

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam sistem informasi pada saat ini. Munculnya teknologi internet dan multimedia telah mendorong berbagai macam usaha untuk melindungi, mengamankan, dan merahasiakan data file digital dari pihak-pihak yang tak memiliki otoritas untuk mengakses data file tersebut. Salah satu usaha untuk mengamankan data dan informasi diantaranya dengan menggunakan kriptografi. Beragam algoritma kriptografi dapat diimplementasikan untuk mewujudkan sistem keamanan data. Diantaranya yaitu algoritma kriptografi Rivest Shamir Adleman (RSA) (Rakhman, 2015). Algoritma RSA dibuat oleh tiga orang peneliti dari MIT (Massachusetts Institute of Technology) pada tahun 1976, yaitu Ron Rivest, Adi Shamir dan Leonard Adleman. RSA adalah salah satu teknik kriptografi dimana kunci untuk melakukan enkripsi berbeda dengan kunci untuk melakukan dekripsi. Kunci untuk melakukan enkripsi disebut sebagai kunci publik, sedangkan kunci untuk melakukan dekripsi disebut sebagai kunci privat. (Rahajoeningroem, 2015).

Samahalnya dengan keamanan data nasabah KPR pada Bank Tabungan Negara BTN demi menjaga seluruh data nasabah yang merupakan tanggung jawab pihak BTN, maka faktor orang sebagai penjaga memegang peranan yang

penting, Terutama jika data tersebut berada dalam suatu jaringan komputer yang terhubung/terkoneksi dengan jaringan internet. Tentu saja data yang penting tersebut masih belum bisa di katakan aman karena tidak ada keamanan tambahan didalamnya. Pasalnya dalam implementasi saat ini pihak BTN masih menggunakan sistem aplikasi yang belum menggunakan enkripsi ataupun dekripsi dalam hal penyimpanan data nasabah KPR.

Pada pembuatan tugas akhir ini, penulis akan mengimplementasikan metode RSA pada sistem repository dokumen pada bank BTN yang di fokuskan untuk data nasabah KPR. Data nasabah KPR dalam bentuk file dokumen akan di enkripsi saat data di inputkan dalam sistem repository menggunakan algoritma RSA, selanjutnya data hanya bisa di akses melalui sistem repository karena file data hanya bisa di dekripsi melauai aplikasi repository. Ini diharapkan dapat meningkatkan keamanan sehingga tidak mudah untuk di akses orang yang tak berkepentingan kecuali user yang telah terdaftar pada sistem repository.

## 1.2 Rumusan Masalah

Dari uraian latar belakang diatas maka dapat dirumuskan beberapa pertanyaan sebagai berikut:

- a. Bagaimana merangkai sebuah aplikasi repository dokumen BTN ?
- b. Bagaimana cara mengimplementasikan metode RSA pada sistem repository dokumen BTN ?

## 1.3 Batasan Masalah

Pembuatan program ini memiliki beberapa pembatasan masalah, yaitu:

- a. Aplikasi repository dokumen ini hanya diperuntukan menyimpan data nasabah KPR.
- b. Aplikasi repository dokumen ini dibuat hanya berbasis web.
- c. Metode RSA di gunakan untuk enkripsi dan dekripsi file data.
- d. File data yang di enkripsi berupa text.

#### 1.4 Tujuan Dan Manfaat Penelitian

##### 1.4.1. Tujuan

Berdasarkan rumusan masalah diatas, tujuan dari laporan ini adalah membangun aplikasi yang mampu melakukan hal-hal berikut ini :

1. Mengetahui cara untuk membangun sistem aplikasi repository dokumen pada BTN.
2. Mengetahui cara untuk membangun sistem aplikasi yang dapat melakukan enkripsi dan dekripsi dengan menggunakan metode RSA.

##### 1.4.2. Manfaat Penelitian

1. Dapat Menambah keamanan file data nasabah KPR pada BTN
2. Diharapkan hasil penulisan laporan tugas akhir ini dapat menjadi tambahan referensi untuk penulisan dan penelitian selanjutnya tentang sistem tersebut.

#### 1.5 Metode Penelitian

Dalam rangka menyusun laporan ini untuk memperoleh data dan informasi yang diperlukan penulis melakukan 3 metode, yaitu:

### 1.5.1. Metode Pengumpulan Data

1. Studi Pustaka : Observasi dan Wawancara.

### 1.5.2. Metode perancangan waterfall

Pada pengembangan aplikasi di mana kemajuannya dipandang sebagai terus mengalir ke bawah (seperti air terjun) melewati fase – fase perencanaan, pemodelan, implementasi (konstruksi), dan pengujian.

Berikut adalah tahapan dalam Metode Waterfall:

1. Requirement (analisis kebutuhan)

Pengumpulan data bisa dengan sebuah penelitian, wawancara, dan studi literatur. Pengumpulan data tersebut yang akan menjadi acuan untuk menerjemahkan kedalam bahasa pemrograman.

2. Design System (sistem desain)

Syarat kebutuhan sebuah perancangan perangkat lunak yang akan digunakan programmer untuk memulai pembuatan sistemnya.

3. Coding & Testing (penulisan sinkode program / implementation)

Bertujuan menemukan kesalahan – kesalahan terhadap sistem tersebut dan kemudia bisa diperbaiki.

4. Penerapan / Pengujian Program (Intergration & Testing)

Tahapan dikatakan final dalam pembuatan sebuah sistem. Setelah melalui analisa, design dan coding. Maka sudah dapat digunakan user.

## 5. Pemeliharaan (Operation & Maintenance)

Maintenance sebuah sistem untuk pengembangan sistem yang baru, dan perubahan permintaan karena pelanggan membutuhkan perkembangan fungsional.

### 1.6 Sistematika Penulisan

Pada penulisan skripsi ini, akan dipergunakan sistematika penulisan sebagai berikut:

#### **BAB I – PENDAHULUAN**

Bab ini berisi gambaran umum penulisan terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan penulisan, metodologi penulisan dan sistematika penulisan

#### **BAB II – LANDASAN TEORI**

Bab ini berisikan tentang teori dasar yang menunjang dalam pembahasan penelitian yang dapat digunakan dalam menyelesaikan permasalahan yang diangkat.

#### **BAB III – ANALISIS DAN PERANCANGAN SISTEM**

Bagian ini berisikan tentang data-data yang dibutuhkan dalam perancangan suatu sistem yang terdiri dari UML, Desain-desain struktur database, serta desain tampilan untuk aplikasi.

## BAB IV – IMPLENTASI SISTEM

Bab ini bersisi tentang implementasi program yang telah dihasilkan, gambaran umum sistem dan evaluasi perancangan model monitoring penggunaan alat tulis kantor pada sistem inventory barang dengan metode tophis.

## BAB V – PENUTUP

Bab ini membahas tentang kesimpulan dan rangkuman dari seluruh tulisan yang telah diuraikan dalam bab-bab sebelumnya. Bab ini juga akan menyampaikan beberapa saran untuk perbaikan sistem yang akan datang.

