ALGORITMA: Jurnal Ilmu Komputer dan Informatika
Volume: 05, Number: 01, April 2021 ISSN 2598-6341 (online)

Penerapan Algoritma Kriptografi Hybrid Subtitusi dan Transposisi Spiral Dalam Mengamankan Data Teks

Nurhanipa Siregar[1], Suriati[2], Ari Usman[3]
Program Studi Teknik Informatika Universitas Harapan Medan
Jl. HM Jhoni No70 Medan, Indonesia
Nh613893@gmail.com

ABSTRACT

Computer-based Data exchange generates one condition in which computers are interconnected with other computers in a computer network, but will also make the opportunity of threats to theft, wiretapping and falsification of data and information. Media communication as a means of sending data or information that crosses a public network such as the Internet or local networks is assumed to be accessible to anyone including people or parties who intend to steal, intercept or alter data. In this research to secure the text data is done using the hybrid cryptographic method by combining the substitution algorithm and transposition Spiral. The results of the study have been conducted that the hybrid algorithm of substitution and spiral transposition managed to secure data by inserting text data.

Keywords: data security, hybrid cryptography, substitution, spiral transposition

ABSTRAK

Pertukaran data berbasis komputer menghasilkan satu kondisi dimana komputer saling terkait dengan komputer lainnya dalam sebuah jaringan komputer, tetapi juga akan membuat peluang adanya ancaman terhadap pencurian, penyadapan dan pemalsuan data dan informasi. Media komunikasi sebagai alat pengiriman data atau informasi yang melintasi jaringan publik seperti internet ataupun jaringan lokal diasumsikan dapat diakses oleh siapapun termasuk orang-orang atau pihak-pihak yang memang berniat untuk mencuri, menyadap atau mengubah data. Pada penelitian ini untuk mengamankan data teks dilakukan menggunakan metode kriptografi hybrid dengan menggabungkan Algoritma Substitusi Dan Transposisi Spiral. Hasil penelitian yang telah dilakukan bahwa algoritma kriptografi hybrid substitusi dan transposisi spiral berhasil mengamankan data dengan menyisipkan data teks.

Kata kunci : pengamanan data,kriptografi hybrid, substitusi, transposisi spiral

1. PENDAHULUAN

Pertukaran data berbasis komputer menghasilkan satu kondisi dimana komputer saling terkait dengan komputer lainnya dalam sebuah jaringan komputer. Perkembangan teknologi jaringan komputer ini tidak hanya membuka banyak peluang dalam pengembangan aplikasi transmisi antar komputer, tetapi juga akan membuat peluang adanya ancaman terhadap pencurian, penyadapan dan pemalsuan data dan informasi. Media komunikasi sebagai alat pengiriman data atau informasi yang melintasi jaringan publik seperti internet ataupun jaringan lokal diasumsikan dapat diakses oleh siapapun termasuk orang-orang atau pihak-pihak yang memang berniat untuk mencuri, menyadap atau mengubah data. Data yang ditransmisikan melalui jaringan sebagai sarana umum harus terjamin keamanannya, apalagi untuk data atau informasi penting yang bersifat sangat rahasia dan seringkali menjadi target bagi para penyerang. Bentuk ancaman yang dilakukan oleh penyerang dapat berupa ancaman pasif (*passive attack*), yaitu dengan sengaja mengambil, membaca dan menampilkan data, dan ancaman aktif yaitu data yang harus terjamin keamanannya adalah data-data

rahasia, sehingga keamaan data tersebut perlu menjadi pertimbangan khusus bagi pembuat dan pengguna data tersebut

Pada penelitian ini akan menggunakan metode kriptografi *hybrid* dengan bentuk penyandian subtitusi dan transposisi spiral , Kriptografi *hybrid* adalah metode gabungan antara algoritma simetri dan algoritma asimetri, [1]. Metode penyandian substitusi adalah penyandian dengan cara mengganti huruf/karakter teks aslinya ke huruf/karakter lain sebagai teks sandinya, baik setiap satu huruf/karakter atau setiap kelompok huruf/karakter atau bisa juga kombinasi dari itu, [2]. Penyandian transposisi *spiral* dilakukan dengan cara menuliskan teks asli secara kolom dari atas kebawah dalam sebuah kisi-kisi imajiner dengan ukuran yang telah disepakati, [3].

