DESAIN DAN IMPLEMENTASI SISTEM KEAMANAN MESIN ANJUNGAN TUNAI MANDIRI (ATM) MENGGUNAKAN ONE-TIME PASSWORD (OTP) BERBASIS SMS GATEWAY

DESIGN AND IMPLEMENTATION SECURITY SYSTEM OF AUTOMATED MACHINE TELLER (ATM) *USING ONE-TIME PASSWORD* (OTP) *BASED ON SMS GATEWAY*

Elga Nurlaela[1], Dr. Nyoman Bogi Aditya Karna[2], Arif Indra Irawan, S.T., M.T.[3]
[1,3]Prodi S1 Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom
[1]gaelgaelga@student.telkomuniversity.ac.id, **[2]aditya@telkomuniversity.co.id**,
[3]arifirawan@telkomuniversity.ac.id

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 Idenification Number* (PIN) bersifat konvesional (tetap).

Upaya untuk meningkatkan pengamanan pada mesin ATM yaitu, dengan mengganti kartu magnetik dengan *smart card* dan mengganti PIN statis dengan pin dinamis. Dalam penelitian ini, OTP dan *smart card* diintegrasikan dengan *Raspberry Pi,* untuk pembangkitan OTP pada sistem menggunakan algoritma *Linear Congruential Generator*. OTP ini akan dikirimkan secara *real time* kepada pengguna SMS dengan menggunakan gammu sebagai penghubung atau SMS *gateway* antara *database server* dan *client.*

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

Kata Kunci: *Security*, OTP, PRNG, LCG, *Skimming*

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 conven- tional (fixed) Personal Identification Number (PIN).

Securing an ATM machine using dynamic PIN containing One Time Password (OTP) can be a solution to this problem 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.

Keywords: Security, OTP, PRNG, LCG, skimming

1. Pendahuluan

1.1 Latar Belakang Masalah

Di era globalisasi yang serba canggih ini, peran teknologi perbankan dalam dunia bisnis tidak perlu diragukan lagi. Salah satu contoh teknologi perbankan adalah Anjungan Tunai Mandiri (ATM). ATM merupakan mesin komputerisasi yang dirancang untuk melakukan transaksi pengguna tanpa perlu ada interaksi dengan manusia. Seiring bergulirnya waktu, pengguna ATM semakin meningkat jumlahnya. Mereka menggunakan kartu ATM untuk transaksi perbankan seperti deposito, transfer, permintaan saldo, penarikan saldo, dan lain-lain [1].

Akhir-akhir ini terdapat beberapa kasus pembobolan pada mesin ATM. Pelaku pembobolan tersebut menggunakan teknik skimming (penyalinan) kartu debit atau kredit dengan cara data yang sudah disalin dari kartu akan dipindahkann ke kartu lain Kejadian ini terjadi disebabkan dari PIN yang masih bersifat konvensional (tetap) [2]. PIN konvensional adalah PIN yang biasanya dapat diubah hanya jika diperlukan, seperti pengguna lupa PIN atau PIN sudah tidak

Salah satu solusi terkait untuk meminimalisir masalah tersebut yaitu mengganti PIN statis menjadi PIN dinamis dengan menggunakan metode *One Time Password* (OTP). Metode autentikasi ini dimana setiap pengguna yang hendak mengakses suatu layanan harus terlebih dahulu memasukkan sebuah *dynamic* PIN. OTP merupakan *password* yang berlaku hanya untuk satu kali sesi atau transaksi saat memasuki suatu akun pada sistem komputer atau perangkat digital lainnya.

2. Dasar Teori

2.1 Skimming

Skimming adalah konsep yang digunakan untuk kejahatan dalam *cyber* dengan metode menggandakan atau menyalin informasi yang terdapat pada *magnetic stripe* yang ada pada kartu kredit mapun ATM atau debit secara illegal[5].

2.2 Personal Identification Number (PIN)

Nomor identifikasi pribadi adalah nomor yang berisikan kata sandi numerik atau alfa numerik yang digunakan dalam proses mengautentikasi pengguna dalam mengakses sistem[4].

