ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI METODE *DATA ENCRYPTION STANDARD* DENGAN METODE *ADVANCED ENCRYPTION SYSTEM* (STUDI KASUS PADA PT. ONE STANDARD GROUP PTE LTD)

Akhmad Budi[1)] dan Arabella Chicali[2)]
[1)]Staf Pengajar Studi Teknik Informatika
[2)]Alumni Program Studi Teknik Informatika
Intitut Bisnis dan Informatika Kwik Kian Gie
Jl. Yos Sudarso Kav.87, Sunter Jakarta Utara 14350

ABSTRACT

The security system within a company is the top priority, one of its application is in web media, where it exist various confidential information in it, such as user information on the company PT. One Standard Group PTE LTD must be kept confidential not to fall into unauthorized parties, therefore a security system to address the information security is needed.

The security system of modern symmetric key cryptography algorithms is considered to be able to overcome these problems which are generally divided into two, namely Data Encryption Standard (DES) dan Advanced Encryption System (AES). From the two algoritmhs, the author make comparisons to obtain more efficient algorithm in terms of security and times.

The method that author use in this research is Extreme Programming Research Methodology, with qualitative methodological analysis technique and in data collection author use direct observation and literature study.

The system that the author created applies additional security for user information which will be directly stored with the AES method and the DES method and the system will display the proccessing time of both.

The conclusion that author can achieve from this thesis is AES method crytographic algorithms is more secure than DES method because AES method has double protection, but from the time aspect efficiency the DES method cryptographic algorithms is more efficient.

Keyword:Data Security, Crytographic, AES, DES

1. Pendahuluan

Pada awal mula perkembangan teknologi, komputer dan telekomunikasi masih sangat terbatas, hingga kini jelas terlihat bahwa perkembangan dan perubahan yang terjadi cukup signifikan. Perkembangan komputer dan teleko munikasi yang cukup signifikan tersebut didukung dengan pemanfaatan internet yang meluas dan membuat suatu informasi dengan cepat berkembang ke pengguna lainnya, namun pemanfaatan komputer untuk menyimpan informasi yang bersifat rahasia (*classified*) dan sensitif baru dilakukan sekitar tahun 1950-an.

Perkembangan teknologi komputer dan telekomunikasi yang berkembang luas dapat bermanfaat untuk mengefisienkan waktu dan mempermudah pengguna, namun pada kenyataannya kecepatan yang ada tidak sebanding dengan tingkat keamanan terhadap suatu informasi yang diberikan kepada pennggguna.

Melihat tingginya kebutuhan akan teknologi dan telekomunikasi saat ini sehingga dapat dikatakan bahwa kita saat ini berada di sebuah "*information-based society*", yang dimana menuntut kemampuan untuk mengakses dan

menyediakan informasi secara cepat dan akurat bagi suatu organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual.

Oleh karena itu dapat dikatakan nilai keamanan sebuah informasi sangatlah penting bagi pengguna teknologi komputer dan telekomunikasi, pengguna seringkali membatasi jumlah akses penerima informasi untuk beberapa pihak demi mengurangi resiko keamanan informasi jenis tertentu yang bersifat rahasia atau sensitif, namun terkadang informasi masih dapat jatuh ke pihak lain sehingga menimbulkan kerugian terhadap beberapa pihak, oleh karena itu pengguna menginginkan terdapat kemanan dari sistem informasi yang digunakan agar kemanan informasi terjamin dalam batas yang dapat diterima.

Menurut G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah atau paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.

Dibalik pentingnya keamanan suatu informasi sering kali sulit untuk mengajak suatu perusahaan atau pemilik sistem informasi untuk melakukan investasi di bidang keamanan tersebut, di karenakan kurangnya kesadaran akan pentingnya suatu kerahasiaan informasi serta kurangnya sosialisai manfaat keamanan suatu informasi dalam masyarakat pengguna luas. Dan dalam jurnal Budi Rahardjo (2002:3) mengangkat kutipan dari majalah *Information Week* yang melakukan survey pada tahun 1997 di Amerika Serikat yang dimana terbukti hanya 22% yang menganggap keamanan sistem informasi sebagai komponen yang penting dan utama, namun 78% sisanya lebih mengutamakan "*reducing cost*" dan "*improving competitiveness*" meskipun bahwa sesungguhnya perbaikan keamanan sistem informasi justru menelan biaya yang lebih besar dibandingkan dengan memperbaiki keamanan sistem informasi yang telah dirusak.

