ABSTRAK

Perkembangan teknologi informasi yang pesat seperti sekarang ini dan dukungan komunikasi yang semakin baik maka dibutuhkan suatu cara untuk menjaga keamanan, integeritas, serta keaslian dokumen digital yang tersimpan hanya berdasar angka biner '0' dan '1'. Timbulnya perkembangan teknik kriptografi memungkinkan pengamanan data dalam arti kerahasiaan dan autentikasi / keaslian dapat diwujudkan.

Tentunya jika seseorang ingin mengirim suatu pesan yang sifatnya rahasia, maka ia pasti mengharapkan agar pesan tersebut tidak diketahui atau bahkan dicuri oleh orang yang tidak berhak. Dan salah satu cara untuk mengatasi hal tersebut adalah dengan mengubah pesan yang dikirim ke dalam suatu bentuk yang tidak bisa dimengerti oleh orang-orang yang tidak berhak yaitu dengan menggunakan algoritma RSA.

Algoritma RSA (Rivest-Shamir-Adleman) adalah sebuah algoritma sistem kripto dengan kunci publik yang paling dikenal. Dimana setiap user mempunyai dua buah kunci yaitu *kunci publik* dan *kunci private*, kunci publik adalah kunci yang boleh diketahui oleh orang lain sedangkan kunci private adalah kunci yang digunakan untuk membuka pesan yang disandikan dan tidak boleh diketahui oleh orang lain. Algoritma ini didasarkan pada pemangkatan modulo dari perkalian dua bilangan prima yang besar atau yang disebut dengan metode *Fast Exponentiation.*

Algoritma ini merupakan satu dari sekian banyak algoritma yang dapat membantu untuk menyandikan pesan yang akan dikirim, sehingga dapat mengurangi kemungkinan untuk diketahui/dicuri oleh orang yang tidak berhak.