MODIFIKASI METODE *LINEAR CONGRUENTIAL GENERATOR* UNTUK OPTIMALISASI HASIL ACAK

I Made Divya Biantara[1)], I Made Sudana[2)], Alfa Faridh Suni, Suryono[3)], Arimaz Hangga[4)]
[1,2,3,4)] Jurusan Teknik Elektro, Pendidikan Teknik Informatika dan Komputer
Universitas Negeri Semarang, Semarang, Indonesia
e-mail : imadenation@students.unnes.ac.id

Abstrak
Pelaksanaan ujian secara konvensional dianggap kurang efektif dan efisien karena membutuhkan biaya yang besar dan waktu yang lama dalam pelaksanaannya sehingga perlu dilakukan perbaikan dengan mengubah sistem ujian menjadi komputerisasi. Dalam setiap pelaksanaan ujian perlu memperhatikan tindak kecurangan yang dilakukan siswa berupa mencontek dan kerja sama bertukar jawaban. Penelitian ini bertujuan untuk memberikan soal acak yang berbeda kepada setiap siswa dengan menggunakan metode Linear Congruential Generator (LCG). Akan tetapi penggunaan metode LCG masih memiliki kelemahan dimana hasil pengacakan mudah ditebak sehingga perlu adanya optimalisasi pengacakan yaitu menggunakan dua LCG dan bantuan matrik yang menjadi metode Coupled Linear Congruential Generator (CLCG). Metode modifikasi CLCG menghasilkan pengacakan yang lebih baik dan pola yang lebih rumit dibandingkan dengan metode LCG.

Kata Kunci : *LCG, CLCG, Pola, Acak*

1. PENDAHULUAN

Pendidikan merupakan hal penting yang harus dimiliki oleh setiap orang. Kualitas pendidikan dapat diketahui dengan melalui pelaksanaan ujian untuk mengetahui pencapaian kemampuan dan keberhasilan dalam memahami bidang studi yang ditempuhnya [1]. Seiring perkembangan teknologi informasi dan komunikasi sistem ujian sudah tidak lagi menggunakan media konvensional melainkan sudah secara komputerisasi. Pelaksaan ujian secara konvensional kurang efektif dan kurang efisien karena membutuhkan biaya yang besar untuk mencetak soal, membutuhkan waktu yang lama untuk distribusi soal dan pemeriksaan jawaban masih secara manual. Selain itu menurut Nasution [5] bahwa pelaksanaan ujian secara konvensional rentan terhadap kebocoran soal yang akan diajukan sebelum ujian dan kecurangan yang dilakukan seperti mencontek jawaban teman. Dengan adanya ujian secara komputerisasi akan memiliki keunggulan berupa pengurangan biaya dan waktu yang dapat menutup kekurangan pada pelaksanaan ujian secara konvensional.

Pelaksanaan ujian secara konvensional maupun komputerisasi perlu memperhatikan terhadap tindak kecurangan yang mungkin saja terjadi. Hal tersebut dipicu karena kepercayaan diri siswa menurun ketika mengerjakan soal ujian sehingga lebih percaya kepada siswa lain. Selain itu pemberian tipe soal ujian yang sama akan memberikan siswa peluang untuk mencontek dan bekerja sama.

Berdasarkan permasalahan di atas, penelitian ini bertujuan untuk memberikan solusi berupa penerapan tipe soal yang berbeda-beda untuk setiap siswa. Penerapan dilakukan pada pelaksanaan ujian secara komputerisasi sehingga dapat meminimalkan biaya dan waktu yang dibutuhkan serta meminimalkan tindak kecurangan yang mungkin dilakukan oleh siswa. Penerapan pengacakan soal pada ujian komputerisasi sering menggunakan metode *Linear Congruential Generator (LCG)*. Akan tetapi penggunaan metode *LCG* masih memiliki kekurangan sehingga pada penelitian ini menggunakan metode *Couple Linear Congruential Generator (CLCG)*.

