

ABSTRAK

Di dalam skripsi ini penulis mengangkat pada pembahasan masalah mengenai keamanan data. XML sebagai salah satu format *database* yang tidak tergantung pada *platform* memudahkan pengguna untuk bertukar data karena hanya tersusun dari sekumpulan teks. Berkembangnya penggunaan XML, mulai muncul permasalahan mengenai keamanan data yang terkandung dalam dokumen XML, mengingat XML hanya berupa teks yang sangat mudah dimengerti oleh manusia maupun program komputer.

Salah satu cara untuk menjamin keamanan data XML adalah dengan menyandikan data XML menjadi kode-kode yang sulit dimengerti atau dengan kata lain menggunakan ilmu kriptografi. Dalam kriptografi terdapat *cipher*, atau algoritma yang berfungsi mengubah data asli menjadi data yang sulit dipahami. Dari sekian banyak algoritma kriptografi yang digunakan, algoritma RSA yang cukup populer. Hal ini karena algoritma RSA cukup mudah, tetapi memiliki keamanan yang kuat. Keamanan algoritma RSA tergantung kepada panjang kunci yang digunakan untuk enkripsi data. Selama algoritma untuk memecahkan RSA belum ditemukan algoritma yang efisien, maka selama itu pula keamanan RSA terjamin.

Keamanan data yang diterapkan dalam skripsi ini adalah keamanan pada saat data disimpan dalam media penyimpanan data XML, berarti algoritma RSA disini merupakan sebuah fungsi yang berguna untuk menyandikan data ketika data dimasukkan dan disimpan dalam dokumen XML.

Kata Kunci: *Kriptografi, enkripsi, dekripsi, plainteks, cipherteks, RSA, XML*



UIN

UNIVERSITAS ISLAM NEGERI
SUNAN GUNUNG DJATI
BANDUNG