BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

"Dialah Allah Yang tidak ada *Illah* (Yang Haq) selain dia, Raja, Yang Maha Suci, Yang Maha Sejahtera, Yang Mengaruniakan Keamanan, Yang Maha Memelihara, Yang Maha Perkasa, Yang Maha Kuasa, Yang Maha Memiliki segala Keagungan, Maha Suci Allah dari apa yang mereka persekutukan. (Qs.Al-Hashr:23)

Ayat diatas menjelaskan bahwa keamanan merupakan jaminan oleh Allah kepada hamba-Nya. Maka dari itu sudah menjadi kewajiban sebagai hamba Allah kita menyerahkan semuanya kepada Allah (*Tawakkal*), akan tetapi disamping kita bertawakkal kita juga harus tetap berusaha (*Ikhtiyar*).

Semakin berkembangya zaman, semakin berkembang pula teknologi yang ada seperti media sosial, *ecommerce*, *egovernment*, dan masih banyak lagi. Keamanan dan kerahasiaan Data sangatlah penting untuk dijaga karena data yang dimasukkan pengguna diantaranya data pribadi, data perusahaan, data instasi dan data lainnya. Keamanan data sangat diperlukan untuk mengatasi pencurian dan penyalahgunaan. Keamanan data ini meliputi beberapa aspek diantaranya: *private* (kerahasiaan), *integrity* (konsisten), *authenticity* (keaslian), *availability* (ketersediaan), dan *access control* [1]. Banyak sekali metode untuk mengamankan data yang salahsatunya metode kriptografi.

Kriptografi merupakan salah satu metode dalam pengamanan data, kriptografi menyamarkan suatu data menjadi kode yang bisa dilihat namun

tidak bisa dimengerti kecuali si pembaca bisa memecahkan kode tersebut. Kriptografi mengolah informasi awal (*plaintext*) menjadi informasi baru yang tidak dapat dibaca oleh bahasa manusia(*ciphertext*) [2]. Adapun penamaan proses tersebut adalah proses enkripsi sedangkan proses kebalikannya adalah proses dekripsi.

Dalam bidang ilmu kriptografi terdapat banyak algoritma untuk mengamankan data. Algoritma kriptografi terbagi menjadi algoritma klasik dan algoritma modern, juga algoritma kunci simetris dan kunci asimetris. Salah satu algoritma klasik dan menggunakan kunci simetris yaitu algoritma *One time pad*. *One time pad* adalah algoritma yang sempurna dan belum terpecahkan sehingga diberi gelar *Unbreakble Cipher*. *One time pad* menggunakan satu kunci untuk satu *plaintext* dan untuk *plaintext* berikutnya menggunakan kunci lain yang telah disediakan dengan metode pengacakan (*random key*) [3]. Untuk mengacak kunci, digunakan metode *cryptographically secure pseudorandom number generator* (CSPRNG) yaitu metode pengacakan yang dinilai paling kompleks dan cocok untuk digunakan sebagai kunci sekali pakai [4].

Layanan login merupakan portal yang menghubungkan pegguna dengan sistem yang dimasukinya, keefisienan suatu layanan login menentukan kenyamanan pengguna dalam menggunakannya. Banyak terjadi pencurian data pada layanan login. Diantaranya, para pencuri menggunakan berbagai macam metode seperti *Sniffing, Replay Attack, Spoofing, dan Man in the middle* [5]. Selain itu, pecurian data juga terjadi ketika para pencuri berhasil memecahkan kunci yang digunakan untuk mengenkripsi data.

Berdasarkan uraian diatas, untuk mengamankan data pengguna, penulis bertujuan untuk mengimplementasikan algoritma kripografi *One Time Pad* (OTP) untuk layanan otentikasi dalam bentuk Tugas Akhir dengan judul "**Implementasi Algortima *One Time Pad* (OTP) Untuk Layanan Otentikasi Web**".

1.2 Perumusan Masalah

1. Bagaimana cara mengimplementasikan algoritma *One Time Pad* untuk layanan otentikasi pada web?
2. Bagaimana tingkat keunikan *password* yang dihasilkan?

