TEKNIK KEAMANAN PESAN MENGGUNAKAN KRIPTOGRAFI DENGAN ALGORITMA VERNAM CHIPER

MESSAGE SECURITY TECHNIQUES USING CRYPTOGRAPHY WITH VERNAM CHIPER ALGORITHM

Edi Haryadi, Siti Madinah Ladjamuddin
Program Studi Teknik Informatika, Institut Sains dan Teknologi Nasional
Edi.haryadi2istn.ac.id, citymadinah07@istn.ac.id

Naskah Diterima tanggal 10 Mei 2017 dan naskah di setujui tanggal 18 Juni 2017

Abstrak
Teknologi komunikasi dan informasi berkembang dengan pesat dan memberikan pengaruh besar bagi kehidupan manusia. Seiring dengan perkembangan teknologi sekarang ini yang semakin pesat maka proses pengiriman data dapat dilakukan dengan mudah dan melalui berbagai macam media yang telah ada antara lain, melalui media internet. Kriptografi, secara umum adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data Tujuan dari penelitian ini adalah untuk meningkatkan keamanan data agar informasi yang bersifat rahasia di enkripsi terlebih dahulu sebelum dikirim melalui internet agar tidak dapat di ketahui dan di modifikasi atau dimanfaatkan oleh orang lain yang tidak berkepentingan. Perancangan program aplikasi akan dilakukan dengan menggunakan bahasa pemrograman visual basic yang di uji cobakan pada Microsoft Visual Basic 2010.
Kata kunci: Kriptografi, Kriptografi vernam, enkripsi, VB 2010

Abstract
Communication and information technology is growing rapidly and has a great impact on human life. Along with the development of technology today is increasingly rapidly the process of data delivery can be done easily and through various media that already exist, among others, through the internet media. Cryptography, in general is a science that studies mathematical techniques related to the security aspects of information such as data confidentiality, data validity, data integrity, and data authentication The purpose of this study is to improve data security so that the information is confidential in encryption before Sent through the internet so that it can not be known and modified or used by others who are not interested. The design of the application program will be done by using visual basic programming language that is tested in Microsoft Visual Basic 2010.
Keyword : *Cryptography, vernam cryptography, encryption, VB 2010*

1. PENDAHULUAN

Teknologi komunikasi dan informasi berkembang dan memberikan pengaruh besar bagi kehidupan manusia. kembangan teknologi Proses pengiriman data dapat dilakukan dengan mudah dan melalui berbagai macam media yang telah ada antara lain, melalui media internet dengan menggunakan fasilitas e-mail, melalui transfer data antar perangkat mobile (handphone, PDA dan flashdisk) maupun dengan teknologi radio frequency (bluethooth, IrDA, GPRS) hingga dengan menggunakan jaringan komputer. Keamanan merupakan salah satu aspek yang penting dalam sebuah sistem informasi.

Banyak orang menyiasati bagaimana cara mengamankan informasi yang dikomunikasikan atau menyiasati bagaimana cara mendeteksi keaslian dari informasi yang diterimanya. Kriptografi adalah ilmu yang mempelajari bagaimana menjaga keamananan suatu pesan (plaintext). Tugas utama kriptografi adalah untuk menjaga agar baik pesan atau kunci ataupun keduanya tetap terjaga kerahasiaannya dari penyadap (attacker).

Penyadap pesan diasumsikan mempunyai akses yang lengkap dalam saluran komunikasi antara pengirim pesan dan penerima pesan. Penyadapan pesan sering terjadi pada komunikasi melalui internet maupun saluran telepon. untuk mendapatkan pesan tanpa melalui kunci sebenarnya dapat dianalisis (analisis sandi), ilmunya disebut cryptanalysis. Analisis sandi juga dapat menemukan kelemahan dalam kriptosistem yang pada akhirnya dapat menemukan pesan atau kunci. Pada sebuah data untuk menjaga keamanan data,data tersebut di enksipsi dan deskripsi. enkripsi dan dekripsi pada umumnya membutuhkan penggunaan sejumlah informasi rahasia, disebut sebagai kunci.

