Jurnal Teknik Elektro Vol. 8 No. 2 ISSN 1411 - 0059
Juli - Desember 2016

Modifikasi *Linear Congruential Generator* untuk Sistem Pengacakan Soal pada *Computer Based Test* (CBT)

Arimaz Hangga[1] dan Hendro Eko Prabowo[2]

[1] *Jurusan Teknik Elektro, Fakultas Teknik, Universitas Negeri Semarang*
Kampus UNNES, Sekaran, Gunungpati, Semarang, Jawa Tengah, 50229, Indonesia
[2] *Jurusan Teknik Informatika, Institut Teknologi Sepuluh November*
Kampus ITS, Keputih, Sukolilo, Surabaya, Jawa Timur, 60111, Indonesia
ari.maz.hangga@gmail.com[1], hendro.prabowo15@gmail.com[2]

Abstrak— Model penilaian *Paper Based Test* (PBT) memiliki kekurangan yaitu rentan tindak kecurangan selama proses ujian berlangsung. Salah satu penyebab terjadinya tindak kecurangan ini adalah adanya kesamaan soal pada masing-masing siswa. Pengembangan model *Computer Based Test* (CBT) diharapkan dapat mengurangi keterbatasan PBT. Sistem pengacakan soal pada CBT merupakan salah satu cara pencegahan kesamaan soal dalam pelaksanaan ujian untuk masing-masing siswa. Algoritma modifikasi *Linear Congruential Generato* (LCG) dapat digunakan untuk membangun sistem pengacakan soal pada CBT. Penggunaan variabel *a,b* dan *m* yang berbeda dalam algoritma modifikasi LCG tidak memberikan perbedaan yang signifikan dalam hal pola acak soal. Penggunaan bilangan koprima dan prima pada algoritma modifikasi LCG akan memiliki pola acak yang sama dengan bilangan koprima, prima dan fibonacci.

Kata kunci— Pengacakan soal, Modifikasi *Linear Congruential Generator, Computer Based Test*

I. PENDAHULUAN

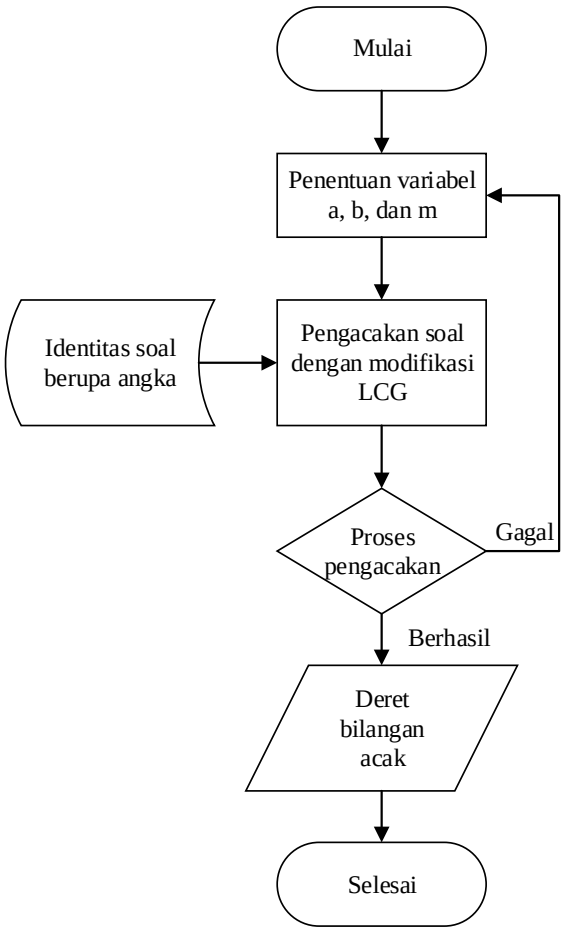
Keberhasilan siswa dalam mempelajari materi yang disampaikan dapat diketahui berdasarkan hasil belajar siswa. Seiring dengan perkembangan teknologi informasi dan komunikasi, penilaian *Computer Based Test* (CBT) mulai diterapkan dalam proses penilaian hasil belajar siswa. Penilaian CBT memiliki beberapa kelebihan dibandingkan dengan *Paper Based Test* (PBT) antara lain : lebih efektif dan efisien dalam penggunaan waktu, sumber daya manusia dan biaya pelaksanaan ujian [1].

