IMPLEMENTASI ALGORITMA AFFINE CIPHER UNTUK KEAMANAN DATA

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	**: IMAL AMRI**
N.P.M	**: 1414370028**
PROGRAM STUDI	**: SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

ABSTRAK

Algoritma AffineCipher merupakan salah satu metode yang dapat mengamankan data berupa text dengan subtitusi menggunakan tabel ASCII. Kriptografi merupakan salah satu metode mengamankan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data sera keaslian pengirim. Kriptografi biasanya dalam bentuk enkripsi dan Deskripsi. Tabel ascci atau yang disebut *American Standard Code for Information Interchange*merupakan suatu standar internasional dalam kode huruf dan simbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal, contohnya 124 adalah untuk karakter "|". Dalam hal ini, penulis berkeinginan mengangkat topik enkripsi dan Deskripsi menjadi sebuah penulisan ilmiah skripsi dengan menggunakan teknologi dekstop yang berkembang saat ini. Algoritma yang dipakai adalah AffineCipher dikombinasikan oleh tabel ASCII.Diharapkan dengan adanya aplikasi ini, mahasiswa serta dosen dapat melakukan uji coba enkripsi menggunakan algoritma AffineCipher.

Kata Kunci: Kriptografi, AffineCipher, Tabel ASCII

DAFTAR ISI

Halaman

DAFTAR GAMBAR

No. Judul **Halaman**

DAFTAR TABEL

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Tuhan Yang Maha Esa, yang telah memberikan rahmat-Nya kepada peneliti, sehingga Skripsi ini dapat diselesaikan oleh peneliti tepat pada waktunya dengan judul Implementasi Algoritma Affine Cipher Untuk Keamanan Data.

Skripsi ini dilakukan guna memenuhi salah satu syarat pemenuhan kurikulum dalam menyelesaikan pendidikan pada Program Studi S1 Sistem Komputer Fakultas Teknik Universitas Pembangunan Panca Budi Medan. Pada kesempatan ini, penulis menyampaikan rasa terima kasih dan penghargaan yang sebesar-besarnya kepada :

1. Bapak Dr. H. Muhammad Isa Indrawan, SE, MM, selaku Rektor Universitas Pembangunan Panca Budi Medan.
2. Ibu Sri Shindi Indira, S.T., M.S.C, selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
3. Bapak Andysyah Putera Utama S, S.Kom, M.Kom, Selaku Pembimbing 1 yang juga telah memberikan pengarahan dan petunjuk Skripsi Ini.
4. Bapak Dr. Muhammad Iqbal, S.Kom., M.Kom Selaku Dosen Pembimbing II yang juga telah memberikan pengarahan dan petunjuk dalam Skripsi ini.
5. Bapak/Ibu Dosen beserta seluruh staf Universitas Pembangunan Panca Budi Medan.

6. Teristimewa kepada Kedua Orang Tua dan Keluarga saya, yang telah banyak memberikan bimbingan dan bantuan baik moril maupun material selama penulis mengikuti pendidikan hingga selesainya Skripsi ini.
7. Kepada seluruh rekan-rekan di program Studi Teknik Komputer Universitas Pembangunan Panca Budi Medan yang telah memberikan dukungan moril kepada penulis.

Penulis menyadari bahwa Skripsi ini masih kurang sempurna. Oleh karena itu, penulis sangat mengharapkan dan menghargai saran maupun kritikan dari pembaca dan semua pihak yang mengarah kepada perbaikan Tuga Akhir ini.

Medan, 30 Agustus 2019
Penulis,

IMAL AMRI
NPM. 1414370028

BAB I

PENDAHULUAN

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 *Affine Chiper*.*Affine Chiper*ini mempunyai 26 kemungkinan karena menggunakan alfabet.*Affine Chiper*merupakan algoritma klasik untuk menyandikan sebuah *plaintext* dengan cara substitusi sehingga dalam memecahkan pesan tersebut akan terasa susah.Penelitian ini menggunakan pemrograman *Visual Basic.Net* 2010.

Algoritma Affine Chiper merupakan salah satu metode kriptografi berbasis protokol. Protokol adalah aturan yang berisi tentang langkah-langkah yang melibatkan dua kunci yang dibuat untuk menyelesaikan suatu kegiatan. Dalam kriptografi, protokol digunakan oleh orang-orang yang terlibat, seperti untuk proses otentifikasi, pengaktifan bilangan acak, bahkan untuk berbagi dan bertukar informasi yang bersifat rahasia. Pengirim dan penerima pesan melakukan penukaran sebanyak tiga tahap untuk mengekripsikan pesan tersebut. Pada

dasarnya,*Algoritma Affine Chiperdi implementasikan* dengan menggunakan satu algoritma enkripsi dan dekripsi yang telah disepakati oleh kedua belah pihak.

Berdasarkan latar belakang yang telah penulis uraikan diatas, maka penulis tertarik untuk memilih judul **"*Implementasi Algoritma Affine Cipher Untuk Keamanan Data*".**

2. Rumusan Masalah

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

a. Bagaimana merancang sebuahkeamanan data teks yang bersifat rahasia?
b. Bagaimana menerapkan metode algoritma *Affine Chiper*dalam proses keamanan data teks yang bersifat rahasia*?*

3. Batasan Masalah

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

a. Implementasi enkripsi dan dekripsi hanya berupa teks.
b. Program yang dibahas menggunakan pemrograman Visual Basic.Net 2010.
c. Menggunakan Tabel Konversi Affine Cipher ke Angka.

4. Tujuan Penelitian

Adapun tujuan dari penelitian ini dengan menggunakan algoritma *Affine Chiper*ini yang ingin dicapai adalah sebagai berikut:

a. Merancang aplikasi keamanan data teks dengan algoritma *Affine Chiper*.
b. Memperkuat keamanan data teks yang bersifat rahasia.

5. Manfaat Penelitian

Adapun manfaat dalam penelitian ini yang diperoleh dari penerapan algoritma *Affine Chiper*adalah sebagai berikut:

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

6. Metodologi Penelitian

Dalam metodologi penelitian ini peneliti menggunakan beberapa metode dalam pengumpulan data untuk melengkapi hasil penelitian ini. Adapun metode tersebut sebagai berikut:

a. Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan dalam penelitian ini adalah sebagai berikut:

1) Studi Pustaka yaitu pengumpulan data yang diperoleh dari sumber tertulis berupa buku-buku, artikel ilmiah, dan penelitian-penelitian yang berkaitan dengan judul penelitian.

2) Studi literature yaitu pengumpulan data yang diperoleh dari literature, jurnal, paper, dan bacaan-bacaan dari berbagai sumber yang berkaitan dengan judul penelitian.

b. Metode pengembangan dan perancangan sistem

Pada kasus ini menggunakan metode *Affine Chiper*yang merupakan salah satu contoh metode kriptografi kunci simetris dengan model penggantian karakter. Metode *Affine Chiper*merupakan metode yang menggunakan kunci berupa angka, sedangkan *Affine Chiper*merupakan metode yang menggunakan kunci abjad sebagai kunci penyandian untuk penggantian karakter dari pesan rahasia yang dikirim. Pada penelitian ini diharap dapat memberi solusi terhadapmasalah keamanan data yang lebih aman.

7. Sistematika Penulisan

Secara garis besar sistematika penulisan tugas akhir ini terdiri dari lima bab yaitu sebagai berikut:

BAB I PENDAHULUAN

Pada bab pendahuluan ini, akan menguraikan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab landasan teori ini, akan memaparkan teori-teori yang digunakan sebagai panduan dalam menyelesaikan skripsi sesuai dengan judul yang diteliti dan dapat diperoleh dari berbagai sumber.

BAB III ANALISA MASALAH DAN RANCANGAN PROGRAM

Pada bab analisa masalah dan rancangan program ini, menjelaskan tentang gambaran pembahasan permasalahan yang terjadi serta perancangan sistem yang ingin diselesaikan.

BAB IV IMPLEMENTASI DAN HASIL UJI COBA PROGRAM

Pada bab implementasi dan analisa hasil uji coba program ini, membahas tentang hasil implementasi yang dibuat serta melakukan analisa terhadap hasil tersebut.

BAB V PENUTUP

Pada bab penutup ini,berisi tentang kesimpulan dan saran yang diperoleh dari hasil penelitian untuk pengembangan serta perbaikan yang di perlukan dari hasil penelitian ini.

BAB II

LANDASAN TEORI

1. Kemanan Data

Pada zaman teknologi informasi sekarang, data atau informasi merupakan suatu asset yang sangat berharga dan harus dilindungi. Hal ini juga diikuti oleh kemajuan teknologi komputer. Kemajuan teknologi komputer membantu semua aspek kehidupan manusia. Dengan adanya kemajuan dalam teknologi informasi, komunikasi dan komputer maka kemudian muncul masalah baru, yaitu masalah keamanan akan data dan informasi dan dalam hal ini akan membuka peluang bagi orang-orang yang tidak bertanggung jawab untuk menggunakannya sebagai tindak kejahatan. Dan tentunya akan merugikan pihak tertentu. Dalam keamanan data ada beberapa aspek yang berkaitan dengan persyaratan kemanan yaitu:

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.

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

Availability. Berhubungan dengan ketersediaan data dan informasi. Data dan informasi yang berada dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak. (Ariyus, 2006)

Lebih lanjut menurut Ariyus (2006), terdapat lima langkah kemanan komputer yang baik untuk diperhitungkan yaitu; aset, analisis resiko, perlindungan, alat dan prioritas.

Keamanan Menurut Para Ahli, Menurut David Icove Berdasarkan lubang kemanan, keamanan komputer dapat dibagi menjadi 4 macam, yaitu :

a. Keamanan Fisik (Physical Security), termasuk akses orang ke gedung, peralatan, dan media yang digunakan.

   Contoh : Wiretapping atau hal-hal yang ber-hubungan dengan akses ke kabel atau

b. komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.

   1) Denial Of Service, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlahpesan).

   2) Syn Flood Attack, dimana sistem (host) yang dituju dibanjiri oleh permintaan sehingga diamenjadi ter-lalu sibuk dan bahkan dapat berakibat macetnya sistem (hang).Keamanan yang berhubungan dengan orang

   Contoh :

   - Identifikasi user (username dan password)
   - Profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).
   - Keamanan dari data dan media serta teknik komunikasi

- Keamanan dalam operasi : Adanya prosedur yang digunakan untuk mengatur danmengelola sistem keamanan
- juga ter-masuk prosedur setelah serangan (post attack recovery).

