PEMBANGKIT BILANGAN RANDOM DENGAN METODE LCM PADA PIN VOUCHER
(Studi Kasus : SMU NEGERI 22 BANDUNG)

Iska Dameuli HN[1], Mahmud Imrona, Drs, MT[2], Retno Novi D, Ssi, MT[3]

[1,2,3]Departemen Informatika Institut Teknologi Telkom, Bandung
[1]angel_4smile@yahoo.com, [2]mhd@stttelkom.ac.id, [3]rvi@stttelkom.ac.id

Abstrak

Pembayaran biaya administrasi sekolah secara manual mempunyai beberapa kelemahan, misalnya siswa harus antri, orang tua/wali murid sulit mengontrol pembayaran anaknya, dan pelayanannya lambat. Oleh karena itu dibutuhkan sistem pembayaran yang bersifat on-line, yang mampu melayani transaksi dan informasi dari siswa, kapan dan dimanapun dengan memanfaatkan SMS Gateway dan web sebagai medianya. Dalam melakukan transaksi, proses authentifikasi dilakukan menggunakan 12 digit PIN yang dihasilkan dari pembangkitan bilangan random dengan metode *Linear Congruent Method* (LCM). Pin tersebut digunakan sebagai alat pembayaran uang sekolah secara on-line, baik via Web maupun SMS gateway.

Hasil pengujian menunjukkan bahwa kualitas dari bilangan random yang dihasilkan oleh *Linear Congruential Generator (LCG)* berbeda-beda, tergantung pada nilai *seed*, nilai parameter a, c, dan m. Oleh karena itu, pemilihan dari tiap nilai parameter tersebut harus diperhatikan. Tidak ada algoritma yang bisa menghasilkan bilangan yang benar-benar random. LCG mengalami kegagalan dalam pengujian menggunakan *The Binary Rank Test for 32x32 matrices*, *The Bitstream Test*, *The Birthday Spacing Test*, *The Binary Rank Test* for 6x8 matrices karena nilai P yang lebih besar dari 0.975, dan dalam *The A Parking Lot Test* karena nilai P yang lebih kecil dari 0.025. Walaupun begitu, LCG tersebut masih dianggap cukup baik dalam membangkitkan bilangan random, karena hanya gagal dalam 5 tes tersebut.

Kata kunci : bilangan random, *Linear Congruent Method*, *Linear Congruential Generator*, SMS Gateway, Web, dan pin

Abstract

Payment of school administration in manual has some weakness, for example students have to queue up the, parent difficult to control payment of his child, service is slowing. Therefore required a system of payment on-line, which capable to serve the transaction and information from student, anytime and anywhere by using SMS Gateway and web as its media. In transaction, authentication process using 12 digit of PIN generated from random number with Linear Congruent Method (LCM). The Pin used as medium of exchange of school fee on-line via Web and also SMS gateway.

Result of the test indicate that the quality of Linear of Congruent Generator (LCG) is different each other, depend on parameter value from seed, a, c, and m. Therefore, elections of each parameter value have to be paid attention too. There is no algorithm which can generate the true random number. LCG has failure in examination use the The Binary Rank Test for 32x32 matrices, The Bit Stream Test , The Birthday Spacing Test, The Binary Rank Test for 6x8 matrices because value of P is larger than 0.975, and in The A Parking Lot Test because value P which is smaller than 0.025. Nevertheless, the LCG still be assumed good enough in generate the number random, because only fail in 5 tests above.

Keyword: number random, Linear of Congruent Method, Linear of Congruential Generator, SMS Gateway, Web, and pin.

1. Pendahuluan

Pada saat ini, bilangan random banyak digunakan dalam kehidupan sehari-hari. Ada banyak aplikasi yang menggunakan bilangan random tersebut, misalnya dalam bidang kriptografi. Kita memerlukan sebuah bilangan untuk melakukan enkripsi pada email, untuk menandatangani dokumen secara digital, pembayaran elektronik dan lainnya. Selain itu untuk permainan (*game*), simulasi matematika dan fisika, statistik dan lain-lain. Dimana dalam semua bidang tersebut, adanya bilangan random sangat membantu dalam melakukan aktivitas kita.

