

ABSTRAK

Pencurian data sangat sering terjadi saat ini, di era modern ini sangat banyak cara yang dapat digunakan untuk mencegah pencurian atau perusakan data tersebut. Salah satu cara adalah dengan menggunakan kriptografi untuk menyamarkan data. Kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi dan entitas. Kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Pada kriptografi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. RSA merupakan salah satu dari Public Key Cryptosystem yang sangat sering digunakan untuk memberikan kerahasiaan terhadap keaslian suatu data digital, Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (signing) dan untuk enkripsi dan salah satu penemuan besar pertama dalam kriptografi kunci publik, oleh karena itu dibutuhkan suatu sebuah sistem yang dapat menjaga dan mencegah pencurian data tersebut. Dengan menggunakan algoritma RSA ini system akan mengenkripsi isi data asli yang diinputkan user menjadi cipherteks, Kemudian user akan mengirimkan terlebih dahulu cipherteks ke rekannya, dan rekannya menginputkan cipherteks agar mengembalikan data ke bentuk semula.

Kata Kunci : RSA, Kriptografi, File PDF

ABSTRACT

Data theft is very common today, in this modern era there are very many ways that can be used to prevent theft or destruction of such data. One way is to use cryptography to disguise data. Cryptography is a science that relies on mathematical techniques for dealing with information security such as confidentiality, data integrity and authentication and entities. Modern cryptography is an improvement that refers to classical cryptography. In modern cryptocurrencies there are various algorithms intended to secure information sent over a computer network. RSA is one of the Public Key Cryptosystems that is very often used to provide confidentiality to the authenticity of digital data, This algorithm was the first algorithm known to be best suited for signing and for encryption and one of the first major inventions in public key cryptography, it therefore needed a system that could maintain and prevent the theft of such data. By using rsa algorithm this system will encrypt the contents of the original data entered by the user into ciphertext, then the user will send the ciphertext first to his partner, and his partner inputs the ciphertext to return the data to its original form.

Keywords : RSA, Cryptography, PDF Files