Perancangan Perangkat Lunak Kriptografi Menggunakan Gronsfeld Cipher, Vernam Cipher dan Ron Code 4 Stream Cipher

Ade Lita Noviani, I Dewa Ayu Eka Yuliani
STMIK Pontianak; Jl. Merdeka Barat No.372 Pontianak,
telp/fax : (0561) 735555 / (0561) 737777
e-mail aa300711@gmail.com, ekanesta@gmail.com

Abstrak

Proses pengiriman data yang dilakukan seperti yang media internet, maupun media lainnya. Pada dasarnya pengiriman data tersebut tanpa ada melakukan pengamanan terhadap konten dari data yang dikirim, sehingga ketika dilakukan penyadapan pada alur pengirimannya maka data yang disadap dapat langsung dibaca penyadap. Untuk itu dibutuhkan perangkat lunak sebagai penunjang menggunakan metode penyandian (kriptografi) tertentu sehingga pesan yang terkandung dalam data yang terkirim tersebut menjadi aman. Adapun teknik pengumpulan data yang digunakan dalam penelitian ini dengan studi literatur untuk memperoleh teori kriptografi Gronsfeld Cipher, Vernam Cipher dan Ron Code 4 Stream Cipher. Sedangkan metode perancangan perangkat lunak menggunakan RAD (Rapid Application Development) Perancangan perangkat lunak menggunakan Bahasa pemograman Microsoft Visual Basic.Net hasil perancangan ini menhasilkan sebuah aplikasi kriptosistem gabungan Gronsfeld Cipher, Vernam Cipher dan Ron Code 4 Stream Cipher. Perangkat Lunak kriptosistem gabungan Gronsfeld Cipher, Vernam Cipher dan Ron Code 4 Stream Cipher dengan adanya perangkat ini, kerahasian dan keaslian informasi akan lebih terjaga.

Kata Kunci - *Perangkat lunak kriptografi, Kriptosistem gabungan, Gronsfeld Cipher, Vernam Cipher dan Ron Code 4 Stream Cipher, Visual Basic.Net, Prototype.*

Abstract

The process of sending data is done as the internet media, and other media. Basically the data transmission without any security to the content of the data sent, so that when the tapping on the flow of the delivery of data that can be intercepted immediately read tappers. For that required software as a supporter using a particular method of encryption (cryptography) so that the messages contained in the data sent to be safe. The data collection techniques used in this study with literature study to obtain the theory of cryptography Gronsfeld Cipher, Vernam Cipher and Ron Code 4 Stream Cipher. While the software design method using RAD (Rapid Application Development) The design of software using Microsoft Visual Basic.Net programming language of this design resulted in a combined cryptosystem application Gronsfeld Cipher, Vernam Cipher and Ron Code 4 Stream Cipher. Combined cryptosystem software Gronsfeld Cipher, Vernam Cipher and Ron Code 4 Stream Cipher in the presence of this device, confidentiality and authenticity of information will be more ***awake.***

Keywords - *Cryptography software, Combined Cryptosystem, Gronsfeld Cipher, Vernam Cipher and Ron Code 4 Stream Cipher, Visual Basic.Net, Prototype.*

1. PENDAHULUAN

Keamanan informasi menjadi sangat penting saat ini. Keamanan data dan menghindari program jahat (SPAM, virus, Trojan dll.) menjadi kebutuhan penting dalam Teknologi Informasi. Beberapa perangkat digital dan perangkat lunak (software) mengamankan sistemnya dengan cara manipulasi bit. Salah satu metode yang biasa digunakan dalam Kemaman Informasi adalah kriptografi. Beberapa metode enkripsi yang di kenal dalam kriptografi (sha-0, sha-1, md5 dll) membuat data atau file yang terenkripsi tidak akan mudah dirusak.

Permasalahan utama dalam proses enkripsi dan dekripsi adalah penentuan algoritma yang tepat dan efisien yang digunakan dalam proses enkripsi dan dekripsi tersebut. Pada proses enkripsi dibutuhkan algoritma yang dapat mengenkripsi data secara aman dan pada proses dekripsi dibutuhkan algoritma yang dapat mendekripsi kembali data tersebut dengan tepat. Ada beberapa contoh macam-macam metode kriptografi untuk membuat pesan rahasia antara lain mulai dari kriptografi klasik, kriptografi modern, kriptografi dengan pertukaran kunci, kriptografi dengan fungsi Hash dan lain sebagainya. Beberapa algoritma berikut tergolong dalam kategori kriptografi klasik, antara lain Caesar, Affine, Monoalphabetic, Polyalphabetic, Vigenere, Beaufort, Playfair, Transposisi, RailFence, Gronsfeld, dan lain-lainnya.

