Perancangan Dan Pengujian Perangkat Lunak Kriptografi Gabungan Playfair Cipher Dan Electronic Code Book (ECB)

Angga Yudia Putra, I Dewa Ayu Eka Yuliani
[1,2]STMIK Pontianak; Jl Merdeka Barat No. 372, (0561) 735555
[3]Jurusan Teknik Informatika, STMIK Pontianak
e-mail: **anggayudiaputra@gmail.com, ekanesta@gmail.com**

Abstrak

Teknologi informasi merupakan seperangkat alat dalam membantu pemprosesan atau penataan data yang mempunyai nilai pengetahuan bagi penggunanya. Dalam menjamin kerahasian dan keamanan suatu data diperlukan metode kriptogafi, yang merupakan studi penyandian untuk menjaga kerahasian pada informasi. Untuk itu dibutuhkan perangkat lunak sebagai penunjang metode penyandian tertentu sehingga pesan terkirim tersebut menjadi lebih aman. Dalam penelitian ini penulis menggunakan bentuk penelitian studi literatur dan eksperimen murni. Sedangkan metode perancangan perangkat lunak menggunakan metode RAD (Rapid Aplication Development) karena proses perkembangan perangkat lunak ini menekankan pada siklus perkembangan yang singkat dan pemanfaatan fungsi yang pada sebelumnya. Adapun teknik pengumpulan data menggunakan Study Literature penulis mempelajari buku-buku, majalah, skripsi, jurnal, pencarian di Internet dengan sumber yang terpercaya serta referensi yang ada yang berhubungan dengan teori-teori kriptografi, algoritma Playfair Cipher dengan Eletronic Code Book (EBC) serta perancangan perangkat lunak.Perancangan perangkat lunak menggunakan bahasa pemrograman Microsoft Visual Basic 6.0. Perangkat lunak gabungan Playfair Cipher dan Electronic Code Book (ECB) cipher telah dijalankan dan sesuai dengan yang diharapkan.

Kata Kunci*— Kriptografi , Enkripsi, Dekripsi, Algoritma Playfair Cipher, Electronic Code Book (ECB).*

Abstract

Information technology is a set of tools to assist the processing or arrangement of the data which has the value of knowledge for its users. In assuring the confidentiality and security of the data required kriptogafi method, which is the study of encryption to maintain the confidentiality the information. It requires software to support specific encoding method so the sent message has become more secure. In this study the authors used a form of research literature and pure experimentation. While the software design methods using RAD (Rapid Application Development) for the software development process emphasize the short development cycles and utilization in the previous function.The data collection techniques using Study Literature, the author studied the books, periodicals, theses, journals, searching the Internet with a trusted source as well as the existing references related to theories of cryptography, algorithms Playfair Cipher with Eletronic Code Book (EBC) and software design. Designing software using Microsoft Visual Basic 6.0. , Combined Playfair Cipher software and Electronic Code Book (ECB) has been run as expected.

Keywords— *Cryptography , Encryption, Decryption, Algorithm Playfair Cipher, Electronic Code Book (ECB).*

1. PENDAHULUAN

Kriptografi pada awalnya merupakan ilmu yang mempelajari penyembunyian pesan. Namun, seiring berkembangnya teknologi, kriptografi ini juga berkembang, perkembangan teknologi ini dapat dilihat dengan adanya internet yang menghubungkan komputer satu sama lain. Dengan adanya perkembangan ini kriptografi sangat dibutuhkan untuk keamanan data yang dikirim kepada komputer lain. Kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan autentikasi entitas.

Ada empat tujuan utama dari kriptografi. Kerahasiaan (confidentiality) di mana kriptografi digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah disandi. Kerahasiaan dijaga dengan melakukan enkripsi (penyandian). Keutuhan (integrity) yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak[1].

