# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Keamanan sistem komputer menjadi semakin penting seiring dengan berkembangnya proses bisnis yang terkomputerisasi. Proses bisnis terkomputerisasi merupakan proses bisnis yang sebagian besar kegiatannya menggunakan teknologi komputer serta menjadikan komputer sebagai media penyimpanan data-data penting sehingga bisa dikatakan media komputer menjadi faktor penting di dalam proses-proses bisnis yang dijalankan. Keamanan sistem komputer yang menjadi sorotan bukan hanya dari perangkat komputernya saja, namun juga keamanan bagi jaringan, *software* atau program aplikasi dan juga keamanan basis data.

Basis data adalah sekumpulan informasi yang disimpan di dalam komputer secara sistematik yang dapat digunakan melalui sebuah program komputer tertentu untuk menjalankannya. Keamanan basis data menjadi pertahanan terakhir ketika suatu sistem komputer mengalami serangan dari pihak luar setelah menembus keamanan jaringan, keamanan sistem operasi dan *software*. Bagi sebagian proses bisnis, keamanan basis data menjadi sangat penting setelah menjamin keamanan pada jaringan dan sistem komputernya. Misalnya pada usaha dibidang penjualan dan kredit elektronik dimana di dalam basis datanya akan menyimpan data-data diri pelanggan, termasuk *account login* pelanggan, dan bila bidang bisnis tersebut (dalam hal ini penjualan dan kredit elektronik) terintegrasi

dengan data lainnya seperti nomor kartu kredit, akan menuntut keamanan yang lebih menjamin kerahasiaan data karena menyangkut harta kekayaan pelanggan. Data password, nomer kartu kredit dan data lainnya yang menyangkut harta kekayaan pelanggan harus dijaga kerahasiaannya bahkan dari administrator sekalipun dimana administrator tidak diizinkan mengakses dan dibuat tidak dapat membaca data-data tersebut. Basis data yang aman akan menjadikan suatu perusahaan mendapat rasa percaya dari penggunanya sehingga menjamin keberlangsungan proses bisnis pada perusahaan tersebut.

Keamanan basis data dapat dilakukan dengan berbagai cara, dimulai dari pembatasan hak akses *user* terhadap basis data itu sendiri, penggunaan nama *field* yang hanya dimengerti oleh administrator sehingga tidak semua pegawai yang diberi izin mengakses basis data mengerti alur basis data yang ada guna menghindari pencurian data, perusakan data dan lain sebagainya, hingga pengimplementasian algoritma kriptografi oleh administrator terhadap *record* dalam basis datanya dengan tujuan membuat *record* yang tersimpan menjadi lebih rahasia dan sulit dibaca oleh pihak lain.

Kriptografi sendiri adalah ilmu dan sekaligus seni untuk mengamankan data yang didalamnya terdapat algoritma tertentu yang bertujuan sebagai *confusion* atau pembingungan, dengan cara mengubah teks polos *(plaintext)* menjadi teks yang tidak bisa dibaca artinya secara langsung oleh manusia *(ciphertext)*. Pada kriptografi, terdapat proses enkripsi yang menubah teks polos menjadi *ciphertext*, dan proses dekripsi yang mengubah *ciphertext* menjadi teks polos kembali. Kedua proses ini menggunakan kunci tertentu, semakin panjang

kunci maka akan semakin sulit untuk dibuka secara paksa. Contoh algoritma kriptografi adalah algoritma RSA (Rivest, Shamir, Adleman), *Data Encryption Standard* (DES), *Advanced Encryption Standard* (AES), *Message Digest-5* (MD5) dan lain sebagainya yang mempunyai tujuan utama untuk menjaga integritas data, mengautentikasi dan merahasiakan data.

Salah satu program aplikasi manajemen basis data atau *Database Management System* (DBMS) yang mendukung cukup banyak algoritma kriptografi adalah Oracle yang merupakan produk dari *Oracle Corporation*. Keunggulan Oracle sehingga digunakan oleh perusahaan besar seperti Alfa Retailindo, Ramayana Lestari, Coca Cola Bottling dan lainnya adalah karena stabilitas yang terjaga, skalabilitas atau kemampuan menangani lebih banyak pengguna secara bersamaan dan simultan tanpa mengurangi performa, serta menawarkan tingkat keamanan basis data yang lebih handal.

