BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Internet adalah teknologi yang berkembang sangat pesat. Keberadaannya sangat melekat pada kehidupan sehari-hari, baik itu pekerjaan, hiburan, maupun sesuatu yang pribadi. Tidak hanya di kota besar, kini *internet* mulai menyebar hingga ke desa. Dan tidak hanya secara konvensional menggunakan *Personal Computer* (PC) dengan modem, *internet* kini bisa diakses menggunakan *notebook* melalui *hotspot* ataupun menggunakan telepon seluler.

Seiring berkembangnya teknologi *internet*, teknologi *website*, sebagai *interface* yang menjembatani antara pengguna dan dunia maya, juga ikut berkembang. Berbagai macam bahasa pemrograman *web* digunakan, dan semakin lama semakin disempurnakan mengikuti perkembangan teknologi-teknologi yang berkaitan. *Web design* juga tak kalah berkembangnya, menjadikan dunia maya lebih menarik. Penggunaan aplikasi berbasis *web* sedang popular pada saat ini, karena perancangan, pembangunan, dan pengimplementasian serta penggunaan aplikasi berbasis *web* dirasa lebih mudah. Juga tergolong lebih mudah dalam hal perubahan dan pengembangan.

Begitu luasnya daerah yang bisa dijangkau oleh *internet*, sehingga dapat dipergunakan untuk penyebaran informasi, transaksi, dan penyimpanan data secara *online*. Penyimpanan *file* secara *online* sudah banyak dilakukan. Teknik ini mempermudah proses pengaksesan data karena tidak dibatasi kapan dan dimana kita membutuhkan *file* tersebut. Tidak lagi memerlukan tempat menyimpan data

dengan kapasitas besar yang harus dibawa kemana-mana. Hanya memerlukan koneksi *internet* dan langsung dapat mengakses *file* yang diinginkan, kapan saja, dimana saja. Telah banyak situs-situs yang menawarkan jasa penyimpanan data secara *online*, baik yang berbayar maupun yang gratis. Namun untuk yang gratis biasanya mendapatkan fasilitas yang lebih terbatas.

Data yang disimpan secara *online* tidak sepenuhnya aman. Padahal keamanan data yang disimpan secara *online* mutlak diperlukan. Mulai dari keamanan dari perubahan oleh yang tidak berhak merubahnya, hingga keamanan dari pencurian data tersebut. Terutama untuk data-data yang sifatnya rahasia, hanya pihak-pihak tertentu saja yang memiliki wewenang mengakses data tersebut. Biasanya, situs-situs penyimpanan data *online* memberikan keamanan penyimpanan data berupa pembatasan akses data menggunakan akun yang dilindungi dengan kata kunci. Namun pada dasarnya sistem ini masih belum aman sepenuhnya, karena data akun dapat di-*hack* oleh orang-orang yang berusaha mengambil data tersebut.

Kriptografi merupakan salah satu teknik pengamanan data dengan cara menyandikan data tersebut (enkripsi data dari plainteks menjadi cipherteks) menggunakan algoritma kriptografi tertentu dengan kunci (*key*) tertentu. Algoritma kriptografi yang sama digunakan pula untuk mengembalikan data yang telah disandikan menjadi kembali seperti semula (proses dekripsi). Kunci, berupa string yang sifatnya rahasia. Hanya pihak-pihak tertentu yang memiliki hak untuk mengakses *file* yang boleh mengetahui kunci ini, sehingga pihak-pihak yang tidak

memiliki kunci yang benar tidak akan bisa menggunakan atau membaca data tersebut.

Banyak ragam dari algoritma kriptografi, baik klasik maupun modern. Baik itu bersifat simetris maupun asimetris. Salah satunya adalah algoritma kriptografi *Vertical Bit Rotation* (VBR), yang merupakan algoritma kriptografi yang terklasifikasi dalam algoritma kriptografi modern, namun memiliki kesederhanaan seperti algoritma kriptografi klasik, sehingga sangat cocok diterapkan dalam enkripsi data yang akan disimpan secara *online*.

