ABSTRACT

An evolution of information technology too rapidly causes information at the moment most valuable. Because of must be protected to the information with anything procedure. One of general procedure to protect is cryptography. Cryptography is branch of mathematical study which exploit process computation for scrambling data which objective for prevent side which not to allow or know for the data.

In cryptography algorithm, in globally can be able difference with key exchange, symmetric key algorithm and asymmetric key algorithm. Both of them found a weakness, one of a weakness in symmetric key is key exchange relatively difficult, and in the asymmetric key a time of encryption is a long time. One of solution for sending data is using symmetric key and for sending key using asymmetric key, the name of case of like this is hybrid cryptosystem. In side of secret a data necessary also integrity and validity of a data. Because of that one of solution is digital signature.

Symmetric algorithm have been researched is DES, TDES, RC5, IDEA, and AES and for asymmetric algorithm using RSA and Elgamal. Whereas hash function using SHA1 for input Digital Signature Algorithm. The analysis subsystem have done based on many parameter time processing, frequency distribution for appear character, variance of distribution, avallanche effect, and time proccess to do brute force attack.

The researched was showing that performance which optimum was reached by AES for symmetric key algorithm and RSA in asymmetric key algorithm for variance and brute force attack. In addition Elgamal own positive side in processing time relatively was compared with RSA.

Keyword: hybrid cryptosystem, hash function, digital signature.