ABSTRAK

Kasus kejahatan perbankan semakin meningkat dalam beberapa tahun terakhir, salah satunya yaitu *skimming* (penyalinan) data atau informasi pada kartu ATM pengguna. Kondisi ini disebabkan oleh sistem keamanan pada Mesin Anjungan Tunai Mandiri (ATM) yang masih menggunakan *Personal Identification Number* (PIN) bersifat konvesional (tetap).

Pengamanan mesin ATM menggunakan PIN dinamis berisikan *One Time Password* (OTP) dapat dijadikan solusi terhadap masalah tersebut. OTP hanya digunakan untuk satu kali sesi dan dengan batas waktu yang singkat. Jika tidak segera digunakan, maka OTP akan kadaluarsa atau hangus. Untuk pembangkitan OTP menggunakan algoritma OTP berbasis sinkronisasi nilai waktu dan dipilih enam karakter secara acak menggunakan *Pseudorandom Number Generator* (PRNG) yaitu *Linear Congruential Generator* (LCG).

Perbandingan dari hasil pengukuran QoS terhadap pembangkitan OTP menggunakan tiga algoritma sebelum dan sesudah mengalami penyerangan DoS, algoritma PRNG menjadi algoritma yang efektif dibandingkan dengan algoritma LCG dan Math.random. Karena, algoritma PRNG menghasilkan *transmission delay* yang lebih rendah dan *throughput* yang tinggi dibandingkan dengan yang lainnya, yaitu *transmission delay* sebelum penyerangan DoS sebesar 16,3864 ms, dan *throughput* sebesar 309,525 bps. Ketika sudah terjadi penyerangan,*transmission delay* bernilai 17,35 ms dan nilai *throughput* 535,92 bps. Pada hasil pengukuran *delay* terhadap SMS, memiliki *delay* sebesar 9,7ms, dan dikategorikan sangat bagus untuk nilai *delay* menurut standar TIPHON. Pada pengujian keacakan deret angka yang dihasilkan dari tiga algoritma, bahwa algoritma LCG yang paling efektif dibandingkan dengan algoritma lainnya. Karena deret angka yang dihasilkan tidak kecenderungan pada salah satu angka.

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