Menurut G. J. Simons

Keamanan informasi adalah bagaimana kita dapat mencegah penipuan (cheating) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Keamanan sistem informasi bisa diartikan sebagai kebijakan, prosedur, dan pengukuran teknis yang digunakan untuk mencegah akses yang tidak sah, perubahan program, pencurian, atau kerusakan.

Karakteristik Penyusup :

a. The Curious (Si Ingin Tahu) – tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang anda miliki.

b. The Malicious (Si Perusak) – tipe penyusup ini berusaha untuk merusak sistem anda, atau merubah web page anda, atau sebaliknya membuat waktu dan uang anda kembali pulih.

c. The High-Profile Intruder (Si Profil Tinggi) – tipe penyusup ini berusaha menggunakan sistem anda untuk memperoleh popularitas dan ketenaran. Dia mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya.

d. The Competition (Si Pesaing) – tipe penyusup ini tertarik pada data yang anda miliki dalam sistem anda. Ia mungkin seseorang yang beranggapan

bahwa anda memiliki sesuatu yang dapat menguntungkannya secara keuangan atau sebaliknya fisik terhadap sistem informasi.

2. Kriptografi

Kriptografi merupakan kata dari bahasa Yunani yaitu cryptography, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Sehingga, bila digabungkan akan menjadi kata yang berarti menyembunyikan/merahasiakan tulisan. Kriptografi (cryptography) merupakan ilmu dan seni penyimpanan pesan, data, atau informasi secara aman. Kriptografi (Cryptography) berasal dari bahasa Yunani yaitu dari kata Crypto dan Graphia yang berarti penulisan rahasia. Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut Cryptology. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (plaintext) ke dalam bentuk data sandi (ciphertext) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (sender) kepada penerima (receiver). Setelah sampai di penerima, ciphertext tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali. Proses tranformasi dari plaintext menjadi ciphertext disebut proses Encipherment atau enkripsi (encryption), sedangkan proses mentransformasikan kembali ciphertext menjadi plaintext disebut proses dekripsi (decryption)

Untuk mengenkripsi dan mendekripsi data. Kriptografi menggunakan suatu algoritma (cipher) dan kunci (key). Cipher adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data.

Suatu pesan yang tidak disandikan disebut sebagai plaintext ataupun dapat disebut juga sebagai cleartext. Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext disebut encryption atau encipherment. Sedangkan proses untuk mengubah ciphertext kembali ke plaintext disebut decryption atau decipherment. Secara sederhana istilah-istilah di atas dapat digambarkan sebagai berikut :

Kriptografi adalah suatu ilmu ataupun seni mengamankan pesan dan dilakukan oleh *cryptographer* (Anonim, 2003). Menurut Rhee (1994) kriptografi digunakan untuk memastikan privasi dan autentifikasi data dalam komunikasi antar sistem komputer. Terdapat dua proses dasar dalam kriptografi yaitu:

a. Enkripsi, adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). (Ariyus, 2006)

b.Deskripsi, adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. (Fresly, 2015)

Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah plaintext. Kemudian setelah disamarkan dengan suatu cara penyandian, maka plain textini disebut sebagai chipper text. Proses penyamaran dari plain text ke cipher text disebut enkripsi (encryption), dan proses

pengembalian dari cipher text menjadi plaintext kembali disebut dekripsi (decryption). (Fresly, 2015). *File* yang dapat dienkripsi dapat berupa teks, gambar maupun audio dan video.

3. Macam-Macam Kriptografi

Kriptografi dibedakan menjadi 3 bagian yaitu kriptografi simetris, kriptografi asimetris dan fungsi hash satu arah.

Kriptografi simetris disebut juga kriptografi kunci rahasia merupakan jenis kriptografi paling intuitif. Ini termasuk penggunaan kunci rahasia yang dikenal hanya pada pengguna komunikasi yang aman. Kode Hill atau lebih dikenal dengan Hill cipher merupakan salah satu algoritma kriptografi kunci simetris dan merupakan salah satu kripto polyalphabetic. Hill cipher diciptakan oleh Lester S. Hill pada tahun 1929 . Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan cipher yang tidak dapat dipecahkan menggunakanteknik analisis frekuensi. Berbeda dengan caesar cipher, hill cipher tidak mengganti setiap abjad yang sama pada plainteks dengan abjad lainnya yang sama pada cipherteks karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. Hill cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini enggunakan sebuah matriks persegi sebagai kunci berukuran m x m sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam Hill cipher antara lain adalah perkalian antar matriks dan melakukan invers pada matriks . Karena menggunakan matriks sebagai kunci, Hill cipher merupakan algoritma kriptografi kunci simetris yang

sulit dipecahkan, karena teknik kriptanalisis seperti analisis frekuensi tidak dapat diterapkan dengan mudah untuk memecahkan algoritma ini. Hill cipher sangat sulit dipecahkan jika kriptanalis hanya memiliki ciphertext saja (chipertext-only), namun dapat dipecahkan dengan mudah jika kriptanalis memiliki ciphertext dan potongandariplaintext-nya(known-plaintext).

Contoh Kriptografi Simetris :

Perhitungan Matematis Dasar dari teknik hill cipher adalah aritmatika modulo terhadap matriks. Dalam penerapannya, Hill cipher menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada hill cipher adalah matriks n x n dengan n merupakan ukuran blok. Jika matriks kunci kita sebut dengan K, maka matriks K.

Kriptografi asimetris sendiri berbeda dengan kriptografi simetris, dimana kriptografi asimetris ini menggunakan dua kunci yang berbeda, yaitu kunci publik dan kunci rahasia atau kunc pribadi. Kunci-kunci tersebut berhubungan secara matematis, tetapi tidak mungkin secara perhitungan untuk menarik kesimpulan satu dengan yang lain. Asimetris, sering juga disebut dengan algoritma kunci publik atausandi kunci publik, menggunakan dua jenis kunci, yaitu kunci publik (public key) dan kunci rahasia (secret key). Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan. Kunci publik bersifat umum, artinya kunci ini tidak dirahasiakan sehingga dapat dilihat oleh siapa saja. Sedangkan kunci rahasia adalah kunci yang dirahasiakan dan hanya orang-orang tertentu saja yang boleh mengetahuinya. Keuntungan utama dari algoritma ini adalah memberikan jaminan

keamanan kepada siapa saja yang melakukan pertukaran informasi meskipun di antara mereka tidak ada kesepakatan mengenai keamanan pesan terlebih dahulu maupun saling tidak mengenal satu sama lainnya.

Contoh Kriptografi Asimetris

Contoh:RSA:

Kunci Publik:

- Pilih bil. prima p = 7 dan q = 11, n = 7.11 =77
- F(n)=(p-1).(q-1)=6.10=60artinya.

F(n)={1,2,3,4,6,8,..,76}={x|gcd(x, n)=1}

- Pilih e dalam {x|gcd(x, 60)=1}, misalnya e=17
- Hapus p dan q dan Kunci Publik n=77, e=17

Kunci Rahasia:

- d = e-1 mod F(n), d .e = 1 mod 60, d =53
- 53 . 17 mod 60 = 901 mod 60 = 1 mod 60

Pengertian Kriptografi Hibrid Permasalahan yang menarik pada bidang kemanan informasi adalah adanya trade off antara kecepatan dengan kenyamanan. Semakin aman semakin tidak nyaman, berlaku juga sebaliknya semakin nyaman semakin tidak aman. Salah satu contohnya adalah bidang kriptografi. Tetapi hal

ini dapat diatasi dengan penggunaan kriptografi hibrida. Kriptografi hibrida sering dipakai karena memanfaatkan keunggulan kecepatan pemrosesan data oleh algoritma simetrik dan kemudahan transfer kunci menggunakan algoritma asimetrik. Hal ini mengakibatkan peningkatan kecepatan tanpa mengurangi kenyamanan serta keamanan. Aplikasi kriptografi hibrida yang ada saat ini pada umumnya ditujukan untuk penggunaan umum atau mainstream yang merupakan pengguna komputer. Aplikasi pada umumnya mengikuti perkembangan hardware komputer yang semakin cepat dari waktu ke waktu. Sehingga hardware yang sudah lama tidak dapat difungsikan sebagaimana mestinya. Selain itu banyak perangkat embedded dengan kekuatan pemrosesan maupun daya yang terbatas. Terutama dengan trend akhir akhir ini, hampir semua orang memiliki handheld device yang mempunyai kekuatan terbatas, seperti telepon seluler.
Dalam tugas akhir ini dibahas mengenai perancangan sebuah aplikasi kriptografi hibrida yang ditujukan untuk kalangan tertentu, terutama pemakai hardware dengan kekuatan pemrosesan yang terbatas. Aplikasi yang ingin dicapai adalah aplikasi yang sederhana, ringan dan cepat tanpa mengurangi tingkat keamanan menggunakan hash. Sistem ini mengggabungkan chiper simetrik dan asimetrik. Proses ini dimulai dengan negosiasi menggunakan chiper asimetrik dimana kedua belah pihak setuju dengan private key/session key yang akan dipakai. Kemudian session key digunakan dengan teknik chiper simetrik untuk mengenkripsi conversation ataupun tukar-menukar data selanjutnya. Suatu session key hanya dipakai sekali sesi. Untuk sesi selanjutnya session key harus dibuat kembali.

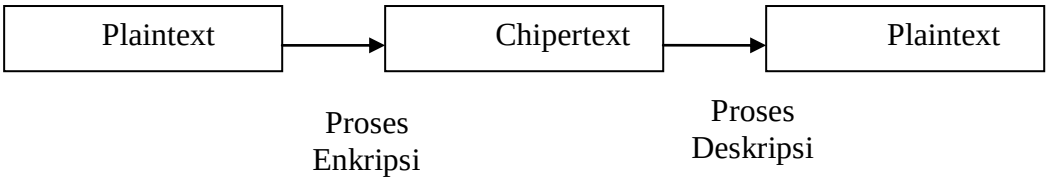
Fungsi *hash* satu arah, juga dikenal sebagai rangkuman pesan atau fungsi kompresi adalah fungsi matematis yang mengambil input panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap.

