BAB I

PENDAHULUAN

I.1. Latar Belakang

Keamanan dalam sebuah informasi merupakan hal yang sangat penting. Dengan adanya keamanan dalam sebuah informasi, maka pengelola informasi akan merasa aman dalam mengelola informasi. Informasi dapat berupa tulisan, gambar, suara dan lain sebagainya. Dalam pengelolaan informasi baik dalam pertukaran informasi, penyimpanan informasi memiliki banyak celah yang memungkinkan pencuri informasi mendapatkan informasi yang mereka butuhkan. Oleh karena itu dibutuhkan sebuah teknik ataupun cara yang dapat mengamankan informasi agar sebuah informasi tersebut tidak dapat di miliki oleh pencuri informasi.

Penulis merekomendasikan sebuah teknik yang disebut kriptografi. Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian kriptografi modern kriptografi adalah ilmu yang berdasarkaan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja terkait dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi. (Sadikin, 2012). Namun untuk menggunakan teknik kriptografi, maka dibutuhkan sebuah metode yang tepat untuk menyandikan sebuah *file.* Oleh karena itu penulis menggunakan metode SHA-512 untuk menyandikan sebuah *file*.

SHA-512 adalah salah satu dari rangkaian algoritma yang diciptakan *United States National Security Agency*. SHA adalah singkatan dari *Secure Hash Algorithm*., SHA-512 menghasilkan digest sebesar 512-bit. Asal-usul SHA-512 adalah dari prinsip-prinsip yang mirip dengan yang digunakan oleh Ronald L. Rivest untuk algoritma MD4 dan MD5. (Azhar, 2012). Dengan latar belakang diatas maka penulis mengambil judul **"Aplikasi Keamanan File Menggunakan Metode SHA-512".**.

I.2. Ruang Lingkup Permasalahan

Ruang lingkup permasalahan yang terdapat pada penelitian ini berdasarkan latar belakang adalah sebagai berikut :

I.2.1. Identifikasi Masalah

Identifikasi masalah dari penulis untuk penelitian ini yaitu :

1. Adanya pencuri informasi yang mengambil data.
2. Kurangnya penerapan metode SHA-512 dalam keamanan sebuah *file*.
3. Sedikitnya Menggunakan aplikasi keamanan *file* menggunakan metode SHA-512.

I.2.2. Perumusan Masalah

Perumusan masalah yang terdapat pada penelitian ini yaitu :

1. Bagaimana mencegah pencuri informasi mengambil data ?
2. Bagaimana menerapkan metode SHA-512 dalam keamanan sebuah *file* ?
3. Bagaimana menghasilkan Aplikasi Keamanan File Menggunakan Metode SHA-512 ?

I.2.3. Batasan Masalah

Agar pembahasan masalah tidak melebar penulis membatasi masalah sebagai berikut:

1. Aplikasi hanya untuk menyandikan *file*.
2. Aplikasi ini tidak dapat mengenkripsi Foto
3. Aplikasi hanya dapat berjalan pada sistem operasi berbasis *windows*.
4. *Input* aplikasi ini sebuah *file* komputer.
5. *Output* aplikasi ini sebuah *file* komputer terenkripsi.
6. Pembuatan Aplikasi ini menggunakan bahasa pemrograman *Visual Basic*
7. Perancangan Aplikasi ini menggunakan pemodelan UML.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Tujuan dari penelitian ini yaitu :

1. Mengamankan sebuah *file* dengan teknik kriptografi.
2. Menerapkan metode SHA-512 dalam keamanan sebuah *file.*
3. Menghasilkan Aplikasi Keamanan File Menggunakan Metode SHA-512.

I.3.2. Manfaat

Manfaat dari penelitian ini yaitu :

1. *File* komputer menjadi lebih aman.
2. Memahami metode SHA-512 dalam keamanan sebuah *file*.
3. Mendapat wawasan dalam pembuatan perangkat lunak kriptografi.