Salah satu fitur keamanan yang diberikan Oracle terhadap *record* di dalam basis datanya adalah dengan memberikan dukungan terhadap algoritma kriptografi baik secara *native* maupun *non-native.* Dukungan secara *native* dari Oracle dengan memberikan fungsi khusus dalam pengimplentasian beberapa algoritma kriptografi menjadikan penerapan algoritma kriptografi tersebut menjadi lebih mudah. Berdasarkan dokumen resmi pada situs Oracle, *http:// docs. oracle. com/ cd/ B19306_01 /appdev. 102/ b14258 /d_crypto.htm* , Algoritma AES, DES dan MD5 merupakan algoritma kriptografi yang didukung secara *native* oleh Oracle 10g. Sementara algoritma lain seperti Diffie-Helman dan RSA tidak didukung secara *native* oleh Oracle.

Algoritma MD5, AES dan DES merupakan jenis algoritma kriptografi simetris. Algoritma kriptografi simetris berarti kunci yang digunakan untuk *encrypt* sama dengan kunci yang digunakan untuk *decrypt.* Pada algoritma kriptografi simetris, panjang kunci tidak fleksibel yang berarti panjang kunci tidak bisa ditentukan oleh pengguna yang mungkin dalam penggunaannya akan berbeda disesuaikan dengan faktor lain seperti kemampuan perangkat keras dan lain sebagainya.

Berbeda halnya dengan algoritma asimetris antara lain : Diffie-Hellman, Knapsack dan RSA (Ronald Rivest, Shamir, Adleman), pada algoritma kriptografi asimetris pasangan kunci untuk mengenkrip berbeda dengan pasangan kunci untuk mendekrip. Pada algoritma asimetris, panjang kunci dapat diatur pengguna, sehingga dapat menyesuaikan dengan kegunaan program aplikasi yang akan dibuat, kemampuan perangkat keras, dukungan perangkat lunak dan faktor lainnya. Algoritma kriptografi asimetris Diffie-Hellman dan Knapsack telah dipecahkan oleh kriptoanalisis, salah satunya dengan metode *polynomial-time algorithm*. Algoritma RSA juga telah dipublikasikan kelemahannya namun metode yang ditemukan masih belum mangkus dalam pemecahan kunci yang sangat panjang. Berdasarkan dokumen resmi di situs Oracle yang telah disebutkan sebelumnya, Oracle 10g tidak mendukung algoritma kriptografi asimetris di dalam daftar *cryptograph support*-nya, algoritma kriptografi asimetris RSA termasuk algoritma yang tidak didukung, yang berarti untuk menggunakan algoritma kriptografi asimetris RSA ini pengguna harus menyusun sintak ke

bahasa pemrograman yang digunakan secara manual berdasarkan algoritma kriptografi RSA.

Dari kondisi tersebut, penulis berkeinginan untuk mencari tahu apakah algoritma RSA dapat diterapkan di Oracle 10g dan apakah algoritma RSA juga dapat mengamankan data di basis data seperti algoritma kriptografi lainnya yang telah didukung oleh Oracle 10g. Maka dari itu penulis mengangkat judul skripsi "**Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) untuk Keamanan Data di Oracle 10g**".

## 1.2 Identifikasi dan Rumusan Masalah

### 1.2.1 Identifikasi Masalah

Berdasarkan latar belakang masalah yang dijelaskan diatas maka dapat diidentifikasikan permasalahan yang mungkin terjadi adalah :

1. Algoritma kriptografi asimetris RSA tidak didukung oleh Oracle 10g sehingga dalam pengimplementasian kriptografi RSA harus disusun sintak secara manual.
2. Diperlukan penjelasan mengenai faktor yang mempengaruhi fleksibilitas panjang kunci algoritma asimetris RSA.

