

# BAB I

## PENDAHULUAN

### I.1. Latar Belakang

Saat ini data dan informasi menjadi hal yang sangat penting. Berbagai perusahaan, instansi, dan lainnya telah memanfaatkan teknologi *database* untuk menyimpan dan juga mengelola data organisasi atau perusahaannya. PT. Permodalan Nasional Madani (Persero) atau PNM adalah perusahaan jasa keuangan yang hadir sebagai solusi peningkatan kesejahteraan melalui layanan pinjaman modal untuk perempuan prasejahtera pelaku usaha ultra mikro melalui program Membina Ekonomi Keluarga Sejahtera (PNM Mekaar). PNM Mekaar dikuatkan dengan aktivitas pendampingan usaha dan dilakukan secara berkelompok. Keamanan terhadap data nasabah pada PT. PNM yang disimpan dalam *database* sudah menjadi hal yang sangat dibutuhkan. Namun keamanan pada *database* dengan pembatasan hak akses sudah tidak lagi dapat menjamin keamanan data karena kebocoran data dapat disebabkan oleh pihak-pihak yang langsung berhubungan dengan *database*.

Data nasabah merupakan data penting yang perlu dijaga keamanannya. Salah satu cara untuk mengamankan sebuah data adalah dengan menggunakan kriptografi. Kriptografi merupakan salah satu solusi untuk menjamin keamanan data dengan cara menyandikan isi informasi (*plaintext*) menjadi isi yang sulit untuk dibaca atau bahkan tidak dipahami (*ciphertext*). Oleh karena itu peneliti merekomendasikan algoritma RC4 (*Rivest Code 4*) yang merupakan algoritma

kriptografi kunci simetris dan bersifat *stream cipher* sehingga panjang karakter hasil enkripsi (*ciphertext*) mempunyai panjang karakter yang sama dengan data asli (*plaintext*). Teknik kriptografi simetris dipilih karena dengan algoritma ini proses enkripsi dan dekripsi data dapat dilakukan dengan waktu yang lebih cepat dibandingkan dengan algoritma kriptografi asimetris.

Berdasarkan pada informasi yang dipaparkan, peneliti membuat sebuah penerapan kriptografi menggunakan algoritma RC4 pada data nasabah PT. PNM. Proses enkripsi pada penelitian ini dilakukan dengan menentukan kolom pada *database* yang akan dienkripsi. Implementasi ini menerapkan metode sistem enkripsi dan dekripsi dengan implementasi algoritma RC4 dalam pengamanan data nasabah.

Dengan latar belakang diatas maka penulis mengangkat judul **“Implementasi Algoritma RC4 Dalam Melakukan Pengamanan Data Nasabah Pada PT. Permodalan Nasional Madani”**.

## **I.2. Ruang Lingkup Permasalahan**

### **I.2.1. Identifikasi Masalah**

Dari latar belakang pemilihan judul, maka identifikasi masalah dari penelitian ini adalah sebagai berikut :

1. Data nasabah pada PT. PNM belum mendapatkan keamanan yang baik.
2. Belum adanya aplikasi pengamanan data nasabah PT. PNM dengan implementasi algoritma RC4.
3. Tidak ada proses enkripsi menggunakan algoritma RC4 pada data nasabah PT. PNM.

### **I.2.2. Perumusan Masalah**

Berdasarkan latar belakang yang telah diuraikan sebelumnya, maka penulis merumuskan masalah adalah sebagai berikut :

1. Bagaimana menerapkan kriptografi dalam meningkatkan keamanan pada data nasabah PT. PNM?
2. Bagaimana merancang sebuah aplikasi pengamanan data nasabah PT. PNM dengan implementasi algoritma RC4 ?
3. Bagaimana melakukan proses enkripsi dan dekripsi menggunakan algoritma RC4 pada data nasabah PT. PNM ?

### **I.2.3. Batasan Masalah**

Batasan masalah pada penelitian ini adalah sebagai berikut :

1. Data yang akan diamankan adalah data nasabah pada PT. PNM.
2. Data yang akan dienkripsi adalah nomor akun, nama dan alamat nasabah.
3. Bahasa pemrograman yang digunakan adalah *Java* dengan *database* MySQL.
4. Pemodelan yang digunakan adalah *Unified Modeling Language* (UML).

## **I.3. Tujuan dan Manfaat**

### **I.3.1. Tujuan**

Adapun tujuan penulis dalam penelitian implementasi algoritma RC4 dalam melakukan pengamanan data nasabah pada PT. Permodalan Nasional Madani adalah :

1. Memberikan keamanan pada data nasabah PT. PNM.
2. Menghasilkan aplikasi pengamanan data nasabah pada PT. PNM dengan implementasi algoritma RC4.
3. Mengetahui proses enkripsi dan dekripsi menggunakan algoritma RC4 pada data nasabah PT. PNM.

### **I.3.2. Manfaat**

Manfaat dari penelitian implementasi algoritma RC4 dalam melakukan pengamanan data nasabah pada PT. Permodalan Nasional Madani adalah :

1. Bagi Ilmu Pengetahuan

Memberikan informasi mengenai pengembangan aplikasi dengan algoritma RC4, penggunaan algoritma RC4 dapat membantu mengamankan data penting untuk menghindari kerusakan data.