2.3 One Time Password (OTP)

One Time Password (OTP) adalah suatu *password* yang hanya digunakan satu kali sesi login atau transaksi tunggal. OTP tidak menggunakan *password* yang sama untuk setiap melakukan transaksi, sehingga jika pihak asing berhasil merekam *password* OTP yang sudah digunakan maka dia tidak akan dapat menyalahgunakan password tersebut karena sudah tidak berlaku lagi [5].

2.4 Pseudorandom Number Generator (PNG)

Biasa dikenal dengan Pembangkit Bilangan Acak Semu. Bilangan acak yang dihasilkan oleh komputer menggunakan rumus-rumus matematika adalah bilangan acak semu (pseudo), karena pembangkit bilangan dapat diulang kembali [6].

2.5 Linear Congruential Generator (LCG)

Salah satu algoritma *pseudorandom number generator* yang tertua dan paling populer adalah *Linear Congruential Generator* (LCG). Algoritma ini diciptakan oleh D. H. Lehmer pada tahun 1951. Teori dari algoritma ini mudah dipahami dan dapat diimplementasikan secara cepat [7].

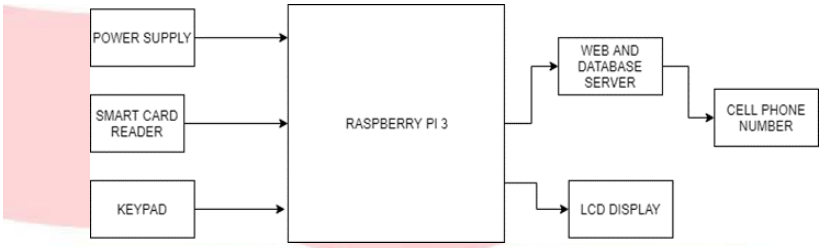
3. Pembahasan

3.1. Desain Sistem

Sistem yang dirancang adalah sebuah Anjungan Tunai Mandiri (ATM) meng- gunakan autentikasi PIN secara realtime atau OTP dan smart card sebagai kartu ATM. Pembangkitan OTP dilakukan menggunakan Linear Congruential Generator (LCG) lalu disimpan pada database lalu dikirimkan ke pengguna melalui SMS atau pesan teks.

3.1.1 Blok Diagram

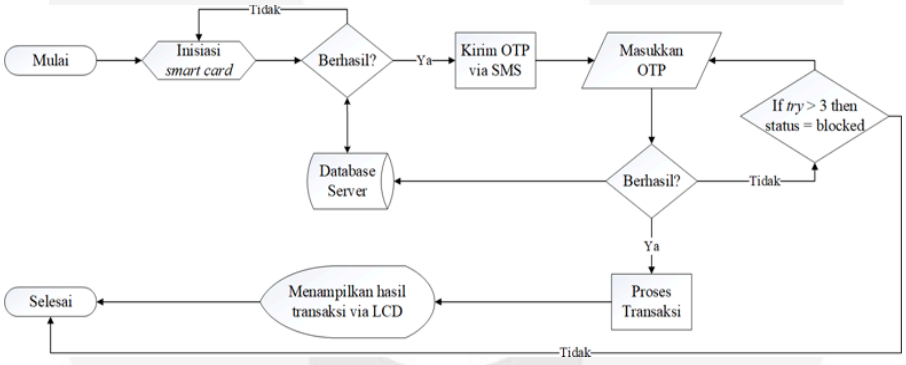
Dalam merealisasikan sistem prototipe ini, dibutuhkan diagram blok yang da- pat menggambarkan sistem secara umum. Masing-masing blok sistem memiliki fungsi tersendiri. Berikut ini gambaran umum dari sistem yang akan dirancang dan diimpelementasikan pada penelitian ini yang dapat dilihat pada gambar 3.1



Gambar 3.1 Blok Diagram Umum Sistem

3.1 Diagram Alir Mesin ATM

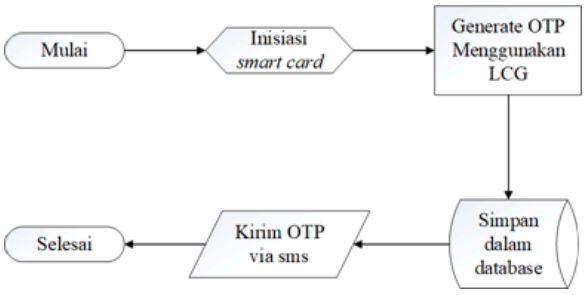
Pada penelitian ini sistem akan mengirimkan OTP melalui SMS, dapat diamati Diagram alir sistem ATM pada gambar 3.2



Gambar 3.2 Diagram Alir Sistem ATM

3.1.2 Cara Kerja Pembangkitan One Time Password (OTP)

Pada penelitian ini, menerapkan PIN pada kartu ATM yang bersifat real-time. Untuk melakukan pembangkitan PIN secara real time yang berisikan bilangan acak diperlukan algoritma untuk dapat melakukan pembangkitan tersebut. Pembangkitan PIN dapat dillihat pada Gambar 3.3.



