ABSTRAK

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dalam hal pertukaran informasi. Salah satu solusi untuk menjaga keamanan dan kerahasiaan pada proses pengiriman data adalah dengan teknik enkripsi. Enkripsi adalah proses pengubahan data dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti.

GOST merupakan salah satu algoritma enkripsi *block cipher* 32 putaran yang menggunakan struktur *Feistel Network* dan masukan kunci sepanjang 256 bit. Dengan struktur Feistel, algoritma enkripsi memiliki struktur yang sama dengan dekripsi. Perbedaannya hanya terletak pada subkunci yang digunakan. Subkunci dihasilkan dari proses penjadwalan kunci (*key-schedule*). Algoritma *key-schedule* pada GOST sangatlah sederhana, sehingga pada keadaan tertentu hal ini menyebabkan rentan terhadap *related-key attack*.

Salah satu pendekatan untuk mencegah serangan tersebut adalah dengan memaksimalkan *avalanche* pada kunci yaitu dengan cara melewatkan kunci utama (masukan pengguna) ke suatu fungsi hash yang kuat sebelum kunci tersebut diperluas dengan algoritma *key-schedule*.

Tugas akhir ini membahas tentang modifikasi algoritma GOST untuk meningkatkan keamanan terhadap *related-key attack* dengan menambahkan fungsi hash yaitu HAVAL dan SHA-256 sebelum proses penjadwalan kuncinya. Dari pengujian yang telah dilakukan, disimpulkan bahwa *related key attack* tidak bisa diterapkan lagi dan diperoleh peningkatan nilai *avalanche effect* pada algoritma modifikasi GOST.

Kata kunci: *block cipher*, GOST, *key-schedule, related-key attack, Feistel Network, sub-key, avalanche effect.*