Peneliti Sebelumnya [4] menjelaskan dengan judul "Pendekatan Kriptografi *Hybrid* pada Keamanan Dokumen Elektronik dan *Hypertext Transfer Protocol Secure* (HTTPS) (Analisis Potensi Implementasi Pada Sistem Keamanan)" dengan kesimpulan dari data hasil analisis dapat disimpulkan bahwa implementasi metode *hybrid* memiliki tingkat keamanan dan waktu komputasi yang lebih baik dibanding hanya menggunakan metode kriptografi simetris ataupun hanya kriptografi asimetris. Hasil implementasi menunjukkan tingkat kerahasiaan, keutuhan atau keotentikan, jaminan atas identitas dan keabsahan yang lebih baik, baik pada implementasi pada e-dokumen maupun pada *Hypertext TransferProtocol Secure* (HTTPS). Peneliti sebelumnya [5] menjelaskan dengan judul "Penyandian *File* Gambar dengan Metode Substitusi dan Transposisi" dengan kesimpulanTeknik penyandian dengan metode *substitusi* dan *transposisi* yang dilakukan oleh program pada gambar dalam format bitmap (BMP) dapat menghasilkan suatu gambar yang tak dapat dikenali lagi. Teknik penyandian dengan metode subtitusi dan transposisi yang diterapkan dalam mengakses langsung bit-bit dari citra tersebut berhasil memanipulasi posisi dan mengacak susunan *pixel* pada gambar. Gambar yang sudah memiliki susunan *pixel* teracak hasil penyandian dapat dikembalikan lagi oleh program ke dalam bentuk semula hingga dapat dikenali lagi. Ketika pengujian dilakukan dalam membandingkan gambar asli sebelum disandikan (*plaintext*) dengan gambar setelah disandikan (*ciphertext*) dan gambar hasil dari penerjemahan sandi (*plaintext*) tidak terdapat perbedaan dalam ukuran gambar.

Adapun tujuan peneliti ini adalah Mengimplementasikan pengamanan data teks menggunakan metode kriptografi *hybrid* dengan algoritma substitusi dan algoritma transposisi *spiral* sehingga dapat Memberikan keamanan tambahan bagi berkas-berkas atau dokumen yang disimpan secara digital.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi berasal dari kata kripto dan grafi. Kripto berarti menyembunyikan, dan grafi yaitu ilmu. Kriptografi *(cryptography)* adalah suatu ilmu yang mempelajari suatu sistem penyandian untuk menjamin kerahasiaan dan keamanan data. Orang yang melakukan disebut Criptographer. Kriptografi merupakan ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, dan integritas data serta autentifikasi data. Sistem kriptografi klasik umumnya menggunakan metode subtitusi atau transposisi dan telah digunakan jauh sebelum komputer ditemukan(Mujito, 2016).

2.2 Hybrid Cryptosystem

Hybrid cryptosystem adalah mengkombinasikan antara algoritma asimetris dengan algoritma simetris. Pada *hybrid cryptosystem* ini mendapat keuntungan dari algoritma asimetris dan algoritma simetris yaitu kelemahan dari tiap algoritma asimetris dan algoritma simetris akan saling menutupi.

2.3 Algoritma Kriptografi Subtitusi

Di dalam *cipher* substitusi setiap huruf pada teks (*plaintext*) digantikan dengan huruf lainyang memiliki selisih posisi tertentu dalam alfhabet. Pada *Caesar cipher*, tiap huruf disubtitusi dengan huruf ketiga berikutnya dari susunan alfabet yang sama (Haryanto 2015).

