PENERAPAN ALGORITMA DATA ENCRYPTION STANDARD PADA PERANCANGAN APLIKASI KRIPTOGRAFI BERBASIS WEB PADA CYBER DEFENCE

Tony Darmanto[1], Riyadi J. Iskandar[2], Soebandi[3]
[1,3] Program Studi Sistem Informasi STMIK Widya Dharma Pontianak
[2] Program Studi Teknik Informatika STMIK Widya Dharma Pontianak
e-mail : [1]tony.darmanto@yahoo.com, [2]riyadijiskandar@gmail.com, [3]soebandi@gmail.com

Abstract

In this era of globalization, many organizations or users who use the internet as a medium of communication or as a tool for sending messages. In the development of many emerging parties intercepting confidential data that is being transmitted or stored confidential data. Currently the security of the data stored in the computer and the data is being transmitted has become an absolute requirement in the Cyber Defence. It is strongly associated with the importance of these data for those interested. If data have been intercepted by unauthorized parties, it can be detrimental. The method used in this research is to study the literature related to the problems. Moreover, the authors use the Unified Modeling Language (UML) to help in the design and use Dreamweaver 8.0 and MySQL in making applications. This research is an application that can be used to secure documents will be stored or shipped. The data used in the encryption process is a .txt file type or user can write its own data to be used in the encryption process. The results of encryption and decryption process will be stored in a .txt file type that will be directly stored in a computer storage medium. The key used in the encryption process, consisting of 8 characters in the process will produce 16 internal key. Plaintext cryptographic process will process up to 8 characters, which will be played 16 times. The conclusion that can be derived from this study are certain parties can be assisted in the process of securing the document. With this application, some may encode documents to be stored or to be sent. Researchers expect further development so that more help those in need. DES algorithm can be replaced by using a 56-bit computing a triple DES algorithm with a key length of 128-bits.

Keywords: Cyber, Defence, DES algorithm, Encryption, Decryption

Abstrak

Pada era globalisasi ini banyak organisasi atau *user* yang menggunakan internet sebagai media dalam berkomunikasi atau sebagai alat untuk mengirimkan pesan. Dalam perkembangannya banyak bermunculan pihak-pihak yang menyadap data rahasia yang sedang dikirim atau data rahasia yang tersimpan. Saat ini keamanan terhadap data yang disimpan dalam komputer maupun data yang sedang dikirim sudah menjadi persyaratan mutlak dalam Cyber Defence. Hal tersebut sangat terkait dengan pentingnya data tersebut bagi orang-orang yang berkepentingan. Apabila data telah disadap oleh pihak yang tidak berkepentingan, maka dapat merugikan. Metode yang digunakan peneliti dalam penelitian ini adalah dengan cara mempelajari literatur-literatur yang berhubungan dengan permasalahan. Selain itu peneliti menggunakan *Unified Modeling Language* (UML) dalam membantu perancangan dan menggunakan *Dreamweaver* 8.0 dan *MYSQL* dalam pembuatan aplikasi. Penelitian ini sebuah aplikasi yang dapat digunakan mengamankan dokumen-dokumen yang akan disimpan atau dikirim. Data yang digunakan dalam proses kriptografi adalah file bertipe .txt atau user dapat menuliskan sendiri data yang akan digunakan dalam proses enkripsi. Hasil dari proses enkripsi dan dekripsi akan disimpan dalam file bertipe .txt yang akan langsung disimpan dalam media penyimpanan di komputer. Kunci yang digunakan dalam proses kriptografi terdiri dari 8 karakter yang dalam prosesnya akan menghasilkan 16 kunci internal. Proses kriptografi akan memproses *plaintext* sepanjang 8 karakter, yang akan diputar sebanyak 16 kali. Kesimpulan yang dapat diperoleh dari penelitian ini adalah pihak-pihak tertentu dapat terbantu dalam proses pengamanan dokumen. Dengan adanya aplikasi ini, sebagian pihak dapat menyandikan dokumen yang akan disimpan atau yang akan dikirim. Peneliti mengharapkan pengembangan lebih lanjut sehingga lebih membantu pihak yang membutuhkan. Algoritma DES dapat diganti dengan menggunakan kunci 56-bit menjadi algoritma TRIPEL DES dengan panjang kunci 128-bit.