Untuk beberapa mekanisme enkripsi, kunci yang sama digunakan baik untuk enkripsi dan dekripsi, untuk mekanisme yang lain, kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Dua tipe dasar dari teknologi kriptografi adalah symmetric key (secret/private key) cryptography dan asymmetric (publickey) cryptography. Pada symmetric key cryptography, baik pengirim maupun penerima memiliki kunci rahasia yang umum. Pada asymmetric key cryptography, pengirim dan penerima masingmasing berbagi kunci publik dan privat. Kriptografi saat ini lebih dari enkripsi dan dekripsi saja. Otentikasi menjadi bagian dari kehidupan kita sama seperti privasi.

Untuk menjamin keamanan dan keutuhan data, dilakukan proses penyandian. Kriptografi mampu menjadi solusi dari masalah tersebut. Kriptografi dapat menjamin keamanan data-data pada suatu file. Data tersebut disandikan atau dienkripsi menjadi suatu symbol tertentu sehingga tidak mampu dibaca selain pihak yang memegang kunci dekripsi. Dalam perkembangan ilmu kriptografi sekarang ini, telah tercipta berbagai algoritma, yaitu algoritma Vernam Chiper. Algortima ini termasuk dalam algoritma kriptografi modern dan merupakan algoritma stream chiper.

Pengertian Kriptografi

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita [Bruce Schneier - *Applied Cryptography*]. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data [A. Menezes, P. van Oorschot and S. Vanstone - *Handbook of Applied Cryptography*]. Tidak semua aspek keamanan informasi ditangani oleh kriptografi. [1]

Menjaga kerahasiaan berita tersebut dilakukan dengan menyandikan pesan atau berita itu. Suatu pesan yang tidak disandikan disebut sebagai *plaintext* (plainteks) ataupun dapat disebut juga sebagai *cleartext*. Sedangkan suatu pesan yang sudah disandikan disebut sebagai *ciphertext* (cipherteks). Proses yang dilakukan untuk mengubah plainteks ke dalam cipherteks disebut *encryption* (enkripsi) atau *encipherment*. Sedangkan proses untuk mengubah *ciphertext* kembali ke *plaintext* disebut *decryption* (dekripsi) atau *decipherment*. Kriptografi secara singkat adalah ilmu yang mempelajari bagaimana caranya menyamarkan pesan dan mengembalikannya ke bentuk semula. Penyamaran pesan dapat dilakukan dengan kunci atau kata sandi yang ditetapkan. Ini akan menambah tingkat keamanan pengiriman data informasi, karena jika informasi berhasil diperoleh baik dengan sengaja maupun dengan tidak sengaja oleh pihak manapun yang bukan pemilik atau yang tidak berkepentingan maka tidak akan mendapatkan informasi atau data asli karena data asli telah disamarkan. Dalam dunia teknologi seperti ini, keamanan data adalah sesuatu yang mutlak dimana semua data disimpan dalam bentuk *digital*. Teknik penyamaran data seperti ini disebut enkripsi dan teknik untuk mengembalikannya disebut deskripsi.[2]

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

Kerahasiaan (*confidentiality*)

Kerahasiaan adalah layanan yang digunakan untuk menjaga informasi dari setiap pihak yang tidak berwenang untuk mengaksesnya. Dengan demikian informasi hanya akan dapat diakses oleh pihak – pihak yang berhak saja.

Integritas data (*data integrity*)
Integritas data merupakan layanan yang bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak – pihak yang tidak berwenang. Untuk meyakinkan integritas data ini harus dipastikan agar sistem informasi mampu mendeteksi terjadinya manipulasi data. Manipulasi data yang dimaksud di sini meliputi penyisipan, penghapusan, maupun penggantian data.

Otentikasi (*authentication*)
Otentikasi merupakan layanan yang terkait dengan identifikasi terhadap pihak – pihak yang ingin mengakses sistem informasi (*entity authentication*) maupun keaslian data dari sistem informasi itu sendiri (*data origin authentication*).