I.4. Metodologi Penelitian

Metode merupakan suatu cara yang sistematik untuk mengerjakan suatu permasalahan. Berikut ini adalah tahapan-tahapan penelitian yang peneliti lakukan untuk menyelesaikan penelitian :

I.4.1. Pengumpulan Data

Pengumpulan data yang peneliti lakukan menggunakan beberapa teknik ataupun cara sebagai berikut :

1. Pengamatan Langsung

   Peneliti melakukan pengamatan langsung terhadap objek yang berkaitan dengan penelitian.

2. Tanya Jawab

   Peneliti melakukan wawancara ataupun tanya jawab kepada ahli kriptografi untuk menanyakan teori yang kurang jelas untuk menyelesaikan penelitian.

3. Sampel

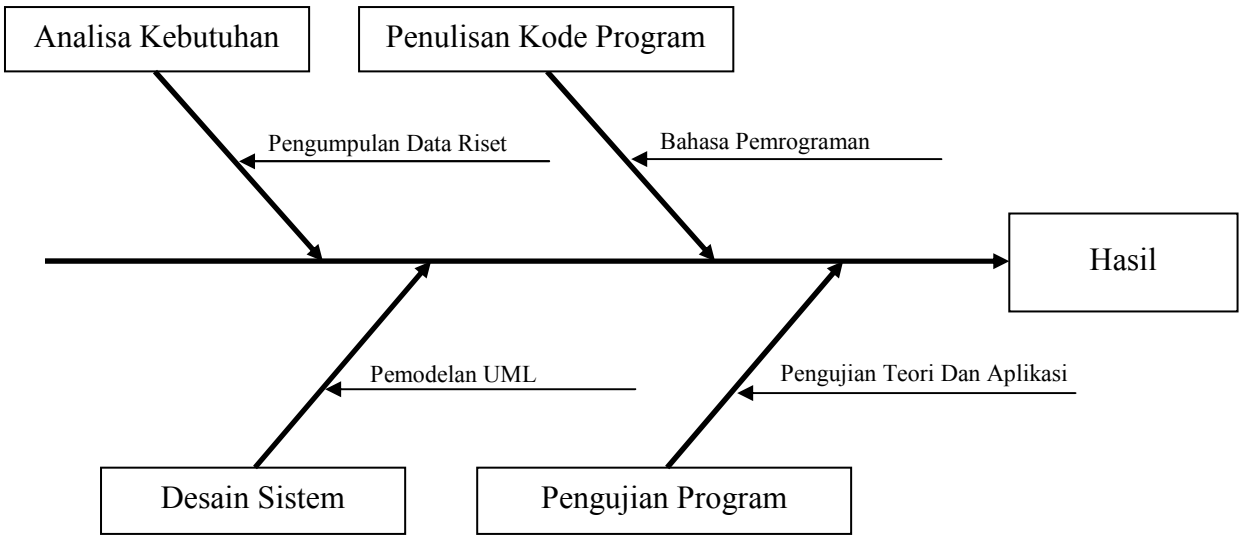
   Peneliti mengumpulkan sampel ataupun contoh data-data yang dapat digunakan untuk penelitin.

4. Penelitian Perpustakaan (*Library Research*)

   Peneliti mencari dan mengumpulkan referensi yang berkaitan dengan penelitian yaitu buku, jurnal dan karya ilmiah.

I.4.2. Arus Analisis Metode Penelitian

Arus analisis dari metode penelitian dimodelkan dalam bentuk *fish bone* yang dapat di lihat pada gambar III.1 sebagai berikut :



Gambar III.1. Diagram *Fish Bone* Metodologi Penelitian

Keterangan :

1. Analisa Kebutuhan

Peneliti menganalisa dan menentukan kebutuhan yang akan digunakan untuk penelitian. *Software* dan *hardware* yang akan digunakan untuk mengimplementasikan dan menguji hasil penelitian. Berdasarkan data-data yang ada ini kemudian dilakukan tahap selanjutnya, yaitu desain sistem.

