ABSTRAK

Algoritma kriptografi Rivest, Shamir and Adleman (RSA) merupakan salah satu algoritma kriptografi asimetris yang berarti menggunakan sepasang kunci yaitu kunci publik dan kunci pribadi. Panjang kunci pada RSA dapat diatur menyesuaikan dengan faktor pendukung program aplikasi yang dibuat. Semakin panjang bit kunci maka semakin sukar untuk dipecahkan karena semakin sulit memfaktorkan dua bilangan yang sangat besar. Oracle adalah basis data yang mempunyai keunggulan dalam skalabilitas yaitu cakupan relasi antar basis data yang luas dan stabilitas dalam pengaksesan banyak pengguna di waktu yang bersamaan. Isu keamanan merupakan sorotan penting dalam penyimpanan data pribadi yang harus dirahasiakan.

Dalam penelitian ini menerapkan algoritma kriptografi RSA untuk enkripsi dan dekripsi kolom suatu tabel pada basis data Oracle 10g.

Hasil dari penelitian ini menunjukkan bahwa algoritma RSA dapat diterapkan pada basis data Oracle 10g dengan dukungan kelas java.

Kata kunci : RSA, Oracle, Enkripsi, Dekripsi, Kelas Java

ABSTRACT

Rivest, Shamir, And Adleman (RSA) cryptographic algorithm is a one of a asymmetric cryptographic algorithms, which means that RSA use two pairs of keys, public keys and private keys. The length of RSA's keys can be set by the user to adjust the supporting factors of the programs. The longer keys will be more difficult to be broke by attack of brute force. Oracle is a database management systems which has a power on stability when accessed by many user in one time and scalability to cover large and many database relational. Security is an important issue highlighted in the storage of personal data shall be keep confidential.

This research has the goal to implement RSA algorithm in the Oracle 10g for security.

The result show that encryption and decryption of RSA algorithm can be implement in the Oracle 10g by the support of Class Java.

Keyword : RSA, Oracle, Encryption, Decryption, Class Java