4. Enkripsi

Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di dekripsi (kebalikan dari proses enkripsi) dahulu. Encryption berasal dari bahasa yunani kryptos yang artinya tersembunyi atau rahasia. Dikarenakan enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi. Di pertengahan tahun 1970-an, enkripsi kuat dimanfaatkan untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain publik, dan saat ini enkripsi telah digunakan pada sistem secara luas, seperti Internet e-commerce, jaringan Telepon bergerak dan ATM pada bank. *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

Enkripsi merupakan hal yang sangat penting dalam kriptografi supaya keamanan data yang dikrimkan bisa terjaga kerahasiaannya. Pesan asli (plaintext) diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan

chiper atau kode. Sama halnya dengan kita yang tidak mengerti sebuah kata, kita akan dapat melihatnya di dalam kamus atau daftar istilah-istilah. Berbeda halnya dengan enkripsi, untuk mengubah plaintext ke bentuk chipertext, kita harus menggunakan algoritma yang dapat mengkodekan data yang kita inginkan. Berikut adalah penggambaran proses enkripsi.



Gambar 1Proses Enkripsi
(sumber: google image)

5. Kriptografi Klasik

Kriptografi berasal dari bahasa Yunani yang secara etimologi terdiri dari dua kata yaitu cryptos yang berarti tersembunyi dan graphein yang berarti menulis. Sedangkan pengertian kriptografi adalah metode untuk mengirimkan pesan secara rahasia (yaitu, dalam penyamaran bentuk) sehingga hanya penerima yang dimaksud yang dapat membaca dan memahami pesan tersebut. (Mollin, 2007). Kriptografi adalah sebuah seni untuk menjaga keamanan pesan. Seni merubah pesan yang sebenarnya menjadi pesan yang tidak berarti sehingga pihak lain yang tidak berkepentingan tidak dapat memahaminya (Bishop, 2003). Menurut Hankerson et al (2004) kriptografi merupakan sebuah analisis dan perancangan teknik-teknik matematika yang dapat mengamankan komunikasi terhadap musuh yang berbahaya.

Keamanan kriptografi modern tidak didasarkan pada kerahasiaan algoritma, tetapi pada kerahasiaan informasi yang relatif sedikit, yang disebut kunci rahasia. Kunci (key) adalah parameter yang digunakan untuk mengontrol transformasi kriptografi (ciphering) dan merupakan elemen yang dapat diubah. Pengguna dapat mengubah kunci setiap saat sedangkan algoritma penyandiannya sendiri adalah elemen konstan dari cryptosystem yang merupakan hasil dari penelitan dan pengujian jangka panjang (Moldovyan, 2007).

Menurut Bishop (2005) kriptografi klasik adalah kriptografi yang disebut juga sebagai kriptografi kunci tunggal atau kriptografi simetris yang menggunakan kunci yang sama untuk enkripsi maupun deskripsi.

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. Metode penulisan rahasia diketahui telah ada sejak 2500 tahun yang lalu. David Kahn, penulis buku "The Code Breakers" mengatakan bahwa kriptografi muncul secara spontan sebagaimana munculnya bahasa dan tulisan. Lalu, karena banyak manusia yang membutuhkan dan tuntutan akan menjaga kerahasiaan komunikasi antara dua atau banyak orang di tengah-tengah kehidupan sosial masyarakat yang mendorong lahirnya ilmu tulisan rahasia atau dikenal dengan kriptografi. (Dooley, 2013). Penggunaan kriptografi telah dikenal sejak masa kuno, yakni bangsa Yunani dan bangsa Roma yang menggunakannya dalam bentuk yang berbeda. Namun, ketika negara Roma mengalami masa keterpurukan, pembelajaran mengenai kriptografi juga menghilang dan akan muncul kembali

pada saat zaman Renaissance di Barat. Berbanding terbalik dengan Roma, kriptografi berkembang di Arab. Hal ini terbukti dengan ditemukannya suatu penemuan penting oleh Abu Yusuf Ya'qub ibn Isaq as-Sabbah al-Kindi yaitu frequency analysis yang bermanfaat sebagai metode memecahkan suatu pesan rahasia. (Dooley, 2013). 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.

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

6. Kriptografi Simestris

Pada kriptografi simetris, kunci yang digunakan pada proses enkripsi dan dekripsi bernilai sama. Proses yang dilakukan dalam kriptografi simetris terbagi atas dua jenisyaitu substitusi dan transposisi. Algoritma simetris *(symmetric algorithm)* adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm.* Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci rahasia *(secret-key algorithm).* Kriptografi simetrik (symetric chipers) adalah kriptografi dimana dalam proses enkripsi dan dekripsi nya menggunakan satu key yang sama. Disebut juga private key atau chiper secret key. Algoritma kriprografi simetris adalah algoritma yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya, sedangkan algoritma kriprografi asimetris mempunyai kunci enkripsi dan kunci dekripsi yang berbeda. Algoritma kriprografi simetris sering disebut algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci, dan mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu. Kelebihan dari algoritma kriprografi simetris adalah waktu proses untuk enkripsi dan dekripsi relatif cepat. Hal ini disebabkan efesiensi yang terjadi pada pembangkit kunci. Karena prosesnya relative cepat maka algoritma ini tepat untuk digunakan pada sistem komunikasi digital.

Kelebihan :

1. Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.

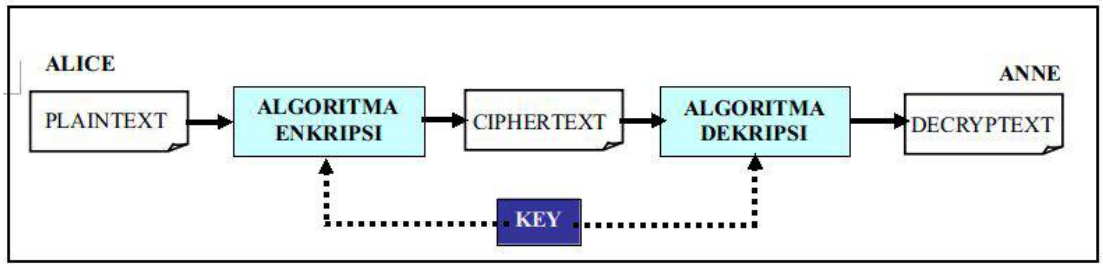
2. Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem *real-time*

Kelemahan :

1. Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.

2. Permasalahan dalam pengiriman kunci itu sendiri yang disebut *"key distribution problem"*

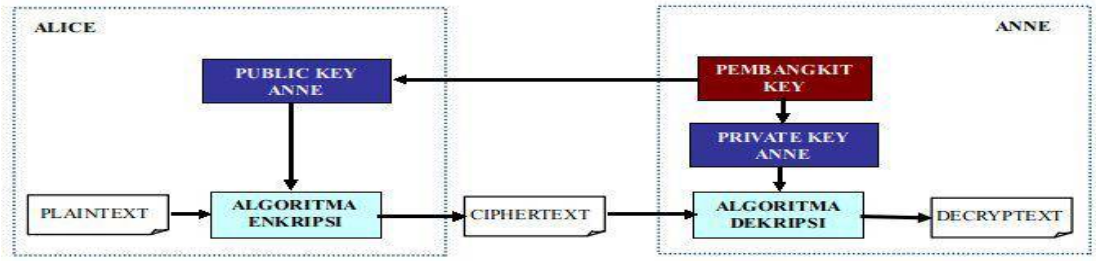
Pada proses substitusi, setiap karakter di ganti dengankarakter lain, sementara pada transposisi, setiap karakter bertukar posisi dengankarakter lain. Hal yang harus diperhatikan pada penggunaan kriptografi simetrisadalah keamanan kunci. Jika, kunci diketahui oleh pihak lain, maka ciphertext yangdirahasiakan dapat dipecahkan. Berikut ini adalah gambar dari proses penggunaankunci simetris.



Gambar 2 Alur Kriptografi Simetris

7. Kriptografi Asimetris

Pada kriptografi asimetris, kunci yang digunakan pada proses enkripsi berbeda dengan kunci yang digunakan untuk proses dekripsi. Kunci enkripsi disebut kunci publik dan kunci untuk dekripsi disebut dengan kunci private. Oleh karena itu, algoritma ini disebut juga dengan kriptografi kunci publik (public key). Berikut ini adalah gambar dari proses penggunaan kunci asimetris, yang ditampilkan pada gambar 1.3 di bawah ini.



Gambar 3 Alur Kriptografi Asimetris (Sadikin, 2012)

Kelebihan kriptografi kunci-publik (asimetri):

1. Hanya kunci privat yang perlu dijaga kerahasiaannya oleh setiap entitas yang berkomuniaksi (tetapi, otentikasi kunci publik tetap harus terjamin). Tidak ada kebutuhan mengirim kunci privat sebagaimana pada sistem simetri.

2. Pasangan kunci publik/kunci privat tidak perlu diubah, bahkan dalam periode waktu yang panjang.

3. Dapat digunakan untuk mengamankan pengiriman kunci simetri.

4. Beberapa algoritma kunci-publik dapat digunakan untuk memberi tanda tangan digital pada pesan.

Kelemahan kriptografi kunci-publik (asimetri):

1. Enkripsi dan dekripsi data umumnya lebih lambat daripada sistem simetri, karena enkripsi dan dekripsi menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar.

2. Ukuran cipherteks lebih besar daripada plainteks (bisa dua sampai empat kali ukuran plainteks).

3. Ukuran kunci relatif lebih besar daripada ukuran kunci simetri.

4. Karena kunci publik diketahui secara luas dan dapat digunakan setiap orang, maka cipherteks tidak memberikan informasi mengenai otentikasi pengirim.

5. Tidak ada algoritma kunci-publik yang terbukti aman (sama seperti block cipher). Kebanyakan algoritma mendasarkan keamanannya pada sulitnya memecahkan persoalan-persoalan aritmetik (pemfaktoran, logaritmik, dan sebagainya) yang menjadi dasar pembangkitan kunci.

8. Cipher Substitusi

Cipher substitusi adalah cipher dengan cara mensubstitusi huruf dengan huruf yanglain sesuai dengan yang ditetapkan.Jenis-jenis cipher substitusi :

a. Cipher Abjad-Tunggal

Monogram Monoalphabetic Cipher adalah cipher yang mengganti setiap huruf pada plainteks dengan huruf yang bersesuaian, sehingga apabila terdapat 26 huruf, maka akan terdapat 26!= 403.291.461.126.605.635.584.000.000 kemungkinan susunan huruf.Salah satu bentuk Monogram Monoalphabetic Cipher adalah cipher yang digunakan oleh kaisar Romawi, Julius Caesar (dinamakan juga Caesar

Chiper), untuk menyandikan pesan yang ia kirim kepada para gubernurnya. Yaitu dengan mengganti (menyulih atau mensubstitusi) setiap karakter dengan karakter lain dalam susunan abjad (alfabet).

b. Cipher Abjad-Majemuk

Pensubstitusian setiap huruf menggunakan kunci yang berbeda. Cipher abjad-majemuk terdiri dari beberapa cipher abjad tunggal yang berbeda-beda. Kebanyakan cipher abjad-majemuk adalah cipher substitusi periodik.Contoh Cipher Abjad-Majemuk adalah Vigenere Cipher.