Untuk menjamin kerahasiaan suatu informasi, dapat dilakukan dengan menggunakan kriptografi. Kriptografi sesungguhnya merupakan studi terhadap penyandian suatu tulisan atau informasi rahasia dengan menggunakan suatu teknik matematis. Dengan menggunakan kriptografi, informasi dapat disandikan ke dalam bentuk yang tidak bisa dimengerti sehingga informasi tersebut tidak dapat diakses oleh orang-orang yang tak berkepentingan. Sebuah algoritma kriptografi dikatakan aman (computationally secure) apabila memenuhi tiga kriteria berikut persamaan matematis yang menggambarkan operasi algoritma kriptografi sangat kompleks sehingga algoritma tidak mungkin dipecahkan secara analitik, biaya untuk memecahkan cipherteks melampaui nilai informasi yang terkandung di dalam ciphertext tersebut serta waktu yang diperlukan untuk memecahkan cipherteks melampaui lamanya waktu informasi tersebut harus dijaga kerahasiaannya..

Gronsfield Cipher merupakan sebuah algoritma kriptografi yang menggunakan suatu kunci numerik dan tabel dalam proses enkripsi dan dekripsi, kunci yang digunakan akan diulang dari kiri jika teks yang akan di enkripsi atau dekripsi lebih panjang dari kunci yang digunakan. Idenya adalah dengan mengganti huruf dengan bilangan desimal maka akan mengakibatkan plainteks tidak akan berupa huruf melainkan hanya berupa susunan angka. Kemudian enkripsi menggunakan prinsip yang sama dengan Algoritma Vigenère yaitu menggunakan tabel yang hanya berukuran 10x10. *Vernam Cipher* merupakan algoritma berjenis symetric key yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara stream cipher yang berasal dari hasi XOR antara bit plaintext dan bit key. Pada metode ini plain text diubah kedalam kode ASCII dan kemudian dikenakan operasi XOR terhadap kunci yang sudah diubah ke dalam kode ASCII. *RC4* merupakan salah satu jenis streamcipher yang didesain oleh *Ron Riverst* di laboratorium *RSA (RSA Data Security inc)* pada tahun 1987. RC4 sendiri merupakan kepanjangan dari *Ron Code* atau *Rivest's Cipher*. RC4 stream cipher ini merupakan teknik enkripsi yang dapat dijalankan dengan panjang kunci yang variabel dan beroperasi dengan orientasi byte. RC4 merupakan stream cipher yang sangat cepat dan aman dari RSA. Data Security, I nc. RC4 digunakan dalam lingkungan dengan sumber daya yang kecil dengan resiko yang tinggi. RC4 tidak dipatenkan meskipun untuk tujuan komersial sekalipun. RC 4 menggunakan panjang kursi variable dari 1-256 byte (mempunyai kemampuan antara 1 – 2048 bit) untuk menginisialisasi 256 –byte state table.

Pada penelitian yang dilakukan tentang penyandian short message service (SMS) pada telepon seluler dengan menggunakan algoritma gronsfeld. Pada penelitian ini di jelas bahwa Teknologi SMS juga tidak menjamin keamanan dan kerahasiaan pesan yang dikirim. Beberapa risiko juga merupakan ancaman bagi keamanan termasuk SMS spoofing, SMS snooping, dan SMS interception. SMS spoofing sendiri adalah sebuah pengiriman SMS di mana nomor pengirim yang tertera bukanlah nomor pengirim yang sebenarnya. SMS snooping lebih sering terjadi karena kesalahan pengguna telepon seluler dan SMS interception adalah pencurian data pesan SMS ketika masih dalam transmisi dari pengirim ke penerima[1].

Pada Penelitiaan yang dilalukan tentang Analisis Kombinasi Metode Caesar Cipher, Vernam Cipher, dan Hill Cipher dalam Proses Kriptografi . didapat kesimpulan bahwa metode Caesar Cipher, Vernam Cipher, dan Hill Cipher adalah jenis kriptografi klasik yang cukup kuat jika dilihat dari segi keamanannya dengan sedikit modifikasi. Ketiga metode ini dapat dikombinasikan menjadi satu dalam proses kriptografi (enkripsi dan dekripsi) dengan tingkat keamanan yang sangat baik dan sulit untuk dipecahkan, Kombinasi metode Caesar Cipher, Vernam Cipher, dan Hill Cipher ini hanya membutuhkan sebuah kunci (key) dalam proses enkripsi maupun dekripsi yang akan memudahkan kita untuk mengingatnya[2].

