ABSTRAK

Algoritma RC4 merupakan algoritma kriptografi modern kunci simetris yang mempunyai mode operasi stream cipher, sehingga dalam memproses data dan informasi pada saat tertentu serta menggunakan dua buah substitution box (s-box) berupa array dengan panjang permutasi 256 dan s-box kedua berupa permutasi yang merupakan fungsi dari kunci publik. Algoritma RC4 digunakan untuk mengekripsi data, pesan atau informasi. Keamanan terhadap data nasabah pada PT. Permodalan Nasional Madani (PNM) yang disimpan dalam database sudah menjadi hal yang sangat dibutuhkan, sehingga data yang tersimpan didalam database harus terjamin kerahasiaan dan keamanannya. Untuk menjaga keamanan data nasabah di dalam database, maka diaplikasikanlah algoritma kriptografi dengan mengenkripsi database. Dengan demikian, data yang terenkripsi pada database tidak akan diketahui arti yang sebenarnya dan sulit untuk dirubah ataupun diganti. Implementasi algoritma RC4 dibuat dengan bahasa pemrograman Java dan database menggunakan MySQL. Berdasarkan hasil, data yang tersimpan dalam database pada PT. PNM terenkripsi sehingga data yang tersimpan di dalam database tersebut terjamin kerahasiaan dan keamanannya.

***Kata Kunci** : Kriptografi, Algoritma RC4, Enkripsi, Database.*

ABSTRACT

The RC4 algorithm is a symmetric key modern cryptographic algorithm that has a stream cipher operating mode, so that it processes data and information at any given moment and uses two substitution boxes (s-boxes) in the form of arrays with a permutation length of 256 and a second s-box in the form of permutations which are function of the public key. The RC4 algorithm is used to encrypt data, messages or information. Security of customer data at PT. Permodalan Nasional Madani (PNM) stored in a database has become a very necessary thing, so the data stored in the database must be guaranteed confidentiality and security. To maintain customer data security in the database, cryptographic algorithms are applied by encrypting the database. Thus, the encrypted data in the database will not be known the true meaning and is difficult to change or replace. The implementation of RC4 algorithm is made with the Java programming language and database using MySQL. Based on the results, data stored in a database at PT. PNM is encrypted so that the data stored in the database is guaranteed confidentiality and security.

***Keywords** : Cryptography, RC4 Algorithm, Encryption, Database*