2.4 Algoritma Kriptografi Transposisi Spiral

Pada *cipher* transposisi, huruf-huruf di dalam plainteks tetap sama, hanya saja urutannya diubah. Nama lain untuk metode ini adalah permutasi atau pengacakan karena metode yang digunakan adalah dengan cara mempermutasikan karakter-karakter yang ada dalam suatu teks (Natsir, 2016).

2.5 Analisis Sistem

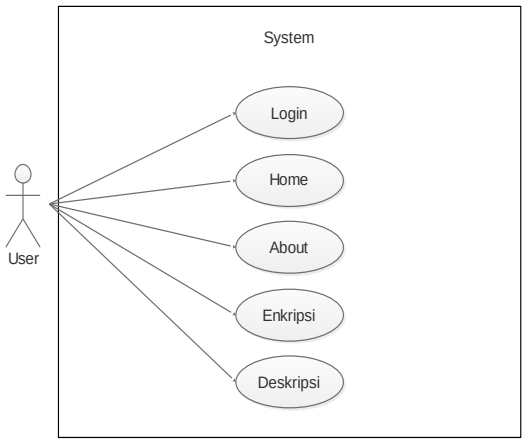
Analisis sistem adalah metode untuk menemukan kelemahan-kelemahan sistem guna memperoleh gambaran terhadap sistem yang akan dikembangkan sehingga dapat diusulkan perbaikannya. Tahapan dalam menganalisa sistem diawali dengan mempelajari bagaimana mengidentifikasi masalah-masalah yang dihadapi, mengidentifikasi pengguna (*user*) sistem serta spesifikasi perangkat lunak yang akan di kembangkan. Pada penelitian ini akan dikembangkan keamanan pada data teks menggunakan Algoritma Kriptografi *Hybrid* Substitusi Dan Transposisi Spiral.

2.6 Perancangan Sistem

Pada tahapan perancangan sistem ini akan di jelaskan tentang proses keamanan data teks atau dokumen, agar proses lebih mudah dimengerti dan jelas sesuai dengan standar *Unified Modern Language* (UML) yang akan dibuat sebuah perancangan dengan menggunakan *usecase*, *activity diagram*.

1. *Use Case Diagram*

Use Case Diagram menggambarkan aktifitas aktor di dalam proses sistem yang akan dirancang dan bagaimana bagian-bagian sistem tersebut diintegrasikan sehingga membentuk sistem yang dapat digunakan oleh pengguna. berikut ini perancangan *use case diagram* sistem yaitu :

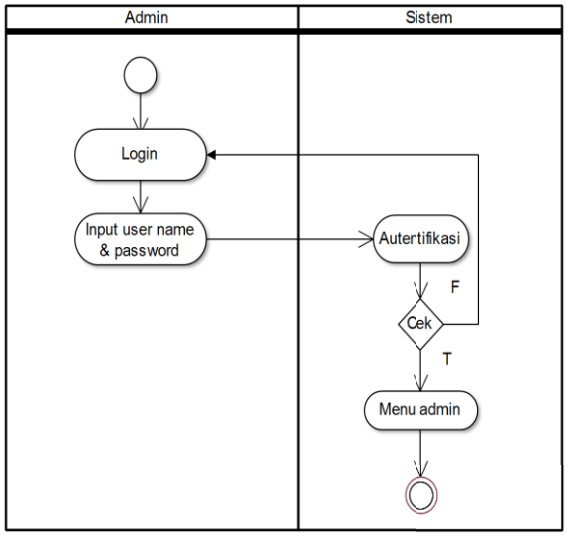


Gambar 1 *Use Case Diagram* sistem

Dalam *Use Case Diagram* diatas dijelaskan bahwa dalam menggunakan sistem keamanan data teks, pengguna sistem harus *login* terlebih dahulu kemudian pengguna dapat mengakses sistem yang sudah dibangun pada *usecase* diatas terdapat menu *home*, *about*, enkripsi dan dekripsi.