Kata kunci : Cyber, Defence, Algoritma DES, Enkripsi, Dekripsi

1. PENDAHULUAN

Pada era globalisasi ini banyak organisasi atau *user* yang menggunakan internet sebagai media dalam berkomunikasi atau sebagai alat untuk mengirimkan pesan. Dalam perkembangannya banyak bermunculan pihak-pihak yang menyadap data rahasia yang sedang dikirim atau data rahasia yang tersimpan. Saat ini keamanan terhadap data yang disimpan dalam komputer maupun data yang sedang dikirim sudah menjadi persyaratan mutlak dalam Cyber Defence. Hal tersebut sangat terkait dengan pentingnya data tersebut bagi orang-orang yang berkepentingan. Apabila data telah disadap oleh pihak yang tidak berkepentingan, maka dapat merugikan. Kerahasiaan data harus diterapkan untuk menjaga informasi dari setiap pihak yang tidak berwenang. Dengan demikian informasi hanya akan dapat diakses oleh pihak-pihak yang berhak saja dan tidak dapat diketahui oleh pihak-pihak yang tidak memiliki hak untuk mengakses berkas tersebut. Salah satu cara yang digunakan untuk menjamin keamanan dari infrastruktur teknologi adalah dengan menjamin keamanan komunikasi. Komunikasi yang aman dimaksudkan untuk melindungi data ataupun informasi ketika dikirimkan atau ditransmisikan kepada pihak lain, sehingga data atau informasi yang ditransmisikan itu tidak dapat disadap, dimanipulasi ataupun dirusak oleh pihak-pihak yang tidak bertanggung jawab. Salah satu cara untuk mengamankan komunikasi adalah dengan menerapkan teknik penyandian /kriptografi. Kriptografi merupakan teknik penyembunyian informasi rahasia, biasanya berupa teknik matematis, koding, maupun cara lainnya dengan tujuan agar pesan yang disimpan dan ditransmisikan hanya dapat diketahui oleh pihak yang berkepentingan saja. Dalam melakukan proses enkripsi banyak pengguna yang menggunakan aplikasi *desktop* dalam mengenkripsi maupun mendekripsi data penting yang tidak ingin diketahui orang lain. Akan tetapi tidak semua orang memiliki aplikasi kriptografi untuk mengenkripsi data yang ingin dirahasiakan maupun digunakan untuk mendekripsikan data yang telah dienkripsi agar dapat dibaca kembali. Menyadari hal tersebut, peneliti melakukan penelitian untuk merancang website yang berfungsi untuk mengenkripsi serta mendekripsi data untuk menjaga keamanan data. Dengan menggunakan website sebagai media enkripsi dan dekripsi, maka pihak-pihak yang ingin mengenkripsi data tidak perlu mencari aplikasi *desktop* yang khusus digunakan untuk proses enkripsi. Dengan memciptakan suatu aplikasi kriptografi berbasis *web*, semua pengguna internet dapat menggunakan fasilitas enkripsi dan dekripsi.

2. METODE PENELITIAN

Bentuk penelitian dan teknik pengumpulan data yang digunakan adalah:

2.1 Rancangan Penelitian

Dalam penyusunan penelitian ini, peneliti melakukan percobaan dan pengujian terhadap aplikasi kriptografi berbasis *web* dengan menggunakan algoritma DES yang dibuat dan dengan cara mempelajari literatur-literatur yang berhubungan dengan materi-materi yang berhubungan.

2.2 Teknik Analisis Data

Teknik analisi sistem yang digunakan peneliti dalam menganalisis penelitian ini adalah *Unified Modeling Language* (UML).

2.3 Teknik Perancangan Sistem

Teknik perancangan sistem yang digunakan peneliti dalam penelitian dengan menggunakan bahasa pemrograman *Dreamweaver* 8.0 dan menggunakan *MYSQL* sebagai *database*.

2.4 Landasan Teori

2.4.1 Informasi

Informasi merupakan fakta-fakta atau data yang telah diubah menjadi konteks yang berarti dan berguna bagi pengguna tertentu. *Information, on the other hand, is facts or conclusions that have meaning within a context*. (Informasi, di sisi lain, adalah fakta atau kesimpulan yang memiliki arti dalam konteks).[1] Selain itu "*Information as data that have been converted into a meaningful and useful context for spesific end user*." (informasi sebagai data yang telah diubah menjadi konteks yang bermakna dan berguna bagi pengguna akhir yang spesifik). [2]

2.4.2 Perancangan Perangkat Lunak

Perancangan perangkat lunak adalah praktek penentuan spesifikasi sehingga menghasilkan gambaran struktur perangkat lunak yang akan diimplementasikan, model dan struktur data yang digunakan oleh sistem, antarmuka antarkomponen atau algoritma-algoritma yang digunakan seperti yang diungkapkan oleh Sommerville[3] yang menyatakan "*A software design is a description of the structure of the software to be implemented, the data models and structures used by the system, the interfaces between system components and, sometimes, the algorithms used*." (Sebuah desain perangkat lunak adalah depenelitian dari struktur perangkat lunak untuk diterapkan, model data dan struktur yang digunakan oleh sistem, antarmuka antarkomponen sistem dan, kadang-kadang, algoritma yang digunakan). Sedangkan menurut beberapa pakar "*Software Design is the*

practice of taking a specification of externally observable behavior and adding details needed for actual computer system implementation, including human interaction, task management, and data management details." (Desain Perangkat Lunak adalah praktek mengambil spesifikasi perilaku yang dapat diamati secara eksternal dan menambahkan detail yang diperlukan untuk implementasi sistem komputer yang sebenarnya, termasuk interaksi manusia, manajemen tugas, dan rincian pengelolaan data) [4].