Pada Penelitian yang dilakukan tentang Metode Pengamanan Ekkripsi RC4 Stream Cipher Untuk Aplikasi Pelayanan Gangguan, didpan kesimpulan Aplikasi web-base merupakan salah satu solusi untuk mewujudkan suatu aplikasi yang bersifat terpusat, akan tetapi karena aplikasi diakses dari media internet/intranet resiko data dicuri atau disalahgunakan oleh orang yang tidak bertanggung jawab pun semakin besar. Mengingat kebocoran data dapat disebabkan oleh orang dalam atau pihak-pihak yang berhubungan langsung dengan data. Pengamanan data melalui metode enkripsi RC4 dapat menjadi salah satu solusi dalam hal pengamanan. Data yang ada tidak dapat langsung dibaca tanpa mengetahui secret key yang digunakan [3].

Berdasarkan uraian tersebut, maka penulis membangun sebuah aplikasi kriptografi *hybrid* dengan menggunakan tiga algoritma, yaitu *Gronsfeld Cipher , Vernam Cipher, dan Ron Code 4 (RC4)* sebagai kriptografi modern dengan menggabungkan algoritma hasil enkripsi, sehingga dapat dimanfaatkan sebagai alat bantu dalam menjaga kerahasiaan sebuah data secara berlapis serta dapat mempelajari dan memahami cara kerja dari ketiga metode kriptografi tersebut.

2. METODE PENELITIAN

Bentuk penelitian yang digunakan adalah bentuk studi literature menyatakan bahwa studi kepustakaan atau studi literatur, selain dari mencari sumber data sekunder yang akan mendukung penelitian, juga diperlukan untuk mengetahui sampai ke mana ilmu yang berhubungan dengan penelitian telah berkembang, sampai ke mana terdapat kesimpulan dan generalisasi yang pernah dibuat sehingga situasi yang diperlukan diperoleh[4]. Metode penelitian yang digunakan adalah metode Experimental menyatakan bahwa “metode penelitian eksperimental dapat diartikan sebagai metode penelitian yang digunakan untuk mencari pengaruh perlakukan tertentu terhadap yang lain dalam kondisi yang terkendalikan”[5].

Metode yang digunakan peneliti dalam melakukan pengumpulan data adalah studi dokumentasi, yaitu peneliti mengumpulkan serta mempelajari bahan-bahan tertulis yang berhubungan dengan penggunaan algoritma Gronsfeld Cipher, Vernam Cipher, dan Ron Code 4 (RC4) yang didapat melalui Jurnal nasional, jurnal Internaional, artikel, buku, e-book dan pencarian diinternet terhadap materi metode Kriptografi algoritma Gronsfeld cipher, Vernam Cipher, dan Ron Code 4 (RC4).

Penulis menggunakan metode perancangan RAD (*Rapid Application Development*) karena proses perkembangan perangkat lunak ini menekankan pada siklus perkembangan yang singkat. Model RAD merupakan sebuah adaptasi dari model sekuensial dimana perkembangan cepat dicapai dengan menggunakan pendekekatan konstruksi berbasis komponen.

Untuk menyajikan algoritma, penulis menggunakan teknik *pseudocode*. *pseudocode* adalah kode yang mirip dengan instruksi kode program yang sebenarnya dan berbasis pada bahasa pemograman yang sesungguhnya. Sehingga *pseudocode* lebih tepat digunakan untuk mengggambarkan algoritma yang akan dikomunikasikan dengan *programmer*.

Untuk melakukan pengujian perangkat lunak kriptografi *Gronsfeld cipher*, *Vernam Cipher* dan *Ron Code 4 (RC4) Stream Cipher* penulis menggunakan proses formal *vertification dan Black Box atau Kotak Hitam.* Pengujian formal *vertification*adalah suatu proses pengujian terhadap perangkat lunak dengan pendekatan formal matematis, yang dilakukan terhadap perangkat lunak itu sendiri dan spesifikasi dari perangkat lunak yang bersesuaian.

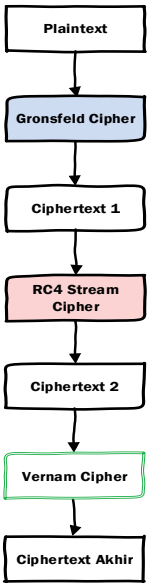
Pengujian black box merupakan pendekatan komplementer dari teknik white box, karena pengujian black box diharapkan mampu mengungkap kelas kesalahan yang lebih luas dibandingkan teknik white box. Pengujian black box berfokus pada pengujian persyaratan fungsional perangkat lunak, untuk mendapatkan serangkaian kondisi input yang sesuai dengan persyaratan fungsional suatu program.

