IMPLEMENTASI ALGORITME *AES* 128 UNTUK APLIKASI SERAH TERIMA DOKUMEN *PROJECT* PADA PT TELKOMSIGMA

Dahlia Damayanti Rusnadi[1)], **Noni Juliasari** [2)]
[1]Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : email.dahlia.damayantir@gmail.com[1)], noni.juliasari@budiluhur.ac.id[2)]

Abstrak

PT. Telkomsigma mempunyai data yang penting untuk disimpan dalam komputer. Namun jika data disimpan tetapi tidak ada dengan pengamanan yang baik maka data tersebut mudah dicuri atau diubah oleh yang tidak berkepentingan dengan data tersebut. Proses serah terima pekerjaan secara manual rentan terhadap kerahasiaan dokumen karena proses serah terima secara manual biasanya mengirimkan dokumen dalam bentuk hardcopy. Oleh karena itu diperlukan suatu aplikasi yang dapat membantu proses serah terima pekerjaan tersebut. Dengan mengutamakan keamanan pada dokumen yang dikirim diperlukan metode pengamanan dengan *system* kriptografi. Metode yang digunakan adalah *Advanced Encryption Standard* (AES) 128 dengan menggunakan kunci enkripsi dan dekripsi yang sama. Dengan adanya aplikasi ini diharapkan proses serah terima pekerjaan menjadi lebih mudah dan aman, sehingga dokumen yang diserahterimakan dapat tersampaikan dengan tepat.

Kata kunci : Kriptografi, Keamanan, *Algoritme* AES-128.

1. PENDAHULUAN

1.1. Latar Belakang

PT Telkomsigma Cipta Caraka mempunyai data yang penting untuk disimpan dalam komputer. Namun jika data tersebut disimpan tetapi tidak ada dengan pengamanan yang baik maka data tersebut mudah dicuri atau diubah oleh yang tidak berkepentingan dengan data tersebut. Oleh karena itu agar tidak ada orang yang berkepentingan dapat mengubah data yang sudah disimpan atau dapat mencuri data yang ada dibutuhkan suatu metode untuk dapat mengamankan data. Penerapan kriptografi untuk Tugas Akhir akan difokuskan pada pengamanan data yang dapat disimpan menjadi aman dan hanya dapat digunakan oleh orang yang berkepentingan pada data tersebut.

Service Operation Management adalah salah satu divisi pada PT Telkomsigma yang bertanggung jawab untuk men*support* customer. Divisi ini adalah pendukung setelah tim *Project* yang diketuai oleh *Project* Manager menyelesaikan tugasnya. Dokumen yang diberikan oleh Tim *Project* berisi file yang bersifat rahasia, oleh karena itu diperlukan pengamanan file untuk mencegah pencurian file pada dokumen tersebut.

Dari aplikasi yang kami buat diharapkan dapat mencegah pencurian data yang dapat membuat salah satu pihak merasa terugikan. Sehingga data-data penting dapat diamakan dengan aplikasi ini.

1.2. Perumusan Masalah

Berdasarkan permasalahan yang telah di uraikan pada latar belakang, maka didapatkan permasalahan sebagai berikut:

a. Bagaimana cara untuk mengamankan file agar tidak bisa dilihat oleh orang yang tidak berkepentingan?
b. Metode apa yang digunakan untuk mengamankan file yang bersifat rahasia?

1.3. Tujuan Penulisan

Adapun tujuan dari pembuatan aplikasi serah terima dokumen project ini adalah agar keamanan data pada PT Telkomsigma dapat tersolusikan dengan baik, diantaranya sebagai berikut :

a. Membuat aplikasi kriptografi yang dapat mendukung keamanan file dokumen.
b. Dengan menggunakan metode Kriptografi *Advanced Encryption Standard* (AES) 128.

1.4. Batasan Masalah

Untuk menyamakan persepsi supaya tidak keluar dari materi pembahasan makan diberikan beberapa batasan masalah seperti berikut:

a. Metode yang di gunakan adalah *Algoritme Advanced Encryption Standard (AES)* untuk mengamankan database yang ingin disimpan.
b. Bahasa pemrograman yang digunakan adalah PHP.
c. Data yang akan di enkripsi dan dekripsi berbentuk file.
d. Database yang digunakan adalah *Mysql*.
e. Aplikasi yang dibuat berbasis *web*, dijalankan dengan menggunakan *browser*.