Ketiadaan penyangkalan (*non-repudiation*)
Ketiadaan penyangkalan adalah layanan yang berfungsi untuk mencegah terjadinya penyangkalan terhadap suatu aksi yang dilakukan oleh pelaku sistem informasi. Secara garis besar kriptografi ilmu dan seni untuk menjaga kerahasiaan (penyandian) sedangkan tujuan dari kriptografi sendiri agar pesan tidak mudah terbaca oleh orang lain.

Jenis Kriptografi
Jenis dari kriptografi ada beberapa macam seperti enkripsi/deskripsi, *encode/decode, hash/one way hash*.

Istilah istilah dalam kriptografi:
- plantext: teks asli (pesan yang akan di enkripsi).
- key: kunci yang akan digunakan untuk kriptografi.
- Algoritma : metode yang digunakan.
- Chipertext : teks atau pesan yang sudah di enkripsi.
- Enkripsi : mengubah plainteks jadi cipherteks.
- Dekripsi : mengembalikan chiperteks jadi planteks
- *Encoding* : mengubah kode menjadi kode acak.
- *Decoding* : mengembalikan kode acak ke kode awal.
- Hash : metode enkripsi yang tidak bisa dikembalikan ke nilai awal atau one way hash contohnya md5.sha-1 dll.

Jenis Kriptografi Berdasarkan Kunci
Algoritma kriptografi berdasarkan jenis kunci yang digunakan dapat dibedakan menjadi dua jenis yaitu:

Algoritma Simetri
Algoritma ini sering disebut dengan algoritma klasik karena memakai kunci yang sama untuk kegiatan enkripsi maupun dekripsi. Bila mengirim pesan dengan menggunakan algoritma ini, si penerima pesan harus diberitahu kunci dari pesan tersebut agar bisa mendekripsikan pesan yang terkirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Jika kunci tersebut diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan. Algoritma yang memakai kunci simetri di antaranya adalah :
- *Data Encryption Standard* (DES),
- RC2, RC4, RC5, RC 6,
- *International Data Encryption Algorithm* (IDEA),
- *Advanced Encryption Standard* (AES),
- *On Time Pad* (OTP),
- A5, dan lain sebagainya.

Algoritma Asimetri
Algoritma asimetri sering juga disebut dengan algoritma kunci public, dengan arti kata kunci yang digunakan melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu :
- Kunci umum (*public key*), kunci yang boleh semua orang tahu (dipublikasikan).
- Kunci rahasia (*private key*), kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).

Kunci-kunci tersebut berhubungan satu sama lain. Dengan kunci public orang dapat mengenkripsi pesan tetapi tidak bisa mendekripsikannya. Hanya orang yang memiliki kunci rahasia yang dapat mendekripsikan pesan tersebut. Algoritma asimetri bisa mengirimkan pesan dengan lebih aman daripada algoritma simetri.

Algoritma yang memakai kunci public di antaranya adalah

- *Digital Signature Algorithm* (DSA),
- *RSA*,
- *Diffle-Hellman* (DH),
- *Elliptic Curve Cryptography* (ECC),
- Kriptografi Quantum, dan lain sebagainya.

Sedangkan berdasarkan besar data yang diolah dalam satu kali proses, maka algoritma kriptogrfi dapat dibedakan menjadi dua jenis yaitu:

Algoritma *block cipher*

Informasi/data yang hendak dikirim dalam bentuk blok-blok besar (misal 64-bit) dimana blok-blok ini dioprasikan dengan fungsi enkripsi yang sama dan akan menghasilkan informasi rahasia dalam blok-blok berukuran sama.

Algoritma *stream cipher*

Informasi/data yang hendak dikirim dioprasikan dalam bentuk blok-blok yang lebih kecil (*byte* atau bit) biasanya satu karakter persatuan waktu proses, menggunakan tranformasi enkripsi yang berubah setiap waktu.