2.3 Pengujian Perangkat Lunak

Pengujian perangkat lunak merupakan seperangkat kegiatan yang ditujukan untuk menunjukkan fungsi perangkat lunak bekerja sesuai dengan persyaratan spesifikasi perangkat lunak dan menemukan cacat sebelum program tersebut digunakan. "*Testing is a set of activities that can be planned in advance and conducted systematically*." (Pengujian adalah seperangkat kegiatan yang dapat direncanakan terlebih dahulu dan dilakukan secara sistematis) [5]. Pengujian ditujukan untuk menunjukkan bahwa sebuah program melakukan apa yang memang program tersebut dimaksudkan dan menemukan cacat sebelum program tersebut digunakan[6], selain itu pengujian perangkat lunak menunjukkan fungsi perangkat lunak bekerja sesuai dengan persyaratan spesifikasi perangkat lunak berkaitan dengan fungsi, fitur, fasilitas dan kinerja [5].

2.4 Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi[7]. Selain itu "*Cryptograpy is the science of keeping secrets secret*." (Kriptografi adalah ilmu menjaga rahasia tetap rahasia) [3]. Tugas mendasar dan klasik dari kriptografi adalah menyediakan kerahasiaan dengan metode enkripsi [3]. Sebuah enkripsi adalah sebuah pemetaan plainteks menjadi cipherteks berdasarkan pada beberapa teks kunci terpilih [8]. Enkripsi adalah proses tranformasi plainteks menjadi cipherteks[9].

2.5 Manajemen Kunci

Tujuan manajemen kunci adalah menjaga keamanan dan integritas kunci pada semua fase di dalam daur hidupnya[7]. Daur hidup kunci, dimulai dari pembangkitan kunci (*key generation*), pendistribusian kunci (*key distribution*), penyimpanan kunci (*key storage*), sampai akhirnya penghancuran kunci (*key destruction*) [10]. Masalah yang muncul dalam pembangkitan kunci adalah bagaimana membuat kunci yang tidak dapat diprediksi. Untuk mengatasi masalah ini dapat digunakan pembangkit bilangan acak yang aman untuk kriptografi untuk membangkitkan kunci. Penyebaran kunci tidak dibutuhkan bila kunci digunakan untuk melindungi informasi yang tersimpan dalam penyimpanan. Dalam hal penyimpanan kunci, kunci sebaiknya disimpan tidak dalam bentuk jelas. Untuk itu, kunci dapat dipecah menjadi beberapa komponan. Jika kunci akan digunakan, setiap komponen direkonstruksi kembali[7]. Untuk menyimpan kunci secara tersebar dapat digunakan skema pembagian rahasia [10]. Secara umum pengelolaan kunci merupakan hal yang sangat penting disamping pemilihan algoritma enkripsi yang baik. Penggunaan algoritma enkripsi yang baik akan menjadi sia-sia bila kunci hilang, dapat ditebak atau dicuri. Oleh karena itu dibutuhkan suatu mekanisme dalam proses pembangkitan dan penyimpanan kunci.

2.6 Data Encryption Standart

Data Encryption *Standart* adalah algoritma *cipher blok* yang populer karena dijadikan standart algoritma enkripsi kunci simetris [11], sedangkan pendapat lain menyatakan algoritma DES merupakan salah satu proposal yang terbaik pada tahun 1977, tidak ada kritik yang datang dari kelangan ilmuan tentang pangjang kunci yang digunakan dan S-*box* yang merupakan bagian internal dari DES. DES dikatakan enkripsi blok karena pemrosesan data baik enkripsi maupun dekripsi, diimplementasikan per blok (dalam hal ini 8 byte). Proses pada algoritma DES terbilang panjang, bahkan jauh lebih panjang dari pada Elgamal, tapi pada implementasinya ternyata proses komputasinya dapat berjalan lebih cepat. Mengapa demikian? karena pada DES tidak ada operasi aritmatika yang berjalan seperti halnya pada Elgamal. Proses yang berjalan pada DES hanya sebatas pergeseran bit-bit pada tiap blok enkripsi/dekripsi. DES (*Data Encrytion Standard*) mengenkripsi *plaintext* sebesar 64 bit (8 byte) dengan panjang unci sekitar 56 bit (7 byte), sebanyak 16 putaran. Data 64 bit akan disubtitusi terlebih dahulu dengan permutasi IP (*initial permutation*). IP digunakan sebelum putaran pertama dari 16 putaran, dan mensubtitusi blok *input* dengan ketentuan sebagai berikut:

IP = 58, 50, 42, 34, 26, 18, 10, 2,
60, 52, 44, 36, 28, 20, 12, 4,
62, 54, 46, 38, 30, 22, 14, 6,
64, 56, 48, 40, 32, 24, 16, 9,
57, 49, 41, 33, 25, 17, 9, 1,
59, 51, 43, 35, 27, 19, 11, 3,
61, 53, 45, 37, 29, 21, 13, 5,
63, 55, 47, 39, 31, 23, 15, 7.