2. METODE PENELITIAN

Penelitian ini menggunakan metode pengacakan yang dimodifikasi untuk mendapatkan kombinasi soal yang berbeda-beda untuk setiap siswa. Pengacakan diterapkan dengan mengimplementasikan metode *CLCG*. Penggunaan metode tersebut dimodifikasi dengan matrik yang digunakan untuk menentukan hasil akhir pengacakan. Percobaan dilakukan terhadap variabel soal sebanyak 10, 20, 30, dan 40. Variabel yang berbeda berfungsi untuk mengetahui tingkat perbedaan pola yang dihasilkan oleh metode *CLCG*.

3. MODEL MATEMATIS

A. Matrik

Matrik merupakan sekumpulan bilangan yang disusun menurut baris dan kolom sehingga membentuk jajaran *(array)* persegi maupun persegi panjang. Matrik yang memiliki i baris dan j kolom disebut matrik $i \times j$ atau matrik berorde $i \times j$. Matrik hanyalah sekedar jajaran sekumpulan bilangan dan tidak memiliki hubungan aritmetis antar elemen-elemennya [6]. Matrik A akan memiliki alamat baris dan kolom yang berbeda-beda seperti yang ditunjukkan pada **Gambar 1.**

$$[A] = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i1} & a_{i2} & a_{i3} & a_{i4} & a_{i5} \end{bmatrix}$$

Gambar 1. Notasi Matrik

Nilai elemen-elemen dari matrik A yang terlihat di **Gambar 1** merupakan bilangan cacah positif sebanyak jumlah soal. Pada penelitian ini, nilai elemen-elemen A digunakan untuk pengacakan soal dengan metode *Coupled Linear Congruential Generator (CLCG)*. Jumlah kolom matrik yang digunakan dalam penelitian ini sebanyak 5 sedangkan jumlah baris yang digunakan sebanyak jumlah soal dibagi jumlah kolom.

B. *Linear Congruential Generator (LCG)*

Linear Congruential Generator merupakan salah satu jenis pembangkit bilangan acak semu. *LCG* menggunakan metode linier dalam membangkitkan bilangan acak dalam jumlah besar dan waktu yang cepat [4]. Model matematis *LCG* dapat dihitung dengan menggunakan persamaan (1) [3] :

$$x_{n+1} = ((a \times x_n) + b) \ mod \ m \qquad (1)$$

Keterangan :

x_{n+1}	=	bilangan acak ke-n dari deretnya
x_n	=	bilangan acak sebelumnya
a	=	faktor pengali
b	=	penambah
m	=	jumlah soal
n	=	0, 1, 2, 3, . . . dan seterusnya

LCG memiliki periode penuh jika dan hanya jika [3] :

1. b relatif prima terhadap m.
2. $a - 1$ dapat dibagi dengan setiap faktor prima dari m.
3. $a - 1$ adalah kelipatan 4 jika m adalah kelipatan 4.

C. *Coupled Linear Congruential Generator*

Coupled Linear Congruential Generator merupakan sebuah metode pembangkit bilangan acak semu dengan menggunakan penggabungan dua persamaan *linear* berbasis metode *LCG*. Model matematis *CLCG* dapat dihitung dengan menggunakan persamaan (2) [2] :

$$x_{n+1} = ((a_1 \times x_n) + b_1) \ mod \ m$$
$$y_{n+1} = ((a_2 \times y_n) + b_2) \ mod \ m \qquad (2)$$

Keterangan :

x_{n+1} = bilangan acak x ke-n dari deretnya
y_{n+1} = bilangan acak y ke-n dari deretnya
x_n = bilangan acak x sebelumnya
y_n = bilangan acak y sebelumnya
a = faktor pengali
b = penambah
m = modulus
n = 0, 1, 2, 3, . . . dan seterusnya