Perkembangan dunia telekomunikasi yang sangat cepat ditandai, salah satunya, dengan munculnya teknologi komunikasi *nirkabel* atau *wireless*. Teknologi ini digunakan oleh beberapa instansi penjual jasa untuk memberikan layanan yang sifatnya *on-line*, antara lain: layanan transaksi dan informasi selama 24 jam.

Seperti kita ketahui, pembayaran biaya administrasi sekolah secara manual mempunyai

beberapa kelemahan, antara lain: dalam melakukan transaksi pembayaran siswa harus antri, orang tua/wali murid kesulitan mengontrol pembayaran anaknya, pelayanan yang lambat dan pihak sekolah lambat dalam mengambil keputusan yang berhubungan dengan masalah keuangan. Untuk itu dibutuhkan sebuah layanan aplikasi yang sifatnya *on-line* kepada peserta didik, wali murid dan masyarakat untuk menangani transaksi pembayaran di sekolah, seperti pembayaran BP3, SPP, dan biaya lainnya, sehingga transaksi dan informasi terhadap pembayaran dapat dilakukan dengan cepat, tepat dan akurat. Wali murid dapat mengontrol pembayaran anaknya dari mana pun dan kapan pun melalui SMS atau web.

Oleh karena itu, dalam tugas akhir ini akan dianalisis dan diimplementasikan suatu aplikasi pembangkit bilangan random dengan menggunakan metode *Linear Congruent Method (LCM),* dimana 12 digit bilangan random yang dihasilkan, digunakan sebagai PIN untuk proses autentifikasi pembayaran, baik melalui SMS *gateway* maupun melalui web.

Berdasarkan paparan tersebut, maka didapatkan masalah-masalah berikut ini:

1. Bagaimana cara kerja metode *Linear Congruent Method* (LCM).
2. Bagaimana membangkitkan bilangan random dengan metode LCM pada pin voucher pembayaran yang dapat digunakan sebagai *validasi/authentikasi* pada saat pembayaran biaya administrasi sekolah.
3. Bagaimana cara mengkonversi data SMS berupa teks ke mode PDU atau sebaliknya dengan menggunakan bahasa pemrograman Visual Basic.
4. Bagaimana cara mengambil data (SMS) dari *handphone* modem dan mengirimkan kembali *request* dari siswa/wali murid melalui GSM modem dengan melakukan *query* terlebih dahulu ke dalam *database* .
5. Bagaimana membuat web yang dapat digunakan untuk melakukan transaksi dan informasi pembayaran biaya administrasi sekolah.
6. Bagaimana membangun *database* yang dapat digunakan untuk merekam transaksi dan informasi pembayaran biaya administrasi sekolah.

Adapun maksud dan tujuan dari pembuatan Tugas Akhir adalah sebagai berikut:

1. Merancang dan membuat pembangkit bilangan random dengan menggunakan metode *Linear Congruent Method* (LCM).
2. Mengukur dan menganalisis kinerja perangkat lunak yang dihasilkan, yakni Pembangkit Bilangan Random dengan metode LCM pada Pin Voucher.
3. Merancang dan membuat SMS *gateway*.
4. Merancang dan membuat web.

Agar pembahasan pada pembuatan tugas akhir terfokus maka penulis memberikan batas masalah sebagai berikut:

1 Aplikasi web dan SMS gateway disini hanya sebagai sistem pendukung aplikasi generator random, sehingga tidak dibahas secara mendalam.
2 Bilangan random yang dihasilkan terdiri dari 12 digit bilangan.
3 SMS gateway hanya dapat memproses SMS bila inbox pesan dalam keadaan kosong, Sehingga tidak bisa melayani SMS yang datang secara bersamaan.

