Abstrak

Pengiriman data-data penting melalui akses internet pada masa sekarang sudah menjadi hal yang biasa. Hal ini menimbulkan semakin berkembangnya dunia kejahatan melalui jaringan internet, seperti penyadapan, pencurian, dan pemalsuan data informasi yang dikirim melalui internet terutama dalam sektor bisnis, perbankan, perdagangan, sampai sektor pemerintahan. Karena itulah kriptografi menjadi pilihan untuk melindungi data.

RSA(Rivers Shamir Adleman) merupakan algoritma kriptografi yang dianggap aman, karena RSA memiliki pemfaktoran bilangan prima yang sangat besar. Sedangkan DES(Data Encryption Standart) merupakan algoritma yang menjadi pilihan untuk menjaga keamanan data. Misalnya digunakan dalam kartu chip yang dimiliki oleh para nasabah bank. DES menggunakan kunci yang sama untuk menyandi (enkripsi) maupun untuk menterjemahan (dekripsi), sedangkan RSA menggunakan dua kunci yang berbeda. Istilahnya, DES disebut sistem sandi simetris sementara RSA disebut sistem sandi asimetris.

Pada Tugas Akhir ini dibuat perangkat lunak untuk menganalisis performansi kedua algoritma dengan parameter : waktu enkripsi, waktu dekripsi, penggunaan memori dan pembengkakan ukuran chipertext. Kesimpulan yang dapat diambil berdasarkan pengujian dan analisis yang dilakukan, didapatkan bahwa RSA dengan menggunakan kunci besar dianggap lebih baik dibandingkan dengan algoritma DES.

Kata kunci: Kriptografi, DES, RSA