Dalam penelitian ini, penulis menggunakan bentuk penelitian studi literature dan eksperimen murni. Penulis melakukan kajian yang berkaitan erat dengan permasalahan yang hendak dipecahkan serta mendefinisikan masalah dengan melakukan eksperimen. Selain itu penulis juga mencari referensi dan informasi yang diperlukan dari buku-buku dan artikel-artikel di Internet. Referensi dan informasi tersebut merupakan dasar pembuatan aplikasi oleh penulis.
Metode penelitian yang digunakan oleh penulis adalah metode eksperimen, yaitu melakukan percobaan (ujicoba) serta manipulasi objek secara langsung, untuk mendapatkan hasil yang memuaskan. Untuk melakukan pengujian perangkat lunak aplikasi kriptografi yang menggunakan algoritma gabungan Playfair Cipher dengan Eletronic Code Book (EBC), penulis menggunakan metode *black-box* dan proses formal *vertification.* Pengujian dilakukan terhadap fungsi-fungsi yang ada dengan menginput data masukan dan meneliti data hasil outputnya. Fungsi kriptografi yang lain adalah autentikasi yang berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui jaringan harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain. Non-repudiation adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman dengan kata lain, terciptanya suatu informasi oleh yang mengirimkan.

Objek Penelitian Sebelumnya Playfair Cipher merupakan salah satu metode yang digolongkan dalam kriptogafi klasik yang proses enkripsinya menggunakan pemrosesan dalam bentuk blok-blok yang sangat besar[2]. Metode ini merupakan salah satu cara untuk mengatasi kelemahan metode kriptografi klasik lainnya yang mudah tertebak karena terdapat korespondensi satu-satu antara plainteks dengan cipherteks. Seperti halnya pesan teks dalam menjaga kerahasiaannya, pesan citra juga memerlukan teknik-teknik enkripsi yang sebisa mungkin sederhana tapi sukar dipecahkan. Proses pengamanan pesan dalam bentuk citra dapat dilakukan dengan mengenkripsi citra ke dalam bentuk citra lagi dengan algoritma tertentu. Ini dimungkinkan mengingat sebuah citra dapat direpresentasikan dalam sebuah matriks yang berisi bilangan-bilangan bulat. Pada penelitian ini Playfair Cipher akan diimplementasikan untuk menyandikan citra dengan format bmp 24 bit, yang mempunyai ukuran 256 x 256 pixel. Citra yang akan diujikan terdiri dari 2 jenis citra yaitu citra dengan tingkat kontras yang berbeda serta citra dengan kategori tingkatan detil yang berbeda. Kunci yang digunakan untuk menyandikan citra menggunakan 2 jenis matrik yang mempunyai ordo 16 x 16. Dari hasil pengujian didapatkan bahwa playfair merupakan metode penyandian klasik yang cocok diterapkan untuk

citra dengan kualitas yang baik dan pada citra dengan kategori citra detil. Hal ini terlihat dari keacakan intensitas warna pada citra yang telah tersandikan. Selain itu karena matrik kunci yang digunakan ukurannya cukup besar mengakibatkan kriptanalisis akan membutuhkan waktu yang cukup lama untuk menemukan matrik kuncinya, karena terdapat 256! kemungkinan bentuk matrik kunci[3].

2. METODE PENELITIAN

Dalam penelitian ini, penulis menggunakan bentuk penelitian studi literature dan eksperimen murni. Penulis melakukan kajian yang berkaitan erat dengan permasalahan yang hendak dipecahkan serta mendefinisikan masalah dengan melakukan eksperimen. Selain itu penulis juga mencari referensi dan informasi yang diperlukan dari buku-buku dan artikel-artikel di Internet. Referensi dan informasi tersebut merupakan dasar pembuatan aplikasi oleh penulis. Metode penelitian yang digunakan oleh penulis adalah metode eksperimen, yaitu melakukan percobaan (ujicoba) serta manipulasi objek secara langsung, untuk mendapatkan hasil yang memuaskan.

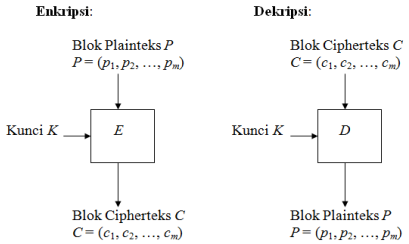
Metode pengumpulan data yang digunakan peneliti dalam melakukan pengumpulan data adalah studi dokumentasi, yaitu peneliti mengumpulkan serta mempelajari bahan-bahan tertulis yang berhubungan dengan penggunaan gabungan algoritma Playfair Cipher dengan Eletronic Code Book (EBC) yang didapat melalui artikel, buku, dan pencarian di internet terhadap materi metode Kriptografi algoritma Playfair Cipher dengan Eletronic Code Book (EBC).