Metodologi pembahasan pada Tugas akhir ini menggunakan metodologi sebagai berikut:

a. Studi Pustaka.
Pengumpulan data dan referensi dari beberapa buku dan literatur serta browsing melalui internet yang berhubungan dengan permasalahan yang ada.
b. Analisis masalah dan kebutuhan perangkat lunak yang akan dibangun.
c. Perancangan dan Implementasi perangkat lunak.
Tahap perancangan perangkat lunak yang terdiri dari :
    1. Perancangan dan pembuatan sistem pembangkit bilangan random sebagai PIN voucher dengan menggunakan metode LCM.
    2. Perancangan dan pembuatan SMS Gateway
    3. Perancangan dan pembuatan Web
d. Pengujian perangkat lunak.
Pengujian ini dilakukan dengan menguji bilangan random yang dihasilkan oleh generator LCG pada Diehard Battery Test suite. Lalu dilakukan uji coba transaksi pembayaran melalui Web dan SMS.
e. Analisis keluaran aplikasi.
Menganalisa output dari hasil pengujian *Diehard Battery Test Suite.*
f. Penyusunan laporan

2. Bilangan Random

2.1 Definisi

Bilangan random sangat penting bagi banyak orang karena banyak digunakan dalam berbagai macam tujuan. Sebagian digunakan untuk kepentingan penelitian ilmiah, sebagian untuk simulasi, memilih pemenang dari suatu undian dan kompetisi atau pada *game* komputer.

Syarat bilangan random yang baik adalah :

1. *Unpredicted*, yaitu bilangan yang muncul tidak dapat ditebak.
2. Tidak mempunyai pola.
3. *Uniformity*, yaitu setiap bilangan mempunyai kesempatan muncul yang sama.

4. *Independent,* yaitu tiap bilangan yang dihasilkan tidak bergantung pada nilai bilangan sebelumnya.

2.2 Random Number Generator

Di dalam buku teks statistik klasik, angka-angka acak diciptakan dengan mengambil bola yang dinomori ke luar dari suatu kotak yang berisi sejumlah bola bernomor yang diketahui jumlahnya. Jika jumlah bola yang ada didalam kotak jumlahnya sedikit, maka hal tersebut masih mungkin dilakukan. Tetapi jika jumlah bolanya dalam jumlah yang sangat besar, maka hal tersebut akan susah dan tidak efektif dilakukan.

Karena hal tersebut dan pertimbangan lainnya, maka dilakukan komputerisasi generator bilangan random/acak. Pembuatan angka-angka yang acak bukan merupakan hal yang mudah, karena komputer adalah suatu mesin deterministik. Karena itulah mustahil untuk membuat angka-angka acak/bilangan yang benar-benar random tanpa adanya perangkat keras tambahan.

2.2.1 True Random Number Generator

True random number secara definisi tidak dapat terprediksi. TRNG dilakukan dengan melakukan sampling entropi sumber dari alam dan memprosesnya melalui komputer. Misalnya Random.org menggunakan *atmospheric noise* dari radio dan Lavarand.sgi.com menggunakan Lava Lite® lamps sebagai entropi sumber.

Tabel 0-1 : Kelebihan dan kelemahan TRNG

True Random Generator	
Kelebihan	**Kelemahan**
Tidak mempunyai periode	Lambat dan tidak efisien
Bilangan random yang dihasilkan tidak dapat diprediksi	Sangat sulit untuk diinstal dan dijalankan
Tidak ada ketergantungan di antara tiap bilangan (*independent*)	Deretan bilangan yang sudah dibangkitkan tidak dapat dihasilkan/diulang kembali.
Tingkat keamanannya tinggi	Biaya implementasinya mahal
Bagus secara konsep, tidak berdasarkan pada suatu algoritma tertentu.	Ada kemungkinan dapat dimanipulasi

2.2.2 Pseudorandom Number Generator

Pseudorandom Number Generator (PNRG) atau dalam bahasa indonesia Pembangkit bilangan acak semu adalah sebuah algoritma yang membangkitkan sebuah deret bilangan yang tidak benar-benar acak. Keluaran dari pembangkit bilangan acak semu hanya mendekati beberapa dari sifat-sifat yang dimiliki bilangan acak. Bilangan acak semu banyak digunakan dalam beberapa seperti untuk simulasi dalam ilmu fisika, matematika, biologi dan sebagainya, dan juga merupakan hal yang sangat penting dalam dunia kriptografi

