PENGAMANAN *FILE* DENGAN MENGGUNAKAN *DIGITAL SIGNATURE ALGORITHM* (DSA) (Studi Kasus : Witdia Solusi Indonesia)

Seno Agung Prakoso

Abstrak

Penelitian ini dilakukan untuk pengamanan *file tender* penawaran yang bersifat rahasia tanpa pengamanan pada *file tender* itu sendiri. Pada perkembangan teknologi informasi memberikan kemudahan dalam pengiriman *file* secara elektronik sehingga timbul sebuah celah pada keamanan, terlebih *file* yang sifatnya rahasia. Pada kasusnya banyak perusahaan yang mengirimkan *file tender* untuk pengajuan penawaran tanpa dilakukan pengamanan pada *file* tersebut. *File tender* itu sendiri merupakan *file* rahasia yang digunakan untuk pengajuan suatu proyek yang memiliki format pdf, oleh karena itu *file tender* membutuhkan pengamanan untuk menjaga kerahasiaan dan keaslian data disinilah kriptografi diperlukan. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan menyandikan kedalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam proses pengamanan *file tender* digunakan kriptografi *digital signature algorithm* yang merupakan golongan kunci asimetri. *Digital signature algorithm* memiliki dua kunci untuk proses enkripsi dan dekripsi. Dalam kriptografi *digital signature algorithm* akan menghasilkan chiperteks pada saat proses enkripsi dan pada proses dekripsi *digital siganture algorithm*, chiperteks dari hasil enkripsi akan kembali kebentuk plainteks. Dengan demikian celah dalam pengiriman *file* secara elektronik dapat diatasi dan diamankan.

Kata Kunci : Pengiriman *File*, *File Tender*, Kriptografi, Kriptografi *Digital Signature*, Enkripsi, Dekripsi

SECURITY FILE USING ELGAMAL ALGORITHM AND DIGITAL SIGNATURE ALGORITHM (DSA) (Case Study: Witdia Solusi Indonesia)

Seno Agung Prakoso

Abstract

This study was conducted is sending the file tender for giving a project offer which is a confidential file without a security for the file. Technology development in the ease way in sending file using media eletronic gived a hole for the security, more than that if the file is a confidential file. In this case, many companies who File tender is a classified file that contain a submission of offer that company offer in a project, this file is PDF file. Therefore this file needs to be secured for confidentiality and authenticity with Cryptography. Cryptography is the pratice and study of techniques for secure information by encoding the messages that the meaning cannot be read or understood. In the process for secureting file tender with Cryptography digital signature algorithm which used asymmetry keys. Digital signature algorithm haved two keys that needed in Encryption and Decryption process. In Digital signature algorithm encryption process Digital signature algorithm will generated chipertext, and with decryption process this chipertext neutralized back into beginning file plaintext. The with this the hole in sending file in media eletronic being solved and secured.

Keywords: File Sending, Tender File, Crytography, Crytography Digital Signature Algorithm, Encryption, Decryption