ABSTRAK

Perkembangan teknologi informasi kian pesat, informasi dapat diperoleh dengan mudah dari berbagai sumber. Sayangnya perkembangan teknologi informasi kerap disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab, data yang berisi informasi penting kerap tersebar dan merugikan banyak pihak.

Agar informasi tersebut tidak disalahgunakan, dapat diantisipasi dengan menerapkan ilmu kriptografi, sehingga informasi yang ada tetap terjaga kerahasiaannya. Banyak metode-metode baru pada ilmu kriptografi yang dapat digunakan untuk menjaga informasi yang bersifat rahasia di *level software* maupun *hardware*.

Dalam tugas akhir ini algoritma *stream cipher* Trivium akan diimplementasikan pada FPGA *(Field-programmable Gate Arrays)* Altera Cyclone IV di level *hardware* atau lebih tepatnya pada *prototype IC*. *Input* yang digunakan berupa *biner*. Metode pembangkit deret bilangan acak yang digunakan pada penelitian ini adalah NFSR (*Non-Linear Feedback Shift Register*) serta akan menggunakan bahasa pemrograman Verilog untuk mendeskripsikan berbagai fungsi rangkaian *digital.* Kemudian *hardware* tersebut dapat melakukan proses enkripsi untuk merubah pesan asli (*plaintext*) menjadi sebuah pesan tersandi *(ciphertext)* dan sebaliknya (dekripsi). Hasil dari pengimplementasian tersebut akan dianalisa berdasarkan aspek pengujian yang telah ditentukan. Kemudian performansi algoritma Trivium akan dibandingkan dengan performansi algoritma *stream cipher* berorientasi *hardware* lainnya.

Kata Kunci : Kriptografi, Trivium, Altera