Jenis Kriptografi Yang Digukan Dalam Simulator

Kriptografi One Time Pad

Dalam dunia kriptografi dikenal sebuah metode penyandian yang sangat kuat sehingga tidak mudah dipecahkan, yaitu metode penyandian *One Time Pad* (OTP). Metode penyandian OTP pertama kali diperkenalkan oleh Gilbert Vernam dalam perang dunia pertama.

Metode penyandian OTP merupakan salah satu variasi dari metode penyandian substitusi dengan cara memberikan syarat-syarat khusus terhadap kunci yang digunakan yaitu terbuat dari karakter / huruf yang acak (kunci acak atau *pad*), dan pengacakannya tidak menggunakan rumus tertentu. Jika kunci tersebut benar-benar acak, digunakan hanya sekali, serta terjaga kerahasiannya dengan baik, maka metode penyandian OTP ini sangat kuat dan tidak dapat dipecahkan. Dalam kriptografi klasik, yaitu kriptografi jaman dulu yang dikenal dengan sebutan kriptografi kertas dan pensil, teks sandi dari metode penyandian OTP ini diperoleh dengan menjumlahkan/ mengurangkan teks aslinya terhadap kunci. Penggunaan kunci ini hanya dan harus hanya sekali pakai. Sedangkan untuk mendapatkan kembali teks aslinya dilakukan pengurangan / penjumlahan teks sandi terhadap kunci tersebut, sebagai kebalikan dari proses menyandi. Untuk memudahkan dalam operasionalnya huruf-huruf diterjemahkan dahulu kedalam angka 1 sampai 26 dengan A = 1; B = 2; dst sampai Z = 26. Dan dalam perhitungan aljabarnya berupa bilangan modulus 26.[3].One Time Pad termasuk dalam kelompok kriptografi simestris. One-time pad (pad = kertas bloknot) berisi deretan karakter-karakter kunci yang dibangkitkan secara acak. Cipher ini diimplementasikan melalui sebuah kunci yang terdiri dari sekumpulan random karakter-karakter yang tidak berulang.

Setiap huruf kunci dijumlahkan modulo 26 dengan huruf pada plaintext. Pada One Time Pad, tiap huruf kunci digunakan satu kali untuk satu pesan dan tidak digunakan kembali.Panjang stream karakter kunci sama dengan panjang pesan. One Time Pad ditemukan pada tahun 1917 oleh Major Joseph Mauborgne.

Cipher ini termasuk ke dalam kelompok algoritma kriptografi simetri. One Time Pad (pad = kertasbloknot) berisi barisan karakter-karakter kunci yang dibangkitkan secara acak. Aslinya, satu buah one time pad adalah sebuah pita (tape) yang berisi barisan karakter-karakter kunci. Satupad hanya digunakan sekali (one time) saja untuk mengenkripsi pesan, setelah itu pad yang telah digunakan dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain. Aturan enkripsi yang digunakan persis sama seperti pada Cipher Vigenere.

Pengirim pesan menggunakan setiap karakter kunci untuk mengenkripsikan satu karakter plainteks.[3.] Enkripsi dapat digambarkan sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci one time pad :

$$ci = (pi + ki) \bmod 26$$

keterangan :

pi : karakter plainteks

ki : karakter kunci

ci : karakter Ciphertek

Setelah pengirim mengenkripsikan pesan dengan **one time pad**, ia menghancurkan **one**

time pad tersebut (makanya disebut satu kali pakai atau one time). Penerima pesan menggunakan one time pad yang sama untuk mendekripsikan karakter-karakter cipherteks menjadi karakter-karakter plaintek dengan persamaan:

$$pi = (ci – ki) \bmod 26$$

Suatu algoritma dikatakan aman, apabila belum ada tidak ada cara untuk menemukan plaintext-nya. Sampai saat ini, hanya algoritma One Time Pad (OTP) yang dinyatakan tidak dapat dipecahkan meskipun diberikan sumber daya yang tidak terbatas. Prinsip enkripsi pada algoritma ini adalah dengan mengkombinasikan masing-masing karakter pada plaintext dengan satu karakter pada kunci. Maka panjang kunci setidaknya harus sama dengan panjang plainte. Untuk mendeskripsi chipertext tanpa mengetahui kuncinya tidak dapat dilakukan sebab jika kunci yang digunakan salah, akan diperoleh hasil yang salah juga, atau bukan plaintext yang seharusnya. Kemudian setiap kuncinya hanya boleh digunakan untuk sekali pesan. Pengambilan kunci harus dilakukan secara acak supaya tidak dapat diterka lawan dan jumlah karakter kunci harus sebanyak jumlah karakter pesan.[3]