Sebagian contoh IP akan memindahkan bit ke-58 dari *plaintext* menjadi bit ke-1, bit ke-50 menjadi bit-2, bit ke-43 menjadi bit ke-3, dan seterusnya. IP dan *invers* IP tidak mempengaruhi keamanan dari DES. Tujuan utamanya yaitu hanya untuk memudahkan dalam memanggil data *plaintext* atau data *ciphertext* ke dalam chip

DES yang berbentuk potongan-potongan byte dalam program komputer. *Plaintext* yang telah disubtitusi akan dipecah menjadi dua bagian sebesar 32 bit kiri (L) dan 32 bit kanan (R). Pada setiap putaranya data kiri akan menjadi data kanan data kanan akan dilakukan operasi data kiri di-XOR-kan dengan fungsi f.

Li = Ri–1

Ri = Li-1 XOR f(Ri-1,Ki)

Kemudian dilanjutkan dengan melakukan subtitusi *invers* IP (IPinv). IPinv merupakan *invers* dari IP dan digambarkan dengan ketentuan sebagai berikut:

IPinv = 40, 8, 48, 16, 56, 24, 64, 32,
39, 7, 47, 15, 55, 23, 63, 31,
38, 6, 46, 14, 54, 22, 62, 30,
37, 5, 45, 13, 53, 21, 61, 29,
36, 4, 44, 12, 52, 20, 60, 28,
35, 3, 43, 11, 51, 19, 59, 27,
34, 2, 42, 10, 50, 18, 58, 26,
33, 1, 41, 9, 49, 17, 57, 25.

dalam putaran terakhirnya, blok R_{16} L_{16} tidak terjadi pertukaran tetapi blok ini menjadi *input* untuk IPinv.

Untuk fungsi f, data sebelah kanan sebesar 32 bit akan dipermutasi dengan *expansion permutation* (E) sehingga akan menghasilkan *ciphertext* sebesar 48 bit, kemudian dilakukan operasi XOR dengan blok kunci dan di-*input*-kan ke dalam *sbox*. *Sbox* terdiri atas 8 buah. Hasilnya akan disubtitusi dengan P-*Box permutation* (P) sekaligus membentuk data menjadi 32 bit lagi. Berikut isi dari E dan P:

E = 32, 1, 2, 3, 4, 5, 4, 5,
6, 7, 8, 9, 8, 9, 10, 11,
12, 13, 12, 13, 14, 15, 16, 17,
16, 17, 18, 19, 20, 21, 20, 21,
22, 23, 24, 25, 24, 25, 26, 27,
28, 29, 28, 29, 30, 31, 32, 1.

P = 16, 7, 20, 21, 29, 12, 28, 17,
1, 15, 23, 26, 5, 18, 31, 10,
2, 8, 24, 14, 32, 27, 3, 9,
19, 13, 30, 6, 22, 11, 4, 25.

Untuk proses depenelitiannya, operasinya akan dibalik dengan operasi enkripsi yaitu:

Ri-1 = Li

Li-1 = Ri XOR f(Li, Ki)

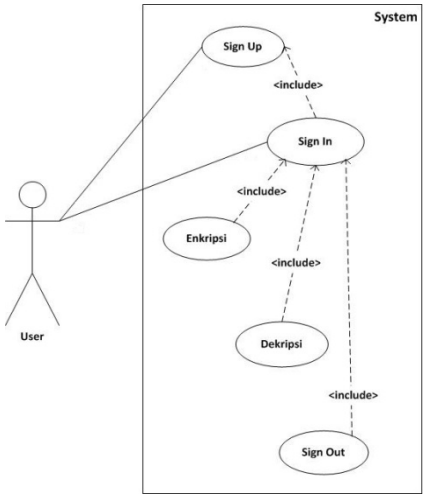
dengan urutan kunci terbalik yaitu dimulai dari blok kunci yang terakhir.

3. HASIL DAN PEMBAHASAN

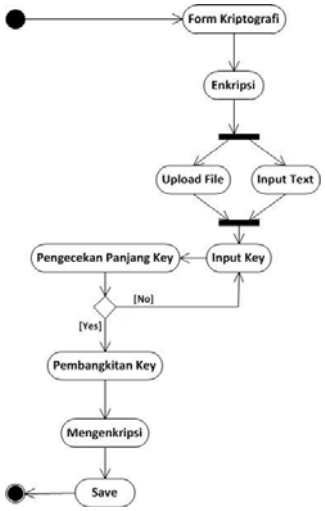
Saat ini, terdapat banyak sekali teknologi yang diciptakan dalam membantu proses pengiriman pesan. *Internet* adalah salah satu media tercepat dalam pengiriman pesan. Akan tetapi dengan perkembangan teknologi yang begitu pesat tidak menutup kemungkinan bahwa masih ada kemungkinan pesan yang sedang dikirim dapat dicuri oleh orang yang tidak memiliki hak untuk membaca. Salah satu cara agar pesan yang dikirim aman adalah dengan mengenkripsi isi dari pesan sebelum dikirimkan dan hanya pihak yang berhak yang dapat mengubah pesan tersebut kembali ke pesan semula (dekripsi). Sehingga isi pesan akan tetap aman meskipun berhasil dicuri oleh pihak yang tidak memiliki hak.