9. Algoritma

Penyelesaian permasalahan dengan menggunakan alat bantu system computer paling tidak akan melibatkan lima tahapan, yaitu:

a. Analisis masalah

b. Merancang algoritma

c. Membuat program computer

d. Menguji hasil program computer

e. Dokumentasi

Poin kedua menerangkan bahwa dalam perancangan sebuah system computer dibutuhkan adanya perancangan algoritma. Sehingga setelahnya dapat dilanjutkan ke tahap-tahap berikutnya hingga dokumentasi.

Algoritma adalah Sistim kerja komputer memiliki brainware, hardware, dan software. Tanpa salah satu dari ketiga sistim tersebut, komputer tidak akan berguna. Kita akan lebih fokus pada softwarekomputer. Software terbangun atas

susunan program (silahkan baca mengenai pengertian program) dan syntax (cara penulisan/pembuatan program). Untuk menyusun program atau syntax, diperlukannya langkah-langkah yang sistematis dan logis untuk dapat menyelesaikan masalah atau tujuan dalam proses pembuatan suatu software. Maka,Algoritma berperan penting dalam penyusunan program atau syntax tersebut.

Pengertian Algoritma adalah susunan yang logis dan sistematis untuk memecahkan suatu masalah atau untuk mencapai tujuan tertentu. Dalam dunia komputer, Algoritma sangat berperan penting dalam pembangunan suatu software. Dalam dunia sehari-hari, mungkin tanpa kita sadari Algoritma telah masuk dalam kehidupan kita.

Pengertian Algoritma adalah susunan yang logis dan sistematis untuk memecahkan suatu masalah atau untuk mencapai tujuan tertentu.

Algoritma adalah kunci dari bidang ilmu komputer, dan pada dasarnya setiap hari kita melakukan aktivitas algoritma. Kata algoritma berasal dari sebutan Algorizm (Abu Abdullah Muhammad Ibn Musa Al Khwarizmi, ahli matematika Uzbeki

1). Algoritma adalah urutan langkah-langkah berhingga untuk memecahkan masalah logika atau matematika
2). Algoritma adalah logika, metode dan tahapan (urutan) sistematis yang digunakan untuk memecahkan suatu permasalahan.
3). Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis dan logis.

4). Algoritma adalah urutan logis pengambilan keputusan untuk pemecahan masalah.

Pembuatan algoritma harus selalu dikaitkan dengan:

a. Kebenaran algoritma

b. Kompleksitas (lama dan jumlah waktu proses dan penggunaan memori)

Kriteria Algoritma yang baik:

1). Tepat, benar, sederhana, standar dan efektif

2). Logis, terstruktur dan sistematis

3). Semua operasi terdefinisi

4). Semua proses harus berakhir setelah sejumlah langkah dilakukan

5). Ditulis dengan bahasa yang standar dengan format pemrograman agar mudah untuk diimplementasikan dan tidak menimbulkan arti ganda.

Apa yang dimaksud dengan algoritma (algorithm)? Dalam ilmu komputer dan matematika, pengertian algoritma adalah suatu urutan dari beberapa langkah logis dan sistematis yang digunakan untuk menyelesaikan masalah tertentu.

Pendapat lain mengatakan definisi algoritma adalah proses atau serangkaian aturan yang harus diikuti dalam perhitungan atau operasi pemecahan masalah lainnya, terutama oleh komputer. Dengan kata lain, semua susunan logis yang diurutkan berdasarkan sistematika tertentu dan digunakan untuk memecahkan suatu masalah dapat disebut dengan algoritma. Algoritma digunakan untuk melakukan penghitungan, penalaran otomatis, serta mengolah data pada komputer dengan menggunakan software. Dalam algoritma terdapat rangkaian terbatas dari beberapa intruksi untuk menghitung suatu fungsi yang jika dieksekusi dan

diproses akan menghasilkan output, lalu berhenti pada kondisi akhir yang sudah ditentukan.

Berikut ini bentuk dasar algoritma:

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

Pengertian Algoritma Menurut Para Ahli

Agar lebih memahami apa itu algoritma, maka kita dapat merujuk pada pendapat para ahli berikut ini:

1. Abu Ja'far Muhammad Ibnu Musa Al-Khawarizmi

   Menurut Abu Ja'far Muhammad Ibnu Musa Al-Khawarizmi (ahli matematika dari Uzbekistan), pengertian algoritma adalah suatu metode khusus yang digunakan untuk menyelesaikan permasalahan.

2. Donald Ervin Knuth

   Menurut Donald Ervin Knuth, definisi algoritma adalah sekumpulan aturan-aturan berhingga yang memberikan sederetan operasi-operasi untuk menyelesaikan suatu masalah tertentu.

3. S. E. Goodman dan S.T. Hedetniemi

   Menurut Goodman dan Hedetniemi, pengertian algoritma adalah urutan terbatas dari operasi-operasi yang terdefinisi dengan baik, dimana masing-masing membutuhkan memori dan waktu yang terbatas untuk menyelesaikan suatu masalah.

4. Seymour Lipschutz dan Marc Lipson

   Menurut Seymour Lipschutz dan Marc Lipson (praktisi matematika dan komputer), pengertian algoritma adalah suatu daftar langkah demi langkah yang terhingga dari intruksi-intruksi yang terdefinisikan dengan jelas yang digunakan untuk memecahkan permasalahan tertentu.

5. Marvin Minsky

   Menurut Marvin Minsky (pakar Artificial Intelligence), pengertian algoritma adalah seperangkat aturan yang memberitahukan kepada kita dari waktu ke waktu, tepatnya bagaimana untuk bertindak.

6. Andrey Andreyevich Markov

   Menurut Andrey Andreyevich Markov (ahli matematika dari Rusia), pengertian algoritma adalah hal umum untuk dipahami sebagai suatu keputusan yang tepat untuk mendefinisikan proses komputasi yang mengarahkan dari data awal hingga hasil yang diinginkan.

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).

Ada Proses, yaitu rencana atau langkah-langkah yang harus dilakukan untuk mencapai tujuan akhir.

2. Ada Output, yaitu solusi atau tampilan akhir yang didapatkan dari suatu algoritma. Algoritma memiliki minimal satu output.

Ada intruksi-intruksi yang jelas dan tidak ambigu, yaitu instrukti yang jelas dalam algoritma sehingga tidak terjadi kesalahan dalam menghasilkan output.
Ada tujuan akhir yang dicapai, yaitu akhir dari program dimana program akan berhenti ketika tujuan akhir telah tercapai.

Tujuan dan Fungsi Algoritma

Pada dasarnya tujuan dan fungsi utama dari algoritma adalah untuk memecahkan suatu masalah. Lebih jelasnya, adapun tujuan dan fungsi algoritma adalah sebagai berikut:

Untuk membantu menyederhanakan suatu program yang rumit dan besar. Untuk memudahkan dalam membuat sebuah program untuk masalah tertentu. Algoritma dapat digunakan berkali-kali untuk menyelesaikan suatu permasalahan. Membantu memecahkan suatu permasalahan dengan logika dan sistematis.
Untuk meminimalisir penulisan program secara berulang-ulang.Agar dapat melakukan pendekatan top-down dan divide and conquer.

Untuk memudahkan membuat program yang lebih rapih dan terstruktu sehingga lebih mudah dipahami dan dikembangkan. Memudahkan proses modifikasi pada program karena bisa dilakukan hanya pada satu modul tanpa harus mengubah modiul lainnya. Ketika terjadi kesalahan, algoritma dapat membantu menemukannya karena alur kerja yang jelas.

Algoritma dapat diklasifikasikan berdasarkan implementasinya. Mengacu pada pengertian algoritma di atas, adapun klasifikasi algoritma adalah sebagai berikut:

Rekursi dan Iterasi; Algoritma rekursi adalah algoritma yang memanggil dirinya sendiri secara berulang-ulang. Sedangkan algoritma iterasi adalah algoritma yang memakai konstrukti berulang dimana terkadang terdapat data tambahan pada struktur yang dibuat.

Logical; Algoritma logical adalah algoritma yang dapat memposisikan diri seperti logika deduksi yang terkontrol.

Serial, Parallel, atau Terdistribusi; Algoritma serial adalah algoritma yang menjalankan satu instruksi saja. Algoritam parallel adalah algoritma yang dapat mengerjakan suatu perintah dalam waktu yang sama. Sedangkan algoritma terdistribusi adalah algoritma yang memakai banyak mesin yang terkoneksi dengan jaringan.

Deterministik atau Non-deterministik; Algoritma deterministik adalah algoritma yang dapat memecahkan suatu masalah dengan keputusan yang tepat. Sedangkan algoritma Non-deterministik adalah algoritma yang memecahkan suatu masalah dengan metode penerkaan.

Tepat atau Perkiraan; Suatu algoritma mungkin saja memiliki solusi yang tepat, atau setidaknya mempunyai perkiraan yang mendekati solusi yang benar. Dalam merumuskannya dapat dilakukan dengan strategi deterministic ataupun secara acak.

Algoritma Quantum; Algoritma quantum adalah algoritma yang menggunakan model realistik dari komputasi quantum.

10. Visual Basic Net

Merupakan sebuah bahasa pemograman dan sebagai sarana (tool) untuk menghasilkan program-program aplikasi berbasiskan windows. Beberapa kemampuan atau manfaat dari Visual Basic diantaranya:

a. Untuk membuat program aplikasi berbasiskan windows.

b. Untuk membuat obyek-obyek pembantu program, seperti Control Active X, File Help, Aplikasi Internet dan sebagainya.

c. Menguji program (debugging) dan menghasilkan program akhir berakhiran ”EXE” yang bersifat executable atau dapat langsung dijalankan.

d. Keistimewaan utama dari Visual Basic adalah:

e. Menggunakan platform pembuatan program yang diberi nama developer studio, yang memiliki tampilan seperti C++ dan visual J++.

f. Memiliki kompiler handal yang dapat menghasilkan File Executable yang lebih cepat dan efisien.

g. Memiliki tambahan saran wizard yang baru. Tambahan kontrol-kontrol baru dan lebih canggih serta peningkatan kaidah struktur bahasa Visual Basic.

h. Kemampuan membuat Active X dan fasilitas internet yang lebih banyak.

i. Sarana akses yang lebih cepat dan andal untuk membuat aplikasi database yang berkemampuan tinggi.

j. Visual Basic.net memiliki beberapa versi baru edisi yang disesuaikan dengan kebutuhan pemakainya.