Jumlah kejahatan terhadap sistem teknologi dan telekomunikasi terutama yang berhubungan dengan sistem informasi terus meningkat, dan salah satu penerapan yang membutuhkan tingkat keamanan yang tinggi yaitu dalam media web. Dimana di dalam web membutuhkan keamanan dari kejahatan baik terhadap sistem teknologi maupun terhadap telekomunikasinya, yang dikarenakan media web berisikan informasi-informasi penting dari suatu organisasi, perguruan tinggi, lembaga pememrintahan, maupun individual. Dan penulis menaruh fokus perhatian pada situs web tambahan dari perusahaan PT.One Standard Group PTE LTD (Tinggal.com) yang akan dibuat yaitu "tep-tinggal.dev" , yang dimana memerlukan keamanan dan menjaga kerahasiaan terhadap informasi dalam perusahaan, supaya tidak terdapat pihak ketiga atau pihak yang tidak berkepentingan untuk mengakses sistem dan informasi penting. Sehingga dibutuhkanlah sistem keamanan yang dapat mengatasi kebutuhan keamanan tersebut.

Oleh sebab itu disiasatilah bagaimana cara menjaga kerahasiaan dan mendeteksi keaslian dari informasi yang dikirim atau diterima sehingga dibutuhkanlah sebuah ilmu di bidang kriptografi dengan penggunaan algoritma yang dimana dapat berguna untuk mengatasi permasalahan diatas. Namun kriptografi sendiri dibagi ke dalam 2 bagian, diantaranya kriptografi klasik dan kriptografi modern yang dimana memiliki *cipher* yang berbeda, *cipher* yang tergolong dalam kriptografi klasik adalah *Cipher* Substitusi (*substitution cipher*) dan *Cipher* Transposisi (*transposition cipher*). Dan *kunci y*ang tergolong dalam kriptografi modern dibagi menjadi dua,

antara lain Kriptografi Kunci Simtetrik (*Cipher* Substitusi dan *Cipher* Transposisi) dan Kriptografi Kunci Asimetrik (*Data Encryption Standard* dan *Advanced Encryption System*).

Batasan Masalah

Berdasarkan uraian identifikasi masalah sebelumnya, maka penulis memutuskan membatasi penelitian dengan ruang lingkup sebagai berikut :

i. Perusahaan kurang memperhatikan sisi keamanan dalam pengiriman informasi yang bersifat pribadi maupun data perusahaan.
ii. Masih terdapat beberapa pihak dari perusahaan yang kurang memahami sistem keamanan algoritma kriptografi *Data Encryption Standard* (DES) dan *Advanced Encryption System* (AES).
iii. Masih terdapat beberapa pihak dari perusahaan yang kurang mengetahui perbandingan efisiensi waktu dan keamanan yang lebih aman antara sistem keamanan algoritma kriptografi *Data Encryption Standard* (DES) dan *Advanced Encryption System* (AES).

Tujuan Penelitian

Penelitian ini bertujuan untuk memberikan informasi mengenai algoritma kriptografi metode *Data Encryption Standard* (DES) dengan metode *Advanced Encryption System* (AES) serta mengetahui perbandingan dua metode dari algoritma kriptografi dalam menjaga keamanan sistem informasi, yaitu metode atau *Data Encryption Standard* (DES) dengan metode *Advanced Encryption System* (AES) pada satu web yang sama untuk mengetahui performa dan waktu kerja metode manakah yang lebih efisien dan cepat.

2. Tinjauan Pustaka

Sistem

Pengertian sistem adalah satu set komponen yang saling terkait, dengan batas yang jelas, bekerja sama untuk mencapai tujuan umum dengan menerima *input* (masukan) dan menghasilkan *output* (keluaran) dalam transformasi yang terorganisir.[6] Sistem memiliki tiga fungsi dasar:

i. Input

Melibatkan, menangkap dan merakit elemen yang masuk ke sistem untuk diproses. Sebagai contoh bahan mentah, energi, data, dan usaha manusia harus diamankan dan diorganisir pengolahan.

ii. Processing

Melibatkan transformasi proses yang menjadi *output* (keluaran). Contohnya adalah proses pembuatan, proses pernapasan manusia, atau perhitungan matematis.

iii. Output

Melibatkan transfer elemen yang telah dihasilkan oleh sebuah transformasi proses ke tujuan akhir. Contohnya yaitu produk jadi, layanan manusia atau jasa, dan informasi manajemen harus dikirimkan untuk pengguna mereka.