Teknik pengumpulan data yang digunakan oleh penulis adalah *Study Literature* penulis mempelajari buku-buku, majalah, skripsi, jurnal, pencarian di Internet dengan sumber yang terpercaya serta referensi yang ada yang berhubungan dengan teori-teori kriptografi, algoritma Playfair Cipher dengan Eletronic Code Book (EBC) serta perancangan perangkat lunak[4]. Untuk melakukan pengujian perangkat lunak aplikasi kriptografi yang menggunakan algoritma gabungan Playfair Cipher dengan Eletronic Code Book (EBC), penulis menggunakan metode *black-box* dan proses formal *vertification.* Pengujian dilakukan terhadap fungsi-fungsi yang ada dengan menginput data masukan dan meneliti data hasil outputnya.

3. HASIL DAN PEMBAHASAN

Electronic Code Book (ECB) cipher merupakan salah satu dari kriptografi modern dengan menggunakan Block. Pada *cipher* blok, rangkaian bit-bit plainteks dibagi menjadi blok-blok bit dengan panjang sama, biasanya 64 bit (tapi adakalanya lebih). Algoritma enkripsi menghasilkan blok cipherteks yang – pada kebanyakan sistem kriptografi simetri – berukuran sama dengan blok plainteks.

Dengan blok *cipher*, blok plainteks yang sama akan dienkripsi menjadi blok cipherteks yang sama bila digunakan kunci yang sama pula. Ini berbeda dengan *cipher* aliran dimana bit-bit plainteks yang sama akan dienkripsi menjadi bit-bit cipherteks yang berbeda setiap kali dienkripsi.



Gambar 1. Skema enkripsi dan dekripsi pada *cipher* blok

Pada mode Electronic Code Book (ECB), setiap blok plainteks dienkripsi secara individual dan independen. Secara matematis, enkripsi dengan mode *ECB* dinyatakan sebagai

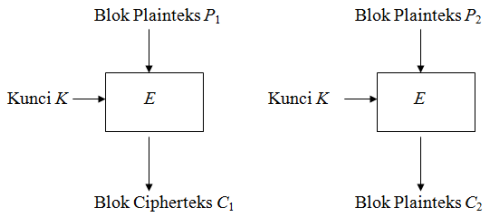
$$C_i = E_K(P_i)$$

dan dekripsi sebagai

$$P_i = D_K(C_i)$$

yang dalam hal ini, P_i dan C_i masing-masing blok plainteks dan cipherteks ke-i.

Gambar berikut memperlihatkan enkripsi dua buah blok plainteks, P_1 dan P_2 dengan mode *ECB*, yang dalam hal ini *E* menyatakan fungsi enkripsi yang melakukan enkripsi terhadap blok plainteks dengan menggunakan kunci *K*.

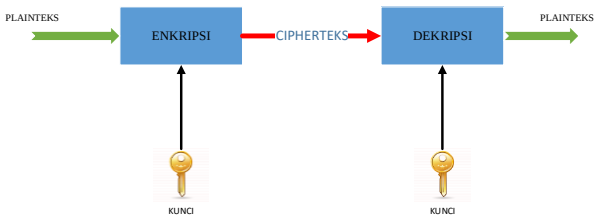


Gambar 2. Skema enkripsi dan dekripsi dengan mode *ECB*

Playfair cipher merupakan salah satu algoritma kriptografi klasik dengan metode substitusi, algoritma ini termasuk kedalam sistem kriptografi simetri yaitu algoritma yang memiliki kunci yang sama dalam melakukan enkripsi dan dekripsi. Hal itu dikarenakan pada waktu itu kriptografi kunci publik belum ditemukan[5].

Algoritma klasik pada dasarnya hanya terdiri dari cipher substitusi dan cipher transposisi. Cipher substitusi adalah proses penyandian dengan mensubstitusi karakter-karakter yang ada pada plaintext. Sedangkan cipher transposisi adalah proses mempertukarkan huruf-huruf yang ada dalam suatu string.

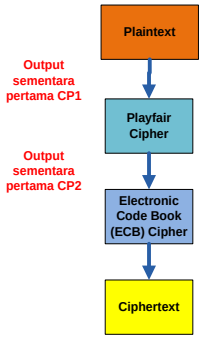
Berikut alur algoritma dari algoritma kriptografi kunci simetris, yang juga diterapkan pada algoritma kriptografi Playfair.



