Abstrak

Pesan *Short Message Service* (SMS) masih merupakan cara berkomunikasi yang banyak digunakan, karena masih dianggap murah, cepat, dan simpel. Ketika informasi yang bersifat rahasia dipertukarkan lewat SMS, penting untuk menjaga kerahasiaan dan keaslian pesan, serta memastikan pesan dikirim dan diterima oleh pihak yang sebenarnya. Salah satu teknik yang biasa digunakan untuk memberikan keamanan adalah enkripsi. Berbagai skema enkripsi telah diterapkan pada SMS, diantaranya skema enkripsi *hybrid*, yaitu menggabungkan skema *symmetric* dan *asymmetric*. Salah satu implementasinya adalah penggunaan AES dan *Elliptic Curve Diffie Hellman* (ECDH). Namun seperti diketahui, protokol *Diffie-Hellman* sebagai metode pertukaran kunci tidak menyediakan otentikasi terhadap pihak yang berkomunikasi, yang mana berarti *Man-In-The-Middle (MITM) attack* memungkinkan untuk dilakukan. *Third party server* adalah solusi yang banyak digunakan untuk menyediakan otentikasi. Penelitian ini mengusulkan solusi alternatif yang menyediakan *end-to-end security* yang menjamin layanan keamanan *confidentiality, integrity, authentication,* dan *non-repudiation* yang dibutuhkan untuk mengamankan SMS. Solusi yang diusulkan diharapkan mengatasi permasalahan tersebut tanpa adanya tambahan *hardware* dan tanpa adanya efek negatif pada performa perangkat *mobile phone.* Telah dirancang dan diimplementasikan skema enkripsi *hybrid peer-to-peer* yang menyediakan layanan keamanan *confidentiality, integrity, authentication,* dan *non-repudiation,* menggunakan kombinasi algoritma *Elliptic Curve Diffie Hellman* (ECDH), *Elliptic Curve Digital Signature* (ECDSA) dan AES. ECDSA digunakan untuk menangani otentikasi pertukaran kunci. Berdasarkan pengujian fungsionalitas, rancangan sistem berhasil diimplementasikan pada sistem operasi android. Berdasarkan pengujian performansi pada *plaintext* sepanjang 218 karakter didapat waktu eksekusi enkripsinya adalah 5.57 ms, waktu eksekusi dekripsinya adalah 2.45 ms, dan menghasilkan *ciphertext* sepanjang 333 karakter. Pada sistem enkripsi SMS ini memberikan waktu komputasi yang cukup cepat, namun memberikan hasil *ciphertext* yang panjang.

Kata kunci: ECDH, ECDSA, AES, enkripsi, SMS, Android