Sistem Informasi

Sistem Informasi dapat berupa gabungan antara orang, perangkat keras, perangkat lunak, jaringan komunikasi, sumber data, dan kebijakan dan prosedur yang menyimpan, mengambil, mengubah, dan menyebarkan informasi dalam sebuah organisasi.

Orang mengandalkan sistem informasi modern untuk berkomunikasi satu sama lain menggunakan berbagai perangkat fisik (perangkat keras), instruksi dan prosedur pemrosesan informasi (perangkat lunak), saluran komunikasi (jaringan), dan data tersimpan (sumber data). Meskipun sistem informasi saat ini biasanya dianggap memiliki kaitan dengan komputer, namun kita telah

menggunakan sistem informasi sejak awal peradaban. Bahkan saat ini kita sering menggunakan sistem informasi yang tidak ada hubungannya dengan komputer.

Informasi

Menurut Marakas dan O'Brien, informasi adalah data yang telah dikonversi menjadi konteks yang berarti dan bermanfaat bagi pengguna tertentu.

Data

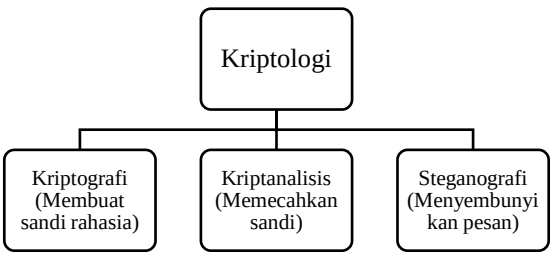
Data adalah reprentasi fakta dunia nyata dunia nyata yang mewakili suatu objek seperti manusia (pegawai, siswa, pembeli, pelanggan), barang, hewan, peristiwa, konsep, keadaan, dan sebagainya, yang diwujudkan dalam bentuk angka, huruf, simbol teks, gambar, bunyi, atau kombinasinya.[2]

Algoritma

Algoritma adalah urutan prosedur instruksi yang terdefinisi dengan baik untuk memecahkan permasalahan, yaitu untuk mendapat keluaran yang diperlukan maka diberikan beberapa nilai atau himpunan nilai sebagai masukan (*input*) yang kemudian diproses dan menjadi keluaran (*output*).

Kriptografi

Pengertian kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi (*cryptology*).[12]



Gambar2.1 Area Bidang Kriptologi

Sumber : Emy Setyaningsih, S.Si., M.Kom.(2015:2)

Pengamanan terhadap data (informasi) dapat dilakukan dengan beberapa cara, yaitu **steganografi** (ilmu menulis atau memyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorang pun yang mengetahui atau menyadari keberadaan suatu pesan rahasia), ***watermarking*** (ilmu yang menyamarkan arti pesan, namun tidak menyembunyikan keberadaan pesan), dan **kriptografi**. Kriptografi (*cryptography*) berasal dari bahasa Yunani, yaitu dari kata *crypto* dan *graphia* yang berarti 'penulisan rahasia'.

Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Perancang algoritma kriptografi disebut kriptografer.

Kriptografi sendiri sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi seperti kerahasiaan, integritas data, autentikasi, dan ketiadaan penyangkalan. Keempat aspek tersebut merupakan tujuan fundamental dari suatu sistem kriptografi. Sehingga dapat dikatakan, kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi.

Algoritma kriptografi sendiri dibagi menjadi dua bagian berdasarkan perkembangan zaman, yaitu :

i. Kriptografi Klasik

Kriptografi klasik merupakan salah sattu metode kriptografi yang dipakai pada zaman dahulu sebelum ada komputer. Bentuk penyandiannya berupa teks (karakter) yang beroperasi pada mode karakter

dengan menggunakan alat tulis berupa kertas dan pensil, atau dengan mesin sandi yang masih sangat sederhana, namun algoritma ini jarang digunakan lagi karena sangat mudah dipecahkan. [12]

Kriptografi klasik sendiri memggunakan algoritma matematis yang digunakan untuk penyandian *plaintext* menjadi *ciphertext* yang dikenal dengan sebutan *cipher*. *Cipher* yang tergolong dalam kriptografi klasik adalah :

a. *Cipher* Substitusi (*substitution cipher*) *Cipher* Substitusi algoritma kriptografi yang mengganti setiap unit *plaintext* dengan satu unit *ciphertext*. Satu unit disini dapat berarti satu karakter, pasangan karakter, atau kelompok lebih dari dua karakter.