3. HASIL DAN PEMBAHASAN

Pada tahap ini, mendaftarkan dan mendefinisikan fungsi-fungsi yang akan dipakai dalam pembuatan Perangkat lunak kriptografi Menggunakan Gronsfeld Cipher, RC4 Stream Cipher, dan Vernam Cipher. Penelitian bertujuan untuk merancang sebuah perangkat lunak kriptografi yang dapat melakukan Enkripsi dan Dekripsi Suatu Pesat Penting.

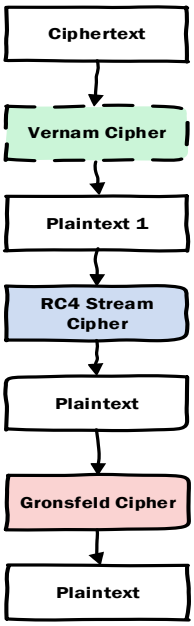
Dengan Diperkuat Algoritma Gronsfeld Cipher, Vernam cipher dan RC4 Stream Cipher Setelah diketahui dari analisa kelemahan algoritma vernam cipher dan RC 4 Stream cipher yaitu mudah dipecahkan dengan metode exhaustive key search dan analisis kemunculan bigram maka dimanfaatkan algoritma penyandian klasik transposisi yaitu dengan menggunakan Gronsfeld cipher untuk mengecoh kriptanalis dalam memecahkan penyandian yang dilakukan dengan system penyandian klasik. Adapun metode enkripsi yang digunakan untuk memperkuat penyandian adalah :

Enkripsi Penggabungan Algoritma Gronsfeld Cipher, Vernam Cipher , dan RC4 Stram Cipher.



Gambar 1 Proses Enkripsi Penggabungan Gronsfeld Cipher, Vernam Sipher, dan RC 4 Stream Cipher

Langkah-langkah enkripsi pada penggabungan penyandian Gronsfeld Cipher,Vernam Cipher , dan RC4 Stream Cipher adalah sebagai berikut :
Plaintext dienkripsi dengan menggunakan Gronsfeld cipher dan akan dihasilkan output chiperteks1 yang merupakan ciphertext sementara pertama. Ciphertext1 menjadi input enkripsi dengan menggunakan RC4 Stream cipher dan akan menghasilkan output ciphertext2 yang merupakan ciphertext sementara kedua. Ciphertext2 menjadi input enkripsi dengan menggunakan Vernam cipher dan akan menghasilkan output ciphertext3 yang merupakan ciphertext akhir yang merupakan hasilkan output ciphertext akhir.
Dekripsi Penggabungan Algoritma kriptografi Gronsfeld Cipher, RC4 Stream Ciper, dan Vernam Cipher



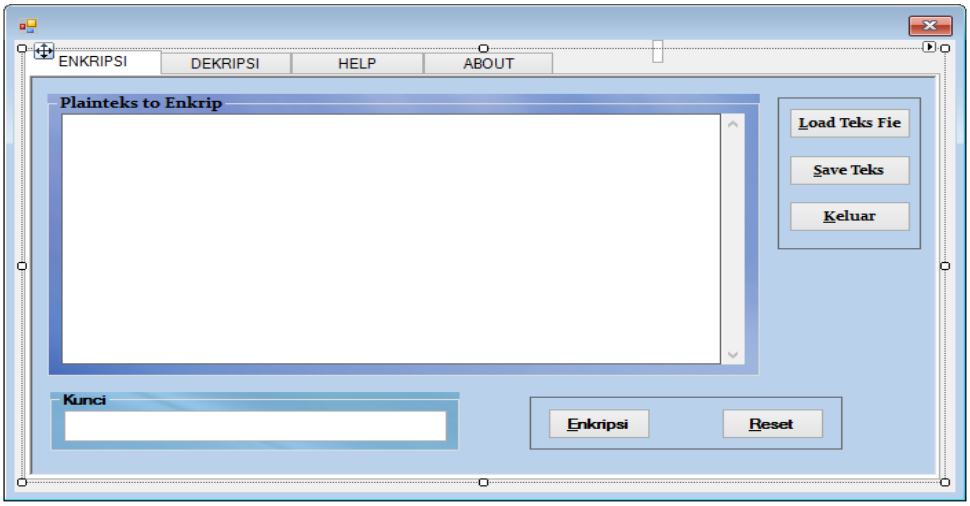
Gambar 2. Proses Dekripsi Penggabungan Gronsfeld Cipher, RC4 Stream Cipher, dan Vernam Cipher

Langkah-langkah dekripsi pada penggabungan algoritma kriptografi *Gronsfeld Cipher* , *RC4 Stream Cipher*, dan *Vernam Cipher* adalah sebagai berikut :
Ciphertext didekripsi dengan menggunakan *Vernam cipher* yang merupakan fungsi kebalikan dari proses enkripsi yang terkahir yang akan dihasilkan output *plaintext1* yang merupakan plaintext sementara.
Plaintext1 menjadi input dekripsi dengan menggunakan *RC4 Stream cipher*, akan dihasilkan output *plaintext2* yang merupakan plaintext sementara.
Plaintext2 menjadi input dekripsi dengan menggunakan *Gronsfeld cipher*, dan akan menghasilkan output plaintext akhir