Gambar 3. Skema kriptografi *Playfair cipher*.Kunci enkripsi sama dengan Kuncidekripsi, yaitu K

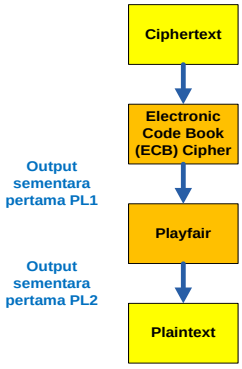
Dengan menggunakan Algoritma Playfair Cipher maka setelah diketahui dari analisa kelemahan algoritma Playfair Cipher yaitu mudah dipecahkan dengan metode ciphertext only attack dan dengan menggunakan Electronic Code Book (ECB) cipher untuk mengecoh

kriptanalis dalam memecahkan penyandian yang dilakukan dengan system penyandian klasik. Adapun metode enkripsi yang digunakan untuk memperkuat penyandian adalah :
Enkripsi Penggabungan Electronic Code Book (ECB) Cipher dan Playfair Cipher



Gambar 4. Proses Enkripsi Penggabungan Algoritma Playfair Cipher dan Electronic Code Book Cipher

Dekripsi Penggabungan Algoritma Algoritma Playfair Cipher dan Electronic Code Book (ECB) Cipher



Gambar 5. Proses Dekripsi Penggabungan Algoritma Playfair Cipher dan Electronic Code Book (ECB) Cipher

Penulis menggunakan informasi yang didapat dalam tahap diatas untuk menentukan banyaknya modul dan form yang akan digunakan dalam program tersebut. Jumlah komponen yang akan terdapat dalam setiap modul dan form akan ditentukan juga. Pada bagian ini, ditampilkan terdapat beberapa pembahasan mengenai tool-tool yang digunakan untuk membuat dan menjalankan kode sumber dari perangkat lunak yang akan dibuat dan implementasi, proses yang utama dalam coding tersebut serta rancangan tampilan aplikasi program yang akan dibuat. Aplikasi ini merupakan program prototype yang dirancang hanya untuk mengamankan pesan dengan Algoritma Playfair Cipher dan Electronic Code Book (ECB) Cipher. Aplikasi ini dirancang dan digunakan untuk membantu agar pesan tidak dapat dibaca oleh orang lain yang tidak diinginkan sehingga kerahasiaan pesan tetap terjaga. Rancangan aplikasi ini pada intinya merupakan suatu bentuk implementasi dari sistem pengamanan dengan menggunakan penyandian klasik Algoritma Playfair Cipher dan Electronic Code Book (ECB) Cipher.

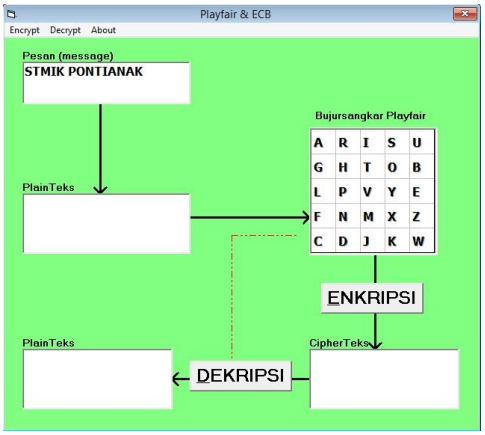
Perangkat lunak kriptografi gabungan Algoritma Playfair Cipher dan Electronic Code Book (ECB) Cipher dirancang dengan menggunakan bahasa pemrograman *Microsoft Visual Basic 6.0* dengan beberapa komponen standar seperti *Microsoft Flex Grid, Text Box, Picture Box, Label, Shape,* dan sebagainya[6]. Selain itu, penulis juga menggunakan aplikasi *Microsoft*

Visio untuk menggambarkan diagram proses pembentukan kunci, proses enkripsi dan proses dekripsi. Perangkat lunak Playfair Cipher dan EBC Cipher ini memiliki beberapa *form*.

Form Splash screen berfungsi sebagai form pembuka perangkat lunak. Pada Form ini terdapat sebuah progress bar yang menandakan aplikasi sedang diproses atau dijalankan. Gambar berikut merupakan desain form Splash screen dan gambar merupakan tampilan dari Splash Screen pada saat program dijalankan.