3.1 Perancangan Sistem

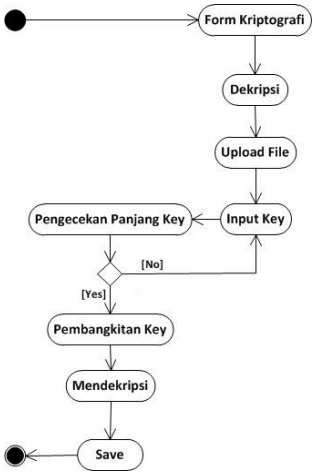
Untuk memberikan gambaran tentang prosedur-prosedur yang terdapat pada sistem akan digunakan Diagram *Unified Modelling Language* (UML). Diagram *Use Case* akan menggambarkan fungsionalitas dari sistem enkripsi dan dekripsi berbasis *web* dengan algoritma DES secara umum. Fungsionalitas dari sistem enkripsi dan dekripsi berbasis *web* dengan algoritma DES antara lain: proses pembuatan *account* baru (*sign up*), proses *login* (*sign in*), proses meng-*upload file* yang akan dienkripsi atau didekripsi, proses enkripsi terhadap file yang telah di-*upload*, proses dekripsi terhadap file yang telah di-*upload*, dan proses *sign out* dari *web*. Diagram *Use Case* akan menggambarkan interaksi antara sistem kriptografi dengan *user*.



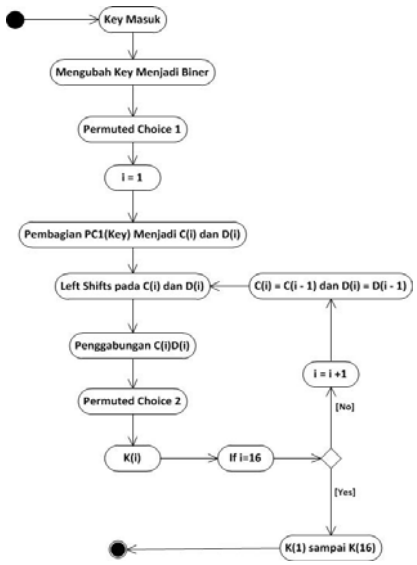
Gambar 1. Diagram Use Case Sistem Kriptografi Berbasis Web Dengan Algoritma DES



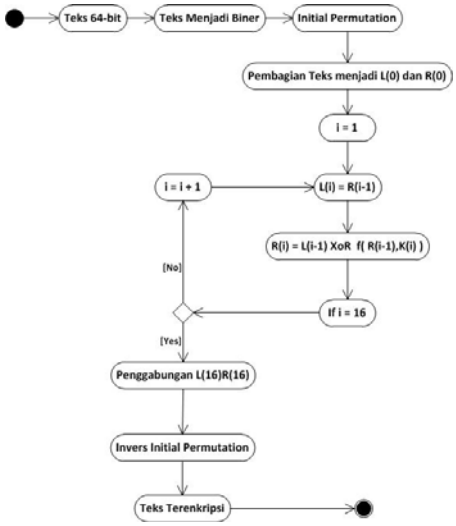
Gambar 2. Diagram Aktivitas Enkripsi



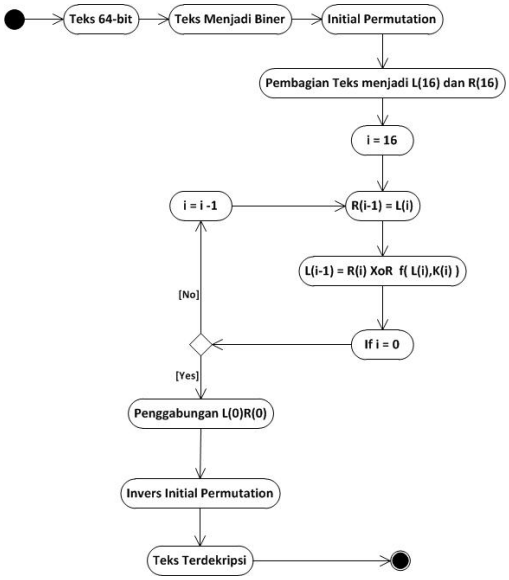
Gambar 3. Diagram Aktivitas Dekripsi



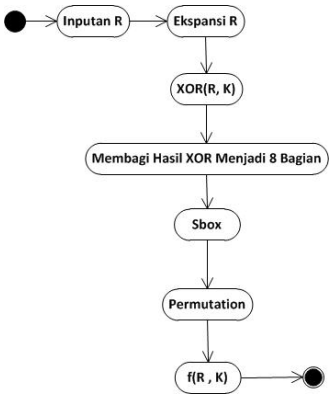
Gambar 4. Diagram Aktivitas Proses Pembangkitan Key