Form Splash screen berfungsi sebagai form pembuka perangkat lunak. Pada Form ini terdapat sebuah progress bar yang menandakan aplikasi sedang diproses atau dijalankan. Gambar 1 berikut merupakan tampilan dari Splash Screen pada saat program dijalankan. Setelah mengetahui arsitektur dari perangkat lunak yang dirancang, dibutuhkan juga sebuah alur kerja sistem untuk menggambarkan secara jelas bagaimana cara kerja dari perangkat lunak tersebut.

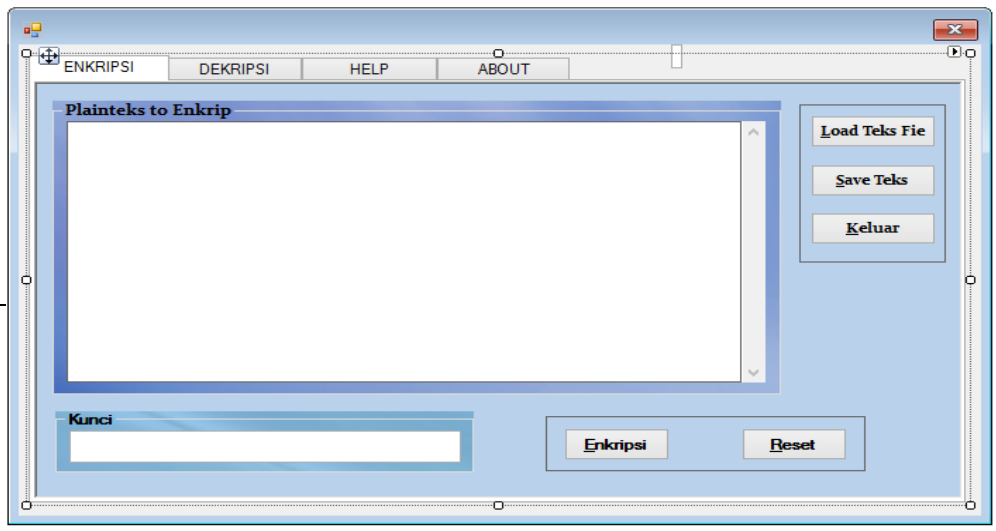
Gambar 3. Form Splash Screen

Form Main berfungsi sebagai *form* utama perangkat lunak dan memiliki beberapa menu, yaitu : menu '*File'* untuk melakukan operasi *file* (*Exit*), untuk melakukan enkripsi, dekripsi, help, about program. pada form ini penulis menggunakan tab control yang ada pada tool visual basic .net untuk membuat tampilan perangkat lunak lebih menarik dan mudah dipahami.



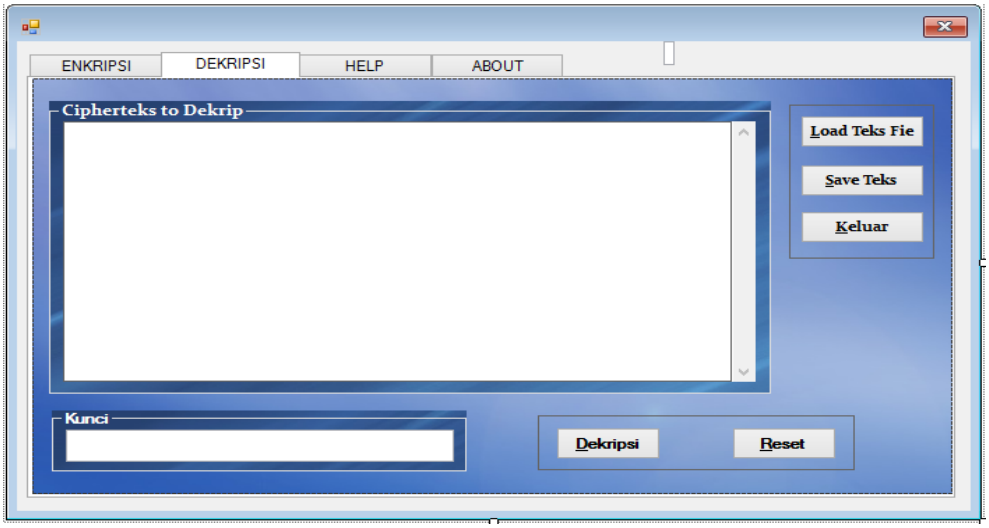
Gambar 4. Form Main

Form Enkripsi digunakan sebagai Tools untuk melakukan Dekripsi menggunakan gabungan algoritma gronsfeld cipher, rc4 Stream cipher, dan vernam cipher. Pada form Dekripsi dirancang terdiri dari lima buah *button* yaitu tombol 'Load text file', 'Save text', 'Enkripsi', 'Reset', dan tombol 'Close'.



