ABSTRAKSI

Global System for Mobile Communication (GSM) merupakan sebuah standar teknologi komunikasi selular yang telah berkembang ke seluruh dunia sejak diperkenalkan pada tahun 1991. Sebagai sebuah standar teknologi komunikasi, GSM memiliki suatu sistem keamanan tersendiri yang digunakan untuk melindungi seluruh sistem untuk menghindari gangguan pihak luar yang tidak bertanggung jawab. Tujuan sistem keamanan tersebut antara lain adalah untuk melindungi identitas pelanggan GSM dan melindungi data-data informasi yang dipertukarkan oleh pengguna. Namun ternyata dari penelitian yang dilakukan oleh beberapa ahli, ditemukan beberapa kelemahan didalam sistem keamanan GSM yang masih memungkinkan untuk ditembus pihak luar.

Tugas akhir ini mensimulasikan pengkombinasian metoda *Elliptic Curve Cryptography* (ECC) dengan algoritma A3, A8, dan A5 pada sistem keamanan jaringan GSM yaitu autentikasi, alokasi TMSI, dan penyandian. Penerapan metoda ECC pada sistem keamanan jaringan GSM tersebut dilakukan pada prosedur registrasi, *roaming*, dan *basic call setup*. Parameter yang digunakan sebagai perbandingan dalam analisis hasil simulasi adalah skema sistem keamanan, waktu proses, *data rate* dan pengujian *avalanche effect* untuk mengetahui ketahanan metoda ECC yang diterapkan kedalam sistem.

Hasil yang diperoleh dari tugas akhir ini menunjukkan bahwa metoda ECC hanya bisa diterapkan pada layanan autentikasi dan perlindungan identitas pelanggan. Metoda ECC tidak bisa diterapkan pada layanan penyandian karena terdapat perbedaan mekanisme dengan algoritma A5 yang digunakan dalam proses penyandian. Dampak yang terjadi akibat pengkombinasian metoda ECC ini adalah adanya penambahan waktu proses prosedur registrasi, *roaming*, dan *basic call setup* serta penambahan *data rate* pada beberapa jalur transmisi. Dari hasil simulasi, penambahan waktu yang terjadi masih bisa ditolerir karena waktu yang dibutuhkan pada pemodelan masih terletak pada alokasi rentang waktu yang diijinkan.

Dari pengujian *avalanche effect* terhadap IMSI, TMSI, SRES, RAND, dan Kc, didapatkan bahwa nilai avalanche effect yang paling baik diperoleh dari pengujian *avalanche effect* untuk perubahan satu bit *cipher text*. Dengan hasil tersebut, bisa disimpulkan bahwa pada proses transmisi, metoda ECC memiliki kemampuan yang baik untuk melindungi parameter-parameter keamanan GSM.