Gambar 5. Diagram Aktivitas Proses Enkripsi



Gambar 6. Diagram Aktivitas Proses Dekripsi



Gambar 7. Diagram Aktivitas Fungsi F

3.2 Perancangan Aplikasi

a. Main Form

Gambar 8. Rancangan Main Form

Berdasarkan pada Main *form* diatas, terdapat 2 tombol yang dapat digunakan oleh *user*. Yaitu tombol *sign in* dan tombol *sign up*, fungsi-fungsi dari kedua tombol berikut dapat dijelaskan dibawah ini :

1) Tombol *Sign In* : Sebagai tombol untuk *login* kedalam *website*. Tapi sebelumnya *user* perlu memasukkan ID dan *Password* yang telah terdaftar di-*database* dengan benar.
2) Tombol *Sign Up* : Sebagai tombol yang akan membawa *user* ke *form sign up*. Dimana *user* dapat membuat *username* baru untuk *login* ke-*website*.

Form ini adalah form utama ketika *user* pertama kali mengakses url. Pada form ini akan *user* dapat memilih 2 tombol. Bagi *user* baru yang belum memiliki ID, dapat memilih tombol *sign up* untuk mendaftarkan *username* baru. Jika *user* telah memiliki ID, dapat langsung melakukan proses *login / sign in*. *User* dapat langsung memasukan ID dan *password* kemudian sistem akan mengecek apakah ID sudah terdaftar atau belum. Jika ID belum terdaftar, maka sistem melakukan klarifikasi bahwa ID belum terdaftar. Dan bila ID telah terdaftar dan *password* yang diisikan benar maka *user* akan langsung masuk ke form berikutnya, yaitu form kriptografi. Form ini juga berisi sejarah singkat tentang kriptografi.

b. Form Sign Up

Terdapat 2 tombol pada form Sign Up yang dapat digunakan oleh *user*. Yaitu tombol *sign up* dan tombol *cancel*, fungsi-fungsi dari kedua tombol berikut dapat dijelaskan dibawah ini :

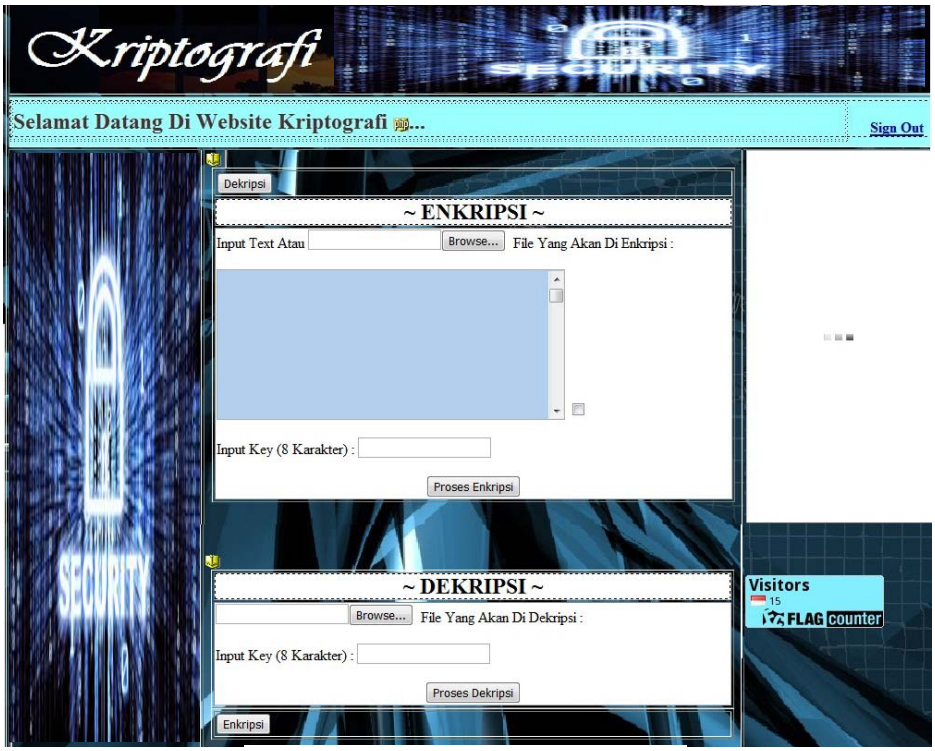
1) Tombol *Sign Up* : Sebagai tombol untuk membuat *username* baru yang digunakan untuk *login* ke-*website*. *User* terlebih dahulu harus mengisi *Username*, *Password*, *Confrim Password*, dan *Name*.
2) Tombol *Cancel* : Sebagai tombol yang akan membawa *user* kembali ke *main form*. Dimana tombol ini berfungsi untuk membatalkan proses pembuatan *username* baru.