Gambar 3.3 Diagram Alir Pembentukan OTP

3.2 Skenario Pengujian

3.2.1 Pengujian Quality of Service (QoS) Pembangkitan OTP

Tahap ini dilakukan pengujian performansi sistem pada Quality of Service (QoS). Pengujian ini dilakukan dengan cara membandingkan pembangkitan OTP pada algoritma math.random, PRNG, dan LCG sesudah dan sebelum penyerangan dengan Denial of Service (DoS). Melakukan penyerangan dengan DoS ini guna mengetahui availability atau ketersediaan yang dibutuhkan suatu informasi.

3.2.2 Pengujian QoS pada SMS gateway

Tahap ini dilakukan pengujian performansi delay terhadap layanan SMS gateway. Pengujian ini dilakukan guna untuk mengetahui kualitas layanan sebagai end user atau penerima OTP pada nasabah

3.2.3 Uji Keacakan Menggunakan Randomness Testing

Tahap ini dilakukan pengujian terhadap kemunculan bilangan acak pada pem- bangkitan OTP menggunakan pendekatan randomness testing. Pengujian ini di- lakukan guna mengetahui tingkat keacakan bilangan yang telah dihasilkan dari pembangkitan OTP.

3.2.4 Pengujian Subjektif Mean Opinion Score

Mean opinion score (MOS) adalah ukuran yang digunakan untuk kualitas dan kinerja keseluruhan dari sistem.

4. Hasil dan Analisis

4.1 Pengujian dan Analisis QoS Sebelum DoS Attack

Implementasi dan Pengujian sistem *One Time Password* (OTP) pada Anjungan Tunai Mandiri (ATM) dilakukan berdasarkan parameter dan performansi kerja sis- tem yang telah dibuat. Pengujian ini dilakukan dengan mengukur QoS sebelum dan sesudah sistem dilakukan serangan *Denial of Service* (DoS) Attack, mengukur Qos pada penerimaan OTP melalui SMS *gateway* menggunakan *tool* wireshark, dan menganalisa perbandingan tingkat keacakan angka yang dihasilkan pada algoritma *Math Random, Pseudorandom Number Generator, dan Linear Congruential Gen- erator* menggunakan pendekatan *randomness testing*

4.2 Pengujian dan Analisis Sistem

Pengujian sistem merupakan hal terpenting dalam melakukan penelitian yang bertujuan untuk menemukan kekurangan-kekurangan sistem yang akan dibuat dan mengetahui sistem bekerja sudah memenuhi kriteria atau parameter yang ditentukan.

4.2.1 Pengujian dan Analisis QoS Sebelum DoS Attack

Pada tahap ini akan dilakukan pengujian terkait performansi sistem yang di- rancang, dengan menyaring protokol Transmission Control Protocol (TCP) yang bekerja pada port yang digunakan pada database server atau MySQL, yaitu port 3306 dengan wireshark. Pada port 3306 menyaring paket sebanyak tujuh (7) paket pada setaip pembangkitan bilangan acak.

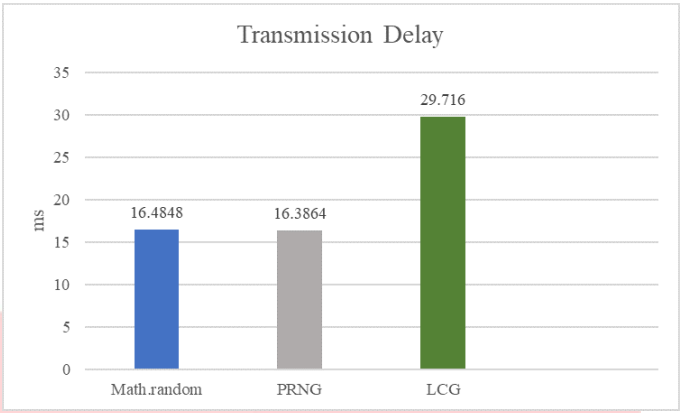
Dibawah ini merupakan hasil pengukuran QoS sebelum mengalami DoS attack pada tabel 4.1.