Gambar 6. Tampilan Form Splash Screen

Form Main berfungsi sebagai *form* utama perangkat lunak dan memiliki beberapa menu, yaitu : menu '*Encrypt'* untuk melakukan operasi *file* enkripsi, menu '*Decrypt*' untuk melakukan proses dekripsi maupun proses dekripsi yang dikerjakan dan menu '*About*' untuk menampilkan data pembuat perangkat lunak. Gambar 7 berikut merupakan desain form Main dan.



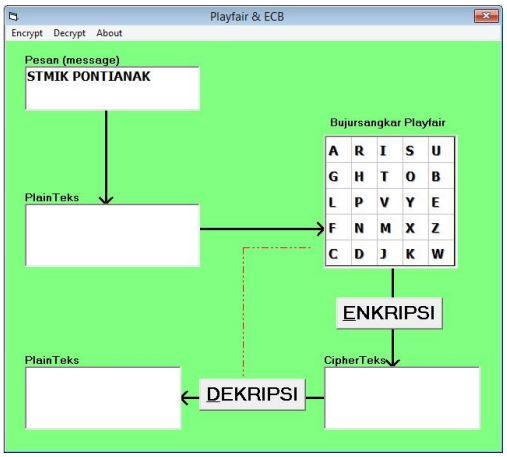
Gambar 7. Tampilan Form Main

Pada form About dirancang terdiri dari sebuah button yaitu tombol 'OK' untuk keluar dari *form*. Gambar 8 berikut merupakan desain form About.

Gambar 8. Tampilan Form About

Form dan modul yang sudah didefinisikan sebelumnya beserta komponennya disatukan untuk membentuk suatu program utuh. Hubungan antara modul dengan form juga didefinisikan oleh penulis.

Berikut ini adalah penjelasan dari proses Enkripsi Pesan, yang diimplementasikan pada rancangan aplikasi Algoritma Playfair Cipher dan Electronic Code Book (ECB) Cipher.

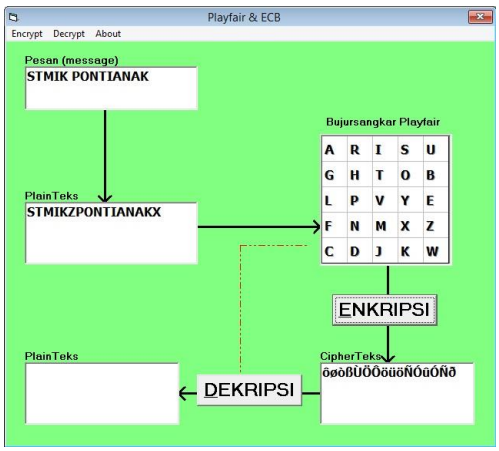


Gambar 9. Proses Input Pesan Plaintext dan Kunci

Dari gambar di atas dapat dilihat proses input pesan pada aplikasi penyandian adalah sebagai berikut : Input teks yang akan dienkripsi pada jendela Input Text, teks ini merupakan plaintext yang nantinya akan dienkripsi dan harus diisi dengan minimal 1 karakter, Input karakter kunci yang digunakan untuk mengenkripsi pesan, harus diisi minimal 1 karakter kunci
Tekan atau klik tombol encrypt untuk mengenkripsi pesan

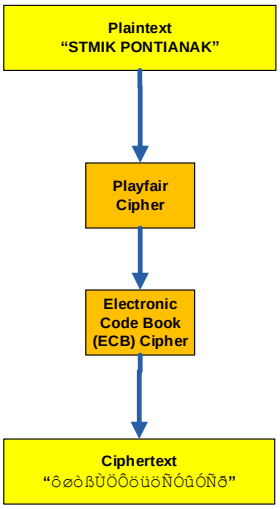
Sebagai contoh diatas :

Plaintext : `STMIK PONTIANAK`



Gambar 10. Hasil Enkripsi Pesan

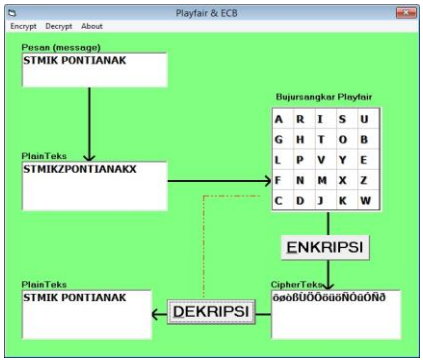
Gambar diatas merupakan hasil enkripsi pesan pada jendela Input Teks setelah ditekan tombol Encrypt dan dilakukan proses penyandian pesan. Pada "`STMIK PONTIANAK`" contoh diatas didapat hasil ekripsinya adalah Pada proses enkripsi pesan diatas dijalankan proses algoritma sebagai berikut :