Dalam pelaksanaan ujian berlangsung perlu memperhatikan tindak kecurangan yang mungkin dilakukan oleh siswa. Salah satu penyebab terjadinya tindak kecurangan pada pelaksanaan ujian dikarenakan adanya kesamaan soal pada masing-masing siswa [2]. Tindak kecurangan dalam pelaksanaan ujian dapat dikurangi dengan menerapkan sistem pengacakan soal pada sistem CBT.

Sistem pengacakan soal ini dapat dibangun dengan menggunakan metode *Pseudo Random Number Generator* (PRNG). Penggunaan metode PRNG dapat menghasilkan bilangan acak melalui algoritma kriptografi dengan sumber pembangkit dari variabel-variabel yang digunakan pada algoritma [3]. Algoritma *Linear Congruential Generator* (LCG) merupakan salah satu algoritma dengan menggunakan metode PRNG. Metode LCG menggunakan algoritma yang bersifat rekursif linear yang dikombinasikan dengan fungsi modulus [4]. Berdasarkan adanya kebutuhan untuk mengurangi tindak kecurangan pada CBT, maka penelitian ini diharapkan dapat memberikan sistem pengacakan soal dengan memodifikasi metode LCG.

II. METODE PENELITIAN

Penentuan nilai variabel yang akan digunakan pada metode modifikasi LCG merupakan tahap awal dalam pembentukan sistem pengacakan soal. Variabel yang harus ditentukan adalah variabel *a*, *b* dan *m*. Penerapan variabel *m* dengan beberapa variasi agar dapat diketahui tingkat perbedaan pola yang dihasilkan pada metode modifikasi LCG. Beberapa variasi variabel *m* yang digunakan antara lain : 10, 20, 30, 40 dimana nilai-nilai ini mewakili jumlah soal yang digunakan pada ujian CBT.Pada variabel *b* menggunakan bilangan prima, koprima dan fibonacci sebagai pembatasan jumlah variabel. Hasil dari pengacakan soal ini akan menunjukkan pola kesamaan soal berdasarkan bilangan yang digunakan pada variabel *b*.



Gambar 1. Algoritma pembangunan sistem pengacakan soal

Gambar 1. terlihat bahwa setelah penentuan identitas soal yang akan digunakan dan penentuan variabel *a*,*b* dan *m* maka dapat dilakukan proses pengacakan soal dengan modifikasi LCG. Sistem akan meminta penentuan ulang variabel *a*,*b* dan *m* apabila terjadi kegagalan selama proses pengacakan soal. Hasil dari pengacakan soal adalah deret bilangan yang merupakan identitas masing-masing soal.

III. Hasil Dan Pembahasan

A. Model Matematis

Penurunan algoritma LCG akan menghasilkan algoritma modifikasi LCG yang digunakan sebagai model matematis dalam sistem pengacakan soal. Metode LCG digunakan untuk menentukan deret angka sedangkan metode modifikasi LCG menggunakan deret tersebut yang akan dimasukan ke dalam matrik. Pada persamaan (1) merupakan model matematis algoritma LCG [5] :

$$x_{i+1} = (ax_i + b)\ mod\ m \quad (1)$$

dimana x_{i+1} adalah bilangan acak ke-i dari deretnya, *a* adalah variabel pengali, x_i adalah bilangan acak sebelumnya, *b* adalah variabel penambah dan *m* adalah variabel modulus. Persamaan (1) akan diturunkan menjadi matrik dengan orde (*x*,*y*). Persamaan (2) dapat digunakan untuk menentukan orde *x* pada baris matrik [6] :

$$x_{i+1} = (a_1 x_i + b_1)\ mod\ m \quad (2)$$

sedangkan model matematis untuk menentukan orde y sebagai kolom matrik dapat menggunakan persamaan (3) :

$$y_{i+1} = (a_2 x_i + b_2)\ mod\ m \quad (3)$$

Dimana x_{i+1} adalah bilangan acak orde x ke-i dari deretnya, y_{i+1} adalah bilangan acak orde y ke-i dari deretnya, x_i adalah bilangan acak sebelumnya pada orde *x* dan y_i adalah bilangan acak sebelumnya pada orde *y*.

Model matematis modifikasi LCG diturunkan dari model matematis LCG yang disesuaikan pada matrik yang digunakan. Jika matrik *M* merupakan matrik yang digunakan pada sistem pengacakan soal maka pembentukan matrik *M* dapat diketahui dengan menggunakan persamaan (4) sebagai berikut [7] :

$$M_i = M[x_{i+1}\ mod\ p][y_{i+1}\ mod\ q] \quad (4)$$

dimana *p* adalah jumlah baris pada matrik, *q* adalah jumlah kolom pada matrik dan *i* adalah bilangan cacah.