Tabel 4.1: Hasil Pengukuran QoS Sebelum DoS Attack

Algoritma	Transmission Delay (ms)	Packet Loss %	Throughput (bps)
Math.random	16,4848	0	308,762
PRNG	16,3864	0	309,525
LCG	29,716	0	169,067

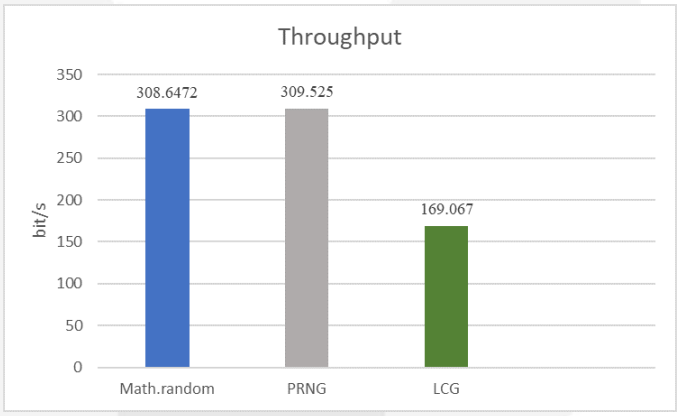
Gambar 4.1 Analisis QoS Sebelum DoS Attack

Pengukuran ini dilakukan selama 29 detik pada setiap pembangkitan bilangan acak. Total paket yang diterima sebesar 628 bytes. Berikut hasil pengukuran berupa grafik pada gambar 4.1



Gambar 4.1: Grafik delay sebelum DoS Attack

Pada gambar diatas, algoritma math.random memiliki nilai *transmission delay* sebesar 16,4848 ms, algoritma PRNG memiliki nilai *transmission delay* sebe- sar 16,3864, sedangkan algoritma LCG memiliki nilai *transmission delay* sebesar 29,716, dari hasil tersebut menunjukan bahwa algoritma PRNG memiliki nilai *delay* paling rendah diantara algoritma lainnya dan nilai *delay* tersebut dikategorikan bagus. Untuk algoritma LCG nilai *delay* yang didapatkan tinggi dibanding algo- ritma pembandingnya, maka nilai *delay* yang dihasilkan berkategorikan buruk. Un tuk hasil pengukuran *throughput* bisa diamati pada gambar 4.2



Gambar 4.2: Grafik *throughput* sebelum DoS Attack

Pada gambar diatas, algoritma math.random memiliki nilai *throughput* sebesar 308,762, algoritma PRNG memiliki nilai *throughput* sebesar 309,525, sedangkan algoritma LCG memiliki nilai *throughput* sebesar 169,067, dari hasil ini menun- jukan bahwa algoritma LCG memiliki nilai *throughput* yang berkategorikan buruk karena nilai tersebut paling rendah dibandingkan dengan algoritma pembandingnya.

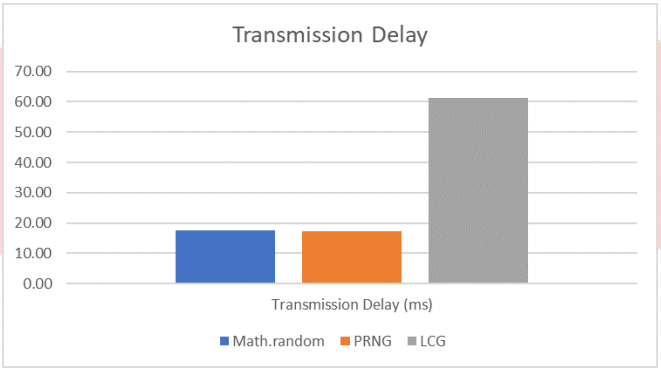
4.2 Pengujian dan Analisis QoS Sesudah DoS Attack

Pada pengujian QoS ini menyaring protokol TCP yang bekerja pada port 3306, dikarenakan MySQL bekerja pada port 3306. Pengujian dilakukan dengan penyerangan DoS.