2. LANDASAN TEORI

2.1. Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani yaitu "*cryptos*" yang artinya "*secret"* (rahasia) dan "*grapheirl"* yang artinya "*writing"* (tulisan) merupakan *Algoritme* untuk mengubah suatu informasi dari bentuk asli ke dalam bentuk yang acak/random yang hanya bisa di gunakan oleh pengguna yang mengetahui passwordnya.

2.2. Jenis Kriptografi

Algoritme terbagi dua jenis, *algoritme* klasik dan *algoritme modern*:

a.Algoritme Kriptografi Klasik

Pada *Algoritme* klasik, ada dua macam teknik yang biasa digunakan, yaitu teknik subtitusi dan teknik transposisi/permutasian.

a) Teknik Subtitusi

Jenis-jenis subsitusi yang dikenal hingga saat ini adalah subsitusi deret campuran kata kunci, subsitusi *monomedinome-trinome*, susbsitusi multirateral varian, subsitusi digrafik, subsitusi persegi empat standar, subsitusi kode *playfair*, subsitusi polialfabet periodik, dan enigma (Tehjah, 2006)[1]

b. **Teknik Transposisi/Permutasian**

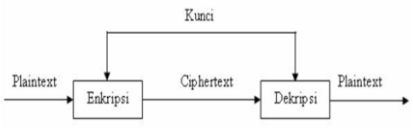
Setelah mengalami beberapa perkembangan, dalam penjelasan dari Agen FBI Rusia Haynen pada tahun 1957, muncul suatu kode rahasia yang rumusnya merupakan penggabungan dari kedua teknik diatas, dikenal dengan nama kode rahasia VIC. Penggunaan *system* campuran ini dapat dilakukan tanpa penggunaan komputer. VIC memerlukan minimum 4 kunci dan 3 kali enkripsi. Sedangkan langkah-langkahnya diuraikan dengan subsitusi, dilanjutkan transposisi dengan lebar baris seragam, dan terakhir teknik transposisi dengan lebar baris bervariasi (Tehjah, 2006)[2].

c. Algoritme Kriptografi Modern

Pada Algoritme kriptografi modern ada dua jenis berdasarkan jenis kunci yaitu kriptografi simetris dan asimetris.

a.*Algoritme* Simetris

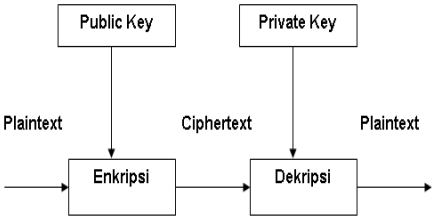
Adalah *Algoritme* yang sama digunakan dalam proses enkripsi maupun deskrpisinya.



Gambar 1 : Algoritme Kripto Simetri.

b. Algoritme Asimetri

Adalah *Algoritme* yang menggunakan dua kunci berbeda untuk proses enkripsi dan deskripsinya(Dony Ariyus, 2006)[3].



Gambar 2 : Algoritme Kripto Asimetri

2.3. *Algoritmma AES 128 (Advanced Encryption Standard 128)*

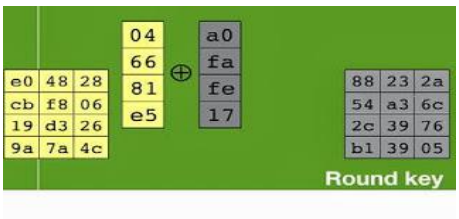
AES-128 (*Advanced Encryption Standard*) adalah lanjutan dari *Algoritme* sebelumnya yaitu *Data Encryption Standard* (DES) yang masa berlakunya dianggap telah usai karena faktor keamanan. Kriteria penilaian yang ditemukan NIST didasarkan pada 3 kriteria utama yaitu aspek keamanan, aspek biaya, dan aspek implementasi dan karakteristik algoritme. Untuk melakukan proses enkripsi dan dekripsi menggunakan AES 128 menggunakan beberapa metode sebagai berikut:

1) Proses Enkripsi

Dalam proses enkripsi menggunakan AES 128 menggunakan 4 metode diantaranya :

a. AddRoundKey

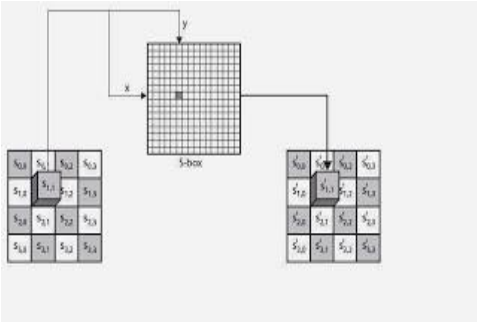
Addroundkey pada dasarnya adalah mengkombinasikan *ciphertext* yang sudah ada dengan *cipherKey* dengan operasi XOR.



Gambar 3 : Skema Addroundkey

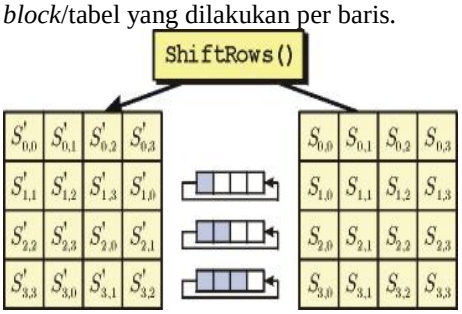
b. Subbytes

Subbytes didefinisikan sebagai proses menukar menukar isi dalam matriks/tabel yang sudah ada dengan matriks/tabel lain.



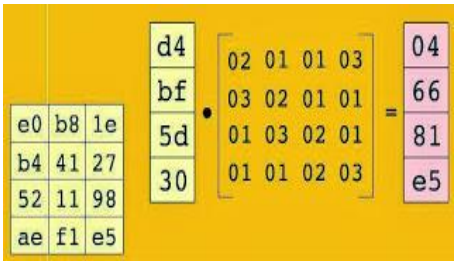
Gambar 4 : Ilustrasi Subbytes

c. Shiftrows
Shift Rows didefinisikan sebagai proses yang melakukan shift atau pergeseran pada setiap elemen dalam *block*/tabel yang dilakukan per baris.



Gambar 5 : Ilustrasi Siftrows

d. MixColumns
Mix Column adalah mengalikan tiap elemen dari *block cipher* dengan matriks



Gambar 6 : Ilustrasi MixColumn

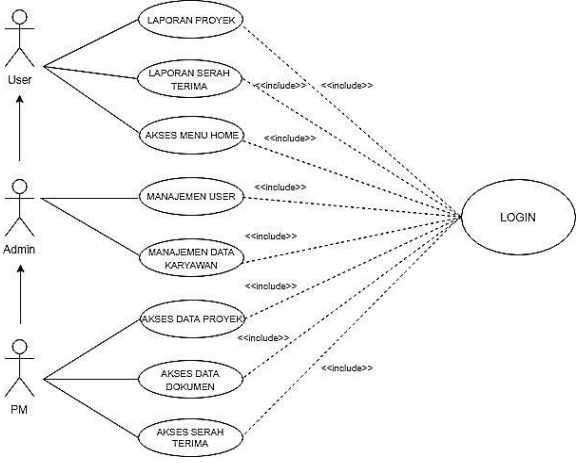
2) Proses Dekripsi
Dalam proses dekripsi menggunakan AES 128 menggunakan 3 metode diantaranya :
a. Invshiftrows
Inshiftrows adalah transformasi byte yang berkebalikan dengan transformasi shiftrows.

b. InvSubBytes
Merupakan transformasi bytes yang berkebalikan dengan transformasi subbytes.
c. InvMixColumn
InvMixColumn didefinisikan sebagai proses pada setiap kolom dalam state dikalikan dengan matriks perkalian dalam AES-128.