B. Hasil Pengacakan Soal Metode Modifikasi LCG

Algoritma modifikasi LCG telah berhasil didapatkan dengan menggunakan perbedaan variabel *m* yang mewakili jumlah soal tes dan pembatasan variabel *b*. Kombinasi deret bilangan koprima, prima dan fibonacci digunakan sebagai manipulasi variabel *b*.

Berdasarkan Tabel I terlihat bahwa pola acak yang dihasilkan dari masing-masing kombinasi variabel *b* hampir memiliki kesamaan. Hal ini dikarenakan manipulasi yang dilakukan hanya pada variabel *b* sedangkan variabel lain (*a* dan *m*) menggunakan nilai yang sama. Jika deret yang terbentuk dari masing-masing kombinasi deret memiliki kesamaan maka pola acak juga akan memiliki kesamaan.

TABEL I. Pola Pengacakan Terhadap Variabel b

Jumlah Soal	Parameter		Koprima dan Fibonacci	Koprima dan Prima	Koprima, Prima dan Fibonacci
	a	m			
10	1	10	2, 2, 2, -8, 7	2, 2, 2, -8, 7	2, 2, 2, -8, 7
20	1	20	12, -8, 12, -8, -3	12, -8, 12, -8, -3	12, -8, 12, -8, -3
30	1	30	12, -18, 12, -18, 17	24, -6, -6, -6, -1	24, -6, -6, -6, -1
40	1	40	-8, -8, 32, -8, 23	-8, -8, 32, -8, -23	-8, -8, 32, -8, -23

TABEL II. BILANGAN PERTAMA UNTUK 4 DERET PERTAMA

Deret Bilangan	Deret untuk Variabel b		
	Koprima dan Fibonacci	Koprima dan Prima	Koprima, Prima dan Fibonacci
1	17	17	17
2	13	9	9
3	3	13	13
4	7	1	1

Tabel II menunjukkan bahwa nomor soal pertama dari hasil pembentukan 4 deret pertama untuk masing-masing kombinasi. Nomor soal pertama pada deret ke-1 memiliki kesamaan bilangan yaitu 17. Hal ini dikarenakan nilai pada variabel *a*, *b* dan *m* memiliki kesamaan. Akan tetapi bilangan selanjutnya pada masing-masing kombinasi variabel *b* memiliki perbedaan. Hal ini dikarenakan adanya perbedaan penentuan variabel *b* akan mempengaruhi pembentukan matrik M. Pembentukan matrik akan menentukan hasil akhir dari pengacakan soal dimana ukuran matrik M akan merubah pola dari x_i dan y_i. Oleh karena itu hasil pengacakan dari masing-masing kombinasi variabel *b* akan berbeda.

IV. KESIMPULAN

Pola acak soal menggunakan metode modifikasi LCG dengan penggunaan pembatasan bilangan pada variabel *b* tidak memberikan perubahan signifikan dibandingkan dengan algoritma LCG. Penggunaan algoritma modifikasi LCG mempunyai pola acak yang sama antara bilangan koprima dan prima dengan bilangan koprima, prima dan fibonacci.

REFERENSI

[1] S. Simin dan A. Heidari, "Computer-based Assessment: Pros and Cons", *Elixir International Journal*, vol. 55, pp. 12732-12734, 2003.

[2] D.L. Mc Cabe dan W.J. Bowers, "Academic Dishonesty Among Males in College : A Thirty Year Perspective", *Journal of College Student Development*, vol. 5, pp 5-10. 1994.

[3] K.M. Martin, "Everyday Cryptography: Fudamental Principles and Applications", *Oxford University Press Inc.*,New York, pp. 253-259. 2012.

[4] D. Salomon, "Data Privacy and Security", *Springer-Verlag New York Inc.*, New York, pp. 97-100. 2003.

[5] D.E. Knuth, "The Art of Computer Programming 2nd Ed.", Addison-Wesley Publishing Company, Canada, pp. 9-16. 1981.

[6] R.S. Katti, dkk, "Pseudorandom Bit Generation Using Coupled Congruential Generator", *IEEE Transactions on Circuits and System II :Express Briefs*, vol. 57, pp.203-207. 2010.

[7] I Made D. Biantara, "Implementation Coupled Linear Congruential Generator Methods for Questions of Pattern Randomization", *International Conference on Vocational Education and Electrical Engineering (ICVEE)*, pp. 247-250, 2015.