2. *Activity Diagram User Login* Sistem

Activity diagram *user login* merupakan aktivitas dari *user* atau pengguna ketika mau *login* atau masuk kedalam system. Gambar 2 desain *activity diagram user login* sistem sebagai berikut :

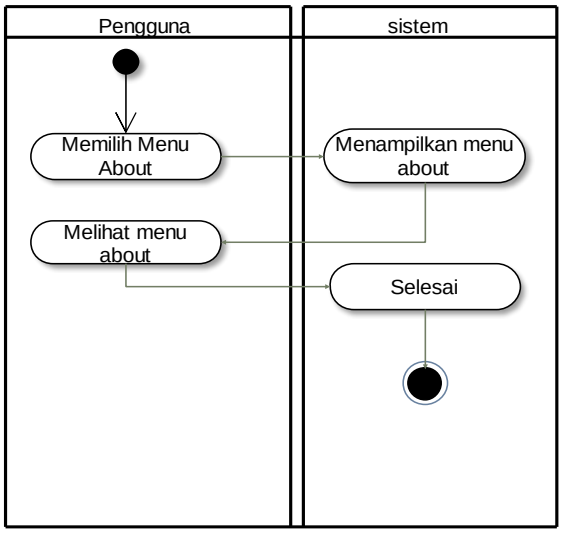


Gambar 2 *Activity Diagram Login User* Sistem

Berdasarkan gambar 2 *activity diagram login user* yang pertama yang harus dilakukan oleh *user* adalah masuk kehalaman *login* / halaman tampilan utama. Kemudian melakukan pengisian *username* dan *password* pada *form login*. Jika *username* dan *pasword* yang di masukan salah, Maka sistem akan menampilkan *form login* kembali dan melakukan pengisian *username* dan *password* lagi. Dan jika benar maka sistem akan menampilkan halaman menu utama dan selanjutnya *user* dapat mengakses menu-menu yang disediakan sistem sesuai *level* masing- masing.

3. *Activity Diagram* Menu *About*

Activity diagram menu *about* merupakan menu yang akan menampilkan informasi tentang aplikasi keamanan dokumen atau data teks. Gambar 3 *activity diagram* menu *about* :

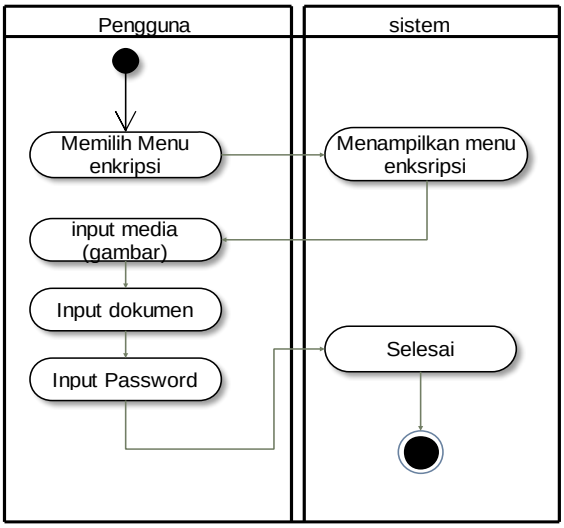


Gambar 3 *Activity Diagram* Menu *About*

Keterangan Gambar 3 *activity diagram* menu *about* terdiri dari pengguna dan sistem akan menampilkan informasi tentang sistem atau aplikasi.

4. *Activity Diagram* Menu Enkripsi

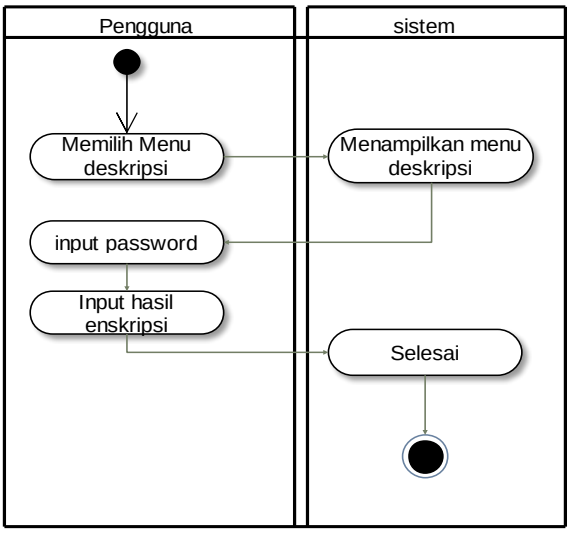
Activity diagram menu enkripsi merupakan menu yang akan menampilkan sebuah *form* input media gambar dan input *password* kemudian *form* input dokumen yang akan diberikan keamanan sehingga tidak secara terbuka ke publik. Gambar 4 *activity diagram* menu enkripsi :



