

BAB I

PENDAHULUAN

I.1. Latar Belakang

Perkembangan teknologi belakangan ini tumbuh dengan sangat pesat. Perkembangan teknologi ini banyak melahirkan keuntungan yang mempermudah kelangsungan hidup manusia. Tapi seiring dengan berkembangnya teknologi, muncul pula masalah-masalah baru, mulai dari privasi, keamanan, hingga hak cipta. Hal inilah yang sering dimanfaatkan oknum-oknum yang tidak bertanggung jawab untuk melakukan hal-hal negatif bahkan tindak kejahatan. Mudah-mudahan penyebaran informasi palsu, pembobolan akun bank, dan maraknya pembajakan merupakan contoh sisi gelap dari perkembangan teknologi. Hal ini membuat para pengembang TI memutar otak untuk menangani masalah-masalah tersebut. Yang tidak pernah habis menjadi pembicaraan adalah pengembangan sistem keamanan (Arief Muhamad, et al. 2015a)

Banyak cara yang dilakukan oleh pengembang TI dalam urusan keamanan, salah satunya menggunakan metode kriptografi. Kriptografi adalah sebuah ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dimengerti atau dibaca, proses ini disebut dengan enkripsi. Untuk membacanya kembali, dilakukan proses dekripsi atau pengembalian ke tulisan aslinya. Hal ini banyak dimanfaatkan untuk menyamakan dokumen-dokumen penting sehingga hanya orang-orang tertentu yang dapat membuka dan membacanya. Selain itu membuat dokumen tersebut aman apabila jatuh ke pihak lain. Seiring dengan perkembangannya, kriptografi

mulai dimanfaatkan untuk menyamarkan *file-file* non dokumen, seperti, gambar, video maupun suara (Arief Muhamad, et al. 2015b).

Seiring berjalannya waktu, keamanan dari penggunaan bahasa pemrograman HTML mulai diragukan. Hal ini ditunjukkan dengan adanya tindak kejahatan di internet. Salah satu tindakan tersebut adalah pencurian data atau informasi penting yang tersimpan di internet. Menurut Harison dan Ahmad Syarif (2016), *HyperText Markup Language* (HTML) adalah sebuah bahasa *markup* yang digunakan untuk membuat sebuah halaman web, menampilkan berbagai informasi di dalam sebuah Penjelajah web Internet dan *formatting hypertext* sederhana yang ditulis kedalam berkas format ASCII agar dapat menghasilkan tampilan wujud yang terintegrasi. Berdasarkan uraian permasalahan yang dipaparkan, maka penulis memutuskan untuk mengambil judul “**Perancangan Aplikasi Keamanan Script HTML Pada Alamat Laman Menggunakan Algoritma AES dan RSA**” dalam penulisan skripsi ini.

I.2. Ruang lingkup Permasalahan

Ruang lingkup permasalahan yang dapat dijabarkan berdasarkan latar belakang adalah sebagai berikut :

I.2.1. Identifikasi Masalah

Dari latar belakang pemilihan judul, maka identifikasi masalah dari peneliti untuk skripsi ini adalah sebagai berikut :

1. Masyarakat kurang mengenal proses enkripsi dan dekripsi pada script

HTML.

2. Penyalahgunaan script HTML pada sebuah alamat laman.
3. Dibutuhkan aplikasi yang dapat mengenkripsi dan dekripsi pada script HTML.

I.2.2. Perumusan Masalah

Perumusan masalah yang berdasarkan identifikasi masalah yang terdapat pada penelitian ini adalah sebagai berikut :

1. Bagaimana merancang aplikasi keamanan Script HTML dengan menggunakan VB.Net ?
2. Bagaimana mengurangi dampak penyalahgunaan Script HTML dengan algoritma AES dan RSA ?
3. Bagaimana merancang aplikasi keamanan Script HTML dengan algoritma AES dan RSA ?

I.2.3. Batasan Masalah

Disebabkan banyaknya permasalahan dan waktu yang terbatas, maka agar pembahasan masalah tidak melebar penulis membatasi masalah sebagai berikut :

1. Aplikasi hanya untuk enkripsi dan dekripsi script HTML dan berjalan pada sistem operasi *windows*.
2. Aplikasi yang dapat memberikan informasi mengenai enkripsi dan dekripsi.
3. Aplikasi ini mengenkripsi dan dekripsi script HTML sebelum di upload.

4. *Input* aplikasi ini berupa script HTML.
5. *Output* aplikasi ini berupa hasil enkripsi dari script HTML.
6. Pembuatan Aplikasi ini menggunakan bahasa pemrograman VB.Net 2010.
7. Perancangan Aplikasi ini menggunakan pemodelan UML.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Tujuan penelitian ini adalah sebagai berikut :

1. Membuat Aplikasi Keamanan Script HTML dengan menggunakan algoritma AES dan RSA.
2. Meminimalisir tindak kejahatan menggunakan Script HTML.
3. Memberikan pengetahuan tentang enkripsi dan dekripsi Script HTML menggunakan algoritma AES dan RSA.

I.3.2. Manfaat

Manfaat yang dihasilkan penelitian ini adalah sebagai berikut :

1. Meminimalisir tindak penyalahgunaan script HTML.
2. Masyarakat jadi mengenal proses enkripsi dan dekripsi script HTML dengan algoritma AES dan RSA.
3. Mendapat pengalaman baru dalam pembuatan aplikasi keamanan script html.