2.2.3 Linear Congruent Method

Jenis PRNG yang dibahas disini adalah Linear Congruential Generator (LCG). LCG ditemukan oleh D.H Lehmer. Tak lama sesudah itu, banyak programmer menggunakan metode LCG tersebut untuk menghasilkan bilangan random dalam jumlah besar dan waktu yang cepat. Programmer pada saat itu hanya membutuhkan kecepatan pembangkitan bilangan random saja, tanpa memperhatikan kerandoman bilangan tersebut secara statistika. Karena itu, ada banyak generator LCG yang gagal melalui pengujian kerandoman statistika.

Linear Congruent Method banyak dipakai untuk mengbangkitkan bilangan acak Y_1, Y_2, Y_3…, Y_n yang bernilai [0,m] dengan memanfaatkan nilai sebelumnya. Untuk membangkitkan bilangan acak ke-n+1 (Y_n+1) dengan LCM, didapat definisi [3]:

$$I_{(n+1)} = (aI_{(n)}+c) \mod \quad (1)$$

Keterangan:
$I_{(n+1)}$ = bilangan random baru yang dihasilkan
I_n = nilai awal atau nilai sebelumnya
a , c, m = parameter
dengan a, c dan m sebagai nilai pembangkit dan I_0 sebagai nilai awal.

3. Contoh ilustrasi

Proses pembangkitan bilangan random pada LCG diinisiasi dengan penentuan nilai konstanta yang sudah ditentukan sebelumnya, yang disebut dengan *seed*. *Seed* ini pada faktanya merupakan I_1, bilangan pertama pada output LCG. LCG dengan parameternya dapat ditulis dengan fungsi notasi seperti LCG(A,C,M,*seed*).
Contohnya LCG(3,0,10,1) akan diinisiasi dengan perhitungan $I_1 = (3 . 1 + 0) \mod 10$, yang hasilnya adalah 3. Lalu iterasi selanjutnya dilakukan dengan mengganti nilai $I_{(n-1)}$ yang sebelumnya 1 menjadi 3. Sehingga iterasi dari LCG(3,0,10,1) akan menghasilkan keluaran 1, 3, 9, 7...

Pemilihan dari parameter LCG, A, C, M menentukan kualitas kerandoman bilangan dari keluaran yang dihasilkan. Karena penggunaan modulus matematika dalam LCGs membentuk sebuah daerah hasil yang tetap, maka sangat mudah untuk menghabiskan atau menyelesaikan periodenya dan berakhir dengan deretan bilangan yang sama secara berulangkali.

Dari formula LCM di atas dapat disimpulkan periode dari Linear Congruential Generator tersebut paling banyak adalah sebesar nilai m, atau bahkan

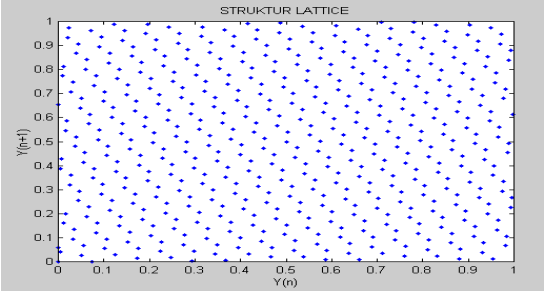
lebih kecil dari itu. Agar LCG mempunyai periode yang *full* (lengkap), maka ada beberapa faktor yang perlu diperhatikan :

1. c and m merupakan bilangan relatif prima.
2. a-1 is bisa dibagi dengan faktor prima dari m.
3. a-1 merupakan kelipatan dari 4, bila m merupakan kelipatan 4.
4. $m > \max(a, c, I_0)$
5. $a > 0, c > 0$