b. *Cipher* Transposisi (*transposition - cipher*)

Cipher Transposisi adalah metode penyusunan kembali karakter dengan menyesuaikan beberapa skema yang sering kali digunakan pada penggambaran beberapa geometri. *Ciphertext* diperoleh dengan pengubahan posisi. Dengan kata lain, algoritma ini mentransposisi rangkaian karakter di dalam teks.

ii. Kriptografi Modern

Algoritma kriptografi modern beroperasi pada mode bit, yang berarti semua data dan informasi (baik kunci, *plaintext*, maupun *ciphertext*) dinyatakan dalam rangkaian (*string*) bit biner (0 dan 1), seperti algoritma enkripsi dan algoritma dekripsi. [12] Rangkaian bit yang menyatakan *plaintext* dienkripsi menjadi *ciphertext* dalam bentuk rangkaian bit, dan demikian juga sebaliknya. Sehingga dapat dikatakan muara dari kriptografi modern adalah menyediakan kemanan pesan di dalam jaringan komputer.

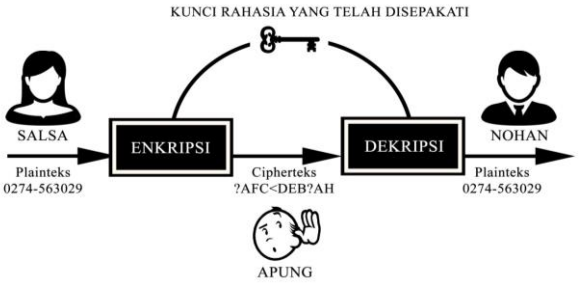
Kriptografi modern memggunakan algoritma yang digunakan untuk penyandian, *kunci y*ang tergolong dalam kriptografi modern antara lain :

(a) Kriptografi Kunci Simetrik

Algoritma kunci simetrik mengacu pada metode enkripsi di mana pengirim dan penerima memiliki kunci yang sama. Algoritma kunci simterik modern beroperasi dalam metode bit dan dapat di kelompokkan menjadi dua kategori :

- Kriptografi *Cipher* Aliran :
  (a) Algoritma RC4 (ARCFOUR)
  (b) Algoritma A5

- Kriptografi *Cipher* Blok (*Block Cipher*) :
  (a) *Data Encryption Standard*
  (b) *Advanced Encryption System*

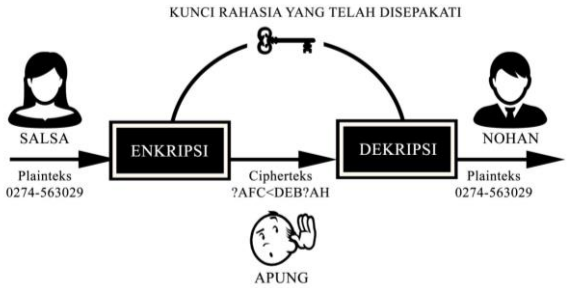


Gambar 2.2 Kriptografi Kunci Simetrik

Sumber : Emy Setyaningsih, S.Si., M.Kom (2015:13)

(b) **Kriptografi Kunci Asimetrik**

Algoritma asimetrik di desain sedemikian rupa sehingga kunci yang digunakan untuk enkripsi berbeda dari kunci yang digunakan untuk dekripsi



Gambar 2.3 Kriptografi Kunci Asimetrik
Sumber : Emy Setyaningsih, S.Si., M.Kom (2015:16)

DES

Pengertian *m*etode DES merupakan salah satu dari kriptografi modern. DES atau *Data Encryption Standard* atau dikenal juga sebagai *Data Encryption Algorithm* (DEA) oleh ANSI (*American National Standards Institute*) dan DEA-1 oleh ISO (*International Organization for Standardization)* merupakan algoritma kriptografi kunci simetrik (menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi) yang paling umum digunakan saat ini.

Algoritma atau *Data Encryption Standard* (DES) dibuat di IBM (*International Business Machines* dengan istilah Algoritma Rijndael, merupakan sebuah algoritma *cipher* blok yang menggunakan teknik substitusi, permutasi, dan sejumlah putaran pada setiap blok yang akan di enkripsi. Sistem permutasi dan substitusi (S-*box*) yang digunakan pada AES tidak menggunakan jaringan Feistel sebagaimana *cipher* blok pada umumnya.

