ABSTRACT

In recent year, the Mobile Instant Messenger (IM) has been growing very rapidly. One aspect of concern is about the security of messages which sent via a public connection (internet). There are several methods that have been developed to improve the security aspects of the data on IM. This study aimed to establish a method to secure data that can be used secure the mobile IM to provide the confidentiality and authenticity of the message.

In this research, digital signature is used to implement authentication on mobile communications IM messages. In addition, this research also apply encryption and decryption processes to provide the confidentiality of the data that is not easily read by unauthorized people. In this research, Elliptic Curve Criptography algorithms (ECC) which used to establish an efficient method of securing the mobile IM.

The results show that implementation of ECC algorithms to secure mobile IM is very efficient. This method give small computational time and the length of the ciphertext is almost similar with the plaintext. Therefore, the method that implements the ECC algorithm is very suitable for mobile communication IM.

Keywords : Authentication, Encryption, *Mobile* IM

INTISARI

Beberapa tahun ini, perkembangan *Mobile Instant Messenger* (IM) sangat pesat. Salah satu aspek yang menjadi perhatian adalah tentang keamanan pesan yang dikirim melalui *mobile* IM yang harus melewati jalur publik (internet). Ada beberapa metode yang telah dikembangkan untuk meningkatkan aspek pengamanan data pada komunikasi IM. Penelitian ini bertujuan untuk membangun metode pengamanan data yang bisa digunakan untuk membangun sistem keamanan *mobile* IM yang dapat memberikan aspek kerahasiaan dan keaslian pesan yang dikirim.

Pada penelitian ini, tanda tangan digital merupakan metode yang digunakan untuk melakukan autentikasi pada pesan *mobile* IM . Selain itu, penelitian ini juga menerapkan proses enkripsi dan dekripsi untuk memberikan aspek kerahasiaan data sehingga tidak mudah dibaca oleh pihak yang tidak memiliki kepentingan. Penelitian ini menerapkan algoritma Kurva Eliptik (*Elliptic Curve Criptography*) untuk membangun metode pengamanan yang efisien pada proses komunikasi *mobile* IM.

Hasil penelitian menunjukkan bahwa penerapan algoritma Kurva Eliptik untuk membangun metode pengamanan pada *mobile* IM sangat efisien. Hal ini dibuktikan dengan waktu komputasi yang kecil serta perubahan panjang pesan relatif sedikit. Oleh karena itu metode pengamanan berbasis Kurva Eliptik sangat cocok untuk komunikasi *mobile* IM.

Kata kunci : Autentikasi, Enkripsi, *Mobile* IM