ABSTRAK

Nama : Yansiska

Program Studi : Teknik Informatika

Judul : Pengamanan Data Digital Signature Dengan Menggunakan Algoritma RSA

Penelitian ini bertujuan untuk menjaga keaslian pesan yang akan dikirim untuk memberikan jaminan kepada penerima bahwa pesan tersebut bebas dari perubahan atau modifikasi yang dilakukan oleh pihak lain. Jika terjadi suatu perubahan terhadap pesan, maka penerima akan mengetahui bahwa pesan tersebut sudah tidak lagi terjaga keasliannya, sehingga penerima pesan terhindar dari penggunaan data yang salah. Untuk menjaga keaslian data digunakan teknik *digital signature* dengan menggunakan algoritma *RSA* sebagai algoritma kunci publik dan fungsi *hash* untuk menghasilkan *message digest* dari pesan yang dikirim. Kombinasi dari kedua algoritma tersebut akan menghasilkan *digital signature* dari setiap file atau dokumen yang dapat dijaga keasliannya.

Kata Kunci : *Digital Signature*, Algoritma *RSA*, *Message Digest*, Fungsi *Hash*.

ABSTRACT

Name : *Yansiska*

Study Program : *Informatic Engineering*

Title : *Digital Signature Data Security Using RSA and Hash Algorithms*

This research aims to maintain the authenticity of the message to be sent to provide assurance to the recipient that the message is free from changes or modifications made by other parties. If there is a change to the message, the recipient will know that the original message is no longer maintained, so that the recipient of the message avoids using the wrong data. To maintain data authenticity, digital signature techniques are used using the RSA algorithm as a public key algorithm and a hash function to produce a message digest of the messages sent. The combination of the two algorithms will produce a digital signature for each file or document that can be maintained as authentic.

Keywords : Digital Signature, RSA Algorithm, Message Digest, Hash Function.