Dalam pemograman berbasiskan OOP (Object Oriented Programming), sebuah program dibagi menjadi bagian-bagian kecil yang disebut dengan obyek.

Setiap obyek memiliki entiti terpisah dengan entiti-entiti lain dalam lingkungannya. Obyek-obyek yang terpisah ini dapat diolah sendiri-sendiri, dan setiap obyek memiliki sekumpulan sifat dan metode yang melakukan fungsi tertentu sesuai dengan yang telah diprogramkan kepadanya.

Adapun obyek-obyek yang dipergunakan dalam program ini adalah:

1. Project

Project adalah sekumpulan modul. Jadi project merupakan aplikasi itu sendiri. Project disimpan dalam file yang berakhiran VBP. Jika kita akan melaksanakan pembuatan program aplikasi, akan terdapat jendela project yang berisi semua file yang dibutuhkan menjalankan program aplikasi Visual Basic.net pada saat pembuatan program aplikasi baru maka jendela project otomatis akan berisi object form1. Pada jendela project terdapat tiga icon yaitu View Code, View Object, dan Toggle Folders. Icon View Code dipakai untuk menampilkan jendela editor kode program. Icon View Object dipakai untuk menampilkan bentuk formulir (form) dan icon Toggle Folders digunakan untuk menampilkan folder

2. Form

Form adalah jendela yang dipakai untuk membuat user interface/tampilan. Secara otomatis akan tersedia form yang baru jika membuat suatu program aplikasi yang baru, dengan nama Form1. pada umumnya dalam suatu form terdapat garis titik-titik yang disebut dengan Grid. Untuk lebih memahami form ini maka di bawah ini terdapat gambar jendela form.

3. Toolbox

Toolbox adalah kumpulan dari obyek yang digunakan untuk membuat user interface (tampilan) serta control bagi program aplikasi. Untuk menempatkan control pada suatu form dapat dilakukan dengan klik ganda control dalam toolbox, kemudian mengubah besar dan ukurannya serta memindahkannya dengan metode Drag and Drop atau dengan cara mengklik kontrol toolbox, kemudian pindahkan pointer mouse jendela form. Kursor berubah menjadi Crosshair lalu tempatkan pada sudut kiri atas dimana kita inginkan kontrol tersebut diletakkan, tekan tombol mouse kiri dan tahan ketika menyeret kursor ke arah sudut kanan bawah.

4. Properties

Properties berisikan daftar struktur setting properti yang digunakan pada sebuah object terpilih. Kotak drop-down pada bagian atas jendela berisi daftar semua object pada form yang aktif. Ada tab tampilan, yaitu alphabetic (urut abjad) dan categorized (urut berdasarkan kelompok).

5. Kode Program

Kode program adalah serangkaian tulisan perintah yang akan dilaksanakan jika suatu obyek dijalankan. Kode program ini mengkontrol dan menentukan jalannya suatu obyek.

6. Event

Event adalah peristiwa atau kejadian yang diterima suatu obyek, misalnya klik, seret, tunjuk, dan lain sebagainya.

7. Metode (Methods)

Metode adalah serangkaian perintah yang sudah tersedia pada suatu obyek yang dapat diminta untuk mengerjakan tugas khusus.

8. Module

Module dapat disejajarkan dengan form, tetapi module tidak mengandung obyek. Module berisikan prosedur umum, deklarasi variabel dan definisi konstanta yang digunakan oleh aplikasi.

11. Tabel ASCII

ASCII merupakan kepanjangan dari (American Standard Code for Information

Interchange), dan pengertian dari ASCII sendiri adalah suatu standar internasional dalam kode huruf dan simbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal, contohnya 124 adalah untuk karakter "|". Ia selalu digunakan oleh computer dan alat komunikasi lain untuk menunjukkan teks.

sedangkan fungsi dari kode ASCII ialah digunakan untuk mewakili karakter-karakter angka maupun huruf didalam komputer, sebagai contoh dapat kita lihat pada karakter 1, 2, 3, A, B, C, dan sebagainya.

Tabel 1 ASCII

DEC	OCT	HEX	BIN	Symbol
0	000	00	00000000	NUL
1	001	01	00000001	SOH
2	002	02	00000010	STX

3	003	03	00000011	ETX
4	004	04	00000100	EOT
5	005	05	00000101	ENQ
6	006	06	00000110	ACK
7	007	07	00000111	BEL
8	010	08	00001000	BS
9	011	09	00001001	HT
10	012	0A	00001010	LF
11	013	0B	00001011	VT
12	014	0C	00001100	FF
13	015	0D	00001101	CR
14	016	0E	00001110	SO
15	017	0F	00001111	SI
16	020	10	00010000	DLE
17	021	11	00010001	DC1
18	022	12	00010010	DC2
19	023	13	00010011	DC3
20	024	14	00010100	DC4
21	025	15	00010101	NAK
22	026	16	00010110	SYN
23	027	17	00010111	ETB
24	030	18	00011000	CAN
25	031	19	00011001	EM
26	032	1A	00011010	SUB
27	033	1B	00011011	ESC
28	034	1C	00011100	FS
29	035	1D	00011101	GS
30	036	1E	00011110	RS
31	037	1F	00011111	US
DEC	OCT	HEX	BIN	Symbol
32	040	20	00100000	

33	041	21	00100001	!
34	042	22	00100010	"
35	043	23	00100011	#
36	044	24	00100100	$
37	045	25	00100101	%
38	046	26	00100110	&
39	047	27	00100111	'
40	050	28	00101000	(
41	051	29	00101001	)
42	052	2A	00101010	*
43	053	2B	00101011	+
44	054	2C	00101100	,
45	055	2D	00101101	-
46	056	2E	00101110	.
47	057	2F	00101111	/
48	060	30	00110000	0
49	061	31	00110001	1
50	062	32	00110010	2
51	063	33	00110011	3
52	064	34	00110100	4
53	065	35	00110101	5
54	066	36	00110110	6
55	067	37	00110111	7
56	070	38	00111000	8
57	071	39	00111001	9
58	072	3A	00111010	:
59	073	3B	00111011	;
60	074	3C	00111100	<
61	075	3D	00111101	=
62	076	3E	00111110	>
63	077	3F	00111111	?
64	100	40	01000000	@

65	101	41	01000001	A
66	102	42	01000010	B
67	103	43	01000011	C
68	104	44	01000100	D
69	105	45	01000101	E
70	106	46	01000110	F
71	107	47	01000111	G
72	110	48	01001000	H
73	111	49	01001001	I
74	112	4A	01001010	J
75	113	4B	01001011	K
76	114	4C	01001100	L
77	115	4D	01001101	M
78	116	4E	01001110	N
79	117	4F	01001111	O
80	120	50	01010000	P
81	121	51	01010001	Q
82	122	52	01010010	R
83	123	53	01010011	S
84	124	54	01010100	T
85	125	55	01010101	U
86	126	56	01010110	V
87	127	57	01010111	W
88	130	58	01011000	X
89	131	59	01011001	Y
90	132	5A	01011010	Z
91	133	5B	01011011	[
92	134	5C	01011100	\
93	135	5D	01011101	]
94	136	5E	01011110	^
95	137	5F	01011111	_
96	140	60	01100000	`

97	141	61	01100001	a
98	142	62	01100010	b
99	143	63	01100011	c
100	144	64	01100100	d
101	145	65	01100101	e
102	146	66	01100110	f
103	147	67	01100111	g
104	150	68	01101000	h
105	151	69	01101001	i
106	152	6A	01101010	j
107	153	6B	01101011	k
108	154	6C	01101100	l
109	155	6D	01101101	m
110	156	6E	01101110	n
111	157	6F	01101111	o
112	160	70	01110000	p
113	161	71	01110001	q
114	162	72	01110010	r
115	163	73	01110011	s
116	164	74	01110100	t
117	165	75	01110101	u
118	166	76	01110110	v
119	167	77	01110111	w
120	170	78	01111000	x
121	171	79	01111001	y
122	172	7A	01111010	z
123	173	7B	01111011	{
124	174	7C	01111100	|
125	175	7D	01111101	}
126	176	7E	01111110	~
127	177	7F	01111111	

128	200	80	10000000	€
129	201	81	10000001	
130	202	82	10000010	‚
131	203	83	10000011	*ƒ*
132	204	84	10000100	„
133	205	85	10000101	…
134	206	86	10000110	†
135	207	87	10000111	‡
136	210	88	10001000	ˆ
137	211	89	10001001	‰
138	212	8A	10001010	Š
139	213	8B	10001011	‹
140	214	8C	10001100	Œ
141	215	8D	10001101	
142	216	8E	10001110	Ž
143	217	8F	10001111	
144	220	90	10010000	
145	221	91	10010001	‘
146	222	92	10010010	’
147	223	93	10010011	“
148	224	94	10010100	”
149	225	95	10010101	•
150	226	96	10010110	–
151	227	97	10010111	—
152	230	98	10011000	˜
153	231	99	10011001	™
154	232	9A	10011010	š
155	233	9B	10011011	›
156	234	9C	10011100	œ
157	235	9D	10011101	
158	236	9E	10011110	ž

159	237	9F	10011111	Ÿ
160	240	A0	10100000	
161	241	A1	10100001	¡
162	242	A2	10100010	¢
163	243	A3	10100011	£
164	244	A4	10100100	¤
165	245	A5	10100101	¥
166	246	A6	10100110	¦
167	247	A7	10100111	§
168	250	A8	10101000	¨
169	251	A9	10101001	©
170	252	AA	10101010	ª
171	253	AB	10101011	«
172	254	AC	10101100	¬
173	255	AD	10101101	
174	256	AE	10101110	®
175	257	AF	10101111	¯
176	260	B0	10110000	°
177	261	B1	10110001	±
178	262	B2	10110010	²
179	263	B3	10110011	³
180	264	B4	10110100	´
181	265	B5	10110101	µ
182	266	B6	10110110	¶
183	267	B7	10110111	·
184	270	B8	10111000	¸
185	271	B9	10111001	¹
186	272	BA	10111010	º
187	273	BB	10111011	»
188	274	BC	10111100	¼
189	275	BD	10111101	½
190	276	BE	10111110	¾