Karena itu, kualitas dari masing-masing LCG berbeda, dipengaruhi oleh parameter di atas. Bila pemilihan nilai parameter I_0, a, c dan m kurang baik, maka tingkat kerandomannya akan kurang baik. Hal ini dapat kita lihat dari struktur *lattice* yang dihasilkan. Sebagai contoh, kita dapat melihat contoh percobaan di bawah :

Percobaan :

Nilai a = 75, c = 2 dan m = 2048, jumlah pembangkitan=1000, hasil struktur *lattice*-nya sebagai berikut :



Gambar 3-1: Struktur Lattice Percobaan

Dari rumus diatas, dapat diketahui bahwa ada hubungan antara bilangan yang dihasilkan sekarang dengan bilangan yang sebelumnya. Untuk mengatasi masalah ketergantungan (*dependent*) tersebut, maka penulis melakukan proses *shuffling* pada bilangan yang dihasilkan sebelumnya.

4. Penutup

4.1 Kesimpulan

Kesimpulan yang diperoleh dalam pengerjaan Tugas akhir ini adalah :

1. Kualitas dari *Linear Congruential Generator* berbeda-beda, tergantung pada nilai parameter nilai awal, a, c, dan m. Oleh karena itu, pemilihan dari tiap nilai parameter tersebut harus diperhatikan.
2. Adanya proses *shuffling*, membantu mengatasi masalah LCG pada properti *independent* (kebergantungan dari bilangan yang muncul berurutan), karena bilangan yang dihasilkan diacak posisinya.
3. Tiap kali melakukan proses pembangkitan bilangan random, ada bilangan yang dibuang karena digit bilangan random kurang dari 12 digit.
4. Bilangan random yang dihasilkan oleh LCG gagal dalam beberapa tes uji kerandoman dari *Diehard Battery Test*, yang menggambarkan bahwa LCG tersebut tidaklah benar-benar random. Tapi masih dianggap cukup baik, karena hanya gagal dalam 4 tes.
5. Tidak ada algoritma yang benar-benar dapat menghasilkan bilangan acak secara sempurna selama pembangkit yang digunakan adalah komputer yang memiliki sifat deterministik.
6. Bilangan yang benar-benar acak hanya dapat dihasilkan oleh True Random Generator melalui perangkat keras (hardware).
7. SMS *Gateway* mampu mengenali *handphone user*, format SMS, PIN yang dikirimkan, dan jenis pembayaran yang diinginkan.
8. Web mampu mengenali *account user*, pin yang dimasukkan, jenis pembayaran, membuat laporan keuangan per hari, per bulan, laporan per tahun dan laporan per siswa

4.2 Saran

Aplikasi ini sangat mungkin untuk dikembangkan dengan lebih baik dan beragam.

1. Penggunaan metode lain, yang lebih baik dari LCM, seperti *Blum-blum shub*, atau *True random generator* agar kualitas dari bilangan yang dihasilkan lebih baik lagi.
2. Penggunaan format SMS yang lebih efesien lagi, agar tidak membingungkan dan merepotkan user.
3. Pengembangan sistem pendukung SMS gateway agar dapat melayani transaski SMS yang datang secara bersamaan.

Daftar Pustaka:

[1] [Feindt,M. G. Quast. M. Kreps. T. Kuhr. J. Heuser. *Moderne Methoden der Datenanalyse.* Fakult¨at f¨ur Physik. 2006..

[2] Hojtsy, Gabor, "*PHP Manual*", PHP Documentation Group, 2005.

[3] "Linear Congruential Method", http://www.wikipedia.com

[4] http://www.itl.nist.gov/div898/handbook/eda

[5] I.L. Heiberg, Lipsiae. *Euclid's Elements in Greek.* Latine interpretatus est.Greek: 1884.

[6] "Inferential Statistic "., http://faculty.vassar.edu/lowry

[7] " *PARADIGM Registration-Randomisation Software"*., http://telescan.nki.nl/paradigm.html

[8] Peebles, P. Z., Jr. " Probability, Random, Variables, and Random Signal Principles ", McGraw-Hill, New York, 2001.