

IMPLEMENTASI ENKRIPSI DAN KOMPRESI ALGORITMA RSA DAN SHANNON-FANO PADA LAYANAN SMS ANDROID

Rachmad Nurhidayat
(12.04.111.00064)

Pembimbing 1 : Mulaab, S.Si., M.Kom.
Pembimbing 2 : Dwi Kuswanto, S.Pd., M.T.

ABSTRAK

Di Indonesia, SMS masih menjadi pilihan untuk mengirim sebuah pesan walau masih dibawah *instant messenger* seperti BBM dan WhatsApp, perbedaan yang terlihat antara SMS dan *instant messenger* selain cara pembayaran pengiriman pesannya adalah tingkat keamanan.

Pada *instant messenger* terdapat fitur untuk mengamankan percakapan dengan metode-metode kriptografi yang beragam, sedangkan SMS tidak memiliki fitur tersebut, oleh karena itu dibuatlah SMS dengan tambahan fitur kriptografi.

Kriptografi yang akan digunakan adalah algoritma RSA, algoritma RSA merupakan kriptografi dengan kunci asimetris yang berarti memiliki dua kunci yang digunakan untuk proses enkripsi dan dekripsi, algoritma RSA akan menjadikan plaintext menjadi bertambah jumlah karakternya, sehingga akan ditambahkan fitur kompresi untuk menekan pertambahan jumlah karakternya.

Algoritma kompresi yang akan digunakan adalah *Shannon-fano*, merupakan algoritma *symbolwise* dimana setiap karakter yang akan dikompresi akan diubah menjadi kode biner yang baru. Kompresi ini ditujukan supaya jumlah karakter dari hasil enkripsi tidak begitu banyak.

Hasil dari penelitian ini menyatakan bahwa semakin panjang kunci yang digunakan akan semakin lama proses dekripsi pesan, nilai-nilai *avalanche effect* untuk algoritma RSA berkisar antara 8.53%-27.18%, kemudian untuk nilai *brute force* masing-masing kunci didapatkan 4.119823716-75603807443 tahun, rata-rata rasio dan *space saving* dari kompresi adalah 1.42 dan 29.85%, dari pernyataan-pernyataan tersebut pengguna disarankan menggunakan kunci antara 32-56 bit.

Kata kunci : kriptografi, RSA, kompresi, *Shannon-fano*, SMS, Android