Corporation - perusahaan Amerika Serikat yang memproduksi dan menjual perangkat keras dan perangkat lunak komputer) dan merupakan modifikasi dari algoritma terdahulu yang bernama Lucifer. Lucifer merupakan algoritma *cipher* blok yang beroperasi pada blok masukan 64 bit dan kuncinya berukuran 128 bit. Pengurangan jumlah bit kunci pada DES dilakukan dengan alasan agar mekanisme algoritma bisa diimplementasikan dalah satu *chip*. Horst Feistel merupakan salah satu periset yang mula-mula mengembangkan atau *Data Encryption Standard* (DES) ketika bekerja di IBM Watson Laboratory di Yorktown Heights, New York. Dan atau *Data Encryption Standard* (DES) baru secara resmi digunakan oleh pemerintah Amerika Serikat pada tahun 1977.

Algoritma atau *Data Encryption Standard* (DES) terbagi menjadi tiga kelompok, yaitu pemrosesan kunci, enkripsi data 64 bit, dan dekripsi data 64 bit, di mana kelompok yang satu dengan yang lain saling berinteraksi dan terkait. Algoritma atau *Data Encryption Standard* (DES) dirancang untuk mengenkripsi dan mendekripsi data dalam blok data yang terdiri atas 64 bit di bawah kontol kunci 64 bit. Dekripsi data harus dikerjakan menggunakan kunci yang sama dengan yang dipakai untuk mengenkripsi data, dengan penjadwalan alamat kunci bit yang diubah sehingga proses membaca merupakan kebalikan dari proses menulis.

AES

Pengertian *Advanced Encryption Standard* (AES) atau yang awal nya dikenal

Algoritma Rijndael pertama kali dikenal oleh masyarakat hasil kemenangan kontes algoritma kriptografi pengganti atau *Data Encryption Standard* (DES) pada November 2001 yang diadakan di

Amerika Serikat, yang kemudian mengalami beberapa proses standarisasi oleh NIST (*National Institute of Standards and Technology*, adalah sebuah badan non-regulator dari bagian Administrasi Teknologi dari Departemen Perdagangan Amerika Serikat) yang kemudian barulah diadopsi menjadi standar algoritma kriptografi secarra resmi pada 22 Mei 2002.

Enkripsi

Enkripsi (*encryption*) adalah proses untuk menyandikan *plaintext* menjadi *ciphertext*.

Proses enkripsi :

$C = E_e (M)$

Keterangan :

M : pesan asli (*plaintext*)
E : proses enkripsi
C : pesan dalam bahasa sandi
E : kunci enkripsi

Dekripsi

Dekripsi (*decryption*) adalah proses untuk memperoleh kembali *plaintext* dari *ciphertext*.

Proses enkripsi :

$C = D_d (M)$

Keterangan :

M : pesan asli (*plaintext*)
D : proses dekripsi
C : pesan dalam bahasa sandi
D : kunci dekripsi

***Class Responsibility Collaborator* (CRC**

CRC pada awalnya diperkenalkan oleh Kent Beck dan Ward Cunningham sekitar tahun 1989 sebagai kelengkapan pemrograman berorientasi objek. CRC sebagai cikal bakal yang menjadi kelas pada saat tahap analisis. CRC digunakan untuk pemetaan (membangun) kelas-kelas yang akan digunakan pada diagram *use case*, diagram kelas, dan diagram objek.

***Entity Relationship Diagram* (ERD)**

Pengertian *Entity Relationship Diagram* (ERD) merupakan landasan teori dari model data. Hubungan data ini dapat digambarkan secara grafis menggunakan diagram hubungan entitas (ERD). ERD awalnya dikenalkan kepada masyarakat oleh Peter Chen [Che77] untuk merancang sistem database relasional dan telah diperepanjang oleh yang lain. Komponen utama ERD antara lain : objek data, atribut, hubungan, dan berbagai jenis indikator. Tujuan utama ERD adalah untuk merepresentasikan objek data dan hubungannya.

Website

Web terdiri dari kumpulan dokumen elektronik di seluruh dunia. Setiap dokumen elektronik di web disebut halaman web (*webpage*), yang dapat berisi teks, grafik, audio, dan video. Dan kumpulan laman web yang terkait, yang disimpan di server web ini yang disebut dengan situs web (*website*). Laman web sering berisi tautan (*link*). Sebuah link, kependekan dari *hyperelink*, adalah koneksi *built-in* dengan dokumen, grafik, file audio, video, halaman web, atau situs web.

