ABSTRAK

IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN ALGORITMA RIVEST SHAMIR ADLEMAN (RSA) UNTUK KEAMANAN PESAN TEXT

Oleh:

BAGUS NUANSYAH
11312503

Keamanan dan kerahasiaan merupakan salah satu aspek yang paling penting pada suatu sistem pesan, data dan informasi. Masalah tersebut masih kurang diperhatikan dari para perancang dan pengelola sistem informasi sehingga masalah keamanan berada di bagian terakhir setelah tampilan. Ilmu yang mempelajari tentang cara-cara mengamankan data atau pesan dikenal dengan istilah Kriptografi, sedangkan dalam langkah-langkah kriptografi disebut algoritma kriptografi. Berdasarkan kunci yang digunakan, algoritma kriptografi dapat dibagi menjadi dua, yaitu algoritma simetrik dan algoritma asimetrik. Pada jurnal Hendri Syahputra yang berjudul "Aplikasi Enkripsi data file teks dengan Algoritma RSA (Rivest Shamir Adleman)" berhasil mengamankan file teks untuk dienkripsi dan dekripsi menggunakan algoritma RSA (Rivest Shamir Adleman), tetapi hanya dapat mengenkripsi dan dekripsi file teks yang panjangnya tidak lebih dari 1000 karakter. Jurnal tersebut yang menjadikan acuan untuk penelitian pertama. Pada jurnal Andi Riski Alvianto yang berjudul "Pengaman Pengiriman Pesan via SMS dengan algoritma RSA berbasis android" berhasil membuktikan bahwa algoritma RSA tidak hanya digunakan untuk keamanan data dan digital signature, tetapi metode ini juga dapat digunakan untuk keamanan pesan teks dengan waktu rata-rata proses enkripsi yaitu 14,925 milisecond per karakter dan dekripsi 4,679 milisecond per karakter, Jurnal tersebut yang menjadikan acuan untuk penelitian kedua. RSA adalah salah satu algoritma kriptografi asimetris (kriptografi kunci-publik) yaitu menggunakan dua kunci yang berbeda (*privatekey)* dan (*publickey*). Kekuatan algoritma RSA tidak hanya terletak pada panjang kuncinya (semakin panjang kunci, maka semakin lama waktu kerja) dan penggunaan kunci-publik dan kunci privat pada umumnya. Kekuatan utama dari algoritma RSA didasarkan pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor prima : faktorkan *n* menjadi dua faktor prima, *p* dan *q*, sedemikian sehingga $n = p \cdot q$.

Kata Kunci: Kriptografi, Kunci, Enkripsi, Dekripsi, Algoritma, RSA.