ABSTRAK

Perkembangan teknologi saat ini membuat keamanan pengiriman suatu data atau dokumen menjadi salah satu hal yang perlu diperhatikan. Karena dengan adanya teknologi saat ini, tidak menutup kemungkinan saat proses pengiriman dokumen tersebut ada campur tangan pihak ketiga yang tidak bertanggung jawab untuk merubah isi dokumen sehingga merusak integritas data *(data integrity)*. Salah satu cara untuk menjaga keamanan dan kerahasiaan dokumen atau pesan *(confidentiality* atau *privacy)* pada saat proses pengiriman yaitu dengan melakukan penyandian menggunakan sistem kriptografi terhadap dokumen atau pesan yang dikirim dengan menjadikannya kode-kode atau bentuk lain yang tidak dapat dipahami sehingga tidak dapat diketahui isi pesan yang sebenarnya. Seiring dengan perkembangan teknologi saat ini, untuk memperkuat keamanan, kerahasiaan, serta otentikasi *(auhentication)* pesan yang dikirim, telah berkembang pengamanan pesan dengan *digital signature.* Namun saat ini dalam penerapannya, *digital signature* masih memerlukan pengembangan lebih lanjut. Dari beberapa penelitian sebelumnya, didapat kesimpulan bahwa pada *digital signature* masih terdapat kelemahan pada perhitungan fungsi *hash* yaitu *collision* pada nilai *hash,* sehingga diperlukan penelitian lebih lanjut mengenai penanganan masalah *data collision* pada fungsi *hash.* Mengingat pentingnya hal tersebut, perlu adanya solusi untuk menangani *data collision* yang terjadi. Oleh karena itu penelitian ini dilakukan untuk menganalisis dan mengimplementasikan algoritma ElGamal dan penerapan fungsi SHA-512 untuk penanganan *data collision* pada *digital signature.* Dari hasil penelitian yang dilakukan, fungsi SHA-512 dapat digunakan bersamaan dengan Algoritma ElGamal untuk menjaga keamanan dan kerahasiaan dokumen atau pesan dan dapat menangani masalah *collision* pada nilai *hash* yang sebelumnya terjadi pada pembuatan *digital signature*.

Kata Kunci: *Digital Signature,* kriptografi, *data collision, hash,* Algoritma ElGamal, *SHA*-512.

ABSTRACT

Current technological developments make a delivery security of data or documents be one thing to note. Because with the current technology, it is possible when the document delivery process there is third party intervention is not responsible for the content of the document change that undermines the integrity of the data (data integrity). One way to maintain the security and confidentiality of documents or messages (confidentiality or privacy) during the delivery process by performing encryption using the cryptographic system of the document or message sent by making the codes or other forms that can not be understood so unknowable contents the actual message. Along with current technological developments, to strengthen the security, confidentiality, and authentication messages sent, has been developing a security message with a digital signature. However, currently in its application, digital signature still requires further development. From previous studies, it could be concluded that the digital signature there are still weaknesses in the calculation of the hash function is collision in the hash value, so further research is needed regarding the handling of the problem of data collision in the hash function. Considering its importance, the need for a solution to handle data collision that happened. Therefore, this study was conducted to analyze and implement algorithms ElGamal and application function SHA-512 for handling data collisions on the digital signature. From the research conducted, the function SHA-512 can be used in conjunction with the algorithm ElGamal for keep the security and confidentiality of documents or messages and can deal with problems collision in the hash value that previously occurred in the manufacture of digital signature.

Keywords: Digital Signature, cryptography, the data collision, hash, ElGamal algorithm, SHA -512.