Form *sign up* adalah form dimana *user* membuat ID baru. Terdapat beberapa data yang perlu diisi oleh *user* dalam membuat ID baru. Yaitu *Username*, *Password*, *Confrim Password*, dan *Name*. Setelah mengisi data tersebut *user* dapat memilih tombol *Sign Up*, dimana sistem akan mengecek apakah *Password* dan *Confrim Password* sama atau tidak. Tujuan dari pengecekan *Password* dan *Confirm Password* adalah

untuk memastikan *password* yang diisi oleh *user* sama dan benar-benar *password* yang di inginkan *user*, karena bentuk *password* yang disamarkan membuat adanya kemungkinan *user* salah pada saat pengetikan *password*. Sehingga digunakan *Confrim Password* untuk memastikan *password* sudah benar. Setelah *Password* dan *Confrim Password* sama, maka sistem akan memeriksa apakah *Username* sudah terdaftar di-*database* atau belum. Jika *Username* sudah terdaftar maka sistem akan memberikan konfirmasi bahwa *Username* tertelah digunakan oleh *user* lain. Jika belum terdaftar, maka sistem akan menyimpan data yang telah terisi dan memberikan konfirmasi bahwa ID baru telah berhasil dibuat. Jika *user* tidak jadi membuat ID baru, *user* dapat memilih tombol *Cancel* untuk kembali ke *main* form.

Gambar 9. Form Sign Up

c. Form Kriptografi



Gambar 10. Rancangan Form Kriptografi

Terdapat 6 tombol pada *form* kriptografi yang dapat digunakan oleh *user*. Yaitu tombol Sign Out, Enkripsi, Dekripsi, *Browse*, Proses Enkripsi, dan Proses Dekripsi. fungsi-fungsi dari kedua tombol berikut dapat dijelaskan dibawah ini :

1) Tombol *Sign Out* : Sebagai tombol untuk keluar dari *website* atau yang lebih dikenal sebagai *logout*.
2) Tombol Enkripsi : Sebagai tombol yang akan mengarahkan *user* ketabel enkripsi yang berada atas halaman *website*.
3) Tombol Dekripsi : Sebagai tombol yang akan mengantarkan *user* ketable dekripsi yang berada di bawah halaman *website*.

4) Tombol *Browse* : Pada *form* kriptografi terdapat 2 buah tombol *Browse* yang memiliki fungsi yang sama, yaitu sebagai tombol *user* untuk meng-*upload* data yang akan dienkripsi atau didekripsi.
5) Tombol Proses Enkripsi : Pada *form* kriptografi terdapat tombol Proses Enkripsi yang memiliki fungsi yaitu sebagai tombol yang akan melakukan proses pengolahan terdapat *key* yang telah di-*input*-kan juga sebagai tombol proses enkripsi. Setelah proses enkripsi selesai, *user* akan diarahkan ke-*save* data yang telah melalui proses enkripsi.
6) Tombol Proses Dekripsi : Pada *form* kriptografi terdapat tombol Proses Dekripsi yang memiliki fungsi yaitu sebagai tombol yang akan melakukan proses pengolahan terdapat *key* yang telah di-*input*-kan juga sebagai tombol proses dekripsi. Setelah proses dekripsi selesai, *user* akan diarahkan ke-*save* data yang telah melalui proses dekripsi.

Form Kriptografi adalah form yang dapat diakses hanya oleh *user* yang telah dengan benar mengisi ID dan *password* di *main* form. Diform ini user dapat melakukan proses enkripsi dan dekripsi. Pada table enkripsi user dapat memilih ingin meng-*upload* data yang ingin dienkripsi dengan memilih tombol *Browse* atau menulis sendiri teks dengan mencentang *checkbox* yang telah disediakan. Setelah mengisi data yang akan dienkripsi, user juga perlu mengisi data *key* yang akan digunakan proses enkripsi. Setelah semua terisi *user* dapat memilih tombol Proses Enkripsi. Jika *user* memilih untuk meng-*upload* data yang akan di enkripsi, maka sistem akan mengecek apakah data yang di-*upload user* berformat .txt atau bukan. Jika bukan berformat .txt maka sistem akan memberikan konfirmasi bahwa data yang di-*upload* bukan berformat .txt dan harus di-upload ulang. Dan jika data yang di-*upload* berformat .txt, maka sistem akan mengecek apakah panjang *key* sudah 8 karakter atau belum. Jika belum sistem akan memberikan konfirmasi bahwa *key* belum lengkap, dan jika *key* telah terdiri dari 8 karakter, maka sistem akan melakukan proses enkripsi pada data yang telah dimasukan *user*. Hasil enkripsi akan di-*save* dalam file berformat .txt, dan akan langsung di-*download* oleh *user*. Pada table dekripsi user dapat memilih ingin meng-*upload* data yang ingin didekripsi dengan memilih tombol *Browse*. Setelah meng-*upload* data yang akan didekripsi, user juga perlu mengisi data *key* yang akan digunakan proses dekripsi. Setelah semua terisi *user* dapat memilih tombol Proses Dekripsi, maka sistem akan mengecek apakah data yang di-*upload* berformat .txt atau bukan. Jika bukan berformat .txt maka sistem akan memberikan konfirmasi bahwa data yang di-*upload* bukan berformat .txt dan harus di-upload ulang. Dan jika data yang di-*upload* berformat .txt, maka system akan mengecek apakah panjang *key* sudah 8 karakter atau belum. Jika belum sistem akan memberikan konfirmasi bahwa *key* belum lengkap, jika telah terpenuhi maka sistem akan melakukan proses dekripsi pada data yang telah dimasukan *user*. Hasil dekripsi akan di-*save* dalam file berformat .txt, dan akan langsung di-*download* oleh *user*. Form ini juga dilengkapi dengan tombol navigasi yaitu tombol Enkripsi dan tombol Dekripsi yang akan mengarahkan *user* langsung ke table enkripsi dan dekripsi. Setelah *user* selesai proses enkripsi atau dekripsi, *user* dapat keluar dari form kriptografi dan kembali ke *main* form dengan memilih tombol *Sign Out.* Pada saat proses *sign out*, semua data user pada saat *login* ke *web* akan dihapus agar keamanan data *user* terjamin.

