ABSTRACT

Digital Signature is an attribute of authenticity to the hard copy data . The existence of this digital signature, which until now cause more people tend to believe the hard copy data than soft copy form. now with high technology in information, people tend to choose a paper signed rather than the form of data files on the computer. Such as diplomas, certificates, and warrants. The presence of digital signature systems is expected to overcome all problems. Digital signatures can provide confidence to the soft copy as great as the belief in hard copy.

In implementation, the digital signature system will combine two types of data security processes, which use a mix of RIPEMD-160 hash algorithm and RSA asymmetric encryption. The results of this system is a digital signature that can express the authenticity of the data.

In this final project, the hash algorithm will be used for the process of securing data and added a second stage process for the asymmetric encryption . in the first stage system will produce a message digest of data. Then the message digest is the one that use in the encryption algorithm on a second stage . Thus, it is expected that data or document to be delivered can be maintained authenticity, or can be known if it has changed.

System designed in this final project can only receive input type text. The resulting digital signature is a combination of characters and numeric characters. after in investigating the methods of chi - square then the obtained results of $x^2 = 0{,}612$ *for the relationship between the original data and message digest is generated. And generated* $x^2 = 0,933$ *for the relationship between the original data with digital signatures. With the number of chi - aquare this then the digital signature system is compliant with* x^2 *for the digital signature system should be worth less than 3.481.*

Keywords: **digital signature, hash algorithm, asymmetric encryption, RIPEMD-160, RSA**