PENGAMANAN DATA PESAN MENGGUNAKAN ALGORITMA ELGAMAL

Hedro Hutabarat (409230019)

ABSTRAK

Algoritma ElGamal merupakan algoritma kriptografi asimetris yangmenggunakan dua jenis kunci, yaitu kunci publik dan kunci rahasia. Tingkat keamanan algoritma ini didasarkan atas masalah logaritma diskret pada grup pergandaan bilangan bulat modulo prima, $\mathbb{Z}_p^* = \{1, 2,..., p-1\}$, dengan p adalah bilangan prima. Sehingga apabila digunakan bilangan prima dan logaritma diskret yang besar, maka upaya untuk menyelesaikan masalah logaritma diskret ini menjadi sia-sia dan dirasakan tidak sesuai dengan isi informasi yang ingin diperoleh.

Pengamanan data pesan dengan menggunakan algoritma ElGamal dapat dilakukan dengan proses penyandian dan tanda tangan digital. Proses penyandian dilakukan dengan tujuan untuk mengubah pesan asli menjadi cipherteks, sehingga pesan tersebut tidak dapat dibaca bagi yang tidak berkepentingan. Sedangkan tanda tangan digital dapat digunakan untuk membuktikan bahwa data yang dikirimkan tidak mengalami modifikasi secara ilegal.