Gambar 4 *Activity Diagram* Menu Enkripsi

5. *Activity Diagram* Menu Dekripsi

Activity diagram menu dekripsi merupakan menu yang akan menampilkan sebuah *form* input *password* kemudian *form* input hasil enkripsi yang akan membuka dokumen yang sudah di enkripsi sebelumnya. Gambar 5 *activity diagram* menu dekripsi :



Gambar 5 *Activity Diagram* Menu Dekripsi

3 HASIL DAN PEMBAHASAN

Setelah sistem dianalisis dan didesain secara rinci, maka akan menuju tahap implementasi. Implementasi meru pakan tahap meletakkan sistem sehingga siap untuk dioperasikan. Implementasi bertujuan untuk mengkonfirmasi modul-modul perancangan, sehinga pengguna dapat memberikan masukan kepada pembangun system.

3.1 Kebutuhan Perangkat Keras

Perangkat keras adalah sebuah komponen atau unsur peralatan yang digunakan untuk mengimplementasikan algoritma kriptografi *hybrid* subsititusi dan transpossi spiral dalam mengamankan data teks. Adapun perangkat keras yang digunakan secara optimal memerlukan spesifikasi minimum komputer sebagai berikut:

1. Processor core i3
2. Kapasitas RAM 4 GB

3. Monitor VGA beresolusi 1024 x 768
4. Keyboard dan Mouse

Secara keseluruhan spesifikasi perangkat keras komputer yang ada sudah memenuhi syarat kebutuhan perangkat lunak yang akan diaplikasikan.

3.2 Analisis Perangkat lunak komputer

Perangkat lunak adalah beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya. Secara luas perangkat lunak dapat diartikan sebagai suaru produser pengoprasian. Adapun perangkat lunak yang digunakan pada algoritma kriptografi *hybrid* subsititusi dan transpossi spiral dalam mengamankan data teks secara optimal memerlukan spesifikasi minimum komputer sebagai berikut:

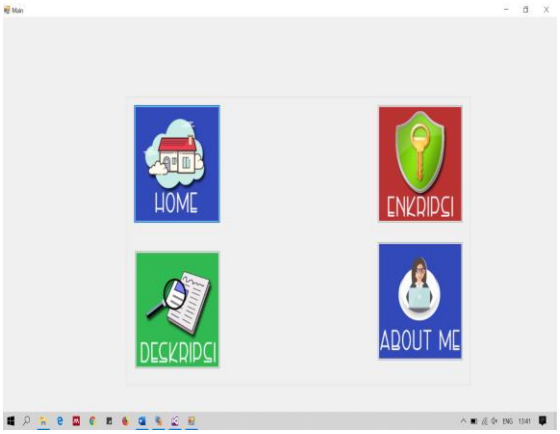
1. Windows 10 64 bit
2. Notepad ++
3. Visual Basic
4. Mysql connector

3.3 Tampilan Sistem *User*

Pada tampilan sistem *user* yang berfungsi sebagai sistem yang digunakan oleh *user* untuk melihat penerapan algoritma kriptografi *hybrid* subsititusi dan transpossi spiral dalam mengamankan data teks. Pada sistem ini berfungsi sebagai media yang dapat digunakan untuk mengamankan data teks dengan algoritma kriptografi *hybrid* subsititusi dan transpossi spiral. Berikut ini adalah tampilan yang dapat dilihat sebagai berikut.

