

## ABSTRAKSI

Perkembangan teknologi *wireless* saat ini berkembang sangat cepat seiring dengan kebutuhan informasi yang makin tinggi. Hal ini disebabkan oleh beberapa faktor, yaitu : kemampuan komunikasi secara bergerak, keandalan sistem semakin meningkat, kerahasiaan informasi terjamin, biaya pembangunan relatif lebih murah daripada *wireline*, dan ketersediaan pelayanan tinggi; tidak terbatas waktu dan tempat sehingga konsumen dapat berkomunikasi kapan dan dimanapun berada.

*Code Division Multiple Access* (CDMA) merupakan salah satu aplikasi teknologi *wireless* yang memiliki banyak keunggulan seperti tersebut di atas. Sistem CDMA yang digunakan di Indonesia berbasis CDMA2000, merupakan perkembangan dari sistem CDMAone. Metode terbaru yang diaplikasikan pada sistem CDMA di Indonesia adalah penggunaan *Removable User Identity Module* (RUIM) *card* untuk otentikasi dan mendukung fleksibilitas pengguna. Pada sistem GSM, penggunaan kartu seperti ini sudah lama diaplikasikan dan dikenal dengan *Subscriber Identity Module* (SIM) *card*.

Otentikasi merupakan proses dimana *base station* (BS) mengkonfirmasi identitas dari *mobile station* (MS). SSD (*share secret data*) digunakan sebagai informasi dalam melakukan otentikasi. Baik pada RUIM maupun jaringan memiliki informasi ESN, 64 bit kunci otentikasi (A-key) dan angka acak untuk perhitungan otentikasi. Algoritma yang dipergunakan dalam perhitungan otentikasi ini dikenal dengan nama *Cellular Authentication and Voice Encryption* (CAVE).

Dalam proyek akhir ini akan dibahas tentang kinerja RUIM terhadap jaringan berdasarkan pertukaran informasi pada kanal CDMA antara BS dan MS atau sebaliknya. Metode yang digunakan dan parameter yang menentukan keberhasilan suatu otentikasi termasuk dalam pembahasan. Selain itu juga kinerja RUIM yang meliputi konfigurasi dan fungsi operasi. Dari analisis ini diharapkan dapat menjadi pembelajaran khususnya untuk peningkatan layanan keamanan data dalam suatu jaringan yang berbasis CDMA2000.