Implementasi Kriptografi Asimetris pada Aplikasi Enkripsi dan Dekripsi Teks Berbasis Web menggunakan Algoritma RSA dan ECC = Implementation of Asymmetric Cryptography in Web-based Text Encryption and Decryption Applications using the RSA and ECC Algorithms

Muhammad Diffa Ananda Lukman, author

Abstrak

Keamanan, kerahasiaan, dan integritas informasi atau data menjadi aspek-aspek penting dalam komunikasi digital saat ini. Alasannya adalah untuk mencegah data untuk dapat diakses oleh pihak ketiga dan menjaga konsistensi data selama proses transmisi antara dua titik komunikasi. Hal tersebut dapat dicapai dengan menerapkan autentikasi, enkripsi, dan signature terhadap suatu data pada skema kriptografi asimetris. Penelitian ini membahas mengenai rancang bangun aplikasi web yang mengimplementasikan skema kriptografi asimetris pada proses enkripsi dan dekripsi teks sebagai data. Algoritma kriptografi yang tersedia pada aplikasi ini adalah RSA (Rivest-Shamir-Adleman) dan ECC (Elliptic Curve Cryptography). Aplikasi web ini akan memiliki fitur-fitur, seperti membentuk kunci public dan private, enkripsi data teks, memberi signature terhadap data teks, dekripsi data teks, dan verifikasi signature data teks. Dari implementasi aplikasi web tersebut, akan dilakukan analisis perbandingan performa antara algoritma kriptografi RSA dan ECC dari sisi konsumsi waktu dalam melakukan proses pembentukan kunci, enkripsi, dekripsi, tanda tangan, dan verifikasi terhadap data di setiap ukuran kunci berdasarkan beberapa tingkat keamanan kriptografi.
.....Security, confidentiality and integrity of information or data are important aspects of today's digital communications. The reason is to prevent data from being accessed by third parties and to maintain data consistency during the transmission process between two communication points. This can be achieved by applying authentication, encryption, and signature to data in an asymmetric cryptography scheme. This study discusses the design and development of web applications that implement an asymmetric cryptography scheme in the process of encrypting and decrypting text as data. The cryptography algorithms available in this application are RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography). This web application will have features, such as forming public and private keys, encrypting text data, giving signatures to text data, decrypting text data, and verifying text data signatures. From the implementation of the web application, a performance comparison analysis will be carried out between the RSA and ECC cryptography algorithms in terms of time consumption in keys generation, encrypting, decrypting, signing, and verifying data at each key size based on several levels of cryptographic security measure.