I.4. Metodologi Penelitian

Metode merupakan suatu cara yang sistematis untuk mengerjakan suatu permasalahan. Penelitian ini akan melalui beberapa tahapan. Tahapan dalam penelitian ini dapat di modelkan pada diagram *Flowchart*. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :

I.4.1. Pengumpulan Data

Dalam pengumpulan data-data yang diperlukan dalam penyusunan penelitian ini, maka peneliti menggunakan beberapa tahapan yaitu :

1. Sampel (*Sampling*)

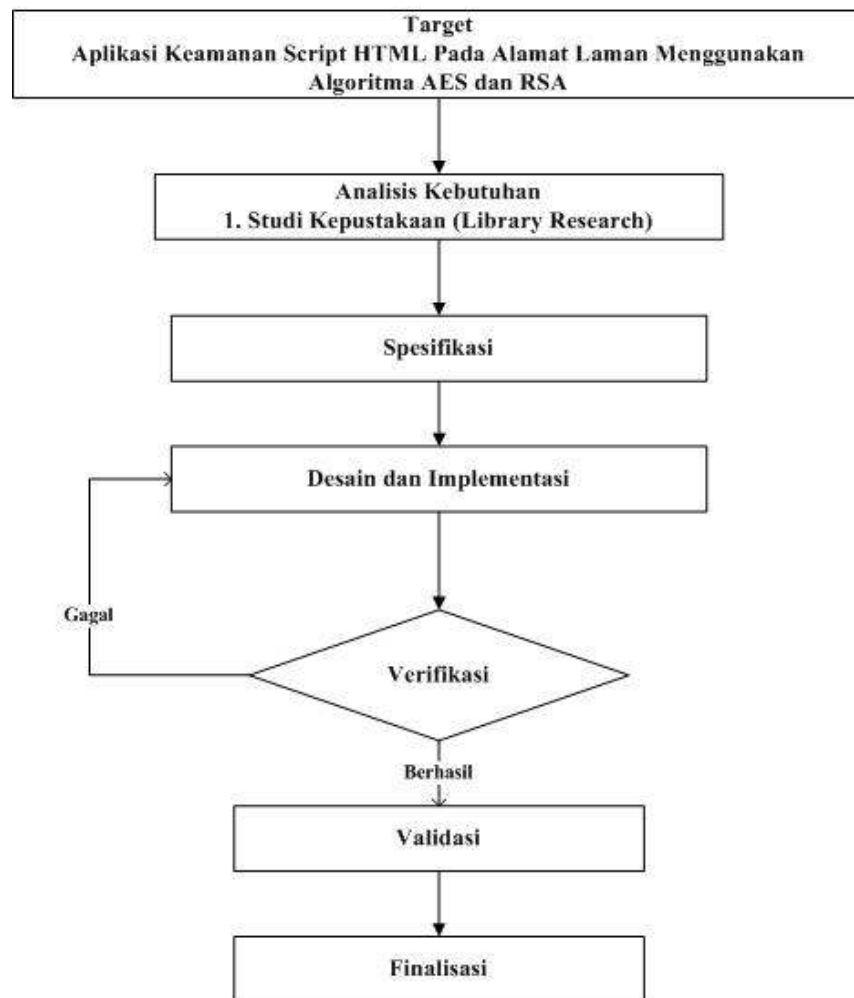
Pada tahapan ini peneliti mengumpulkan beberapa contoh berupa aplikasi, jurnal dan buku untuk referensi penelitian.

2. Penelitian Perpustakaan (*Library Research*)

Peneliti mengumpulkan teori berupa buku dan jurnal untuk referensi pada penelitian ini.

I.4.2. *Flowchart* Metode Penelitian

Berikut adalah *flowchart* metode penelitian yang digunakan dalam penulisan skripsi ini.



Gambar I.1. Flowchart Metode Penelitian

Keterangan :

1. Analisa Kebutuhan

Pada tahapan ini peneliti mengumpulkan data-data yang berkaitan dengan penelitian. Peneliti juga menentukan *software* dan *hardware* yang akan digunakan untuk membuat penelitian.

Berikut adalah *software* yang digunakan untuk pembuatan sistem :

- a. Sistem operasi *windows 7*

- b. Sublime Text 3
- c. Visual Basic Net. 2010

Berikut adalah *hardware* yang digunakan untuk penerapan sistem :

- a. *Laptop/ Computer*
- b. *Mouse*

Berikut adalah bahan bacaan yang digunakan untuk teori :

- a. Buku
- b. Jurnal

2. Desain Sistem

Untuk mendesain sistem peneliti menggunakan beberapa pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.

3. Penulisan Kode Program

Dalam penulisan kode program, peneliti menggunakan bahasa pemrograman HTML dan *Visual Studio 2010*.

4. Pengujian Program

Pengujian dilakukan dengan dua cara yaitu dengan teori dan dengan praktek. Pengujian dengan teori menggunakan *blackbox tesing* dan pengujian dengan praktek menggunakan *Visual Studio 2010*.

5. Hasil

Hasil yang diperoleh pada penelitian ini yaitu Aplikasi Keamanan Script HTML Pada Alamat Laman Menggunakan Algoritma AES dan RSA.

I.5. Kontribusi Penelitian

Kontribusi yang dihasilkan penelitian ini adalah sebagai berikut :

1. Masyarakat diberikan informasi mengenai Enkripsi dan Dekripsi pada Script HTML.
2. Dengan Algoritma RSA dan AES, masyarakat diberikan pengetahuan tentang Enkripsi dan Dekripsi pada Script HTML.
3. Membuat masyarakat tahu proses Enkripsi dan Dekripsi pada Script HTML.

I.6. Lokasi Penelitian

Lokasi penelitian yang peneliti lakukan yaitu pada *Personal Computer / Laptop*.

I.7. Sistematika Penulisan

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 yang dapat dibuat berdasarkan uraian yang telah disimpulkan dan saran.