**ABSTRAK**

**NURFADHILAH SUHAN, 2013.** Penerapan Algoritma Kriptografi RSA pada Pengiriman Pesan Rahasia.Skripsi. Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam. Universitas Negeri Makassar (dibimbing oleh Rahmat Syam dan Maya Sari Wahyuni).

Penelitian ini adalah penelitian pustaka yang bertujuan untuk mengetahui algoritma kriptografi Rivest-Shamir-Adleman (RSA) dan penerapannya. RSA merupakan salah satu algoritma kriptografi asimetri yang menggunakan dua jenis kunci, yaitu kunci publik dan kunci privat. Keamanan algoritma ini terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor prima. Tahap pertama dalam penelitian ini adalah mengetahui konsep matematis yang melandasi pembentukan algoritma RSA berdasarkan Teorema Euler dengan sifat-sifat bilangan prima dan aritmatika modulo. Tahap kedua yaitu proses enkripsi dan dekripsi sekaligus pembuatan tanda tangan digital pada pesan. Langkah-langkah proses enkripsi dan dekripsi sekaligus pemberian tanda tangan digital adalah 1) Pihak pengirim dan penerima pesan masing-masing melakukan pembentukan kunci; 2) Pengirim mengenkripsi pesan dan membuat tanda tangan digital pada pesannya; 3) Penerima pesan mendekripsi pesan serta memverifikasi tanda tangan digital.Enkripsi adalah proses untuk mengubah pesan asli (*plaintext*) menjadi pesan sandi (*ciphertext*) sedangkan dekripsi adalah proses untuk mengembalikan *ciphertext* menjadi *plaintext*. Berdasarkan hasil penelitian ini diperoleh bahwa dengan menyisipkan tanda tangan digital pada pesan, penerima dapat mengetahui apakah pesan masih utuh atau telah berubah/ dimodifikasi.

**Kata Kunci :** *Kriptografi, RSA, enkripsi, dekripsi, kunci, tanda tangan digital.*

***ABSTRACT***

**NURFADHILAH SUHAN, 2013.** Implementation of RSA Cryptography Algorithm on Secret Message Delivery. Thesis. Department of Mathematics, Faculty of Mathematics and Natural Sciences. Makassar State University (advisor by Rahmat Sham and Maya Sari Wahyuni​​).

This research is a library that aims to identify a cryptographic algorithm Rivest-Shamir-Adleman (RSA) and its application. RSA is one of the asymmetric cryptographic algorithm that uses two types of keys, ie public key and a private key. Security of this algorithm lies in the difficulty in factoring the non-prime numbers into prime factors. The first phase of this research was to determine the mathematical concepts that underlie the formation of RSA algorithm based on Euler's theorem with the properties of prime numbers and modulo arithmetic. The second phase of the process of encryption and decryption at the same time making the digital signature on the message. Step-by-step process of encryption and decryption as well as provision of digital signatures is 1) The sender and recipient each perform key establishment; 2) The sender encrypts the message and create a digital signature on the message; 3) The recipient decrypts the message and verifies the signature digital. Encryption is the process to transform the original message (plaintext) into a coded message (ciphertext) whereas decryption is the process to restore the ciphertext into plaintext. Based on the results of this study showed that by inserting a digital signature to the message, the receiver can determine whether the message is still intact or has been changed / modified.

**Keywords:** *Cryptography, RSA, encryption, decryption, key, digital signatures.*