Dalam pengujian ini, dimana paket yang dikirim sebesar 999999 dengan setiap paket memiliki nilai sebesar 250 bit dan menyerang secara spesifik pada port 3306. Penyerangan DOS dilakukan pada target Amazon RDS yang merupakan database server. Pengujian dilakukan dengan waktu rata-rata 16 detik dari ketika melakukan *login* pada sistem prototipe hingga *logout* dan menghasilkan OTP baru. Berikut hasil pengukuran QoS yang sudah mengalami DoS attack pada tabel 4.3

Tabel 4.3: Hasil Pengukuran Setelah DoS *Attack*

Algoritma	Transmission Delay	Packet Loss %	Throughput
Math.random	17,53	0	517,97
PRNG	17,35	0	535,92
LCG	61,39	0	167,32



Gambar 4.2 Grafik Delay Setelah DoS Attack

Pada gambar diatas setelah dilakukan penyerangan DoS, algoritma math.random memiliki nilai transmission delay sebesar 17,53 ms, algoritma PRNG memiliki nilai transmission delay sebesar 17,35 ms sedangkan algoritma LCG memiliki nilai transmission delay sebesar 61,39, dari hasil tersebut menun- jukan bahwa algoritma LCG memiliki nilai transmission delay yang berkategorikan buruk, karena nilai transmission delay yang dihasilkan oleh LCG paling tinggi.

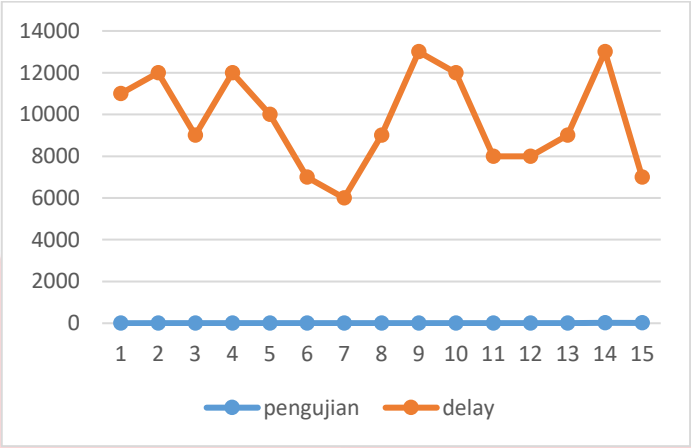
4.3 Pengujian dan Analisis Delay Pengiriman SMS

Pengujian ini akan dilakukan dengan menggambil 15 sample data untuk men- ganalisis *delay*, sehingga didapatkan nilai rata-rata *delay*. Hasil pengukuran bisa diliat pada tabel 4.4

Tabel 4.4 Delay SMS

Pengujian Ke-	Delay (ms)
1	11000
2	12000
3	9000
4	12000
5	10000
6	7000
7	6000
8	9000
9	13000
10	12000
11	8000
12	8000
13	9000
14	13000

15	7000
RATA RATA	9733,33 ms



Gambar 4.3 Delay SMS

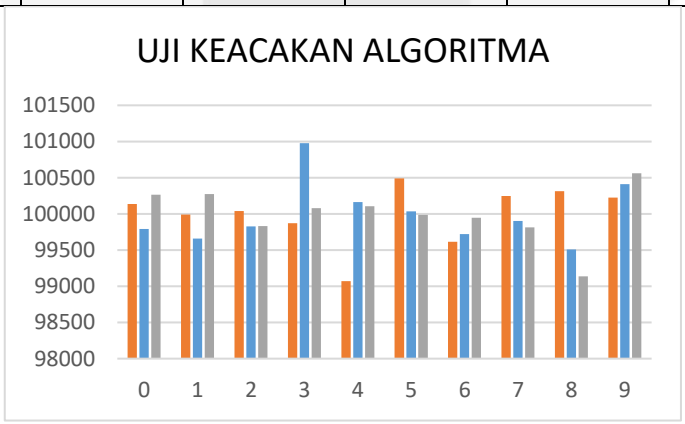
Hasil pengamatan menunjukan bahwa nilai rata-rata *delay voice* pada SMS sebesar 9,7 ms. Gambar 4.3 menunjukan *delay* terendah yaitu 7000 ms dan *delay* tertinggi 13000 ms

