IMPLEMENTASI METODE COUPLED LINEAR CONGRUENTIAL GENERATOR (CLCG) PADA APLIKASI PENGACAK SOAL

Skripsi

diajukan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Pendidikan Program Studi Pendidikan Teknik Informatika dan Komputer

Oleh

I Made Divya Biantara NIM. 5302411099

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS NEGERI SEMARANG

2015

PERSETUJUAN PEMBIMBING

Nama : I Made Divya Biantara

NIM : 5302411099

Program Studi : S-1 Pendidikan Teknik Informatika dan Komputer

Judul Skripsi : Implementasi Metode *Coupled Linear Congruential Generator* (CLCG) Pada Aplikasi Pengacak Soal

Skripsi/TA ini telah disetujui oleh pembimbing untuk diajukan ke sidang panitia ujian skripsi Program Studi S-1 Pendidikan Teknik Informatika dan Komputer Fakultas Teknik UNNES.

Semarang, 1 Oktober 2015

Pembimbing,

Dr. I Made Sudana, M.Pd.

NIP. 195605081984031004

PENGESAHAN

Skripsi dengan judul Implementasi Metode *Coupled Linear Congruential Generator* (CLCG) Pada Aplikasi Pengacak Soal telah dipertahankan di depan sidang Panitia Ujian Skripsi Fakultas Teknik UNNES pada 6 November 2015.

Oleh

Nama : I Made Divya Biantara

NIM : 5302411099

Program Studi : S-1 Pendidikan Teknik Informatika dan Komputer

Panitia :

Ketua Panitia		Sekretaris
Drs. Suryono, M.T.		Feddy Setio P., S.Pd., M.T.
NIP. 195503161985031001		NIP. 197808222003121002
Penguji I	**Penguji II**	**Penguji III**
Tatyantoro A., S.T., M.T.	Anggraini M., S.T., M.Eng.	Dr. I Made Sudana, M.Pd.
NIP. 196803161999031001	NIP. 197812262005012002	NIP. 195605081984031004

Mengetahui :

Dekan Fakultas Teknik UNNES

Dr. Nur Qudus, M.T.

NIP. 196911301994031001

PERNYATAAN KEASLIAN

Dengan ini saya menyatakan bahwa :

1. Skripsi ini, adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, magister, dan/atau doktor), baik di Universitas Negeri Semarang (UNNES) maupun di perguruan tinggi lain.
2. Karya tulis ini adalah murni gagasan, rumusan dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan Pembimbing dan masukkan Tim Penguji.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya ini, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi ini.

Semarang, 1 Oktober 2015

yang membuat pernyataan,

I Made Divya Biantara

NIM. 5302411099

UNNES
UNIVERSITAS NEGERI SEMARANG

MOTTO DAN PERSEMBAHAN

- *Only those who will risk going too far can possibly find out how far one can go.* (**T. S. Eliot)**

- *You have to be able to risk your identity for a bigger future than the present you are living.* (**Fernando Flores)**

- *It's not because things are difficult that we dare not venture. It's because we dare not venture that they are difficult.* (**Seneca)**

Skripsi ini saya persembahkan untuk :

1. Ibu Titik Suwarni dan Bapak I Made Mastra tercinta yang senantiasa mendoakan dan memberikan segalanya kepadaku.
2. Kakakku I Putu Swastika dan Eny Maftukhah yang selalu memberikan semangat dan doa.
3. Teman-teman PTIK seperjuangan yang menjadi teman diskusi dan pemberi semangat.

UNNES
UNIVERSITAS NEGERI SEMARANG

ABSTRAK

Biantara, I Made Divya. 2015. Implementasi Metode *Coupled Linear Congruential Generator* (CLCG) Pada Aplikasi Pengacak Soal. Pendidikan Teknik Informatika dan Komputer.
Pembimbing : Dr. I Made Sudana, M.Pd.

Pelaksanaan ujian secara konvensional masih rentan terhadap tindak kecurangan serta dirasa kurang efektif dan efisien karena membutuhkan waktu dan biaya yang banyak. Dengan adanya pelaksanaan ujian berbasis komputer diharapkan dapat mengatasi permasalahan yang ada. Tujuan dari penelitian ini adalah mengembangkan metode *Coupled Linear Congruential Generator* agar mengasilkan pola pengacakan yang lebih rumit yang selanjutnya diterapkan sebagai pengacak soal agar setiap siswa mendapatkan soal dengan nomor yang berbeda.

Metode eksperimen digunakan dalam penelitian ini dengan tujuan untuk mencari perlakuan tertentu terhadap perubahan hasil dari pengujian *trial and error*. Hasil tersebut digunakan untuk memperbaiki kekurangan-kekurangan yang terjadi pada proses pengacakan. Penelitian dilakukan dengan menganalisis beberapa aspek perubahan hasil pengacakan berupa kombinasi nilai variabel, kombinasi ukuran matrik, kasus khusus, distribusi kesamaan, dan hasil perbandingan dengan metode lain.

Hasil penelitian menunjukkan bahwa metode *Coupled Linear Congruential Generator* efektif diterapkan untuk mengacak soal. Kelebihan metode ini adalah deret bilangan acak yang dihasilkan memiliki pola bilangan yang lebih rumit dibandingkan metode *Linear Congruential Generator* sehingga lebih bagus untuk diterapkan sebagai pengacak soal. Selain itu, semakin banyak kombinasi yang digunakan maka akan semakin banyak deret bilangan acak yang dihasilkan dengan pola yang berbeda, akan tetapi tidak semua kombinasi dapat dilakukan sehingga perlu adanya analisis matematika yang teliti.