Algoritma kriptografi VBR merupakan algoritma kriptografi yang baru. Saat ini belum ada penelitian khusus terhadap algoritma kriptografi VBR sehingga belum diketahui sejauh mana tingkat keamanan algoritma kriptografi VBR tersebut. Untuk menilai tingkat keamanan sebuah algoritma kriptografi dapat menggunakan banyak cara. Salah satunya adalah dengan menghitung nilai *avalanche effect* dari data yang telah dienkripsi menggunakan algoritma kriptografi tersebut. Dengan mengetahui nilai *avalanche effect* dapat disimpulkan tingkat keamanan dari algoritma kriptografi tersebut.

Bila ingin menyimpan data secara *online* dengan menggunakan teknik kriptografi, biasanya data tersebut dienkripsi terlebih dahulu menggunakan perangkat lunak tertentu, lalu disimpan pada penyimpanan data *online*. Namun alangkah lebih mudah bila seseorang yang ingin menyimpan data secara *online* dengan teknik kriptografi tanpa perlu memasang (*install*) perangkat lunak untuk mengenkripsi terlebih dahulu. Hal ini bisa terjadi bila proses enkripsi data terjadi

di *server*, sehingga data yang disimpan tidak perlu dienkripsi terlebih dahulu, namun tersimpan dalam bentuk terenkripsi (cipherteks).

1.2 Identifikasi Masalah

Karena terdapat masalah-masalah seperti yang telah dipaparkan pada latar belakang, yaitu :

1. data yang disimpan secara *online* tidak sepenuhnya aman, karena masih bisa diambil oleh pihak-pihak yang tidak memiliki hak dengan cara menembus keamanan yang telah dibuat,
2. diperlukan sebuah aplikasi berbasis web untuk menyimpan data dengan enkripsi menggunakan algoritma kriptografi secara *online*, sehingga tidak diperlukan perangkat lunak lain untuk melakukan enkripsi sebelum melakukan penyimpanan secara *online*,
3. belum diketahui sejauh mana tingkat keamanan algoritma kriptografi Vertical Bit Rotation (VBR), karena belum ada pengujian secara resmi,

maka diperlukan sebuah aplikasi dapat membantu memecahkan masalah-masalah tersebut.

Oleh karena itu dapat dirumuskan masalah bagaimana membangun Aplikasi Penyimpanan *File Online* Dengan Enkripsi Menggunakan Modifikasi Algoritma *Vertical Bit Rotation* (VBR) 32 Bit, serta melakukan penelitian lebih lanjut mengenai tingkat keamanan dari algoritma kriptografi *Vertical Bit Rotation* (VBR).

1.3 Maksud dan Tujuan

Dari masalah-masalah yang telah dirumuskan, dimaksudkan untuk membuat sebuah Aplikasi Penyimpanan *File Online* Dengan Enkripsi Menggunakan Modifikasi *Algoritma Vertical Bit Rotation* (VBR) 32 Bit, serta melakukan penelitian lebih lanjut mengenai tingkat keamanan dari Algoritma kriptografi *Vertical Bit Rotation* (VBR).

Adapun tujuan dari penelitian dan pembuatan aplikasi ini adalah :

1. membuat aplikasi penyimpanan *file online* berbasis *web*,
2. meningkatkan keamanan penyimpanan *file online* dengan enkripsi data menggunakan algoritma kriptografi, yaitu algoritma kriptografi VBR,
3. menganalisa tingkat keamanan algoritma kriptografi VBR dengan menghitung nilai *Avalanche Effect*-nya, melakukan pengembangan dan perbaikan pada algoritma kriptografi VBR agar memiliki tingkat keamanan yang tinggi.

1.4 Batasan Masalah

Aplikasi yang akan dibangun adalah aplikasi berbasis web dengan kemampuan :

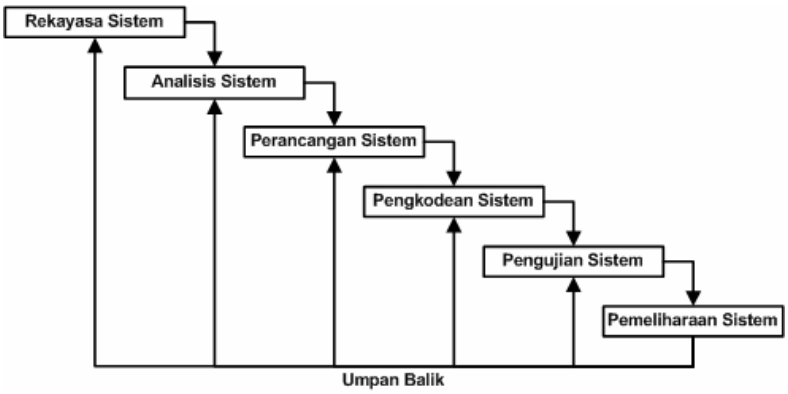
1. menyimpan (*upload*) data berupa *file* pada penyimpanan *file online*,
2. meng-enkripsi *file* pada saat penyimpanan *file online*,
3. mendekripsi *file* ketika *file* tersebut diambil (*download*) dari penyimpanan *file online*,
4. mengambil (*download*) data berupa *file* yang terdekripsi dari penyimpanan *file online*,