Gambar 11. Proses Enkripsi Pesan

Berdasarkan proses diatas maka hasil dari enkripsi pesan yang diperoleh adalah: ôøòßÙÖÔöüöÑÓûÓÑð

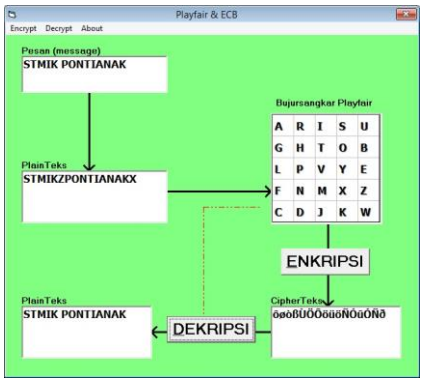
Berikut ini adalah penjelasan dari proses Dekripsi Pesan, yang diimplementasikan pada rancangan aplikasi penggabungan Algoritma Playfair Cipher dan Electronic Code Book (ECB) Cipher..



Gambar 12. Proses Input Pesan Ciphertext dan kunci

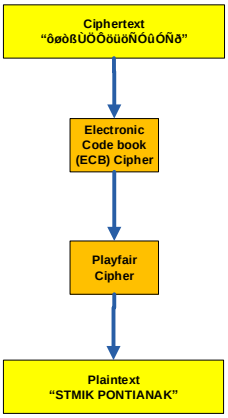
Dari gambar di atas dapat dilihat proses input pesan dekripsi pada aplikasi penyandian adalah sebagai berikut : Input teks yang akan didekripsi pada jendela Input Text, teks ini merupakan ciphertext yang nantinya akan didekripsi dan harus diisi dengan minimal 1 karakter Input karakter kunci yang digunakan untuk mendekripsi pesan, harus diisi minimal 1 karakter kunci Tekan atau klik tombol decrypt untuk mendekripsi pesan

Sebagai contoh diatas :



Gambar 13. Hasil Dekripsi Pesan

Gambar diatas merupakan hasil dekripsi pesan pada jendela Input Teks setelah ditekan tombol Decrypt dan dilakukan proses penyandian pesan. Pada contoh diatas dilakukan dekripsi pesan pada "ôøòßÙÖÔöüöÑÓûÓÑð". Pada proses dekripsi pesan diatas dijalankan proses algoritma sebagai berikut :



Gambar 14. Proses Dekripsi Pesan

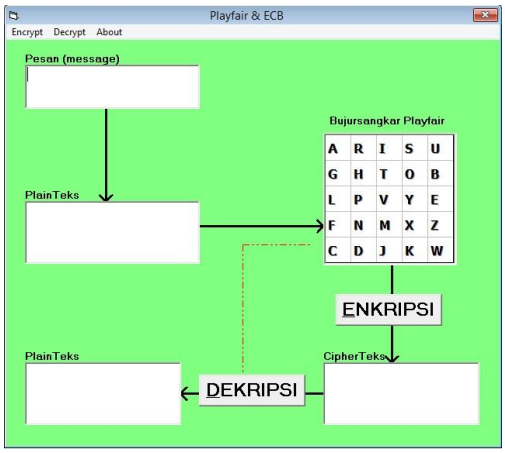
Berdasarkan proses diatas maka hasil dari dekripsi pesan yang merupakan plaintextnya adalah :

STMIK PONTIANAK

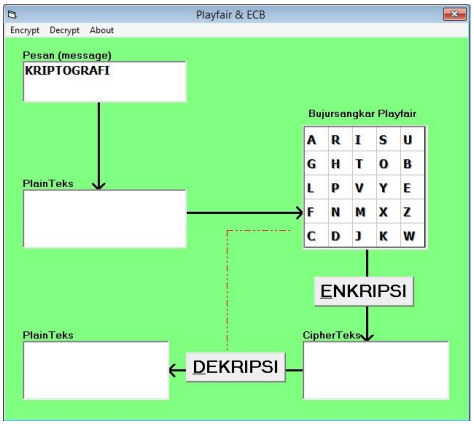
Penulis membangun aplikasi kriptografi Gabungan algoritma Playfair Cipher dan Electronic Code Book Cipher ini menggunakan program Visual Basic 6, dengan instrumen penelitian berupa *algoritma dan pseudocode.*

