ABSTRACT

Banking crime cases have increased in recent years, one of which is skimming (copying) data or information on the user's ATM card. This condition is caused by a security system on an Automated Teller Machine (ATM) that still uses a conventional (fixed) Personal Identification Number (PIN).

Securing an ATM machine using dynamic PIN containing One Time Password (OTP) can be a solution to this problem. OTP is only used for one session and with a short time limit. If it is not immediately used, then the OTP will expire or expire. This OTP generate using an OTP algorithm based on time value synchronization and randomly selected six characters using Pseudorandom Number Generator (PRNG), namely the Linear Congruential Generator (LCG).

Comparison of the results of QoS measurements on OTP generation using three algorithms before and after the DoS attack, the PRNG algorithm is an effective algorithm compared to the LCG and Math.random algorithms. Because, the PRNG algorithm produces lower transmission delay and high throughput compared to the others, namely the transmission delay before the DoS attack is 16.3864 ms, and 309.525 bps. When an attack has occurred, it is worth 17.35 ms and a value of 535.92 bps. On the results of measurements of SMS, has a value of 9.7ms, and is categorized very good for the value according to TIPHON standards. In testing the randomness of the sequence of numbers generated from three algorithms, that the LCG algorithm is the most effective compared to other algorithms. Because the sequence of numbers produced is not a tendency to any of the numbers.

Keywords: *security, one time password, pseudorandom number generator, linear congruential generator, skimming*.