BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Kesimpulan yang dapat diambil setelah memaparkan pembahasan-pembahasan yang telah disajikan pada bab sebelumnya antara lain:

1. Algoritma kriptografi asimetris RSA (Rivest, Shamir, Adleman) dapat diterapkan sebagai keamanan data di Oracle 10g.
2. Fleksibilitas panjang kunci pada algoritma RSA ditentukan oleh besarnya nilai prima awal p dan q. Semakin besar nilai prima awal p dan q maka akan semakin panjang kunci yang bisa dihasilkan.

6.2 Saran

Saran dari penulis dalam penerapan algoritma kriptografi RSA pada basis data Oracle sebagai berikut :

1. Gunakan kelas Java sebagai tempat untuk proses pembentukan kunci agar dapat menggunakan tipe data bigInteger sehingga panjang kunci dapat lebih besar dibandingkan jika proses pembentukan kunci berada pada PL/SQL dengan tipe data integer.
2. Penggunaan tabel konversi dengan pola dan nilai yang berbeda akan membutuhkan penyesuaian dalam penerapan algoritma dekripsi. Penggunaan tabel konversi yang didalamnya terdapat kelipatan 10 akan menyebabkan algoritma dekripsi tidak dapat menghasilkan nilai balik yang benar jika hasil dekripsi hanya dideretkan dan dikonversi balik karena

hasil dekripsi akan menghasilkan pola panjang deret yang berbeda dibanding dengan penggunaan tabel konversi yang didalamnya tidak terdapat nilai konversi kelipatan 10.

3. Untuk mengurangi atau memperkecil panjang *ciphertext* dapat diterapkan fungsi konversi ke karakter yang berbeda. Maksudnya adalah, *ciphertext* yang masih berbentuk deret bilangan, panjang deretnya dapat dikurangi menjadi setengah deret sebelumnya jika deret *ciphertext* dikonversi lagi dengan tabel konversi yang mengonversi per dua digit bilangan ke satu buah *char*.
4. Penerapan algoritma kriptografi pada basis data akan mempengaruhi waktu akses dari data yang melewati proses enkripsi dan dekripsi, baik panjang kunci yang kecil maupun panjang kunci yang besar. Dengan penempatan algoritma kriptografi pada basis data, akan memberikan peluang yang lebih besar pada *intruder* jika jaringan pengiriman data tidak diamankan sehingga jalur pengiriman data sebaiknya diperhatikan juga keamanannya.