ABSTRAK

Algoritma RSA (Rivest-Shamir-Adleman) adalah sebuah algoritma sistem kripto dengan kunci publik yang paling dikenal. Algoritma ini didasarkan pada pemangkatan modulo dari perkalian dua bilangan prima yang besar. Sebuah *plaintext* harus dipangkatkan terlebih dahulu sebelum dikirimkan dengan sebuah bilangan, yaitu e (*public key*). Untuk mengetahui isi pesan tersandi atau *chipertext* itu, penerima harus memangkatkannya dengan kunci miliknya sendiri, yaitu d (*private key*).

Tugas Akhir ini memberikan sebuah observasi baru pada algoritma RSA berkaitan dengan pasangan kunci enkripsi/dekripsi yang tidak tunggal yaitu satu kunci enkripsi mempunyai pasangan kunci dekripsi lebih dari satu, seharusnya 1 kunci enkripsi hanya berpasangan dengan 1 kunci dekripsi saja.

Pertama-tama, akan ditunjukkan gejala ketaktunggalan pada algoritma RSA ini, yaitu dari segi ketaktunggalan kunci enkripsi/dekripsinya. Kemudian, akan dicarikan solusi supaya pasangan kunci enkripsi/dekripsinya tunggal.

Fokus Tugas Akhir ini adalah menganalisa secara matematis pasangan kunci enkripsi/dekripsi algoritma RSA yang tak tunggal. Dengan dua buah bilangan prima p, q dan sebuah kunci publik (e) yang dapat mengenkrip sebuah message (m), kita memperoleh beberapa kunci privat (d) sehingga pasangan kunci publik dan kunci privat tidak tunggal dan agar pasangan kunci publik dan kunci privat tunggal maka syarat yang harus dipenuhi, yaitu : $d_{\phi(n)} \leq d_{\lambda(n)}$. untuk memenuhi syarat tersebut, maka harus mengganti kunci publik (e).

Untuk mempermudah penganalisaan dibuatlah desain prosesnya kemudian dibuat sebuah software sebagai pembantu. Software yang dibuat hanya untuk mempercepat perhitungan proses-proses yang ada karena Tugas Akhir ini merupakan analisa terhadap ketaktunggalan pasangan kunci enkripsi/dekripsi pada algoritma RSA.

Dalam ujicobanya akan diberikan beberapa contoh singkat sebagai ilustrasi argumen-argumen yang ada.