a. Tampilan Menu Utama User

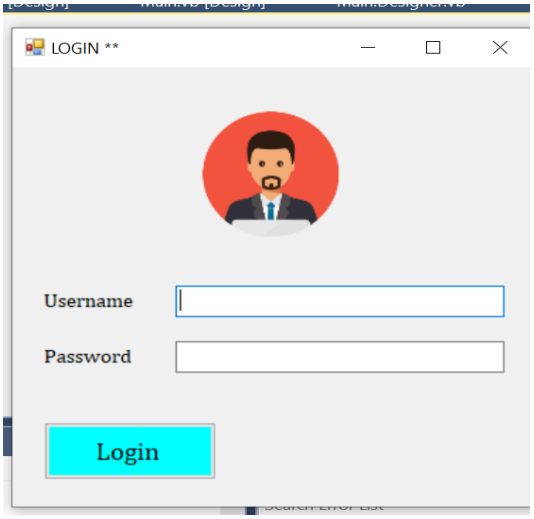
Pada menu utama user akan menampilkan *form* dalam melakukan cara untuk pengamanan terhadap data teks.



Gambar 6 Tampilan Menu Utama *User*

b. Tampilan Menu *Login* Admin

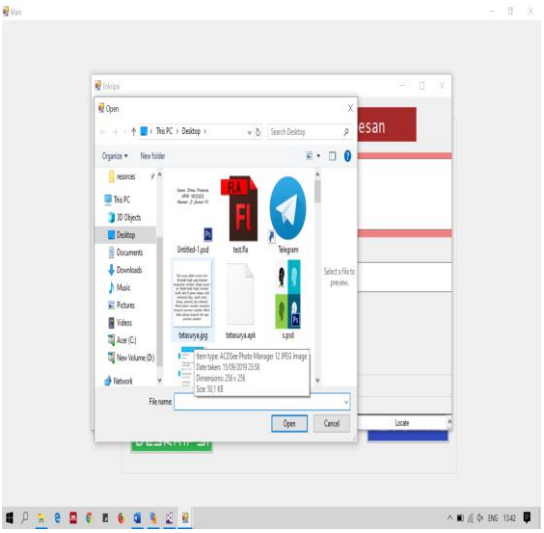
Pada menu *Login user* pada sistem terdapat *form username* dan *password*, *username* ialah id pengguna yang sudah terdaftar didalam database, *username* juga merupakan identitas yang tidak ada duanya dalam sebuah aplikasi jika sudah mengguna *id* tertentu saat mendaftar pada sebuah aplikasi maka orang lain tidak dapat mendaftar dengan *id* yang sama.



Gambar 7 Tampilan Menu *Login* Admin

c. Tampilan Membuka Media Dokumen

Tampilan membuka media dokumen sebagai wadah dalam melakukan penyisipan pesan didalam media dokumen, system akan menyediakan button pilih *file* kemudian user dapat memlih jenis dokumen sesuai dengan keinginan atau kebutuhan sistem.



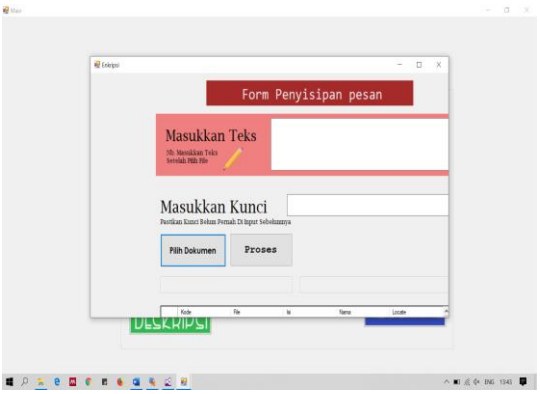
Gambar 8 Tampilan Membuka Dokumen

Keterangan Gambar 8 sebagai berikut:

1. Terdapat menu *browse* dokumen yang diinginkan oleh pengguna
2. Setelah dokumen dipilih pengguna dapat melakukan *open* dokumen sehingga dokumen dapat masuk kedalam sistem

d. Tampilan Penyisipan Pesan

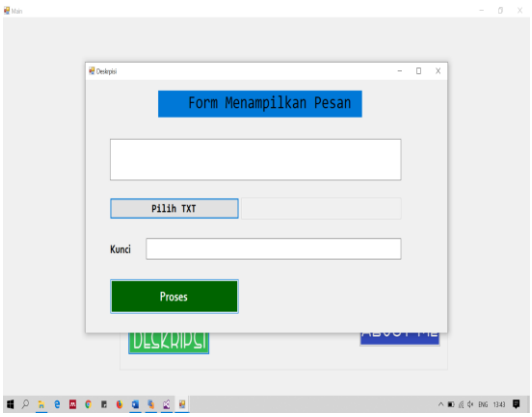
Tampilan menu penyisipan pesan merupakan menu yang digunakan untuk melakukan penyisipan pesan didalam media dokumen, pengguna tinggal memasukan pesan apa yang ingin disisipkan didalam media dokumen.



Gambar 9 Tampilan Menu Penyisipan Pesan

e. Tampilan Menu Menampilkan Pesan

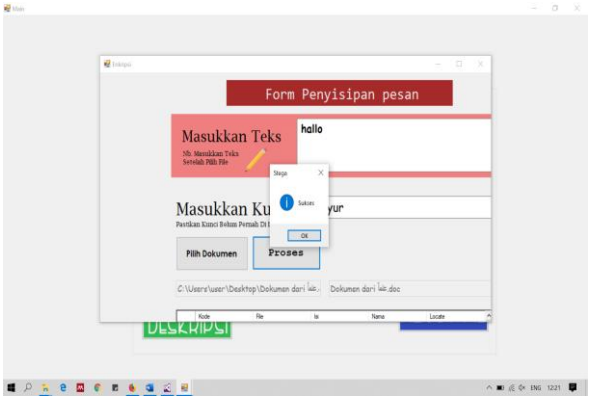
Pada sistem menu menampilkan pesan akan ditampilkan form menampilkan pesan dengan mengisi kunci pesan tersebut.



Gambar 10 Tampilan Menu Menampilkan Pesan

f. Tampilan Penyisipan Pesan Berhasil

Tampilan menu menyisipkan pesan sukses berfungsi menyisipkan isi pesan yang akan ditampilkan oleh *system* sesuai dengan media dokumen yang digunakan.

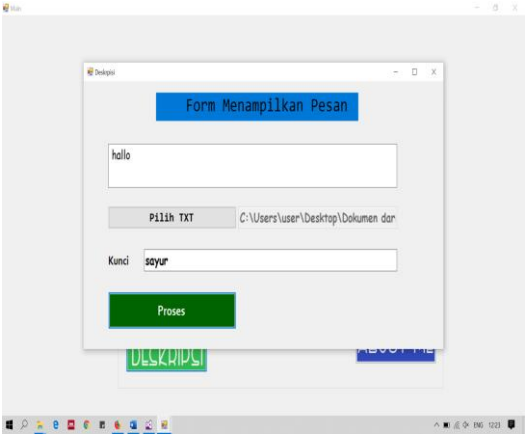


Gambar 11 Tampilan Penyisipan Pesan Berhasil

Keterangan Gambar 11 akan menjelaskan bahwa pada tampilan penyisipan pesan sukses berfungsi memberitahukan kepada pengguna bahwa pesan yang telah berhasil disisipkan pada sistem keamanan dokumen.

g. Tampilan Menampilkan Pesan Berhasil

Tampilan menu menampilkan pesan sukses berfungsi menampilkan isi pesan yang akan ditampilkan oleh *system* sesuai dengan media dokumen yang digunakan