4. KESIMPULAN

Berdasarkan hasil pengolahan data, tingkat keamanan dokumen yang disimpan ataupun dikirim masih belum optimal. Hal tersebut disebabkan dokumen tersebut mudah dibaca atau dilihat oleh pihak yang tidak memiliki hak.

a. Dokumen tanpa pengamanan yang tepat dapat mudah diakses dan dilihat oleh pihak yang tidak memiliki hak untuk mengakses maupun melihat isi dari dokumen tersebut, untuk itu sebaiknya dokumen terlebih dulu dienkripsi atau disandikan isinya sehingga pihak lain tidak dapat mengerti isi dokumen meskipun berhasil dilihat.
b. Tidak semua orang memiliki aplikasi kriptografi yang digunakan untuk mengenkripsi atau mengdekripsi, untuk itu dengan adanya aplikasi kriptografi berbasis web ini diharapkan dapat membantu sebagian orang sehingga tidak perlu memiliki aplikasi khusus dalam melakukan proses enkripsi atau dekripsi.

5. SARAN

Adapun saran dalam mengembangan Aplikasi Kriptografi Berbasis *Web* dengan Algoritma DES adalah sebagai berikut :

a. Algritma DES masih menggunakan kunci 56-bit, diharapkan dapat dikembangkan menjadi TRIPEL DES sehingga panjang kunci menjadi 128-bit.
b. Kriptografi dapat dikembangkan tidak hanya terbatas pada teks bertipe .txt sehingga mempermudah *user* dalam memasukan data yang akan dienkripsi atau didekripsi.

UCAPAN TERIMA KASIH

Dalam penelitian jurnal ini, peneliti telah banyak mendapat bantuan berupa bimbingan, petunjuk, saran maupun dorongan moril dari berbagai pihak, maka pada kesempatan ini peneliti mengucapkan terima kasih yang sebesar-besarnya kepada seluruh Civitas akademika STMIK Widya Dharma Pontianak.

DAFTAR PUSTAKA

[1] Oz, Effy. (2009). *Management Information Systems Sixth Edition*. Course Technology.

[2] O'Brien, James A. and George M. Marakas. (2007). *Management Information Systems*. McGraw-Hill/Irwin.

[3] Delfs, Hans and Helmut Knebl. (2007). *Introduction to Cryptography Principles and Applications Second Edition*. Springer-Verlag. Berlin.

[4] Dunn, Wiliam L. and J. Kenneth Shultis. (2012). *Exploring Monte Carlo Methods*. Elsevier.

[5] Agarwal, B. B., S. P. Tayal and M. Gupta. (2010). *Software Engineering & Testing An Introduction*. Jones and Bartlett Publishers.

[6] Sommervile, Ian. (2011). *Software Engineering Ninth Edition*. Addison Wesley.

[7] Munir, Rinaldi. (2006). *Kriptografi*. Informatika Bandung. Bandung.

[8] Van Tilborg, Henk C. A. (2005). *Enclycopedia of Cryptography and Security*. Springer Science + Business Media, Inc.

[9] Konheim, Alan G. (2007). *Computer Security and Cryptography*. John Wiley & Sons, Inc.

[10] Oppliger, Rolf. (2005). *Contemporary Cryptography*. Artech House.

[11] Munir, Rinaldi. (2007). *Kriptografi*. Informatika. Bandung

[12] Aryus, Doni. (2008). *Kriptografi Keamanan Data dan Komunikasi.* Graha Ilmu. Yogyakarta.