***Model-View-Controller* (MVC)**

Model-View-Controller (MVC) adalah sebuah konsep yang diperkenalkan untuk meng-enkapsulasi data bersama dengan pemrosesan (*model*), mengisolasi dari proses manipulasi (*controller*) dan tampilan (*view*) untuk direpresentasikan pada sebuah user interface. MVC mengikuti pendekatan yang paling umum dari *Layering*. *Layering* hanyalah sebuah logika yang membagi kode kita ke dalam

fungsi di kelas yang berbeda. Pendekatan ini mudah dikenal dan yang paling banyak diterima. Keuntungan utama dalam pendekatan ini adalah penggunaan yang (*reusability*) kode.

i. *Model*

Model, digunakan untuk mengelola informasi dan memberitahu pengamat ketika ada perubahan informasi. Hanya *model* yang mengandung data dan fungsi yang berhubungan dengan pemrosesan data. Sebuah *model* meringkas lebih dari sekedar data dan fungsi yang beroperasi di dalamnya. Pendekatan *model* yang digunakan untuk komputer *model* atau abstraksi dari beberapa proses dunia nyata. Hal ini tidak hanya menangkap keadaan proses atau sistem, tetapi bagaimana sistem bekerja. Sebagai contoh, programmer dapat menentukan *model* yang menjembatani komputasi *back-end* dengan *front-end* GUI (G*raphical Uuser Interface*).

ii. *View*

View, bertanggung jawab untuk pemetaan grafis ke sebuah perangkat. View biasanya memiliki hubungan 1-1 dengan sebuah permukaan layar dan tahu bagaimana untuk membuatnya. *View* melekat pada *model* dan me-render isinya ke permukaan layar. Selain itu, ketika *model* berubah, *view* secara otomatis menggambar ulang bagian layar yang terkena perubahan untuk menunjukkan perubahan tersebut. Terdapat kemungkinan beberapa *view* pada *model* yang sama dan masing-masing *view* tersebut dapat merender isi *model* untuk permukaan tampilan yang berbeda.

iii. *Controller*

Controller, menerima masukan (*input*) dari pengguna dan menginstruksikan *model* dan *view* untuk melakukan aksi berdasarkan masukan tersebut. Sehingga, *controller* bertanggung jawab untuk pemetaan aksi pengguna akhir terhadap respon aplikasi. Sebagai contoh, ketika pengguna mengklik tombol atau memilih item menu, *controller* bertanggung jawab untuk menentukan bagaimana aplikasi seharusnya merespon.

Penulis menggunakan metode *eXtreme Programming* atau yang lebih dikenal dengan sebutan XP. Pengertian XP (*eXtreme Programming*) merupakan metode yang paling dikenal atau paling banyak digunakan dalam metode *agile*. [4] Penamaan ini diciptakan oleh Kent Beck (2000) karena pendekatan ini dikembangkan dengan *practice* yang bagus seperti *iterative development*, sampai ke level *extreme*, yang dimana dibagi ke dalam empat tahapan, yaitu :

i. *Planning* (Perencanaan)

Tahap ini dimulai dengan pemahaman konteks bisnis dari aplikasi, mendefinisikan keluaran (*output*), fitur yang ada pada aplikasi, fungsi dari aplikasi yang dibuat, penentuan waktu dan biaya pengembangan aplikasi, serta alur pengembangan aplikasi.

ii. *Design* (Perancangan)

Tahap ini menekankan pada desain aplikasi secara sederhana. Alat untuk mendesain pada tahap ini dapat menggunakan kartu CRC (*Class Responsibility Collabolator*). CRC digunakan untuk pemetaan (membangun) kelas-kelas yang akan digunakan pada diagram *use case*, diagram kelas, dan diagram objek.

Berikut dePenelitian tentang kartu CRC:

a. Nama kelas (*Class Name*): memberikan nama kelas.
b. Kelas Induk (*Superclass*): merupakan kelas induk (orang tua) dalam konsep pewarisan yang akan dibuat CRC-nya.
c. Kelas turunan (*Subclass*): merupakan kelas anak dalam konsep pewarisan yang akan dibuat CRC-nya.
d. Tanggung Jawab (*Responsibilities*): atribut, operasi (*methods*) yang ada pada kelas yang dibuat CRC-nya.
e. Kelas terkait (*Collabolators*): kelas yang terkait dengan kelas yang dibuat CRC-nya tetapi bukan kelas induk (orang tua) atau kelas anak (turunan).

iii. *Coding* (Pengkodean)

Hal utama dalam pengembangan aplikasi dengan menggunakan XP adalah *pair programming* (dalam membuat program melibatkan 2 atau lebih programmer).

iv. *Testing* (Pengujian)

Tahap ini memfokuskan pada pengujian fitur-fitur yang ada pada aplikasi sehingga tidak ada kesalahan (error) dan aplikasi yang dibuat sesuai dengan proses bisnis pada klien (pelanggan).[15]

Untuk pengumpulan data mengenai studi kasus ini penulis melakukan studi pustaka.