Untuk memudahkan pemahaman, bisa diperhatikan contoh berikut :

Contoh :
Plainteks : MESRAN
Kunci : ALDYAN
Maka
Plainteks : M E S R A N
Kunci : A L D Y A N
Hasil : M P V P A A

Deretan Abjad

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Ilustrasi Enkripsi

Plainteks	:	M	E	S	R	A	N	->	12	4	18	17	0	13
Kunci	:	A	L	D	Y	A	N		0	11	3	24	0	13 +
Chiperteks	:?								12	15	21	41	0	26

C = (P + K) MOD 26

12	15	21	15	0	0	<- Hasil * Mod 26	
M	P	V	P	A	A	-->	Chiperteks

Ilustrasi Dekripsi

Chiperteks	:	M	P	V	P	A	A	->	12	15	21	15	0	0
Kunci	:	A	L	D	Y	A	N		0	11	3	24	0	13 -
									12	4	18	-9	0	-13

P = (C - K) MOD 26

12	4	18	17	0	13	<- Hasil * Mod 26	
M	E	S	R	A	N	-->	Plainteks

Metode penyandian OTP ini kekuatannya bertumpu pada keacakan kuncinya, sehingga kunci yang digunakan untuk proses penyandian tersebut harus dilindungi dengan baik. Metode enkripsi *one-time pad t*ermasuk golongan metode enkripsi kunci simetris, kategori *stream cipher*. Metode ini juga disebut *Vernam Cipher,* yang merupakan metode enkripsi kunci simetris yang tidak terpecahkan (*unbreakable by exhaustive search*). Metode enkripsi *one-time pad* merupakan metode yang sempurna (*perfect methods*) namun paling sederhana.

Metode ini disebut sebagai *perfect methods* karena beberapa hal yaitu :

- Tidak mungkin bisa dipecahkan dengan melakukan perhitungan matematis.
- Tidak mungkin ada dua buah pesan (*plaintext*) yang berbeda menjadi dua buah *ciphertext* yang sama.(karena seperti contoh di atas huruf B pada teks sandi bisa didapat dari penjumlahan dengan hasil 2 dan 28).

2. METODOLOGI PENELITIAN

Analisis Kebutuhan

Analisis kebutuhan terdiri dari 2 bagian yaitu :

Analisis Kebutuhan Informasi

Dalam pengembangan teknik keamanan pesan kebutuhan suatu sistem sangatlah penting karena dari sistem keamanan pesan anda dapat mengetahui sistem yang perlu diperiksa agar dapat mengambil keputusan yang baik untuk pengembangan sistem. Kelemahan sistem keamanan pesan di perusahaan - perusahaan saat ini adalah pemborosan waktu dan biaya karena masih menggunakan kalimat yang tidak disandikan sehingga pesan tidak aman untuk diberikan kepada orang yang berhak menerima pesan. Diharapkan dengan menggunakan sistem yang baru dapat memperbaiki kekurangan pada sistem yang lama.

Analisis Kebutuhan Teknologi

Software (Perangkat Lunak)

Software adalah bagian komputer yang tidak bisa dilihat tetapi ada didalam suatu komputer. Software yang dibutuhkan untuk membuat aplikasi teknik keamanan pesan adalah microsoft visual studio 2010.

Hardware (Perangkat Keras)
Hardware adalah bagian komputer yang dapat terlihat dan disentuh oleh manusia. Untuk pengembangan sistem yang dapat merubah kalimat maka dibutuhkan perangkat keras seperti komputer dan laptop.