3. ANALISIS MASALAH DAN RANCANGAN PROGRAM

3.1. Analisis Kebutuhan

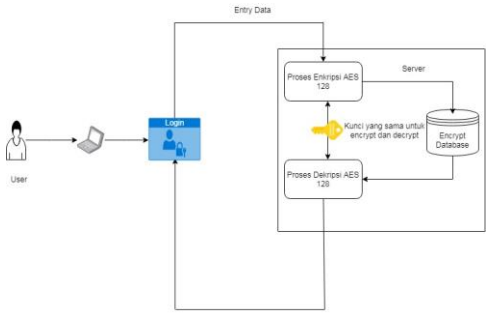
Program yang akan dibuat terdiri dari 8 tampilan menu, yang terdiri dari *Login*, menu *Home* (*Dashboard*), menu *User*, menu Karyawan, menu *Project*, Menu Serah Terima *Project*, Menu Serah Terima *Support*, Menu Data *Project*, dan Menu Laporan Serah Terima.



Gambar 7. Use Case Diagram Menu Utama

3.2. Arsitektur *System*

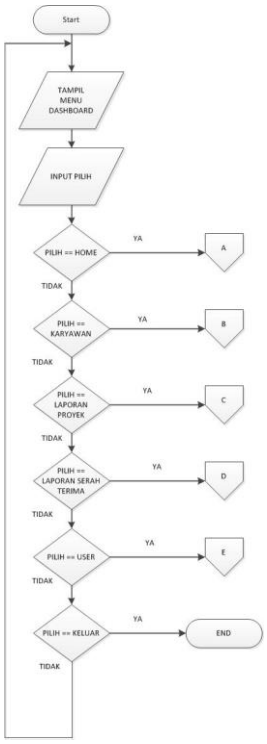
Agar dapat memahami konsep dari aplikasi yang akan dibanngun dapat dilihat pada gambar dibawah ini :



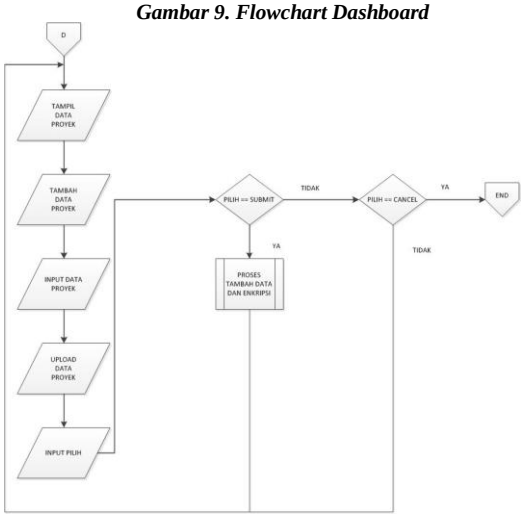
Gambar 8 Arsitektur System

3.3. Flowchart Program

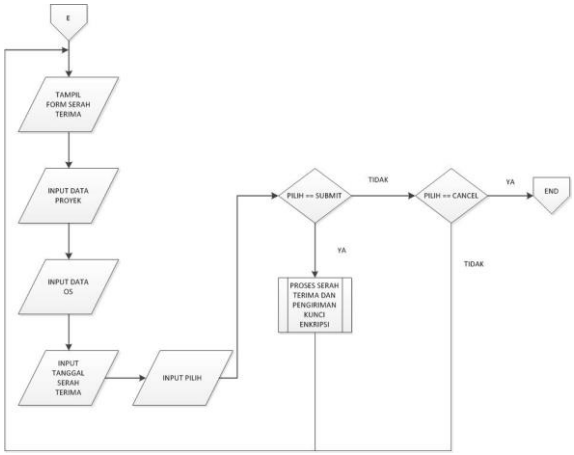
Untuk menggambarkan urutan proses pada aplikasi akan digunakan *flowchart. Flowchart* ini terdiri dari *Dashboard*, Menu Karyawan, Menu *Project*, Menu Serah Terima *Project*, Menu Serah Terima Support, Laporan Serah Terima, dan Laporan *Project*. Pada Menu *Project* dan Menu Serah Terima Support terdapat proses enkripsi dan dekripsi file dokumen.