3. Metode Penelitian

Teknik Analisis Data

Pada penelitian ini, penulis menggunakan metodologi penelitian kualitatif. Metode penelitian kualitatif adalah metode penelitian yang berlandaskan pada filsafat postpositivisme (aliran yang ingin memperbaiki kelemahan pada positivisme), digunakan untuk meneliti pada kondisi obyek yang alamiah, dimana peneliti adalah sebagai instrumen kunci, teknik pengumpulan data dilakukan secara gabungan, analisis data bersifat induktif / kualitatif, dan hasil penelitian kualitatif lebih menekankan makna dari pada generalisasi.

Penelitian ini menggunakan teknik analisis dan metodologi kualitatif dikarenakan data yang penulis kumpulkan tidaklah berupa angka dan dalam penarikan kesimpulan data tidak menggunakan rumus tertentu seperti pada metode kuantitatif. [14]

Tiga komponen analisis dari metodologi kualitatif antara lain :

i. Reduksi Data

Reduksi data dapat diartikan sebagai proses pemilihan, pemusatan perhatian pada penyederhanaan data yang muncul dari catatan-catatan tertulis dari data yang diperoleh. Reduksi data merupakan suatu bentuk analisa yang menajam, menggolongkan, mengarahkan, membuang data yang tidak perlu.

ii. Penyajian Data

Penyajian data dibatasi sebagai kumpulan informasi tersusun yang memberi kemungkinan adanya penarikan kesimpulan dan pengambilan tindakan. Dengan penyajian tersebut akan dapat memahami apa yang harus dilakukan, menganalisis apakah tindakan berdasarkan pemahaman yang didapat dari penyajian-penyajian tersebut.

iii. Penarikan Kesimpulan

Penarikan kesimpulan hanyalah sebagian dari suatu kegiatan konfigurasi yang utuh. Kesimpulan awal yang dikemukakan masih bersifat sementara, dan akan mengalami perubahan apabila tidak ditemukannya bukti-bukti yang kuat dan mendukung pada tahap pengumpulan data

berikutnya. Dengan demikian kesimpulan dalam penelitian kualitatif mungkin dapat menjawab rumusan masalah yang dirumuskan sejak awal, tetapi mungkin juga tidak. Masalah dan rumusan masalah dalam penelitian kualitatif masih bersifat sementara dan akan berkembang setelah peneliti berada di lapangan.

Teknik Pengumpulan Data

Dalam rangka pengumpulan data dalam pembuatan penelitian tentunya penulis mengumpulkan data kemudian memiliki dugaan berdasarkan teori yang penulis gunakan, yang dimana dugaan ini disebut dengan "hipotesis". Untuk membuktikan hipotesis secara empiris, seorang peneliti membutuhkan pengumpulan data untuk diteliti secara lebih mendalam, antara lain dengan pendekatan :

i. Primer

Berikut merupakan teknik pengumpulan data primer yang penulis gunakan dalam menyusun laporan ini :

a. Observasi Langsung

Teknik pengumpulan data dengan observasi langsung adalah teknik pengumpulan data dengan cara mengamati secara langsung proses sistem yang berjalan di PT.One Standard Group PTE LTD, yang dilakukan sejak April 2017 bersamaan dengan proses magang kerja berlangsung. Hal ini dilakukan untuk memahami pada bagian mana kekurangan sistem yang sedang berjalan untuk kemudian dikembangkan.

ii. Sekunder

Berikut merupakan teknik pengumpulan data sekunder yang penulis gunakan dalam menyusun laporan ini :

a. Tinjauan Pustaka

Teknik yang penulis gunakan dalam pengumpulan data-data sebagai landasan teori dalam penelitian yang dilakukan yaitu dengan meninjau kembali pustaka-pustaka yang berkaitan dengan penelitian yang dilakukan.