191	277	BF	10111111	¿
192	300	C0	11000000	À
193	301	C1	11000001	Á
194	302	C2	11000010	Â
195	303	C3	11000011	Ã
196	304	C4	11000100	Ä
197	305	C5	11000101	Å
198	306	C6	11000110	Æ
199	307	C7	11000111	Ç
200	310	C8	11001000	È
201	311	C9	11001001	É
202	312	CA	11001010	Ê
203	313	CB	11001011	Ë
204	314	CC	11001100	Ì
205	315	CD	11001101	Í
206	316	CE	11001110	Î
207	317	CF	11001111	Ï
208	320	D0	11010000	Đ
209	321	D1	11010001	Ñ
210	322	D2	11010010	Ò
211	323	D3	11010011	Ó
212	324	D4	11010100	Ô
213	325	D5	11010101	Õ
214	326	D6	11010110	Ö
215	327	D7	11010111	×
216	330	D8	11011000	Ø
217	331	D9	11011001	Ù
218	332	DA	11011010	Ú
219	333	DB	11011011	Û
220	334	DC	11011100	Ü
221	335	DD	11011101	Ý
222	336	DE	11011110	Þ

223	337	DF	11011111	ß
224	340	E0	11100000	à
225	341	E1	11100001	á
226	342	E2	11100010	â
227	343	E3	11100011	ã
228	344	E4	11100100	ä
229	345	E5	11100101	å
230	346	E6	11100110	æ
231	347	E7	11100111	ç
232	350	E8	11101000	è
233	351	E9	11101001	é
234	352	EA	11101010	ê
235	353	EB	11101011	ë
236	354	EC	11101100	ì
237	355	ED	11101101	í
238	356	EE	11101110	î
239	357	EF	11101111	ï
240	360	F0	11110000	ð
241	361	F1	11110001	ñ
242	362	F2	11110010	ò
243	363	F3	11110011	ó
244	364	F4	11110100	ô
245	365	F5	11110101	õ
246	366	F6	11110110	ö
247	367	F7	11110111	÷
248	370	F8	11111000	ø
249	371	F9	11111001	ù
250	372	FA	11111010	ú
251	373	FB	11111011	û
252	374	FC	11111100	ü
253	375	FD	11111101	ý

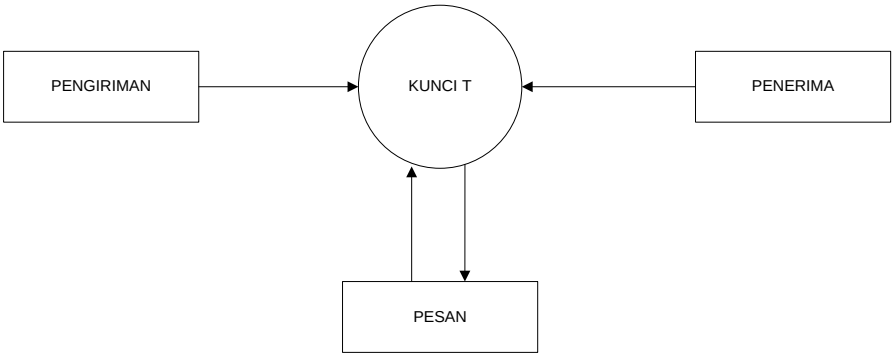
254	376	FE	11111110	þ
255	377	FF	11111111	ÿ

BAB III

ANALISA DAN PERANCANGAN SISTEM

1. Analisa Permasalahan yang Berjalan

Pertukaran data dalam hal ini pesan rahasia berbentuk teks dengan menggunakan metode tradisional yaitu dengan cara bertukar kata kunci tunggal. Diagram dibawah adalah penggambaran bagai mana pertukaran pesan rahasia menggunakan kunci tunggal terjadi.



Gambar 4 Skema Pengiriman Pesan

Pemberitahuan kata kunci dari pengirim ke penerima menggunakan media yang umum digunakan oleh banyak orang.

2. Analisa Kelemahan Yang Berjalan

a. Penggunaan kata kunci tunggal berpotensi terjadinya salah pemahaman dalam hal ini kemungkinan penerima salah mengartikan kunci yang diberikan oleh pengirim adalah hal yang dapat terjadi.

b. Pemberitahuan atau pertukaran kata kunci yang dikirimkan oleh pengirim kepenerima memiliki potensi dapat diketahui oleh orang lain sehingga pesan rahasia dapat terbongkar.

3. Solusi Pemecahan Masalah

Pemecahan masalah yang penulis lakukan adalah dengan melakukan penerapan metode ini yang didalamnya terdapat Algoritma *Affine Cipher*. Penggunaan metode ini dapat digunakan sebagai solusi agar pengirim dan penerima tidak lagi harus bertukar kunci tunggal untuk membuka pesan melainkan dapat memiliki kata kunci masing-masing.

Tabel 2 Tabel Perencanaan Rancangan

No	Sistem yang Berjalan	Sistem yang Diusulkan	Hasil yang Ingin Dicapai
1.	Penggunaan kunci tunggal yang harus diketahui oleh pengirim dan penerima untuk membuka pesan.	Pengirim dan penerima memiliki kunci masing-masing untuk membuka pesan	Tidak ada lagi kesalahan pemahaman atau salah tafsir kunci tunggal karena pengirim dan penerima memiliki kunci yang dapat ditetapkan masing-masing pihak.
2	Pertukaran kunci	Pengirim dan	Kemungkinan

	tunggal menggunakan media komunikasi yang rentan untuk dapat diketahui orang lain.	penerima dapat menentukan sendiri kunci yang ingin digunakan untuk membuka pesan.	bocornya kunci saat proses pertukaran informasi kunci tunggal dapat dihindari.

4. Analisa Proses

Visual basic 2010 akan menjadi sarana untuk menciptakan perangkat lunak ini. Padaanalisa proses ini penggunaan digunakan sebagai metode yang di dalamnya terdapat kombinasi dari algoritma *Affine Cipher*. Algoritma *Affine Cipher* digunakan oleh pengirim untuk mengenkripsi pesan yang akan dikirimkan..

Perhitungan secara matematis dilakukan sebagai penggambaran proses yang akan terjadi pada metode ini yang didalamnya terdapat algoritma *Affine Cipher* .Berikut tahapannya:

a. Proses Enkripsi Pesan Asli oleh Pengirim

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

Plaintext : AFFINECIPHER

Kunci A : 5

Kunci B : 8

plaintext:	A	F	F	I	N	E	C	I	P	H	E	R
x:	0	5	5	8	13	4	2	8	15	7	4	17

(5x+8)	8	33	33	48	73	28	18	48	83	43	28	93
(5x+8) mod 26	8	7	7	22	21	2	18	22	5	17	2	15
ciphertext:	I	H	H	W	V	C	S	W	F	R	C	P

b. Proses Deskripsi Pesan Asli oleh Pengirim

ciphertext:	I	H	H	W	V	C	S	W	F	R	C	P
y:	8	7	7	22	21	2	18	22	5	17	2	15
21(y-8):	0	-21	-21	294	273	-126	210	294	-63	189	-126	147
(21(y-8)) mod 26:	0	5	5	8	13	4	2	8	15	7	4	17
plaintext:	A	F	F	I	N	E	C	I	P	H	E	R

5. Analisa Kebutuhan

Analisa kebutuhan berfungsi untuk memahami apa-apa saja yang diperlukan sebuah perangkat lunak hingga menjabarkan alur atau proses yang akan dibuat oleh perangkat lunak yang dirancang tersebut.

a. Kebutuhan Fungsional

Kebutuhan fungsional merupakan kebutuhan yang harus dipenuhi oleh sistem, dalam perancangan perangkat lunak ini berikut adalah kebutuhan fungsional yang harus dipenuhi tersebut:

1) User pengirim merupakan pihak yang harus menentukan kunci *Affine Cipher* yang akan digunakan.

2) Enkripsi pesan, system menjalankan proses enkripsi pesan berdasarkan kunci yang telah ditetapkan menggunakan algoritma *Affine Cipher*.

3) Deskripsi pesan, pengirim mendeskripsikan pesan pari pihak kedua atau pihak penerima dengan menggunakan algoritma *Affine Cipher*.

b. Kebutuhan Non Fungsional

Menjalankan kebutuhan fungsional yang telah dijabarkan sebelumnya, membutuhkan dukungan dari kebutuhan non fungsional. Adapaun kebutuhan non fungsional terdiri dari:

1) Sistemoperasimenggunakan windows 10

2) Visual basic 2010

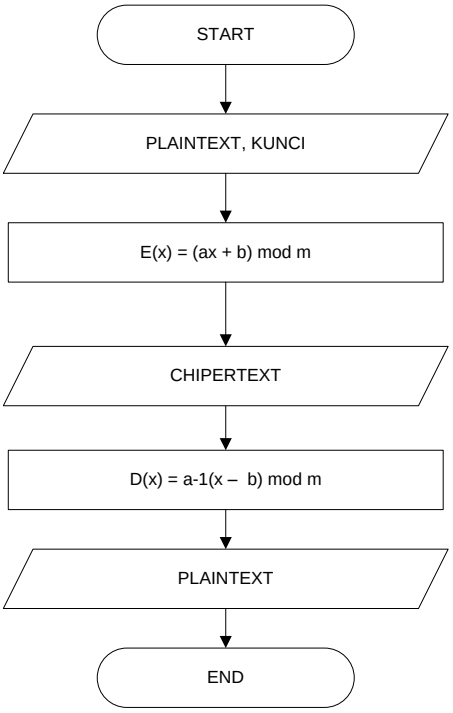
6. *Flowchart*

Flowchart merupakan langkah awal pembuatan program.Dengan adanya flowchart urutan proses kegiatan menjadi lebih jelas. Bila terdapat penambahan proses maka dapat dilakukan lebih mudah. Setelah flowchart selesai disusun,selanjutnya pemrogram (programmer) menerjemahkannya ke bentuk program dengan bahasa pemrograman.