4.4 Pengujian Testing Randomness Terhadap Algoritma LCG

Data yang didapatkan dari hasil pengujian dapat dilihat pada Tabel 4.8

Tabel 4.4 Uji Keacakan Algoritma

PRNG		Math.Random		LCG	
Serial Test	Amount	Serial Test	Amount	Serial Test	Amount
0	99793	0	100135	0	100266
1	99660	1	99989	1	100274
2	99828	2	100041	2	99831
3	100975	3	99872	3	100080
4	100165	4	99071	4	100107
5	100037	5	100492	5	99985
6	99722	6	99615	6	99947
7	99902	7	100246	7	99812
8	99507	8	100313	8	99136
9	100410	9	100225	9	100561
SUM	999999	SUM	999999	SUM	999999



Gambar 4.4 Grafik Uji Keacakan Algoritma

Dalam grafik ini menjelaskan bahwa tingkat keacakan pada algoritma LCG lebih baik dibanding dengan algoritma PRNG dan Math.random, karena tidak memperlihatkan kecenderungan pada salah satu angka acak walaupun pada angka 7 dan 8 terlihat mengalami penurunan yang signifikan.

5. Kesimpulan

1. Metode dengan One Time Password bisa menanggulangi kasus tindak ke- jahatan skimming pada mesin ATM karena OTP ini bersifat dinamis atau berubah-ubah untuk satu kali penggunaan.
2. Perbandingan dari hasil pengukuran QoS terhadap pembangkitan OTP meng- gunakan tiga algoritma sebelum dan sesudah mengalami penyerangan DoS, algoritma PRNG menjadi algoritma yang efektif dibandingkan dengan algo- ritma LCG dan Math.random. Karena, algoritma PRNG menghasilkan *trans- mission 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 ter- jadi penyerangan,*transmission delay* bernilai 17,35 ms dan nilai *throughput* 535,92 bps. Nilai *delay* pada masing-masing algoritma mengalami kenaikan karena penyerangan DoS yang menyerang *database server* membuat kinerja sistem menjadi lambat.
3. Di penelitian ini menggunakan provider telkomsel untuk dapat mengirimkan SMS ke *user* sehingga hasil rata-rata *delay* yang didapatkan pada SMS adalah 9,7 ms. Dengan hasil tersebut delay tersebut dikategorikan sangat bagus menurut standar TIPHON.
4. Pada uji keacakan bilangan yang dihasilkan algoritma LCG, tingkat keacakan pada algoritma LCG cukup optimal, karena tidak memperlihatkan kecen- derungan pada salah satu angka acak walaupun pada angka 7 terlihat men- galami penurunan yang tidak signifikan.
5. Berdasarkan responden dari kuesioner mengenai penelitian ini adalah bahwa pengguna ATM dan mempunyai kartu debit setuju jika cybercrime sangat berbahaya seperti skimming, dan juga setuju jika penelitian ini diimplemen- tasikan dimasyarakat.

Daftar Pustaka:

[1]M. M. K. Al Rawahi and S. S. K. Nair, “Detecting skimming devices in atm through image processing,” in *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*.IEEE, 2015, pp. 1–5.

[2]E. D. Dimaunahan, A. H. Ballado, F. R. G. Cruz, and J. C. Dela Cruz, “Mfcc and vq voice recognition based atm security for the visually disabled,” in *2017IEEE 9th International Conference on Humanoid, Nanotechnology, In- formation Technology, Communication and Control, Environment and Man- agement (HNICEM)*, Dec 2017, pp. 1–5.

[3]V. Padmapriya and S. Prakasam, “Enhancing atm security using finger- print and gsm technology,” *International Journal of Computer Applications*, vol. 80, no. 16, 2013.

[4]H. Swathi, S. Joshi, and M. K. Kiran Kumar, “A novel atm security system using a user defined personal identification number with the aid of gsm tech- nology,” in *2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC)*, Feb 2018, pp. 1–5.

[5]D. Kumar, A. Agrawal, and P. Goyal, “Efficiently improving the security of otp,” in *2015 International Conference on Advances in Computer Engineering and Applications*, March 2015, pp. 912–915.