Sistem operasi yang wajib dimiliki adalah windows xp service pack 3, windows 7 dan windows 8.
Spesifikasi komputer dan laptop yang dibutuhkan adalah prosesor dengan kecepatan 1.6GHz, harddisk free space 3 GB, direct 9, display layar komputer 1024 x 768.

Brainware (Pemakai Komputer)
Brainware adalah orang yang menggunakan komputer.

Kebutuhan brainware dalam pembuatan aplikasi ini adalah sebagai berikut :

- Sistem pemeriksa bertugas untuk mempelajari suatu kesalahan pada aplikasi dan kesalahan pada aplikasi dapat diselesaikan dengan komputer.
- Manusia bertugas untuk menggunakan komputer

Karakteristik Sistem
Suatu sistem memiliki karakteristik atau sifat tertentu yaitu :

Komponen Sistem
Suatu sistem terdiri sejumlah komponen yang saling berhubungan artinya saling bekerjasama membentuk satu kesatuan sistem yang dapat bekerja dengan baik. Komponen – komponen sistem atau elemen dapat berupa suatu subsistem atau bagian – bagian dari sistem seperti menu pada aplikasi.

Penghubung Sistem
Penghubung adalah media penghubung antara suatu sistem dengan sistem yang lainnya. Melalui media penghubung ini memungkinkan sumber – sumber daya terhubung menjadi satu pada aplikasi.

Tujuan Sistem
Suatu sistem mempunyai tujuan yaitu menghasilkan aplikasi yang berguna bagi kebutuhan masyarakat yang dapat digunakan untuk bidang jasa.

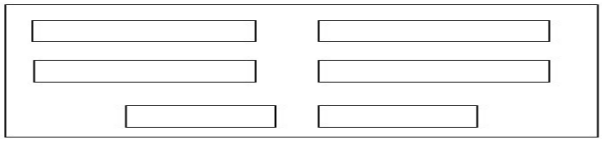
Pengembangan Sistem
Pengembangan sistem adalah tahapan menyusun suatu sistem yang baru untuk mengganti sistem yang lama secara keseluruhan atau perbaikan pada sistem yang telah ada dengan harapan sistem yang baru dapat mengatasi permasalahan yang timbul pada sistem yang lama. Perbaikan - perbaikan itu antara lain :

- Kinerja yaitu terjadi peningkatan terhadap hasil kerja sistem yang baru sehingga menjadi lebih cepat dalam memproses sistem yang dijalankan.
- Pengendalian yaitu bagaimana meningkatkan pengendalian untuk menemukan dan memperbaiki kesalahan – kesalahan pada sistem.
- pelayanan yaitu bagaimana meningkatkan pelayanan yang diberikan oleh sistem.

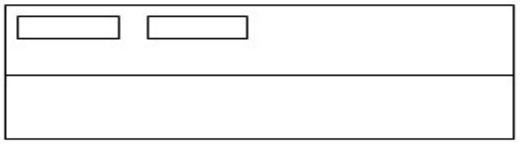
Analisis Perancangan Output
Perancangan output dilakukan dengan memberikan cara pemakaiannya untuk manusia tentang sistem yang akan di buat. Rancangan ini memeriksa bagian - bagian sistem yang akan dirancang. Tujuan perancangan sistem adalah

- Untuk memenuhi kebutuhan pemakai sistem.
- Untuk memberikan cara pemakaian yang jelas dan rancangan yang lengkap kepada manusia.
- Rancangan sistem harus berguna, mudah dimengerti dan mudah digunakan.