5. tidak ada pembatasan tipe *file*, namun akan dibatasi dengan maksimal ukuran sebesar 20 MB,
6. proses enkripsi dan dekripsi *file* menggunakan bahasa pemrograman PHP, menggunakan modifikasi algoritma kriptografi VBR 32 bit.

Untuk pengembangan algoritma kriptografi VBR, tetap menggunakan prinsip-prinsip dasar dari algoritma kriptografi VBR, yaitu perputaran bit secara vertikal, dan dilakukan pengujian menghiung nilai *Avalanche Effect* sebagai parameter tingkat keamanan.

1.5 Metodologi Penelitian

Dalam sebuah penelitian diperlukan sebuah metodologi agar penelitian menjadi lebih sistematis dan terarah, sehingga maksud dan tujuan dari penelitian tersebut dapat tercapai sesuai dengan yang telah direncanakan. Metodologi penelitian ada beberapa macam. Pada penelitian ini akan digunakan salah satu metodologi penelitian. Karena penelitian ini memiliki rentang waktu yang terbatas dan relatif pendek, serta memiliki waktu-waktu *deadline*, maka akan digunakan metodologi penelitian *Waterfall*. Adapun skema dari metodologi penelitian *Waterfall* dapat dilihat seperti pada gambar 1.1.



Gambar 1.1 Skema metodologi penelitian *Waterfall*

Rekayasa Sistem	:	Tahap ini merupakan kegiatan pengumpulan data sebagai pendukung pembangunan sistem serta menentukan ke arah mana aplikasi ini akan dibangun.
Analisis Sistem	:	Mengumpulkan kebutuhan secara lengkap kemudian dianalisis dan didefinisikan kebutuhan yang harus dipenuhi oleh aplikasi yang akan dibangun. Tahap ini harus dikerjakan secara lengkap untuk bisa menghasilkan desain yang lengkap.
Perancangan Sistem	:	Perancangan antarmuka dari hasil analisis kebutuhan yang telah selesai dikumpulkan secara lengkap.
Pengkodean Sistem	:	Hasil perancangan sistem diterjemahkan ke dalam kode-kode dengan menggunakan bahasa pemrograman yang sudah ditentukan. Aplikasi yang dibangun langsung diuji baik secara unit.
Pengujian Sistem	:	Penyatuan unit-unit program kemudian diuji secara keseluruhan.
Pemeliharaan Sistem	:	Mengoperasikan aplikasi dilingkungannya dan melakukan pemeliharaan, seperti penyesuaian atau perubahan karena adaptasi dengan situasi yang sebenarnya.

Umpan Balik : Merupakan respon dari pengguna sistem yang bisa digunakan untuk mengetahui sejauh mana aplikasi yang dibangun diterima oleh penggunanya.

1.6 Sistematika Penulisan

Sistematika penulisan laporan penelitian ini dibagi dalam beberapa bab dengan pokok pembahasan secara umum sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, perumusan masalah, maksud dan tujuan, batasan masalah, metodologi penelitian, sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini akan membahas semua literatur yang menjadi dasar dibangunnya aplikasi ini. Semua teori yang dipakai akan dibahas secara detail dan lengkap.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi analisis kebutuhan dalam membangun aplikasi ini sesuai dengan metode pembangunan perangkat lunak yang digunakan. Selain itu terdapat juga perancangan antarmuka untuk aplikasi yang akan dibangun sesuai dengan hasil analisis yang telah dibuat.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini berisi hasil implementasi dari hasil analisis dan perancangan yang telah dibuat disertai juga dengan hasil pengujian dari aplikasi ini yang dilakukan secara local maupun *online*.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan tentang keseluruhan dari pembangunan aplikasi ini dan saran tentang aplikasi ini untuk penelitian selanjutnya.