagari dan Penyalurannya Bagi Mahasiswa dan Pelajar Kurang Mampu di Kenagarian Barung-Barung*

Jakarta: Salemba Empat.

Komputindo, Elex Media, 2016. *Pengenalan HTML dan CSS*. Jakarta: PT Elex Media Komputindo.

Krismiaji, 2015. *Sistem Informasi Akuntansi*. Bogor: Ghalia Indonesia.

Kurniwati, Ana & Muhammad Dwiky Darmawan, 2016. *Implementasi Algoritma Advanced Encryption Standard (AES) Untuk Enkripsi dan Deskripsi Pada Dokumen Teks*. Jurnal. Depok: Universitas Guna Darma.

Ladjamuddin, Bin Al-Bahra, 2013. *Analisis dan Desain Sistem Infornasi*.

Lusiana, Veronica, 2013. *Implementasi Kriptografi Pada File Dokumen Menggunakan Algoritma AES-128*. Jurnal. Semarang: Universitas Stikubank Semarang.

Mariance, U. C. (2018). Analisa dan Perancangan Media Promosi dan Pemasaran Berbasis Web Menggunakan Work System Framework (Studi Kasus di Toko

Mandiri Prabot Kota Medan). Jurnal Ilmiah Core IT: Community Research Information Technology, 6(1).

Mulyadi, 2016. *Sistem Akuntansi*. Jakarta: Salemba Empat.

Penerbit Mediakom.

Prabowo, Heri, Herlawati & WIda Prima Mustika, 2014. *Sistem Informasi Panduan Trayek Angkutan Umum Berbasis Mobile Smartphone Pada Dinas Perhubungan Jakarta*. Jurnal Pilar Nusa Mandiri. Jakarta Pusat: Program Studi Sistem Informasi, Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri Jakarta.

Putri, N. A. (2018). Sistem Pakar untuk Mengidentifikasi Kepribadian Siswa Menggunakan Metode Certainty Factor dalam Mendukung Pendekatan Guru. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 78-90.

Rahim, R. (2018, October). A Novelty Once Methode Power System Policies Based On SCS (Solar Cell System). In International Conference of ASEAN Prespective and Policy (ICAP) (Vol. 1, No. 1, pp. 195-198).

Romney, Marshal R. & Paul John Steinbart, 2015. *Sistem Informasi Akuntansi*.

Sadikin, Rifki, 2012. *Kriptografi Untuk Kemanan Jaringan*. Yogyakarta: Andi Offset.

Sarif, M. I. (2017). Penemuan Aturan yang Berkaitan dengan Pola dalam Deret Berkala (Time Series).

Sarif, M. I. Classification Of Feasibility Of Basic Food Recipients In Kelurahan Tanjung Morawa A, Tanjung Morawa Sub-District Using Naïve Bayes Classifier Algorithm.

Sibero, Alexander F.K, 2014. *Web Programming Power Pack*. Yogyakarta:

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

Sitorus, Z., Saputra, K, S., Sulistianingsih, I. (2018) C4.5 Algorithm Modeling For Decision Tree Classification Process Against Status UKM.

South-Western Cengage Learning.

Sumartono, I., Siahaan, A. P. U., & Mayasari, N. (2016). An overview of the RC4 algorithm. IOSR J. Comput. Eng, 18(6), 67-73.

Tullah, Rahmat, Muhammad Iqbal Dzulhaq & Yudi Setiawan, 2016. *Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma Advanced Encryption*

Standard (AES). Jurnal SISFOTEK GLOBAL. Tanggerang: STMIK Bina Sarana Global.

Tulloh, Rahmat Aditia, Yurika Permanasari & Erwin Harahap, 2016. *Kriptografi Advanced Encryption Standard (AES) Untuk Penyandingan File Dokumen*. Prosiding Matematika: Bandung: Prodi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Islam Bandung.

Url: (https://id.m.wikipedia.org/wiki/Bahasa_pemograman).

Wahana, Komputer, dkk, 2014. *Sistem Informasi Penjualan Online Untuk Tugas Akhir*. Semarang: Penerbit Wahana Komputer.

Website:

Wikipedia Ensiklopedia, 2018. *Bahasa Pemograman*. Wikipedia Bahasa Indonesia. Diakses pada tanggal 15 Desember 2018.