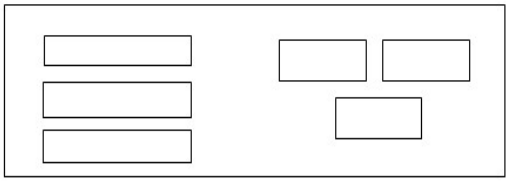
Perancangan output



Gambar 2. Rancangan Form Menu Utama



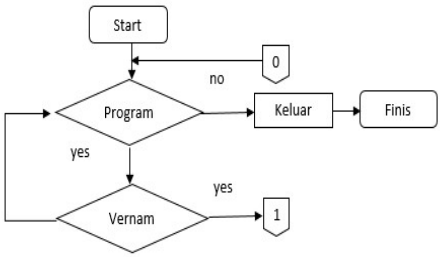
Gambar 3. Menu aplikasi



Gambar 4. Rancangan Aplikasi

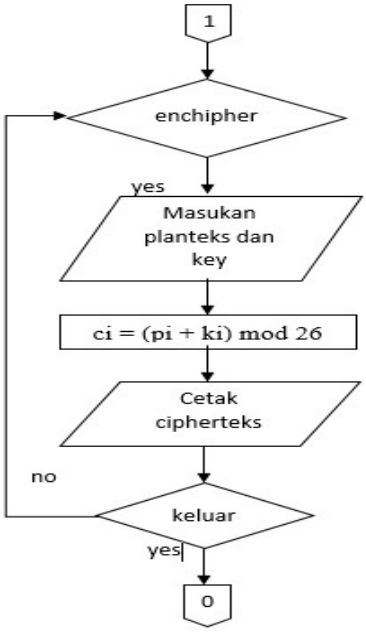
Digram alir (Flowchart)

Digram alir atau flowchart merupakan serangkaian bagan bagan yang menggambarkan alir program. Pada diagram alir ini digambarkan urutan prosedur dalam program simulator kriptografi vernam



Gambar 5. Diagram alir menu utama

Diagram Alir Vernam



Gambar 6. Diagram Alir Vernam

3. HASIL DAN PEMBAHASAN

Implementasi merupakan tahap dimana program aplikasi siap dioperasikan pada keadaan yang sebenarnya sehingga dari sini akan diketahui apakah program aplikasi benar-benar dapat menghasilkan keluaran yang sesuai dengan tujuan yang diinginkan.

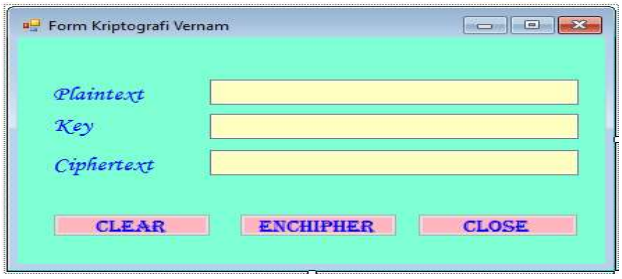
Tampilan Antar-muka Splashscreen

Form splashscreen ini merupakan main-form dalam program kriptograpi dan untuk mengakses ke form berikutnya, yaitu form login.

Gambar 7. Tampilan Aplikasi kriptografi vernam

Tampilan Menu Aplikasi

Di dalam form menu aplikasi terdapat aplikasi yang akan dijalankan.



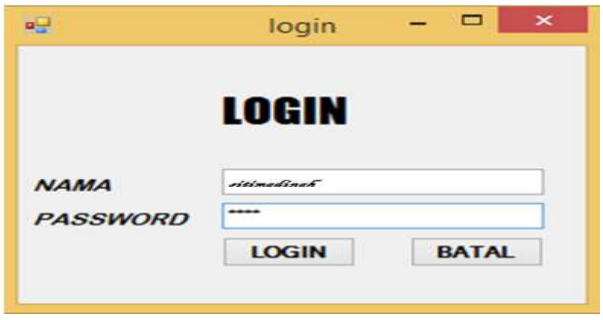
Gambar 8. Tampilan Form aplikasi

Tampilan Aplikasi dan Cara Kerja Login

Form login digunakan sebagai otoritas akses menjalankan program. Halaman login akan mengecek username dan password yang dimasukkan operator ataupun admin. Adapun username (edy haryadi) dan password (istn).