Flowchart merupakan urutan-urutan langkah kerja suatu proses yang digambarkan dengan menggunakan simbo -simbol yang disusun secara sistematis.(Iswandy, 2015)

7. Flowchart *Affine Cipher*

Flowchart Affine Cipher yang digunakanolehpengirimuntuk mengenkripsi dan mendeskripsi plaintext hingga mendapatkan ciphertext digambarkan sebagai berikut:

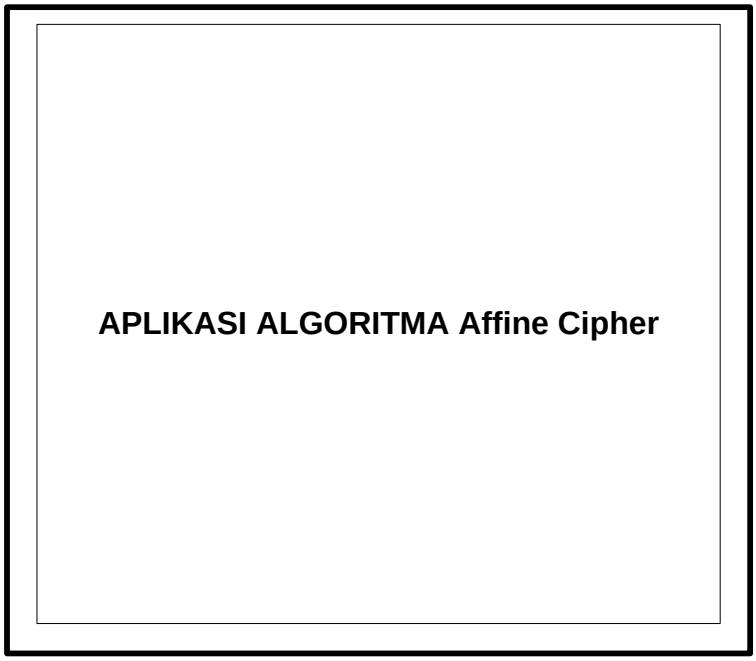


Gambar 5 Flowchart Affine Cipher

8. Perancangan Antarmuka

a. Rancangan Halaman Judul

Halaman judul merupakan halaman yang pertama muncul pada saat program dijalankan

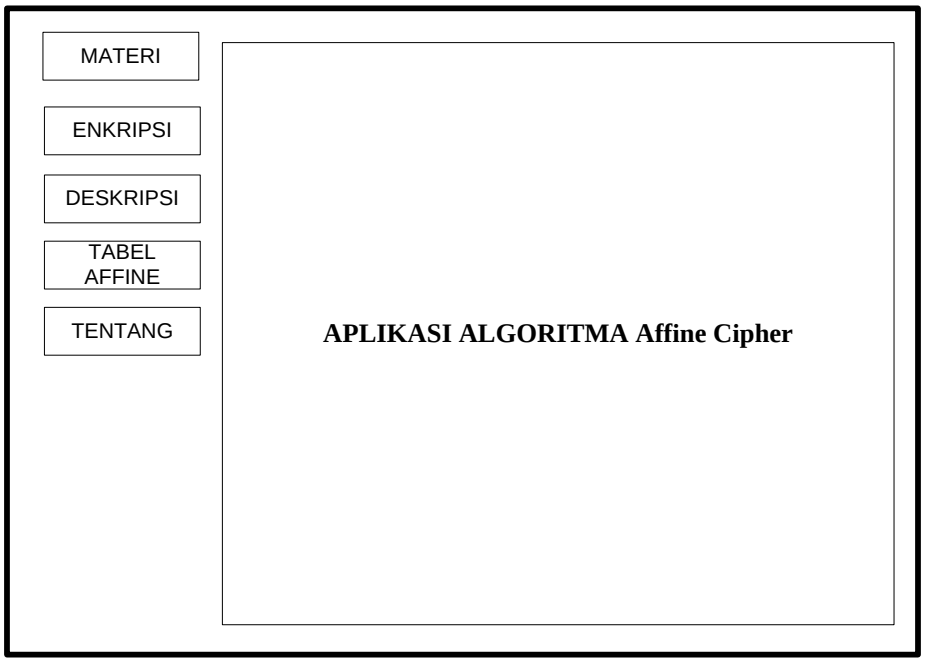


Gambar 6 Rancangan Halaman Judul

Pada rancangan di atas akan menampilkan judul yang kemudian akan pindah keform menu utama dengan menggunakan timer.

b. Rancangan Halaman Menu Utama

Form ini berisi tombol-tombol seperti menu Materi, Enkripsi, Deskipsi, tentang, dan Keluar.



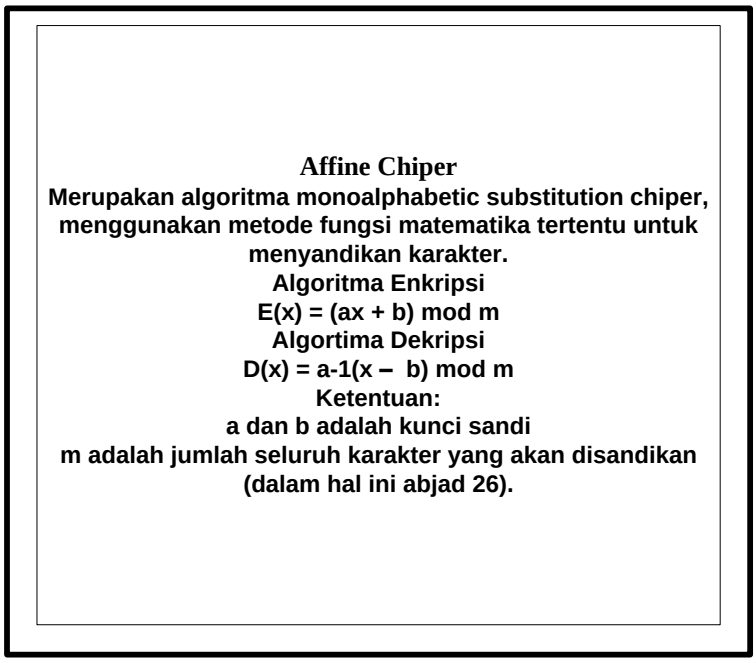
Gambar 7 Rancangan Halaman Menu Utama

Pada tampilan di atas terdapat 5 tombol yaitu Materi, Enkripsi, Deskripsi,Tabel Affine, Tentang dan keluar.

- Tombol Materi berfungsi untuk menghubungkan pengguna ke form materi.
- Tombol Enkripsi berfungsi untuk menghubungkan pengguna ke form Enkripsi.
- Tombol Deskripsi berfungsi untuk menampilkan form Deskripsi.
- Tombol Tentang berfungsi untuk menghubungkan pengguna ke form tentang.
- Tombol Keluar berfungsi untuk keluar dari program.

c. Rancangan Halaman Materi

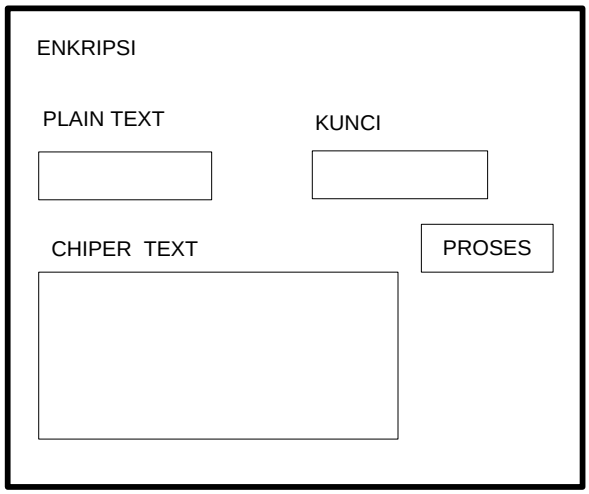
Form ini digunakan untuk menjelaskan cara kerja penyandian, dimulai dari plaintext kemudian kunci yang dikonversikan dalam bentuk angka. Setelah itu dilakukan proses penjumlahan dan jika hasil penjumlahan maka akan dikurangi 6 lalu hasilnya akan dikembalikan lagi ke dalam bentuk huruf.



Gambar 8 Rancangan Halaman Materi

d. Rancangan Halaman Enkripsi

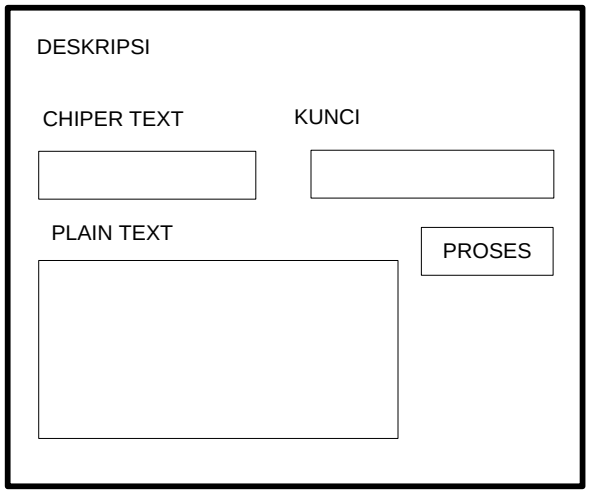
Berisi penjelasan mengenai Enkripsi. Pengguna memasukkan tulisan asli atau *plaintext* ke dalam tombol masukan *plaintext* kemudian dimasukkan juga kunci. Setelah itu, ditekan tombol Proses Enkripsi yang kemudian akan menampilkan ciphertext atau tulisan yang telah disandikan.



Gambar 9 Rancangan Halaman Enkripsi

e. Rancangan Halaman Deskripsi

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



Gambar 10 Rancangan Halaman Deskripsi

Pada gambar di atas terdapat kotak input Deskripsi berfungsi untuk memasukkan tulisan yang telah disandikan. Kemudian terdapat tombol Proses

Deskripsi untuk mengembalikan ke tulisan asli jika kunci yang dimasukkan sama dengan kunci pada saat penggunaan plaintext.

BAB IV

HASIL DAN PEMBAHASAN

1. Pengujian Sistem

Pengujian dilakukan dengan memasukkan karakter atau huruf dari file berformat .txt selanjutnya diproses oleh aplikasi apakah aplikasi tersebut dapat memberikan hasil yang sesuai. Proses yang akan dilakukan pengujian dalam aplikasi ini adalah simulasi pengiriman pesan dengan menggunakan metode algoritma *Affine Cipher* 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 .

a. Tampilan Awal/ Home

Tampilan pada gambar 1 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 *read me!* yang akan mengarahkan pengguna ke form yang menjelaskan tata cara penggunaan dari aplikasi ini.