### 1.2.2 Rumusan Masalah

Dari identifikasi masalah yang telah dijelaskan diatas, maka rumusan masalah sebagai berikut :

1. Apakah algoritma RSA dapat diterapkan pada Oracle 10g untuk mengamankan data yang tersimpan didalam basis data.

2. Bagaimana alur proses algoritma kriptografi asimetris RSA sehingga menjadi fleksibel dalam pembentukan panjang kunci.

## 1.3 Batasan Masalah

Batasan masalah dibuat untuk membatasi ruang lingkup permasalahan yang akan diteliti dan dikembangkan oleh penulis. Batasan masalah dari penelitian ini adalah :

1. Penerapan algoritma RSA di Oracle 10g akan mencakup proses pembentukan kunci, enkripsi dan dekripsi suatu *record* yang masuk ke dalam basis data.
2. Form data diri pengguna merupakan simulasi inputan data yang berisikan data diri pengguna, diantaranya adalah *username*, nama depan, nama belakang, pekerjaan, usia, nomor rekening dan *password*. Pada penelitian kali ini, data yang akan dienkripsi adalah nomor rekening dan password.
3. Pembentukan kunci terjadi pada PL/SQL dengan tipe data Numerik, dengan panjang kunci maksimal 6-digit.
4. Tidak membahas distribusi pasangan kunci, diasumsikan kedua pasangan kunci disimpan di dalam sebuah tabel pada basis data.

## 1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini sebagai berikut :

1. Menerapkan algoritma RSA ke dalam DBMS Oracle 10g untuk keamanan data.
2. Menjelaskan fleksibilitas algoritma RSA dalam penentuan panjang kunci.

## 1.5 Kegunaan Penelitian

Kegunaan penelitian ini dapat dibedakan menjadi kegunaan praktis dan kegunaan akademis yang akan dijelaskan sebagai berikut ini :

### 1.5.1 Kegunaan Praktis

Penelitian tentang penerapan algoritma RSA pada Oracle 10g ini diharapkan dapat menjadi referensi pengguna Oracle 10g dalam membangun sistem keamanan basis data menggunakan algoritma kriptografi asimetris RSA.

### 1.5.2 Kegunaan Akademik

1. **Bagi Penulis**

   Kegunaan atas penelitian yang dilakukan bagi penulis adalah sebagai berikut :

   a. Berguna dalam menambah atau memperkaya wawasan pengetahuan baik teori ataupun praktek.
   b. Belajar menganalisa dan melatih daya fikir dalam ilmu keamanan basis data.

2. **Bagi Pengembangan Ilmu**

Kegunaan bagi pengembangan ilmu yaitu dapat digunakan sebagai dasar atau referensi dalam penerapan algoritma kriptografi asimeteris RSA ke dalam suatu bahasa pemrograman, program aplikasi, *database management system* dan progam aplikasi yang belum mendukung algoritma RSA secara *native* seperti Oracle 10g.

## 1.6 Lokasi dan Waktu Penelitian

Berikut jadwal lokasi dan waktu penelitian penerapan algoritma RSA pada Oracle 10g :

**Tabel 1.1** Jadwal Penelitian

| No | Kegiatan | Tahun 2012 | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Maret | | | | April | | | | Mei | | | | Juni | | | | Juli | | | |
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 1 | Studi Pustaka | | | | | | | | | | | | | | | | | | | | |
| 2 | Analisis Kebutuhan Sistem | | | | | | | | | | | | | | | | | | | | |
| 3 | Perancangan Sistem | | | | | | | | | | | | | | | | | | | | |
| | a. Pembuatan Rancangan Algoritma RSA | | | | | | | | | | | | | | | | | | | | |
| | b. Pembuatan Flowchart | | | | | | | | | | | | | | | | | | | | |
| | c. Pembuatan Rancangan Antar Muka | | | | | | | | | | | | | | | | | | | | |
| 4 | Implementasi Algoritma dan Pembuatan Program | | | | | | | | | | | | | | | | | | | | |
| | a. Struktur Program | | | | | | | | | | | | | | | | | | | | |

**Tabel 1.2 Jadwal Penelitian (lanjutan)**

| No | Kegiatan | Tahun 2012 | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Maret | | | | April | | | | Mei | | | | Juni | | | | Juli | | | |
| | | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| | b. Struktur Menu | | | | | | | | | | | | | | | | | | | | |
| | c. Pengkodean | | | | | | | | | | | | | | | | | | | | |
| 5 | Pengujian Sistem | | | | | | | | | | | | | | | | | | | | |
| 6 | Evaluasi Sistem | | | | | | | | | | | | | | | | | | | | |