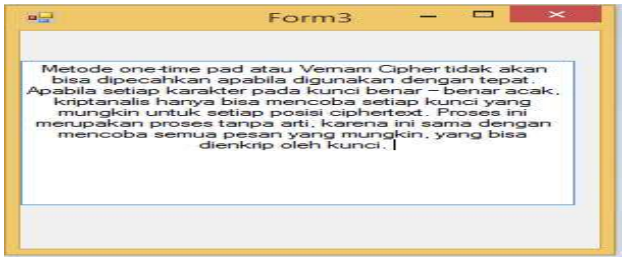
Menu Utama

Di dalam form menu utama pada aplikasi kriptograpi vernam, terdapat beberapa menu yang ditampilkan diantaranya menu aplikasi, menu abaut dan keluar.



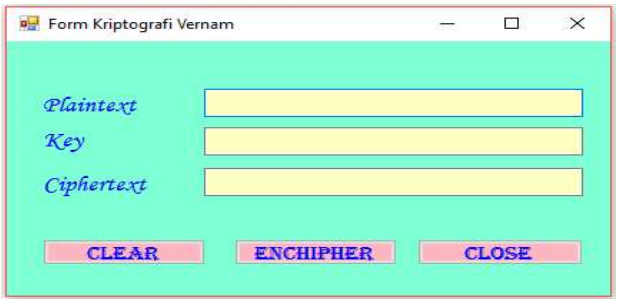
Gambar 9. Tampilan Menu Utama

jika di pilih menu about akan muncul tampilan seperti ini.



Gambar 10. Tampilan Menu About

Dan jika dipilih menu aplikasi akan muncul seperti ini.

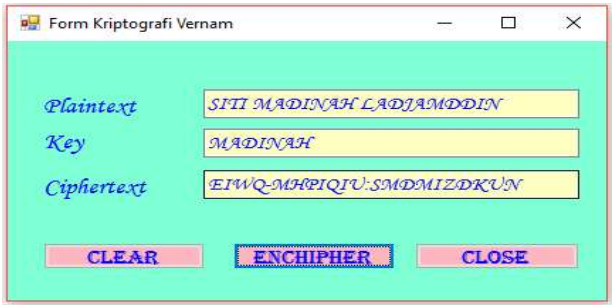


Gambar 11. Tampilan Enchiper

Dan masukaan plaintext dan key seperti ini.

Gambar 12. Tampilan enchiper

Lalu di enchiper, dan akan muncul sandi yang telah di enchipher di ciphertext.



Gambar 13. Tampilan Enchiper

4. SIMPULAN

Dari uraian hasil dan pembahasan diatas, dapat disimpulkan bahwa:

- Untuk menyisipkan suatu informasi pesan dibutukan suatu metode yaitu metode kriptograpi vernam karena dengan menggunakan metode ini pesan dapat disandikan secara efektif.
- Untuk melindungi suatu informasi pesan ke dalam kriptograpi dibutuhkan key atau password. Dengan password ini pesan dapat terjaga keamanannya dengan baik.

Saran-saran yang dapat digunakan dalam membuat suatu aplikasi :

- Aplikasi kriptograpi vernam diharapkan menjadi tambahan materi untuk matakuliah kriptografi.
- Tampilan ini belum menggunakan set up untuk lebih disempurnakan agar lebih memudahkan user untuk mengoperasikan aplikasi ini.

DAFTAR PUSTAKA

Fahmi, Husni dan Haret Faidah, 2006. Tutorial Kriptografi Klasik dan Penerapannya dalam Visual Basic.NET. Ilmukomputer.com

Febrian. Jack. 2004. Pengetahuan Komputer dan Teknologi Informasi. Bandung : CV.Informatika

Kahn, D. 1996. The Codebreakers : The Story of Secret Wiriting, New York : Scribner

Munir, Rinaldi. 2007. Kriptografi. Bandung : CV. Informatika

Munir, Rinaldi. 2001. Algoritma dan Pemrograman dalam Bahasa Pascal dan C. Bandung : CV. Informatika

Schneier, Bruce.1996. applied Cryptografy, Protocol, Algoritma, and Source Code n C. John Wiley & Sons. Inc.

Stallings, Willam. 2003. Cryptografy and Network Security, Principles and Practices. Pearson Prentice Hall.