Abstract

Indonesia's Telecommunication World has never been more eventful with the abundance of service through the telephone network that had been provided by sellular operators. Along with cheaper cost for providing cellular service, service providers tend to provide much more than just the traditional phonecall and text messaging via Short Message Service (SMS)

Multimedia Messaging Service (MMS) has been used and enjoy by cellular user for some time now in Indonesia, fast service and relatively cheap cost for data transmission has deemed MMS to be an interesting service for users.

In this paper entitled, "*Implementation of Public Key Cryptography on Multimedia Messaging Service with the Usage of ElGamal Encryption"*, a software to encrypt files of format text and image using the MMS Service using the Public Key Cryptography with ElGamal Encryption is implemented. And then the output of the system will be analyzed according to following parameters: security, encryption and decryption time and the percentage of filesize ratio between plaintext-ciphertext.

It is concluded from this research that public key implementation is indeed valid for message encryption, with the advantage in key distribution while lacking in the lengthy encryption process and that there is a message expansion.

Security level analysis is conceived from the point of view of key recovery, that is to ecstract the private key from the corresponding public key. Since this problem in the ElGamal corresponds with the Discrete Logarithm Problem, hence the usage of the Pollard's Rho algorithm. And it shows that with the usage of a 256-bit keys,a popular Intel Pentium Dual Core 1.8GHz can recover the private key in approximately 3 months time, but this lacking in security can be dealt with preventive measure such as the usage of a more lengthy keys or the generation of new keys periodically.

Keywords: Cryptography, Multimedia Messaging Service (MMS), Public Key Cryptography, ElGamal Encryption