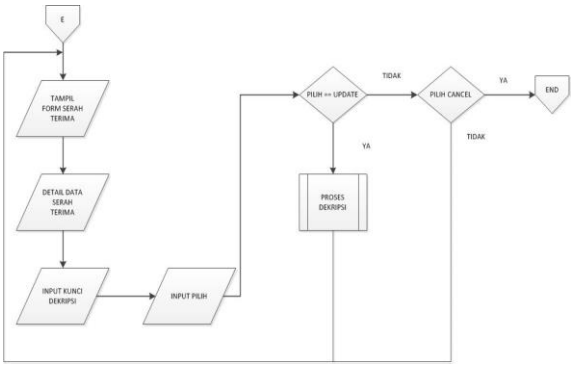
Gambar 9. Flowchart Dashboard



Gambar 10 : Flowchart Tambah Data Project



Gambar 11 : Flowchart Serah Terima Project



Gambar 12 : Flowchart Serah Terima Support

4. IMPLEMENTASI DAN UJI COBA PROGRAM

4.1. Tampilan Layar Program

Pada bagian ini, diuraikan mengenai tampilan layar aplikasi *system* informasi serah terima dimulai dari aplikasi ini dijalankan sampai aplikasi ini selesai dijalankan. Untuk lebih jelasnya diberikan penjelesan dengan gambar mengenai tampilan-tampilan yang ada pada aplikasi *system* informasi serah terima dokumen *project*.

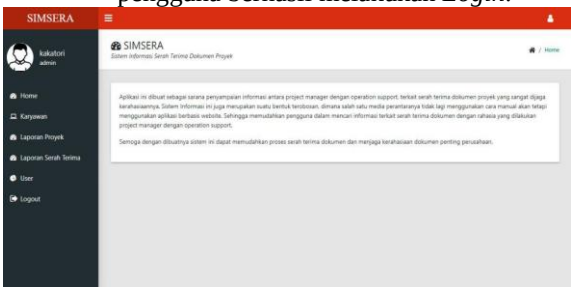
4.1.1 Tampilan Layar Login

Tampilan layar *form Login*, seperti terlihat pada gambar dibawah ini, berfungsi sebagai akses menuju menu utama.

Gambar 13. Tampilan Login

4.1.2 Tampilan Layar Menu Utama

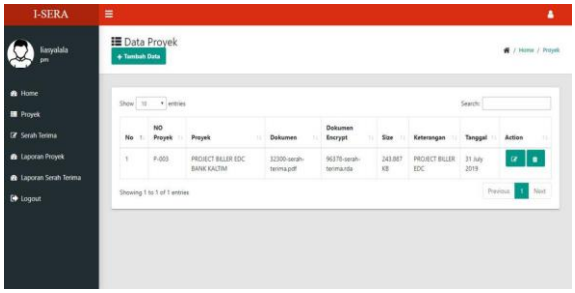
Tampilan layar pada menu utama dapat dilihat pada gambar. *Form* ini pertama kali muncul pada saat pengguna berhasil melakukan *Login*.



Gambar 14. Tampilan Layar Menu Utama

4.1.3 Tampilan Layar *Project*

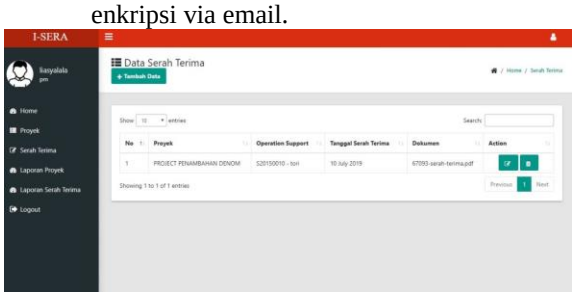
Pada Tampilan Layar *Project* ini terdapat data *project* yang ada di dalam sebuah tabel, pada data *project* tersebut ada dokumen file yang akan di enkripsi ke dalam database.



