Abstrak

Algoritma A5/3 merupakan algoritma versi terbaru dari algoritma A5 yang digunakan untuk enkripsi suara dari *mobile phone* ke *Base Transceiver Station* (BTS). Algoritma ini dibuat berdasarkan algoritma KASUMI, yaitu sebuah blok *cipher* yang menghasilkan 64 bit input dari 64 bit output di bawah control kunci 128 bit. Keluaran dari algoritma ini yaitu dua buah blok 114 bit yang akan digunakan untuk enkripsi/dekripsi pada *uplink* dan *downlink.* Aplikasi algoritma A5/3 dibuat sebagai suatu simulator untuk mensimulasikan algoritma tersebut. *Avalanche effect,* waktu proses, dan perubahan besar file, dijadikan sebagai parameter untuk mengukur ketahanan algoritma ini. Berdasarkan pengujian *avalanche effect* yang dihasilkan oleh algoritma A5/3 adalah 51.053% untuk kasus beda satu bit kunci dengan plainteks yang sama. Sedangkan, untuk kasus beda satu bit plainteks dengan kunci yang sama nilainya adalah 0.877%. Waktu proses bertambah sebanding dengan ukuran file, di mana makin besar file maka makin lama waktu prosesnya. Pada aplikasi ini, ukuran file output sama dengan ukuran file input. Hal itu sesuai dengan algoritma A5/3 yang merupakan algoritma *stream cipher*.

Kata kunci: A5/3, enkripsi, dekripsi, *avalanche effect*, waktu proses, besar file