Abstract

Electronic mail or better known as E-mail, has become a communication media that is very commonly used today. Most people would have to know and use this facility, but not everyone is aware of the dangers that exist. An email is very vulnerable to cyber crimes i.e. tapping, modifying the contents of the email, and the email forgery. A cryptographer named Phil R Zimmermann seeks to solve the email security problems by developing hybrid cryptographic technology called PGP (Pretty Good Privacy). Pair of cryptographic algorithms that are often used to encrypt a message using PGP are CAST and DH/ElGamal algorithm. CAST and DH/ElGamal algorithm become the default algorithm on some versions of PGP.

In this final project will be built a hybrid cryptosystem for email security using AES as a replacement of CAST algorithm and HE-RSA as a replacement of DH/ElGamal. In addition, the need for email for data delivery in secure is data integrity checking and verification process, so the cryptosystem in this final project also apply a digital signature to the hash function SHA3 as input. Performance analysis is done using the parameters of the time process of encryption and decryption, the value of avalanche effect, and bruteforce attack.

The results showed that of the average processing time of encryption and decryption, hybrid cryptosystem AES and HE-RSA is lower than the hybrid cryptosystem CAST and DH/ElGamal. The results of the average value of the avalanche effect of AES-128 algorithm for testing the plaintext difference is 50.9%, higher than the CAST-128 algorithm with a value of 49.4%. And for the average value of the avalanche effect of AES-128 algorithm for testing the key difference is 51.8%, higher than the CAST-128 algorithm with a value of 47.3%. Time bruteforce attack for the HE-RSA 1024 algorithm is $5.70x10^{294}$ years, much longer than the bruteforce attack algorithms DH/ElGamal with time $2.85x10^{294}$ years.

Keywords: email security, encryption, hybrid cryptosystem, PGP, AES, HE-RSA.