4. Hasil dan Pembahasan

Dari pembuatan laporan ini maka penulis memperoleh hasil bahwa algoritma kriptografi metode *Advanced Encryption System* (AES) lebih aman dibandingkan algoritma kriptografi metode *Data Encryption Standard* (DES) dikarenakan metode AES memiliki keamanan ganda yang dimana memiliki block size yang lebih besar yaitu 128 bit dibandingkan dengan metode DES yang hanya 64 bit, namun dari efisiensi segi waktu maka algoritma kriptografi metode DES lebih efisien.

Factor	DES	AES
Panjang *Key*	56 bits	128, 192 or 256 bits
Block Size	64 bits	128, 192, or 256 bits
Cipher Text	*Symmetric block cipher*	*Symmetric block cipher*
Developed	1977	2000
Security	Proven inadequate	Considered secure
Possible keys	2^{56}	2^{128},2^{192} and 2^{256}
Possible ASCII printable character key	95^{7}	95^{16}, 95^{24} or 95^{32}

5. Kesimpulan

Berdasarkan pembuatan laporan Penelitian ini penulis telah sedikit banyak menyajikan dan mengutip informasi mengenai pentingnya keamanan informasi dengan memanfaatkan algoritma kriptografi, terutama dengan metode AES (*Advanced Encryption* Standard) dan metode DES (*Data Encryption Standard*). Dan dari penulisan ini penulis mengambil kesimpulan bahwa :

i. Sistem yang dibuat dapat menyelesaikan permasalahan yang ada dan memberikan informasi mengenai pentingnya menjaga keamanan informasi dalam pengiriman informasi terutama menjaga keamanan pada sisi keamanan informasi user dari sebuah perusahaan.
ii. Sistem yang dibuat ini memberikan informasi kepada pembaca mengenai sistem keamanan algoritma kriptografi dan pentingnya kemanan informasi, terutama dengan metode *Data Encryption Standard* (DES) dan *Advanced Encryption System* (AES).
iii. Sistem yang dibuat ini memberikan informasi kepada pembaca mengenai perbandingan efisiensi waktu dan keamanan yang lebih aman antara sistem keamanan algoritma kriptografi *Data Encryption Standard* (DES) dan *Advanced Encryption System* (AES).

6.Daftar Pustaka

Basri (2016), Kriptografi Simetrik dan Asimetrik dalam Prespektif Keamanan Data dan Kompleksitas Komputasi, Jurnal Ilmiah Ilmu Komputer - Vol. 2, No. 2.

Fathansyah (2015), Basis Data, Revisi ke – 2, Bandung: Informatika Bandung.

Hasrul, Lamro Herianto S. (2016) , Penerapan Teknik Kriptografi pada Database Menggunakan Algoritma *One Time Pad*, Jurnal Elektronik Sistem Informasi dan Komputer, Vol.2 No.2.

Ian, Sommerville (2011), *Software Engineering* (*ninth edition*), Pearson Education, Inc.

Levitin, Anany (2012) , *Introduction to The Design and Analysis of Algorithms*, *Third Edition*, Pearson Education, Inc.

Marakas dan O'Brien (2013) , *Introduction to Information Systems, Sixteenth Edition.*Mc Graw Hill, New York – USA.

Marakas dan O'Brien (2011), *Management Information Systems, Tenth Edition.*Mc Graw Hill, New York – USA.

Megah Mulya (2013), Perbandingan Kecepatan Algoritma Kriptografi Asimetri, *Journal of Research in Computer Science and Applications* - Vol. I, No. 2.

Pressman, Roger S. (2015) , *Software Engineering : a practitioner's approach (Eighth Edition),* McGraw-Hill Education.

Rahardjo, Budi (2002) , *Kemanan Sistem Informasi Berbasis Internet,* PT.Insan Indonesia-Bandung & PT INDOCISC - Jakarta.

Santiago Pericas-Geertsen, Manfred Riem (2015) , MVC : *Model, View, Controller* API, *Oracle Corporation*.

Setyaningsih, Emy (2015) , *Kriptografi & Implementasinya menggunakan MATLAB,* CV.Andi *Offset*.

Simanjuntak, Pastima dan Arwin Kasnady (2016) , Analisis *Model View Controller* (MVC) pada Bahasa PHP, Jurnal ISD Vol.2 No.2.

Sugiyono (2016), Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta.

Suryantara, I. Gusti Ngurah (2017), Merancang Aplikasi dengan Metodologi *Exteme Programmings*, PT.Elex Media Komputindo.

Vermaat, dkk. (2016) , *Discovering Computer : Tools, Apps, Devices, and the Impact of Technology, Cengage Learning*.