ABSTRAK

Keamanan data merupakan aspek yang sangat penting pada era teknologi informasi. Transmisi data yang tidak aman dapat menyebabkan kerugian yang besar. Untuk mengatasi masalah tersebut, diperlukan ilmu kriptografi. Ilmu kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek-aspek keamanan informasi seperti kerahasiaan dan keaslian data, autentikasi entitas, dan autentikasi sumber data. Contoh-contoh algoritma kriptografi yang sering digunakan saat ini adalah *Elliptic Curve Cryptography* (ECC) dan RSA. ECC menggunakan grup siklik pada himpunan titik pada kurva eliptik di bawah operasi penjumlahan titik untuk melakukan operasi-operasi kriptografi. Salah satu kriptosistem yang termasuk ke dalam ECC adalah *Simplified Elliptic Curve Integrated Encryption Scheme* (S-ECIES). Kriptosistem RSA adalah kriptosistem yang didasarkan pada sulitnya memfaktorkan sebuah bilangan menjadi dua buah bilangan prima yang berbeda. Dalam penelitian ini akan disajikan pengembangan kriptosistem S-ECIES dan RSA dengan cara menggabungkannya dan implementasinya berupa program komputer. Penggabungan kedua kriptosistem tersebut bertujuan untuk mempersulit kriptanalis untuk memecahkan *ciphertext*.

Kata kunci: *Elliptic Curve Cryptography*, *Simplified Elliptic Curve Integrated Encryption Scheme,* Kriptosistem RSA

ABSTRACT

Data security is a very important aspect in the era of information technology. Unsecured data transmission may cause big losses. Cryptography is needed to solve this problem. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Examples of widely used cryptographic algorithm nowadays is Elliptic Curve Cryptography (ECC) and RSA. ECC uses the cyclic group on the set of points in elliptic curve under operation of point addition to do cryptographic operations. One cryptosystem which is classified into ECC is Simplified Elliptic Curve Integrated Encryption Scheme (S-ECIES). RSA cryptosystem is a cryptosystem which is based on the difficulty of factoring a number into two different prime numbers. This research presents the development of S-ECIES and RSA cryptosystem by combining them and implementing the result into a computer program. Combinating those two cryptosystem aims to complicate cryptanalyst to solve the ciphertext.

Keywords: Elliptic Curve Cryptography, Simplified Elliptic Curve Integrated Encryption Scheme, RSA Cryptosystem