Gambar 5. Form Enkripsi

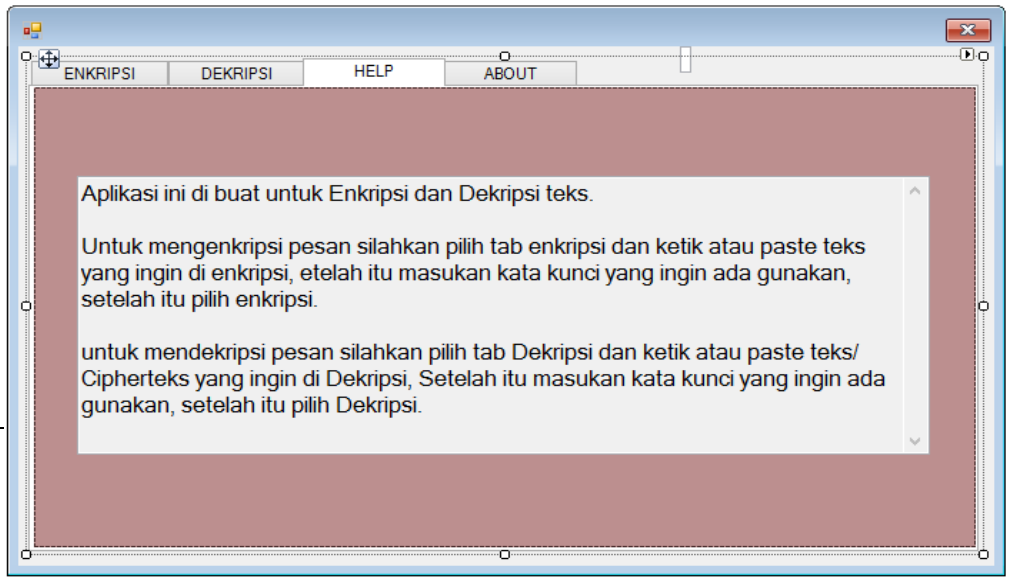
Form Help digunakan sebagai Tools untuk informasi kegunaan perngkat lunak menggunakan gabungan algoritma gronsfeld cipher, rc4 strem cipher, dan vernam cipher. Pada form dirancang terdiri dari textbox yang berisikan informasi mengnai perangkat lunak cryptosystem.



Gambar 6. Form Deskripsi

Form Deskripsi digunakan sebagai Tools untuk melakukan Dekripsi menggunakan gabungan algoritma gronsfeld cipher, rc4 Stream cipher, dan vernam cipher. Pada form Dekripsi dirancang terdiri dari lima buah *button* yaitu tombol ‘Load text file’, ‘Save text’, ‘Enkripsi’, ‘Reset’, dan tombol ‘Close’. Gambar 4.7 berikut merupakan desain form Dekripsi dan gambar 4.8 merupakan tampilan dari Form Dekripsi pada saat program dijalankan

.