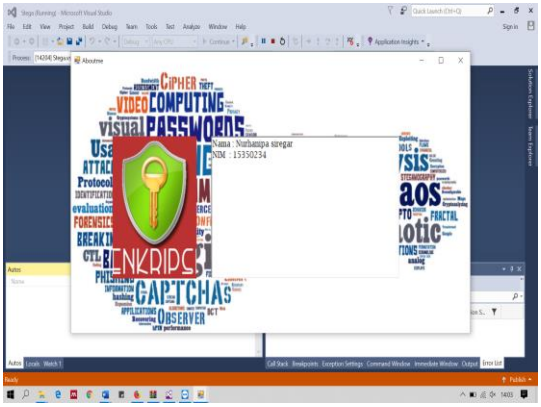


Gambar 12 Tampilan Menampilkan Pesan Berhasil

Keterangan Gambar 12 akan menjelaskan bahwa pada tampilan menampilkan pesan sukses berfungsi memberitahukan kepada pengguna bawa pesan yang telah berhasil dilakukan deskripsi.

h. Tampilan Menu *About*

Tampilan menu *about* merupakan tampilan informasi dari pengembang aplikasi penyisipan pesan.



Gambar 13 Menu *About*

4. PENUTUP

4.1 Kesimpulan

Dalam uraian rangkaian mulai dari proses Penerapan Algoritma Kriptografi *Hybrid* Substitusi Dan Transposisi Spiral Dalam Mengamankan Data Teks yang menggunakan bahasa pemograman visual basic, dapat ditarik beberapa kesimpulan penting antara lain:

1. Metode hybrid memiliki tingkat keamanan dan waktu komputasi yang lebih baik disbanding hanya menggunakan metode kriptografi simetri ataupun hanya kriptografi asimetri.
2. Menghasilkan sebuah program yang dapat melakukan pengamanan data teks menggunakan metode kriptografi *hybrid* dengan menggabungkan algoritma substitusi dan algoritma transposisi *spiral*.
3. Pada program atau aplikasi untuk mengamankan data teks telah dilakukan pengujian dimenu enkripsi dan dekripsi ketika teks dan kunci dimasukan kemudian pilih txt maka aplikasinya dapat diperoleh atau berhasil.

4.2 Saran

Dari Penelitian yang telah penulis lakukan tentunya tidak akan terlepas dari kekurangan, oleh karena itu perlu adanya perbaikan dan pengembangan sistem lebih lanjut kedepannya, maka diperlukan dan harus diperhatikan beberapa, diantaranya:

1. Dalam tahap pengembangan selanjutnya, disarankan bagi siapa saja yang akan meneruskan Penerapan Algoritma Kriptografi *Hybrid* Substitusi Dan Transposisi Spiral Dalam Mengamankan Data Teks yang menggunakan bahasa pemograman *visual basic* ini dapat menambahkan fasilitas- fasilitas seperti dapat mengamankan *file* teks lewat media gambar.
2. Perlu adanya pengembangan yang lebih baik lagi seperti aplikasi dapat dikombinasikan dengan algoritma kriptografi yang lain dengan mengikuti perkembangan ilmu keamanan data.

DAFTAR PUSTAKA

[1.] Sihombing (2017), *Graca Lamudur Arta*. *Hybrid Cryptography Stream Cipher and RSA Algoritma with Digital Signature As a Key*. InfoTekjar (Jurnal Nasional Informatika dan Teknologi Jaringan) Vol 1, No 2 Hal. 75-83.

[2.] Haryanto, T, M Apriani, and T Sefyanto. "*Peran Algoritma Caesar Cipher dalam Membangun Karakter Akan Kesadaran Keamanan Informasi*". Yogyakarta, November 2012

[3.] Natsir, M. (2016). *Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java. Jurnal Sistem Informasi (JSI)*, *6*(2), 87–105.

[4.] Basri. (2015). *Pendekatan Kriptografi Hybrid Pada Keamanan Dokumen Elektronik dan Hypertext Transfer Protocol Seruce (HTTPS*) (Analisis Potensi Implementasi pada Sistem Keamanan). No.2 . 2442-4512.

[5.] Adi Supriyanto,. Eka Ardhianto. (2015). *Penyandian File Gambar Dengan Metode Subtitusi dan Transposisi*. *Teknologi Informasi Dinamik*. XIII. No.2. 0854-9524.