Gambar 15. Tampilan Layar Project

4.1.4 Tampilan Layar *Serah Terima Project*

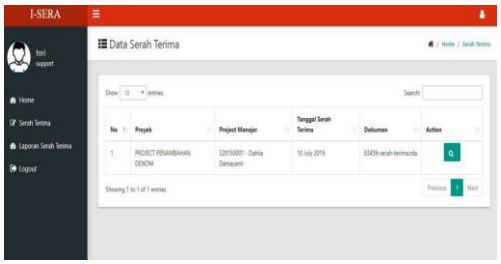
Pada Tampilan Layar Serah Terima *Project* ini terdapat terdapat data serah terima *project*, pada menu ini terdapat proses pengiriman kunci enkripsi via email.



Gambar 16. Tampilan Layar Serah Terima Project

4.1.5 Tampilan Layar Serah Terima Support

Pada Tampilan Layar Serah Terima *Support* terdapat data serah terima, pada menu ini terdapat proses dekripsi dokumen.



Gambar 17 : Tampilan Layar Serah Terima Support

4.2. Pengujian Program

Pengujian program dilakukan setelah semua kebutuhan telah terpenuhi baik dari software maupun hardware, tahap selanjutnya adalah uji coba aplikasi yang sudah dibuat. Metode yang digunakan untuk pengujian kali ini adalah metode *black box* yang merupakan proses pengujian terhadap fungsionalitas *input*/*output* dari suatu perangkat lunak. Penguji melakukan beberapa kondisi input kemudian melakukan sejumlah pengujian terhadap program sehingga menghasilkan suatu output yang nilainya dapat dievaluasi.

No	Rancangan Proses	Hal yang di harapkan	Hasil	Keterangan
1.	Mengisi Form *Login*	Masuk ke Halaman Utama	Sesuai	Jika di Input Benar
2.	Klik Menu Data Karyawan	Masuk ke Halaman List Data Karyawan	Sesuai	Jika ke Halaman List Data Karyawan
3.	Klik Button Tambah Data Karyawan	Masuk ke Halaman Form Tambah Data Karyawan	Sesuai	Jika ke Halaman Form Tambah Data Karyawan
4.	Mengisi Form Tambah Data Karyawan	Input Data Karyawan	Sesuai	Jika di Input Benar
5.	Klik Link Ubah	Masuk ke Halaman Form Ubah Data Karyawan	Sesuai	Jika ke Halaman Form Ubah Data Karyawan
6.	Mengisi Form Ubah Data Karyawan	Input Data Karyawan	Sesuai	Jika di Input Benar
7.	Klik Link Hapus	Data setelah di klik akan terhapus	Sesuai	Jika di Klik
8.	Klik Menu Data Proyek	Masuk ke Halaman List Data Proyek	Sesuai	Jika ke Halaman List Data Proyek
9.	Klik Button Tambah Data Proyek	Masuk ke Halaman Form Tambah Data Proyek	Sesuai	Jika ke Halaman Form Tambah Data Proyek
10.	Mengisi Form Tambah Proyek	Dokumen Proyek Terenkripsi kedalam database	Sesuai	Jika di Input Benar
11.	Klik Link Ubah	Masuk ke Halaman Form Ubah Data Proyek	Sesuai	Jika ke Halaman Form Ubah Data Proyek
12.	Mengisi Form Ubah Proyek	Data Proyek dapat di Ubah dan terenkripsi kembali apabila ada dokumen yang di *upload*	Sesuai	Jika di Input Benar
13.	Klik Link Hapus	Data setelah di klik akan terhapus	Sesuai	Jika di Klik
14.	Klik Menu Serah Terima	Masuk ke Halaman List Serah Terima	Sesuai	Jika ke Halaman List Serah Terima
15.	Klik Button Tambah Serah Terima	Masuk ke Halaman Form Tambah Serah Terima	Sesuai	Jika ke Halaman Form Tambah Serah Terima
16.	Mengisi Form Serah Terima	Proses serah terima dan pengiriman kunci enkripsi via email	Sesuai	Jika di Input Benar
17.	Klik Link Ubah	Masuk ke Halaman Form Ubah serah terima	Sesuai	Jika ke Halaman Form Serah terima
18.	Mengisi Form Ubah Customer	Proses serah terima dapat di ubah dan pengiriman kunci enkripsi kembali	Sesuai	Jika di Input Benar
19.	Klik Link Hapus	Data setelah di klik akan terhapus	Sesuai	Jika di Klik
20.	Klik Menu Laporan Serah Terima	Masuk ke Halaman List Laporan Serah Terima	Sesuai	Jika ke Halaman List Laporan Serah Terima
21.	Input Tanggal Serah Terima	Input Tanggal Mulai dan Berakhir	Sesuai	Jika Terdapat List Laporan Serah Terima
22.	Klik Menu Logout	Keluar ke Halaman *Login*	Sesuai	Jika ke Halaman *Login*