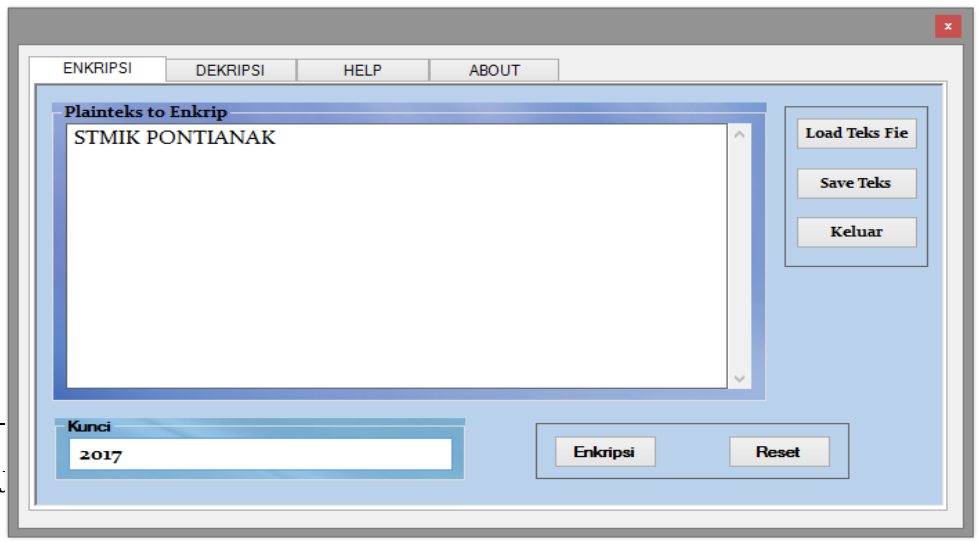


Gambar 7. Rancangan Form Help

Form Help digunakan sebagai Tools untuk informasi kegunaan perngkat lunak menggunakan gabungan algoritma gronsfeld cipher, rc4 strem cipher, dan vernam cipher. Pada form dirancang terdiri dari textbox yang berisikan informasi mengnai perangkat lunak cryptosystem.

Gambar 8. Rancangan Form About

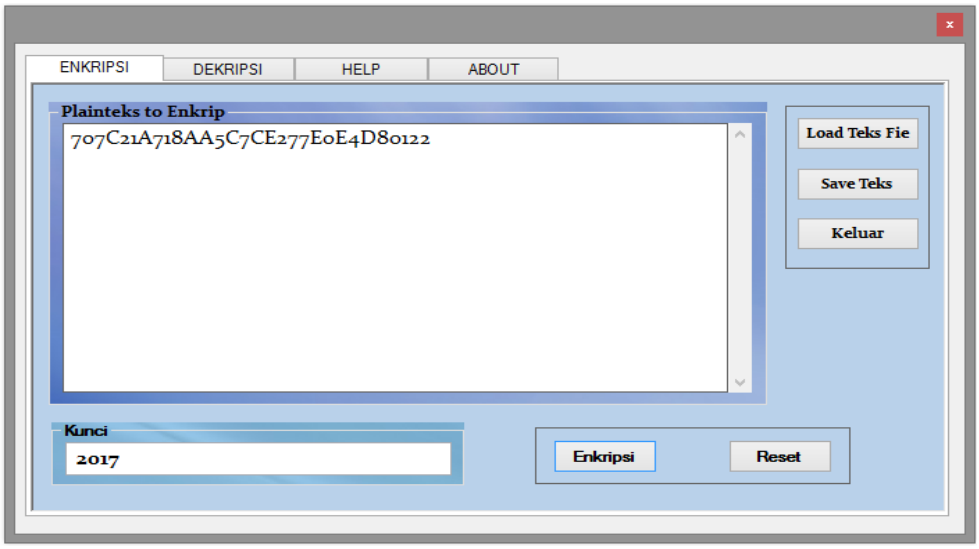
Pada *form About* dirancang terdiri dari sebuah *label dan textbox* yang berisikan informasi dari pembuat perngkat lunak kriptografi menggunakan Gronsfeld cipher, Vernam Cipher, dan RC4 Stream Cipher.



Gambar 9. Proses Input Pesan Plaintext dan Kunci

Berikut ini adalah penjelasan hasil proses enkripsi Pesan, yang diimplementasikan pada rancangan aplikasi penggabungan Algoritma *Gronsfeld Cipher, Vernam Cipher,* dan *RC4 Stream Cipher*.
Dari gambar di atas dapat dilihat proses input pesan pada aplikasi penyandian adalah sebagai berikut :

a. Input teks yang akan dienkripsi pada jendela Input Text, teks ini merupakan *plaintext* yang nantinya akan dienkripsi dan harus diisi dengan minimal 1 karakter
b. Input karakter kunci yang digunakan untuk mengenkripsi pesan, harus diisi minimal 1 karakter kunci
c. Tekan atau klik tombol Enkripsi untuk mengenkripsi pesan
   Sebagai contoh diatas :
   Plainteks : STMIK PONTIANAK
   Kunci : 2017



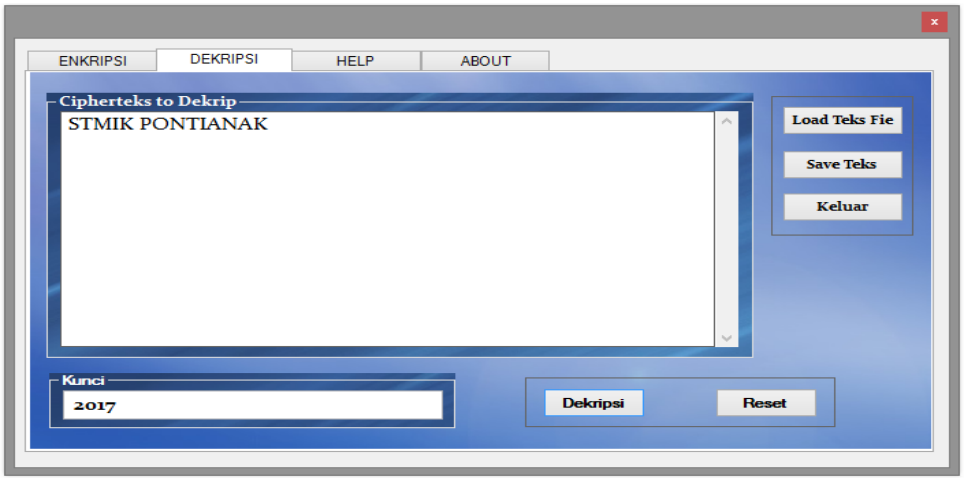
Gambar 10. Hasil Enkripsi Gronsfeld Cipher, Vernam Cipher, dan RC4 Stream Cipher

