Abstrak

Multimedia Messaging Service / MMS telah beberapa waktu ini dapat dinikmati oleh pengguna layanan seluler di Indonesia, proses yang cepat dengan harga layanan dan kebutuhan gadget yang relative murah dianggap sebagai layanan tambahan yang cukup menarik.

Didalam Paper berjudul "Implementasi Public Key Cryptography pada Multimedia Messaging Service Menggunakan Enkripsi ElGamal" ini, diimplementasikan perangkat lunak untuk melakukan enkripsi pada file teks dan image menggunakan layanan MMS menggunakan metode Kriptografi Kunci Publik dengan algoritma ElGamal untuk dapat mengenkripsi file multimedia sebelum dikirimkan. Analisa yang dilakukan berfokus pada parameter tingkat keamanan, waktu enkripsi-dekripsi dan rasio ukuran *ciphertext-plaintext*.

Dari penelitian ini disimpulkan bahwa implementasi menggunakan public key memiliki kelebihan dalam hal distribusi kunci, namun memiliki kekurangan pada lamanya proses enkripsi dan terjadinya *message expansion* pada *ciphertext.*

Analisa tingkat keamanan dilakukan dari sudut pandang kemungkinan ekstraksi private key dari public key. Karena masalah ini dalam ElGamal sama dengan Permasalahan Logaritma Diskrit, maka pengukuran dilakukan menggunakan algoritma Pollard's Rho. Pengukuran menunjukkan untuk kunci dengan panjang bit 256 dapat dipecahkan dalam ±3 bulan dengan mesin Intel Pentium Dual Core 1.8 GHz, namun dengan tindakan preventif seperti pembangkitan kunci dengan panjang bit yang lebih besar atau pembangkitan kunci baru secara berkala dapat memperbaiki kekurangan keamanan ini.

Kata Kunci: Kriptografi, *Multimedia Messaging Service (MMS)*, Kriptografi Kunci Publik, Enkripsi ElGamal