4.3. Evaluasi Hasil Uji Coba Program

Setelah proses pengujian dilakukan evaluasi hasil uji coba program untuk mengevaluasi pencapaian pada penelitian tersebut, apakah perlu adanya pengembangan pada aplikasi tersebut atau untuk mengetahui apakah aplikasi tersebut sudah dapat di implementasikan.

4.4. Analisa Dan Uji Coba Program

Dari proses pengujian program dapat dilihat kelebihan dan kekurangan program tersebut, apakah proses enkripsi dan

dekripsi sudah dapat mensolusikan masalah yang ada pada perusahan tersebut. Pada proses pengujian program ini terdapat beberapa kelebihan dan kekurangan dari aplikasi ini, yaitu sebagai berikut :

4.4.1. Kelebihan Program

a) Dokumen akan lebih aman, karena dokumen tersebut sudah terenkripsi.
b) Dokumen lebih tersimpan dengan baik karena tersimpan pada database aplikasi.
c) Tidak ada kekurangan informasi dikemudian hari.

4.4.2. Kekurangan Program

a) Tidak dapat diakses tanpa menggunakan internet.
b) Aplikasi hanya mengenkripsi dokumen dalam bentuk pdf
c) Aplikasi hanya bisa menggunakan database yang sudah ditentukan oleh pengembang.

5. PENUTUP

Dari uraian permasalahan dan penyelesaian masalah diatas, dapat disimpulkan program aplikasi *system* informasi serah terima berbasis web menggunakan Kriptografi dengan metode *Advanced Encryption Standard* 128 (AES-128) sangat diperlukan.

5.1. Kesimpulan

Kesimpulan dari aplikasi kriptografi yang telah dibuat adalah sebagai berikut :

a) Pengguna sudah dapat mengimplementasikan dan sudah mengerti dengan baik aplikasi ini.
b) Implementasi kriptografi dengan metode AES 128 dapat digunakan untuk mengamankan dokuman.
c) Solusi keamanan dokuman pada PT Telkomsigma sudah terpenuhi.
d) Aplikasi ini telah diatur oleh system sehingga dokumen serah terima dapat tersimpan dengan baik.
e) Dokumen serah terima dapat terjaga kerahasiaannya.

5.2. Saran

Agar dapat dilakukan pengembangan yang lebih baik, adapun saran yang diberikan antara lain:

a. Pengembangan aplikasi menggunakan kriptografi dengan metode AES 128 yang lebih baik..
b. Adanya pengembangan aplikasi berbasis *mobile* dengan menggunakan *Algoritme* AES 128.
c. Aplikasi ini dapat diimplementasikan dengan pengembangan fitur yang jauh lebih baik dan detail.

6. DAFTAR PUSTAKA

[1] Ariyus, Doni. 2008. Pengantar ilmu Kriptografi, Teori, analisis dan Implementasi. Yogyakarta: Penerbit Andi.

[2] Ariyus, Doni 2006. Kriptografi Keamanan Data Dan Komunikasi. Yogyakarta : Graha Ilmu.

[3] Gumira, Gilang. Khairil, Emawati, dan Erlansari, Aan. (2016). Implementasi Metode *Advanced Encryption Standard* (AES) dan Message Digest 5 (MD5) Pada Enkripsi Dokumen.. Jurnal Rekursif, 4(3)

[4] Howard, John D. "An Analysis Of Security Incidents On The Internet 1989 - 1995," PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 1997.

[5] Ilyas, Imron Abdul. dan Widodo, Suryarini. (2014). KRIPTOGRAFI FILE MENGGUNAKAN METODEAES DUAL PASSWORD. Jurnal Ilmiah.