Gambar diatas merupakan hasil enkripsi pesan pada jendela Input Teks setelah ditekan tombol Enkripsi dan dilakukan proses penyandian pesan, maka didapat hasil enkripsi "707C21A718AA5C7CE277E0E4D80122" .
Dari gambar di atas dapat dilihat proses input Cipherteks yang akan di dekripsi pada aplikasi penyandian adalah sebagai berikut :

a. Input teks yang akan didekripsi pada jendela Input Text, teks ini merupakan ciphertext yang nantinya akan didekripsi dan harus diisi dengan minimal 1 karakter
b. Input karakter kunci yang digunakan untuk mendekripsi pesan, harus diisi minimal 1 karakter kunci
c. Tekan atau klik tombol dekripsi untuk mendekripsi pesan

Sebagai contoh diatas :

Cipherteks : 707C21A718AA5C7CE277E0E4D80122
Kunci : 2017



Gambar 11. Hasil Dekripsi Gronsfeld Cipher, Vernam Cipher, dan RC4 Stream Cipher

Gambar diatas merupakan hasil dekripsi pesan pada jendela Input Cipherteks setelah ditekan tombol Dekripsi dan dilakukan proses dekripsi pesan

.4. KESIMPULAN

Dalam penelitian ini memberikan kesimpulan yang mengindikasikan diperlukannya pengamanan data dengan menggunakan teknik kriptografi. Teknik penyandian kriptografi klasik pada kenyataanya masih layak untuk digunakan sebagai sistem keamanan suatu pesan, namun haruslah diperkuat dengan metode tertentu, salah satunya adalah dengan memper kuat penyandian klasik metode subsitusi dengan metode modern.

Sistem penyandian seperti ini menghasilkan suatu metode kriptografi enkripsi yang memiliki kelebihan sebagai berikut :

Merupakan suatu sistem penyandian klasik yang lebih baik, karena menggabungkan konsep difusi yang dimiliki oleh sandi subtitusi dan konsep kriptografi modern dengan pergeseran bit yang dimiliki oleh sandi kriptografi.

Memperkecil kemungkinan pembobolan sandi klasik oleh kriptanalis dan meningkatkan kerumitan hubungan antara plainteks dan cipherteks.
Sistem penyandian terbilang sederhana dan mudah untuk diimplementasikan karena hanya berdasarkan metode pergeseran bit dan metode pergantian karakter alphabet atau subsitusi, namun sandi ini terbilang cukup rumit untuk dapat dipecahkan.

5. SARAN

Mekanisme enkripsi dan dekripsi yang digunakan dalam penelitian kali ini memang masih terbilang cukup sederhana, akan tetapi diharapkan dapat berguna sebagai langkah awal untuk masuk ke dalam dunia kriptografi, khususnya dalam implementasi pengamanan pesan dengan menggunakan penyandian klasik. Untuk kedepannya, diharapkan penelitian ini dapat dikembangkan, digunakan serta diterapkan pada bidang-bidang kehidupan yang lain yang lebih kompleks.

DAFTAR PUSTAKA

[1] Azanuddin, Penyandian Short Message Service (SMS) Pada Telepon Selular Dengan Menggunakan Algoritma Gronsfeld, Pelita Informatika Budi Darma, Volume : IV, Nomor: 1, Agustus 2013 ISSN : 2301-9425
[2] Khairani Puspita1, M. Rhifky Wayahdi2.,2015. Analisis Kombinasi Metode Caesar Cipher, Vernam Cipher, dan Hill Cipher dalam Proses Kriptografi , ISSN 2302-3805
[3] Dwi Irfianti,Asti., (2007)., Metode Pengamanan Ekkripsi RC4 Stream Cipher Untuk Aplikasi Pelayanan Gangguan. ISSN : 1907-5022
[4] Nazir, M. 2005. *Metode Penelitian*. Jakarta: Ghalia Indonesia
[5] Sugiyono. 2012. Metode Penelitian Kombinasi (Mixed Methods). Bandung: Alfabeta