Gambar 11 Tampilan Awal/ Home

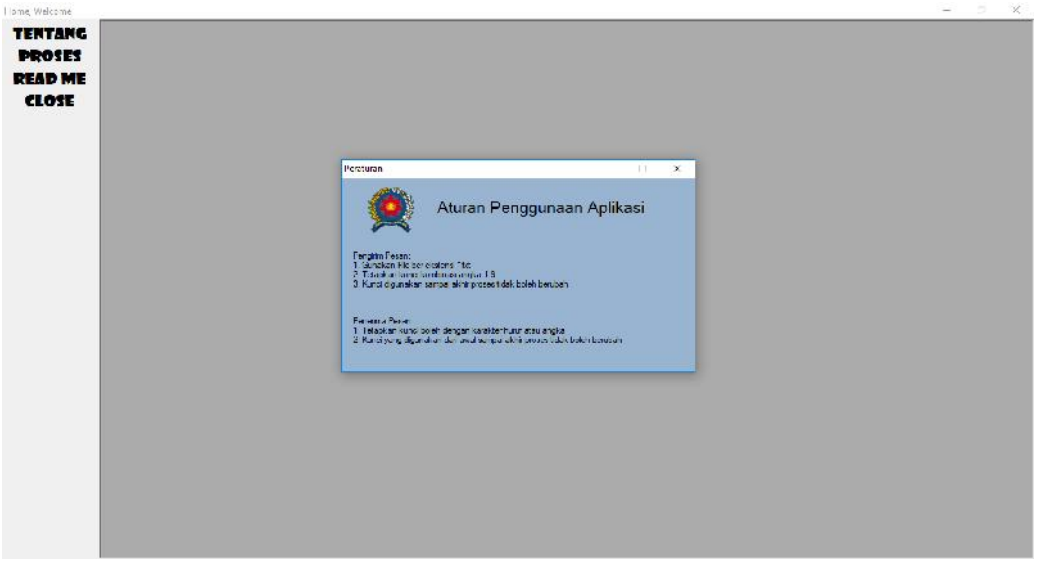
b. Tampilan Halaman Tentang

Tampilan berikut ini menampilakan halaman atau form yang berisi tentang profil dari aplikasi ini. Didalamnya terdapat judul dari aplikasi beserta maksud dari pembuatannya beserta nama dan nomor pokok mahasiswa penulis.

Gambar 12 Tampilan Halaman Tentang

c. Tampilan Aturan Penggunaan Aplikasi

Tampilan aturan penggunaan aplikasi merupakan tampilan halaman atau form yang berisi tentang tata cara penggunaan aplikasi yang dijalankan. Pada halaman tersebut dijelaskan apa-apa saja yang menjadi kewajiban bagi pengirim dan penerima saat menjalankan simulasi algoritma *Affine Cipher*.

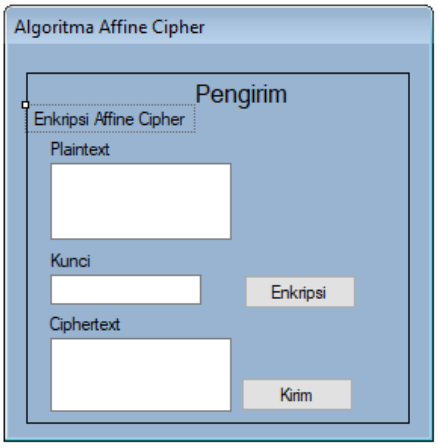


Gambar 13 Tampilan Aturan Penggunaan Aplikasi

d. Tampilan Halaman Pengirim Pesan

Tampilan berikut merupakan tampilan pengiriman pesan pada aplikasi ini.algoritma *Affine Cipher*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

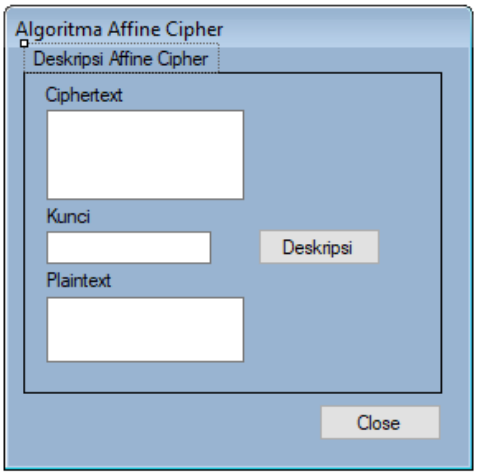
mengenkripsi pesan dan kemudian untuk mendekripsi pesan tanpa perlu mengetahui kunci yang lainnya



Gambar 14 Tampilan Halaman Pengirim Pesan

e. Tampilan Halaman Penerima Pesan

Tampilan berikut merupakan tampilan penerima pesan pada aplikasi ini.



Gambar 15 Tampilan Halaman Pengirim Pesan

2. HasilEnkripsi Pesan

Pesan : AFFINECIPHER

Kunci A : 5

Kunci B : 8

Penyelesaian Enkripsi

plaintext:	A	F	F	I	N	E	C	I	P	H	E	R
x:	0	5	5	8	13	4	2	8	15	7	4	17
(5x+8)	8	33	33	48	73	28	18	48	83	43	28	93
(5x+8) mod 26	8	7	7	22	21	2	18	22	5	17	2	15
ciphertext:	I	H	H	W	V	C	S	W	F	R	C	P

Penyelesaian Deskripsi

Pesan : IHHWVCSWFRCP

Kunci A : 5

Kunci B : 8

ciphertext:	I	H	H	W	V	C	S	W	F	R	C	P
y:	8	7	7	22	21	2	18	22	5	17	2	15
21(y-8):	0	-21	-21	294	273	-126	210	294	-63	189	-126	147
(21(y-8)) mod 26:	0	5	5	8	13	4	2	8	15	7	4	17
plaintext:	A	F	F	I	N	E	C	I	P	H	E	R

3. Kelebihan dan Kekuarangan Sistem

Adapun kelebihan dan kekurangan dari media pembelajaran ini adalah sebagai berikut:

a. Kelebihan Sistem

- Keamanan Pesan lebih terjamin.
- Proses kemanan pesan lebih mudah dan cepat.
- Proses membaca pesan lebih mudah dan cepat.

b. Kekurangan Sistem

- Masih bersifat jaringan local.
- Sebaiknya dapat digunakan pada Android.

BAB V

PENUTUP

1. Kesimpulan

Berdasarkan pembahasan dalam perancangan Penerapan Algoritma *Affine Cipher*dalam Meningkatkan Keamanan Data, maka dapat diambil kesimpulan sebagai berikut :

a. Perangkat lunak ini dirancang untuk menampilkan simulasi pengiriman pesan berekstensi yang diinputkan kedalam text box antara pengirim dan penerima.

b. Pengirim mengirimkan pesan menggunakan dua kunci yang ditentukan sendiri oleh pengirim.

c. Penerima pesan menggunakan kunci yang diberikan oleh pengirim pesan, agar bisa membuka pesan asli yang dikirimkan oleh pengirim.

2. Saran

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

1. Diharapkan adanya kombinasi algoritma keamanan data lainnya.
2. Proses pengamanan data yang dilakukan oleh penulis masih menggunakan visual studio, diharapkan ada yang menggunakan diandroid agar bisa digunakan pada mobile.

DAFTAR PUSTAKA

Hasugian. A. H, 2013, Implementasi Algoritma Hill Cipher Dalam Penyandian Data, Pelita Informatika Budi Darma, Volume : IV, Nomor: 2, Agustus 2013.

Hartanto, S. (2017). Implementasi fuzzy rule based system untuk klasifikasi buah mangga. TECHSI-Jurnal Teknik Informatika, 9(2), 103-122.

Harumy, T. H. F., & Sulistianingsih, I. (2016). Sistem penunjang keputusan penentuan jabatan manager menggunakan metode mfep pada cv. Sapo durin. In Seminar Nasional Teknologi Informasi dan Multimedia (pp. 6-7).

Havena, M., & Marlina, L. (2018). The Technology of Corn Processing as an Effort to Increase The Income of Kelambir V Village. Journal of Saintech Transfer, 1(1), 27-32.

Inggiantowi, Hafid. 2010. Studi Implementasi Algoritma Block Cipher pada Platform Android.http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/Makalah1/Makalah1-IF3058-Sem1-2010-2011-080.pdf. Tanggal akses 5 April 2012.

Indra permana, A. M. I. N. U. D. D. I. N. "Sistem pakar mendeteksi hama dan penyakit tanaman kelapa sawit pada pt. moeis kebun sipare-pare kabupaten batubara." (2013).

Khairul, K., Haryati, S., & Yusman, Y. (2018). Aplikasi Kamus Bahasa Jawa Indonesia dengan Algoritma Raita Berbasis Android. Jurnal Teknologi Informasi dan Pendidikan, 11(1), 1-6.

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

Lee, Wei Meng. 2009. SMS Messaging in Android. http://mobiforge.com/developing/story/sms-messaging-android. Tanggal akses 5 April 2012.

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).

Pakpahan, Hombar. 2009. Pengertian SMS. http://www.ombar.net/2009/09/pengertian-sms.html. Tanggal akses 10 April 2012.

Made Sudarma. 2012. *Konsep Pemrograman Komputer*. Udayana University Press. Bali

Marlina, L., Putera, A., Siahaan, U., Kurniawan, H., & Sulistianingsih, I. (2017). Data Compression Using Elias Delta Code. Int. J. Recent Trends Eng. Res, 3(8), 210-217.

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

Muttaqin, Muhammad. "Analisa pemanfaatan sistem informasi e-office pada universitas pembangunan panca budi medan dengan menggunakan metode utaut." Jurnal Teknik dan Informatika 5.1 (2018): 40-43.

Munir. R, 2012, *Algoritma Enkripsi Citra dengan Pseudo One-Time Pad yang Menggunakan Sistem Chaos*, Konferensi Nasional Informatika – KNIF 2011

Perwitasari, I. D. (2018). Teknik Marker Based Tracking Augmented Reality untuk Visualisasi Anatomi Organ Tubuh Manusia Berbasis Android. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 8-18.

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

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

Putra, Randi Rian, and Cendra Wadisman. "Implementasi Data Mining Pemilihan Pelanggan Potensial Menggunakan Algoritma K Means." INTECOMS: Journal of Information Technology and Computer Science 1.1 (2018): 72-77.

Putri, R. E., & Siahaan, A. (2017). Examination of document similarity using Rabin-Karp a lgorithm. International Journal of Recent Trends in Engineering & Research, 3(8), 196-201.

Rifki Sadikin. 2012. *Kriptografi Untuk Keamanan Jaringan.* Andi. Yogyakarta

Surian. D, 2016, *Algoritma Kriptografi Aes Rijndael*, TESLA**,** Jurnal Teknik Elektro, Vol. 8 No. 2, 97 – 101 (Oktober 2016)

Yosef Murya. 2014. *Pemograman Android.* Jasakom. Jakarta