Berdasarkan hasil persamaan x_{n+1} dan y_{n+1} maka akan didapatkan deret bilangan acak yang akan diubah ke dalam orde matrik. Orde x didapatkan dari hasil perhitungan modulus x_{n+1} terhadap jumlah baris sehingga didapatkan persamaan (3) :

$$M_{(x,0)} = x_{n+1} \bmod i \quad (3)$$

Orde y didapatkan dari hasil perhitungan modulus y_{n+1} terhadap jumlah kolom dengan sehingga didapatkan persamaan (4) :

$$M_{(0,y)} = y_{n+1} \bmod j \quad (4)$$

Model matematis untuk hasil bilangan acak dengan menggunakan matrik baru dapat dihitung dengan menggunakan persamaan (5) :

$$M_n = M[x_{n+1} \bmod i][y_{n+1} \bmod j] \quad (5)$$

Keterangan :
M_n = hasil bilangan acak ke-n dari deretnya
x_{n+1} = bilangan acak x ke-n dari deretnya
y_{n+1} = bilangan acak y ke-n dari deretnya
i = baris matrik
j = kolom matrik
n = 0, 1, 2, 3, . . . dan seterusnya

Dengan menggunakan alamat orde matrik M_n dapat dilakukan pengambilan nilai dengan menyesuaikan alamat orde matrik secara urut berdasarkan hasil acak dari matrik A.

4. ALGORITMA

Pengacakan soal dengan metode *LCG* dilakukan melalui empat tahapan. Penentuan jumlah soal yang diacak (m) merupakan tahap pertama yang dilakukan dalam peneltian ini. Setelah itu dilakukan tahap penentuan nilai variabel faktor pengali (a). Tahap ketiga merupakan tahap penentuan variabel penambah (b). Tahap akhir pengacakan soal dengan metode *LCG* adalah perhitungan kombinasi dari variabel a, b, dan m dengan menggunakan persamaan (1).

Hal ini berbeda dengan pengacakan soal dengan metode *CLCG*. Tahap pertama dengan metode *CLCG* adalah penentuan jumlah baris dan kolom matrik A dimana jumlah elemennya sesuai dengan jumlah soal yang diacak. Selanjutnya dilakukan perhitungan variabel a, b, dan m dengan tahap yang sama seperti *LCG* dan harus diulang 2 kali. Tahap ketiga dari metode *CLCG* adalah perhitungan bilangan acak x dan y sesuai dengan persamaan (2). Pembentukan matrik Mn dan penyesuaian orde matrik M_n dengan matrik A sesuai dengan persamaan (3-5) merupakan tahap akhir dari pengacakan soal dengan metode *CLCG*.

5. HASIL PENELITIAN DAN PEMBAHASAN

Untuk mengetahui batas dari hasil pengacakan dan pola yang terbentuk dilakukan ujicoba terhadap variabel soal yaitu 10, 20, 30, dan 40. Dengan menggunakan metode *LCG* dan *CLCG* didapatkan hasil pola dengan jumlah yang berbeda pada setiap variabel ditunjukkan pada **Tabel 1.**

Tabel 1. Pola Pengacakan Terhadap Variabel Soal

Jumlah soal	Parameter			*LCG*	*CLCG*
	a	b	m		
10	11	7	10	-3	2, -3
20	21	17	20	-3	2,7,2,7,7
30	31	17	30	-13, 17	3,8,3,3,8
40	21	17	40	-17, 3	-7,18,-7,13,-2,13,-2,13,-7,18

Berdasarkan tabel tersebut dapat disimpulkan bahwa jumlah pola yang terbentuk dipengaruhi terhadap variabel soal. Semakin banyak variabel soal yang digunakan maka jumlah pola yang terbentuk akan semakin banyak baik pada metode *LCG* maupun *CLCG*. Hasil pola pengacakan yang dihasilkan oleh *LCG* lebih sedikit dikarenakan proses pengacakan dengan persamaan linier menghasilkan sebuah deret bilangan acak yang sama artinya merupakan sebuah vektor baris atau vektor kolom dari sebuah matrik. Sebaliknya, metode *CLCG* menghasilkan pola yang lebih banyak dikarenakan proses yang dilakukan menggunakan dua persamaan linier dan hasilnya membentuk dua buah vektor yaitu vektor baris dan vektor kolom. Kedua vektor terebut digabungkan sehingga membentuk sebuah matrik kompleks. Hasil pengacakan didapatkan seuai urutan dari pasangan deret yang terbentuk.

