ABSTRAK

IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD* (AES) DAN *ELLIPTIC-CURVE CRYPTOGRAPHY* (ECC) PADA KEAMANAN LAYANAN PESAN

IBNU AZIZ NURROHMAN – 1157050071
Jurusan Teknik Informatika

Isu kemanan layanan pesan selalu menjadi perhatian penting dalam era digital seperti saat ini. Pengiriman pesan melalui jaringan internet memungkinkan seseorang melakukan pencurian data pesan ditengah pengiriman yang dilakukan. Untuk mengatasi kekurangan dari keamanan layanan pesan tersebut, diperlukan adanya suatu metode kriptografi. Enkripsi adalah salah satu metode yang digunakan untuk mengamankan sebuah data. Enkripsi mengubah data yang dapat dibaca (*plaintext*) menjadi data yang tidak dapat dibaca (*chipertext*) menggunakan algoritma tertentu. *Advanced Encryption Standard (AES)* adalah algoritma enkripsi simetrik yang memerlukan kunci yang sama untuk proses enkripsi dan dekripsi. Algoritma AES-128 sering digunakan untuk mengamankan data yang bersifat besar, karena kecepatan dan efisiensinya tetapi memiliki kekurangan manajemen yang komplek dan tidak aman. *Elliptic Curve Cryptography (ECC)* adalah algoritma asimetrik yang memerlukan kunci yang berbeda untuk proses enkripsi dan dekripsi. ECC memiliki manajemen key dan keamanan yang baik namun hanya cocok untuk data berukuran kecil. Metode yang diimplementasikan pada penelitian ini adalah menggabungkan algoritma AES-128 dan ECC pada aplikasi berbasis *website* dengan cara data pesan dienkripsi menggunakan algoritma AES dengan kunci yang didapat dari algoritma ECC sehingga didapatkan *chipertext* dan hasil enkripsi yang baik. Kunci yang digunakan merupakan kunci yang diambil dari kurva yang disediakan oleh modul. Metode pengujian menggunakan *black box testing* dimana *black box testing* merupakan metode yang digunakan untuk menemukan kesalahan dan mendemonstrasikan fungsional sistem saat dioperasikan. Setelah melewati tahap pengujian pada implementasi keamanan layanan pesan, maka dapat disimpulkan bahwa sistem keamanan data pesan pengguna menggunakan algoritma AES-128 dan ECC telah berhasil dibangun.

Kata kunci : *AES-128*, *ECC*, dekripsi, enkripsi, keamanan, *chipertext*

ABSTRACT

IMPLEMENTATION OF ALGORITHM *ADVANCED ENCRYPTION STANDARD* (AES) AND *ELLIPTIC-CURVE CRYPTOGRAPHY* (ECC) ON MESSAGE SERVICE SECURITY

The issue of messaging service security has always been an important concern in today's digital era. Sending message over the internet allows someone to steal message data in the middle of the transmission. Encryption is one of the methods used to secure data. To overcome the shortcomings of the security of the message service, it is necessary to have a cryptographic method. Encryption converts readable data (plaintext) into unreadable data (ciphertext) using a specific algorithm. *Advanced Encryption Standard* (AES) is a symmetric encryption algorithm that requires the same key for encryption and decryption. The AES-128 algorithm is often used to secure large data, because of its speed and efficiency, but it lacks complex and insecure management. *Elliptic Curve Cryptography* (ECC) is an asymmetric algorithm that requires different keys for encryption and decryption. ECC has good key management and security but is only suitable for small data sizes. The method implemented in this research is combining AES-128 and ECC methods in website-based applications by means of encrypted message data using the AES-128 algorithm with key obtained from ECC algorithm, then chipertext is obtained and good encryption results. The key used is the key taken from the curve provided by the modul. The testing method uses black box testing where black box testing is a method used to find errors and demonstrate the system's functionality when it is operated. After passing the testing phase on the implementation of message service security, it can be concluded that the user message data security system using the AES-128 and ECC algorithms has been successfully built.

Keywords: AES-128, ECC, decryption, encryption, security, ciphertext