ABSTRACT

TIME COMPLEXITY COMPARISON ANALYSIS OF ASYMMETRIC CRYPTOGRAPHY ALGORITHM (RSA, ECC, AND ELGAMAL) IN THE ENCRYPTION, DECRYPTION, AND DIGITAL SIGNATURE PROCESS

By
Melinda Utami
17102133

The development of digitalization that is happening at this time makes a shift in people's behavior in carrying out daily activities to be online or digital. The more activities that are carried out online, the more data will be uploaded and transmitted via the internet. This can lead to online crimes such as hacking, data theft, illegal use of personal data, and others. To avoid various types of digital crimes, a solution that can be used is to implement a security system using cryptography. This study compares the encryption time, data decryption and digital signature as well as the time complexity value of the RSA asymmetric cryptography algorithm, ElGamal. The parameters used in this study are key generation time for encryption and decryption, encryption time, decryption time, key generation time for digital signatures, and digital signature creation time. The system used in the study was built using C++ language with the NTL (Number Theory Library) library. The data obtained is in the form of time data which is then compared from each algorithm. The time complexity value is obtained from the sum of the complexity of each step contained in the pseudocode of each algorithm. The results of the time comparison show that the RSA algorithm is better than the ECC and Elgamal algorithms in encryption, decryption, and digital signature times and has a constant time growth and does not increase too much. The RSA algorithm has the highest complexity value with a value of $O(n \log n^2)$ which indicates that the time growth is linear multiplied by logarithm. The lowest complexity value is ElGamal with a value of $O(\log n)$ which indicates that the time growth is logarithmic.

Keywords: Cryptography, RSA, ECC, ElGamal, Time Complexity.