Hasil pola pengacakan tersebut didapatkan dengan menghitung hasil acak dari setiap deret menggunakan metode *LCG* dan *CLCG* ditunjukkan pada **Tabel 2**. Parameter yang digunakan dalam metode tersebut adalah m = 20, a = 21, dan b = 17 :

Tabel 2. Hasil Perbandingan *LCG* dan *CLCG*

Tanpa Pengacakan	Pengacakan *LCG*	Pola Acak	Pengacakan *CLCG*	Pola Acak
1	5	-3	7	2
2	2	-3	14	7
3	19	-3	16	2
4	16	-3	3	7
5	13	-3	10	7
6	10	-3	12	2
7	7	-3	19	7
8	4	-3	1	2
9	1	-3	8	7
10	18	-3	15	7
11	15	-3	17	2
12	12	-3	4	7
13	9	-3	6	2
14	6	-3	13	7
15	3	-3	20	7
16	20	-3	2	2
17	17	-3	9	7
18	14	-3	11	2
19	11	-3	18	7
20	8	-3	5	7

Tabel tersebut menunjukkan bahwa hasil pengacakan *LCG* dipengaruhi oleh penentuan variabel b yang membentuk pola secara naik maupun turun. Pola naik adalah bilangan awal akan mengalami kenaikan dari yang semula bernilai kecil menjadi besar pada urutan selanjutnya dan sebaliknya pola turun adalah bilangan awal akan mengalami penurunan dari yang semula bernilai besar menjadi kecil. Sedangkan hasil pengacakan *CLCG* selain dipengaruhi oleh penentuan variabel a dan b pada x_n dan y_n juga dipengaruhi oleh pembentukan matrik A. Pembentukan matrik menentukan hasil akhir dari pengacakan dimana ukuran matrik A akan merubah pola dari x_n dan y_n menjadi pasanagan ordo matrik x dan y pada persamaan (3-5). Dengan demikian hasil pengacakan dan jumlah pola yang terbentuk dengan metode *CLCG* lebih rumit dibandingkan dengan *LCG*.

6. KESIMPULAN

Hasil simulasi menunjukkan metode *Couple Linear Congruential Generator* memiliki pola pengacakan yang lebih rumit dibandingkan metode *Linear Congruential Generator*. Pola pengacakan dipengaruhi oleh nilai m dan banyaknya pemberian kombinasi nilai pada variabel a dan b. Semakin banyak kombinasi nilai variabel a dan b maka semakin banyak pengacakan yang dihasilkan. Selain itu, semakin banyak nilai variabel m maka semakin rumit pola pengacakan yang dihasilkan. Karena dimodifikasi menggunakan matrik sehingga hanya pada kondisi tertentu dimana jumlah soal yang diacak harus sama dengan jumlah elemen yang terdapat dalam matrik. Apabila diimplementasikan dalam pengacakan soal dianjurkan menggunakan metode *Coupled Linear Congruential Generator* dikarenakan pola dan hasil pengacakan yang lebih bagus.

7. DAFTAR PUSTAKA

Ichsan M. 2014. Menutup Celah Ujian Online. http://www.bppk.kemenkeu.go.id/publikasi/artikel/419-artikel-teknologi-informasi/20318-menutup-celah-ujian-online, diakses 25 Juli 2015.

Katti, R. S., Kavasseri. R. G. 2008. Secure Pseudo-random Bit Sequence Generation using Coupled Linear Congruential Generator. International Symposium Circuits and Systems (ISCAS 2008). May 18-21. IEEE: 2929-2932.

Knuth, D. E. 1981. The Art of Computer Programming. 2nd Edition. Addison-Wesley Publishing Company, Inc. Canada.

Munthe, D. 2014. Implementasi Linier Congruent Method (LCM) Pada Aplikasi Tryout SNMPTN. Jurnal Pelita Informatika Budi Darma 7(2): 111-115.

Nasution, S. D. 2013. Penerapan Metode Linier Kongruendan Algoritma Vigenere Chiper Pada Aplikasi Sistem Ujian Berbasis LAN. Jurnal Pelita Informatika Budi Darma 4(1): 94-102.

Stroud, K. A. 1996. The program and the questions Mathematics To techniques (Ed. 4). Standard-Erwin Sucipto. Jakarta: Erlangga.