Berikut adalah *software* yang digunakan untuk pembuatan sistem :

a. Sistem operasi *windows* 7

b. *Netbeans* 8.0

c. *Notepad* ++

d. *Xampp*

e. *Google Chrome*/ *Mozilla Fire Fox*

Berikut adalah *hardware* yang digunakan untuk penerapan sistem :

a. *Laptop/ Computer*

b. *Hardisk*

c. *Mobile Android*

2. Desain Sistem

Perancangan dan desain sistem yang digunakan pada penelitian ini menggunakan pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.

3. Penulisan Kode Program

Penulisan kode program menggunakan bahasa pemrograman HTML, PHP, *Java*, XML, *Javascript* dan *database* MySQL.

4. Pengujian Program

Pengujian program dilakukan untuk mengetahui hasil dari perancangan sistem yang telah dibuat dan untuk mengetahui kekurangan sistem. Apabila terdapat kekurangan sistem atau program tidak berjalan dengan baik, maka akan dilakukan perbaikan sampai seluruh program berjalan dengan baik.

5. Hasil

Pada tahap ini program akan diterapkan untuk informasi unit kegiatan mahasiswa. Pada tahap ini juga sistem sudah dapat diimplementasikan kepada kasus yang sebenarnya.

I.5. Kontribusi Penelitian

Kontribusi penelitian mengenai penelitian yang penulis buat, dapat dilihat dan dibandingkan dari beberapa jurnal yang terdapat pada tabel I.1. kontribusi penelitian.

Tabel I.1. Kontribusi Penelitian

No	Nama/ Tahun	Referensi	Judul	Hasil Penelitian
1.	Setiawan (2011)	Jurnal	Analisis dan Perbandingan Algoritma Whirlpool dan SHA-512 sebagai Fungsi Hash	Kedua algoritma memiliki kelebihan dan kekurangannya masing-masing. Algoritma hash SHA-512 yang memiliki algoritma yang sederhana, tetapi dapat menghasilkan nilai hash yang kuat, serta menggunakan memori yang lebih sedikit jika dibandingkan dengan algoritma hash Whirlpool. Tetapi, nilai hash yang dihasilkan memiliki kekuatan sebagai kata kunci yang tidak stabil. Terkadang nilai kata kunci yang diberikan sangat kuat, tetapi terkadang nilai kata kunci yang diberikan sangat lemah.
2.	Sholeh, dkk (2013)	Jurnal	Mengamankan Skrip Pada Bahasa Pemrograman PHP Dengan Menggunakan Kriptografi Base64	Dengan adanya cara pengamanan ini, pengembang aplikasi yang menggunakan bahasa pemograman PHP dapat menyembunyikan

				skrip php supaya tidak mudah disalin, diubah sebagian/ seluruhnya oleh orang yang tidak berhak.

I.6. Sistematika Penulisan

Adapun sistematika penulisan yang diajukan dalam skripsi ini adalah sebagai berikut :

BAB I : PENDAHULUAN

Pada bab ini menerangkan tentang latar belakang, ruang lingkup permasalahan, tujuan dan manfaat, metode penelitian dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menerangkan teori dasar yang berhubungan dengan program yang dirancang serta bahasa pemrograman yang digunakan.

BAB III : ANALISA DAN DESAIN SISTEM

Pada bab ini mengemukakan analisa masalah program yang akan dirancang dan rancangan program yang digunakan pada penulisan skripsi ini.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini mengemukakan tentang hasil implementasi sistem yang dirancang mencakup uji coba sistem, tampilan serta perangkat

yang dibutuhkan. Analisa sistem dirancang untuk mengetahui kelebihan dan kekurangan sistem yang dibuat.

BAB V : KESIMPULAN DAN SARAN

Dalam bab ini berisikan berbagai kesimpulan dan saran yang dapat dibuat berdasarkan uraian yang telah disimpulkan.