2. Bagi Perusahaan

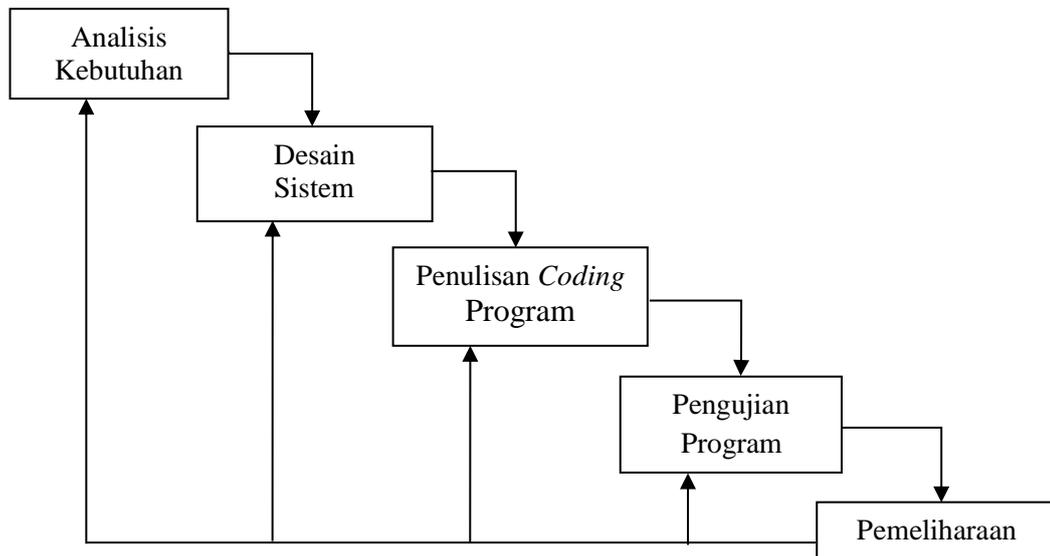
Implementasi algoritma RC4 terhadap aplikasi data nasabah diharapkan dapat mengamankan data nasabah sehingga menghindari kehilangan data nasabah.

3. Bagi Peneliti Selanjutnya

Dapat dijadikan sebagai referensi untuk melakukan pengembangan aplikasi dengan algoritma RC4 pada penelitian lain.

#### I.4. Metodologi Penelitian

Untuk menganalisa data tersebut di atas maka digunakan alur analisis yang disusun dengan langkah - langkah berbentuk diagram alir seperti pada gambar I.1 ini :



**Gambar I.1. Model Waterfall**

Dalam pengembangannya, metode *waterfall* memiliki beberapa tahapan yaitu :

1. Analisis Kebutuhan

Berisi tentang hal-hal yang harus ada pada hasil perancangan agar mampu menyelesaikan masalah yang ada sesuai tujuan. Data yang dibutuhkan dalam melakukan perancangan sistem adalah data nasabah PT. PNM dan bahasa pemrograman yang digunakan untuk membuat aplikasi adalah *Java*.

## 2. Desain Sistem

Secara umum implementasi algoritma RC4 dalam melakukan pengamanan data nasabah pada PT. PNM menggunakan model perancangan *Unified Modeling Language* (UML).

## 3. Penulisan *Coding* Program

*Coding* merupakan penerjemahan desain dalam bahasa yang bisa dikenali oleh komputer. Dilakukan oleh *programmer* yang akan menterjemahkan transaksi yang diminta oleh *user*. Tahapan inilah yang merupakan tahapan secara nyata dalam mengerjakan suatu sistem. Dalam artian penggunaan komputer akan dimaksimalkan dalam tahapan ini. Setelah pengkodean selesai maka akan dilakukan *testing* terhadap sistem yang telah dibuat tadi. Tujuan *testing* adalah menemukan kesalahan-kesalahan terhadap sistem tersebut dan kemudian bisa diperbaiki.

## 4. Pengujian Program

Pada tahap ini dilakukan pengujian aplikasi secara menyeluruh, meliputi pengujian fungsional dan pengujian ketahanan sistem. Pengujian secara *blackbox (interface)* yaitu pengujian perangkat lunak yang tes fungsionalitas dari aplikasi yang bertentangan dengan struktur internal atau kerja. Pengetahuan khusus dari kode aplikasi/struktur internal dan pengetahuan pemrograman pada umumnya tidak diperlukan, pengujian tersebut untuk masing-masing blok peralatan yang dirancang.

## 5. Pemeliharaan Sistem

Perangkat lunak yang susah disampaikan kepada pelanggan pasti akan mengalami perubahan. Perubahan tersebut bisa karena mengalami kesalahan karena perangkat lunak harus menyesuaikan dengan lingkungan baru (*peripheral* atau sistem operasi baru), atau karena pelanggan membutuhkan perkembangan fungsional.

### **I.5. Kontribusi Penelitian**

Berdasarkan penjelasan di latar belakang tersebut, penulis menemukan kontribusi penelitian berupa dengan adanya aplikasi ini bisa membantu kebutuhan akan layanan keamanan data sehingga pengguna informasi yang bersifat rahasia atau pribadi dapat terjaga dan program aplikasi ini dapat dijadikan sebagai salah satu media alternatif untuk melakukan pengamanan data.

### **I.6. Sistematika Penulisan**

Adapun sistematika penulisan yang diajukan dalam penelitian 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 tentang teori-teori dan metode yang berhubungan dengan topik yang dibahas atau permasalahan yang

sedang dihadapi yaitu berupa pembahasan mengenai sistem keamanan, UML dan normalisasi.

### **BAB III : ANALISIS DAN PERANCANGAN**

Pada bab ini mengemukakan tentang analisa sistem yang sedang berjalan, evaluasi sistem yang berjalan dan desain sistem secara detail.

### **BAB IV : HASIL DAN UJI COBA**

Pada bab ini menerangkan hasil dan pembahasan program yang dirancang serta kelebihan dan kekurangan sistem yang dirancang.

### **BAB V : KESIMPULAN DAN SARAN**

Pada bab ini berisi kesimpulan penulisan dan saran dari penulis sebagai perbaikan di masa yang akan datang untuk sistem.