1.3 Batasan Masalah

1. Layanan otentikasi yang digunakan yaitu layanan login pada web.
2. Parameter keberhasilan adalah keamaan pada layanan otentikasi.
3. Algortima yang digunakan adalah algortima enkripsi *One Time Pad*.
4. Metode untuk membangkitkan kunci yang digunakan adalah *metode* CSPRNG (*cryptographically secure pseudorandom number generator*).
5. Metode otentikasi yang digunakan adalah *password* sekali pakai.
6. Metode perancangan berbasis orientasi objek.

1.4 Tujuan Penelitian

1. Mengimplementasikan algortima *One Time Pad* untuk layanan otentikasi pada web.
2. Membangun sistem otentikasi yang dapat menjaga keamanan data pengguna.
3. Mengetahui tingkat keunikan *password* yang dihasilkan.

1.5 Manfaat Penelitian

Penelitian ini bermanfaat untuk menghasilkan sebuah sistem otentikasi yang dapat menjaga keamanan data pengguna dengan mengimplementasikan algoritma *one time pad*.

1.6 Kerangka Pemikiran

Tabel 1. 1 Kerangka Pemikiran

Problem
Keamanan otentikasi harus lebih diperhatikan karena bebagai penyerangan terus terjadi. Oleh karena itu, Dalam proses otentikasi akan lebih aman apabila digunakan algortima kriptografi yang kuat bahkan belum terpecahkan.
↓
Opportunities
Dengan mengimplementasikan algoritma *one time pad* pada layanan otentikasi maka akan lebih terjamin keamanannya karena algoritma *one time pad* belum terpecahkan.
↓
Approach
Analisis dan implementasi algoritma *one time pad* untuk layanan otentikasi web.
↓
Software Development
SDLC : *Rapid Application Development*, Perancangan : *UML*, Bahasa : *PHP*, *Javascript*
↓
Software Implementation
Aplikasi berbasis web yang dibangun menggunakan Bahasa pemrograman php, *framework* laravel, dan *database* Mysql.
↓
Result
Aplikasi keamanan untuk layanan otentikasi web.

1.7 Metodologi Penelitian

1.7.1 Tahap Pengumpulan Data

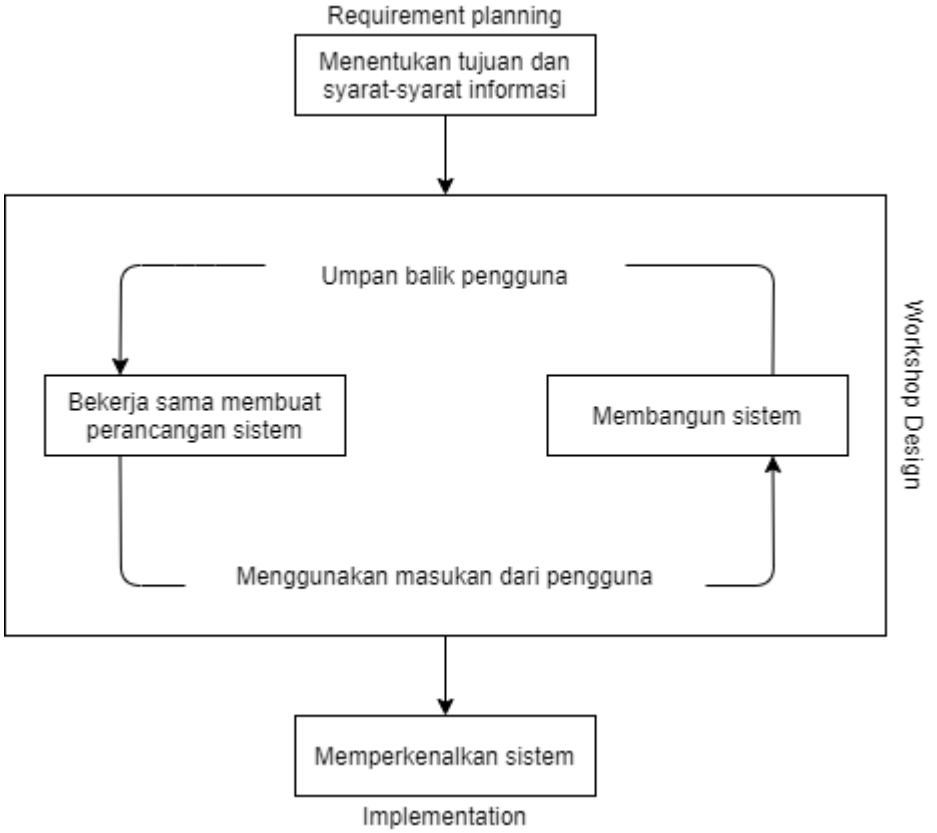
Pengumpulan data untuk peneilitian ini menggunakan sebuah metode penelitian deskriptif, metode ini memiliki tujuan untuk memberikan gambaran permasalahan secara objektif atau lengkap. Berikut metode pengumpulan data yang digunakan pada penelitian ini:

a. Wawancara, merupakan kegiatan interaksi secara dengan narasumber langsung untuk mendapatkan informasi. Dalam kegiatan ini narasumber merupakan masyarakat umum dan orang yang ahli dalam bidang penelitian yang berkaitan.
b. Observasi, merupakan pengamatan terhadap objek bidang penelitian yang dilakukan secara langsung untuk mendapatkan data-data yang dibutuhkan.
c. Studi Literatur, merupakan kegiatan pengumpulan data yang dilakukan secara tertulis dari beberapa sumber seperti studi ilmiah , kajian literatur dan laporan penelitian yang berkaitan dengan bidang yang diteliti.

1.7.2 Tahap Pengembangan Sistem

Model pengembangan perangkat lunak yang dipakai pada penelitian ini menggunakan model *Rapid Application Development* (RAD). Model RAD dipilih karena dinilai cocok dengan melihat aplikasi yang dikembangkan adalah aplikasi yang tidak membutuhkan waktu yang lama dalam pengerjaannya dan sangat sederhana, model RAD adalah model yang diperuntukkan untuk pengembangan aplikasi

yang bisa dikerjakan dalam jangka waktu pendek, berikut adalah gambar model RAD yang terlihat pada gambar 1.1:



Gambar 1. 1 Model Pengembangan RAD

Adapun proses pengembangan metode RAD ini dapat dijelaskan sebagai berikut [6]:

a. *Requirement planning*

Pada tahap pertama, aplikasi atau persyaratan sistem ditentukan sebelumnya oleh pengembang untuk menentukan tujuan, batasan sistem, batasan, dan alternatif solusi untuk masalah tersebut. Analisis

digunakan untuk mengetahui perilaku sistem dan mengetahui aktivitas apa saja yang ada di dalam sistem.

b. *Workshop Design*

Tahapan ini merupakan tahapan mencari alternatif solusi dan memilih solusi terbaik untuk masalah desain dan perawatan. Pengembang melakukan desain proses bisnis dan desain program untuk data yang telah diperoleh dan dimodelkan dalam arsitektur sistem informasi. *Tools* yang digunakan dalam pemodelan sistem biasanya menggunakan Unified Modeling Language (UML).

c. *Implementation*

Pada tahap ini dilakukan implementasi atau pengkodean sistem. Menyelesaikan implementasi dengan melihat aktivitas yang dilakukan yaitu menentukan lingkungan implementasi perangkat lunak, perancangan basis data, pemrograman dan antarmuka. Kemudian hasil yang didapat akan menjadi *database* utama dan kode program sehingga sistem atau aplikasi tersebut dapat digunakan.

1.8 Sistematika Penulisan

Sistematika penyusunan laporan tugas akhir ini disusun ke dalam lima bab sebagai berikut:

BAB I PENDAHULUAN

Bab pertama merupakan pendahuluan atau deskripsi masalah, yang akan dibahas pada bab selanjutnya. Bab ini terdiri dari beberapa tema yaitu latar

belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistem penulisan.

BAB II STUDI PUSTAKA

Bab kedua adalah penjelasan teori-teori yang berkaitan dengan penelitian, yang akan digunakan dalam implementasi perancangan dan sistem. Bab ini juga berisi tentang *state of the art* yang merupakan penjelasan dari penelitian sebelumnya terkait dengan penelitian penulis.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ketiga membahas tentang analisis dan desain sistem berdasarkan pertanyaan yang diajukan pada bab sebelumnya.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab keempat membahas tentang persyaratan pengembangan aplikasi, implementasi pengembangan aplikasi, spesifikasi aplikasi dan pengujian aplikasi.

BAB V PENUTUP

Bab ini merinci kesimpulan hasil penelitian yang tertulis pada bagian abstrak dokumen, serta menyarankan penelitian lebih lanjut terkait penelitian penulis.