

ABSTRAK

Judul : Implementasi Pengamanan Data Menggunakan Algoritma Elgamal Berbasis Java Dekstop Pada SMP Negeri 5 Kota Tangerang Selatan

Oleh : Randy Adytia Rahmadany (1511502203)

SMP Negeri 5 merupakan Sekolah Menengah Pertama Negeri Kota Tangerang Selatan. Sebagai instansi yang bergerak di bidang pendidikan, Sekolah Menengah Pertama Negeri 5 mempunyai masalah lokal terkait soal ujian. Untuk melindungi data soal ujian, perlu diterapkan teknologi terkini untuk mengamankan data. Untuk mengamankan data bisa dilakukan dengan cara mengenkripsi. Enkripsi adalah proses mengamankan suatu data dengan suatu algoritma tertentu yang membuat data tersebut tidak dapat dibaca. Supaya data tersebut dapat dibaca, dilakukan proses yang disebut dengan dekripsi. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Dalam melakukan proses dekripsi data dibutuhkan suatu pengetahuan khusus, yaitu kunci. Teknik yang bisa digunakan untuk mengenkripsi serta mendekripsi data adalah kriptografi. Algoritma kriptografi yang digunakan adalah Algoritma Kriptografi ElGamal. Pemilihan Algoritma ElGamal dalam metode kriptografi dikarenakan dalam pembentukan salah satu kuncinya menggunakan bilangan prima dan menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit. Sehingga dengan menggunakan memanfaatkan bilangan prima yang besar dan serta masalah logaritma diskrit yang cukup meyulitkan, maka keamanan kuncinya akan lebih terjamin. Berdasarkan analisis dan perancangan, pembuatan, serta serangkaian uji coba dalam program dari aplikasi kriptografi, hasil penelitian dengan adanya program ini proses penyimpanan dan pertukaran informasi menjadi lebih aman. Data yang dapat digunakan pada aplikasi ini berupa file dokumen dengan ekstensi *.doc, *.xls, *.pdf, dan *.txt.

Kata kunci : Kriptografi, Enkripsi, Dekripsi, Elgamal

LXXIV+74 halaman; 62 gambar; 6 tabel; 3 lampiran