Setelah modul dirancang ke dalam program tersebut, penulis melakukan testing pada form yang membuat modul tersebut. Setelah setiap modul dan form terbentuk dan diuji, semua modul dan form tersebut kemudian disatukan dan dilakukan pengujian kembali akan integritasnya, termasuk didalamnya pengujian validitas input tiap form. Implementasi sistem dalam perangkat lunak pembelajaran ini mencakup spesifikasi kebutuhan perangkat keras (*hardware*) dan spesifikasi perangkat lunak (*software*).

Setelah aplikasi dijalankan akan muncul form awal (pembuka) berupa splash screen yang kemudiaan akan muncul tampilan *form* '*Main*'. *Form* '*Main*' memiliki menu - menu yang digunakan untuk memanggil *form* sesuai dengan fungsi perangkat lunak kriptografi gabungan Playfair Cipher dan Electronic Code Book (ECB) cipher.



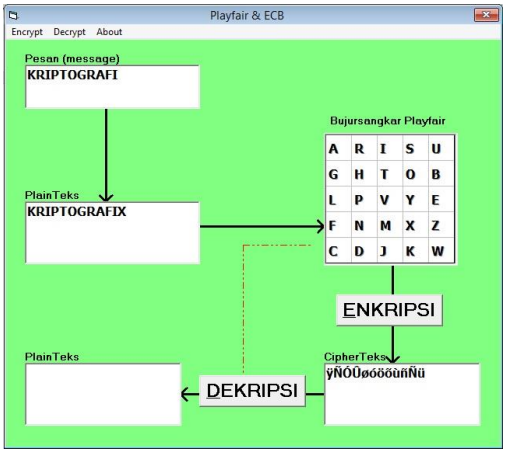
Gambar 15. Tampilan Awal



Gambar 16. Contoh Input Plaintext

Gambar diatas dilakukan pengujian terhadap file teks dengan nama file Coba.txt. Berikut Plainteksnya :

```
KRIPTOGRAFI
```

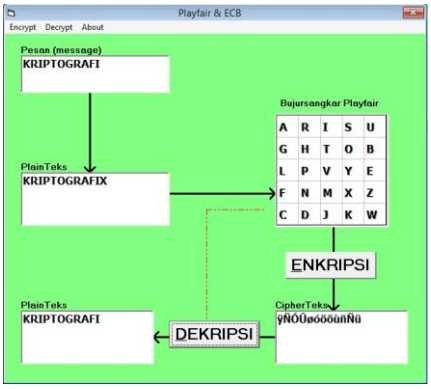


Gambar 17. Tampilan Hasil Proses Enkripsi

Setelah dilakukan Proses Enkripsi, maka didapatkan hasil Ciphertext sebagai berikut:

```
ÿÑÓÛøóõõùñÑü
```

Gambar berikut merupakan proses Dekripsi, tampak pada hasil proses Dekripsi didapatkan bahwa ciphertext yang didekrip akan menhasilkan plaintext kembali.



Gambar 18. Tampilan Hasil Proses Dekripsi

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 block.

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, misalnya dapat mengenkripsikan semua bentuk file yang dapat digunakan serta diterapkan pada bidang-bidang kehidupan yang lain yang lebih kompleks.

DAFTAR PUSTAKA

[1] Anindita Septiarini dan Hamdani (2011), *Sistem Kriptografi untuk Text Message Menggunakan Metode Affine*, Jurnal Informatika Mulawarman, Vol. 6 No.1 Februari 2011, pp 50-53.

[2] Ariyus, Dony, 2008, *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*, Andi, Yogyakarta.

[3] Suryadharma, Yoseph. 2006. *Studi Algoritma Cipher Blok Kunci Simentri Blowfish Cipher, Jurnal Informatika*.

[4] Sugiyono, 2010, *Metode Penelitian Kuantitatif Kualitatif dan R&D*, Alfhabeta, Bandung

[5] Munir, Rinaldi, 2006, *Kriptografi*, Infomedika Bandung, Bandung.

[6] Budiharto, Widodo, 2005, *Aplikasi Database Oracle 10g dengan VB6/Vb.NET*, PT Elex Media Komputindo, Jakarta.