UNNES
UNIVERSITAS NEGERI SEMARANG

KATA PENGANTAR

Segala puji dan syukur penulis ucapkan kehadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul Implementasi Metode *Coupled Linear Congruential Generator* (CLCG) Pada Aplikasi Pengacak Soal. Skripsi ini disusun sebagai salah satu persyaratan meraih gelar Sarjana Pendidikan pada Program Studi S-1 Pendidikan Teknik Informatika dan Komputer Universitas Negeri Semarang. Penulis menyadari bahwa penyelesaian karya tulis ini tidak lepas dari bantuan berbagai pihak, oleh karena itu pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada :

1. Bapak Drs. Suryono, M.T. selaku Ketua Jurusan Teknik Elektro UNNES.
2. Bapak Feddy Setio Pribadi, S.Pd., M.T. selaku Ketua Prodi PTIK UNNES.
3. Bapak Dr. I Made Sudana, M.Pd. selaku dosen pembimbing yang telah memberikan bimbingan, arahan, nasehat serta motivasi dalam penyusunan skripsi ini.
4. Bapak Arimaz Hangga, S.T., M.T., Alfa Faridh Suni S.T., M.T, dan seluruh dosen Jurusan Teknik Elektro yang telah memberi bekal pengetahuan yang berharga.
5. Rekan-rekan PTIK UNNES 2011 yang telah membantu menyusun laporan skripsi ini.

UNNES
UNIVERSITAS NEGERI SEMARANG

Demi kesempurnaan Skripsi ini, saran dan kritik yang sifatnya membangun sangat penulis harapkan. Semoga laporan skripsi ini bermanfaat dan dapat memberikan sumbangan yang berarti bagi pihak yang membutuhkan.

Semarang, 1 Oktober 2015

Penulis

UNNES
UNIVERSITAS NEGERI SEMARANG

DAFTAR ISI

COVER i

PERSETUJUAN PEMBIMBING ii

PENGESAHAN iii

PERNYATAAN KEASLIAN iv

MOTTO DAN PERSEMBAHAN v

ABSTRAK vi

KATA PENGANTAR vii

DAFTAR ISI ix

DAFTAR TABEL xi

DAFTAR GAMBAR xii

BAB I PENDAHULUAN 1

1.1. Latar Belakang 1

1.2. Batasan Masalah 4

1.3. Rumusan Masalah 4

1.4. Tujuan Penelitian 5

1.5. Manfaat Penelitian 5

BAB II LANDASAN TEORI 6

2.1. *Random Number Generator* 6

2.2. Matrik 8

2.3. *Linear Congruential Generator* 9

2.4. *Coupled Linear Congruential Generator* 11

2.5. Pemrograman Java 13

2.6. Penelitian Terdahulu 14

UNNES
UNIVERSITAS NEGERI SEMARANG

2.7. Kerangka Berfikir 15
BAB III METODE PENELITIAN 17
3.1. Metode Penelitian 17
3.2. Desain Penelitian 17
3.3. Tempat dan Waktu Penelitian 36
3.4. Teknik Pengumpulan Data 36
3.5. Teknik Analisis Data 37
BAB IV HASIL DAN PEMBAHASAN 38
4.1. Deskripsi Data 38
4.2. Analisis Data 38
4.3. Pembahasan 62
BAB V PENUTUP 71
5.1. Kesimpulan 71
5.2. Saran 71
DAFTAR PUSTAKA 72
LAMPIRAN A 74
LAMPIRAN B 79
LAMPIRAN C 81
LAMPIRAN D 87
LAMPIRAN E 92

UNNES
UNIVERSITAS NEGERI SEMARANG

DAFTAR TABEL

Tabel 2.1. Penelitian Terdahulu 14

Tabel 3.1. Pelaksanaan Penyusunan Skripsi 36

Tabel 4.1. Elemen dan Orde Matrik A 39

Tabel 4.2. Tahap 1 Pengacakan..... 40

Tabel 4.3. Tahap 2 Pengacakan..... 42

Tabel 4.4. Uji Kombinasi Beda Nilai Variabel $b1$ dan $b2$ 45

Tabel 4.5. Uji Kombinasi Beda Nilai Variabel $b2$..... 48

Tabel 4.6. Uji Kombinasi Beda Matrik..... 52

Tabel 4.7. Perbandingan LCG dan CLCG 56

Tabel 4.8. Hasil Distribusi Kesamaan Soal..... 58

Tabel 4.9. Uji Kehandalan 61

Tabel 4.10. Daftar Faktor Prima 62

Tabel 4.11. Tabel Kombinasi 64

Tabel 4.12. Kelompok Kesamaan Pola Pengacakan..... 69

UNNES
UNIVERSITAS NEGERI SEMARANG

DAFTAR GAMBAR

Gambar 2.1. Matrik 2 × 3 8

Gambar 2.2. Notasi Matrik 9

Gambar 2.3. Kerangka Berfikir 16

Gambar 3.1. Desain Penelitian 17

Gambar 3.2. Diagram Alir Penelitian 18

Gambar 3.3. Alur Model Sekuensial Linier 19

Gambar 3.4. Struktur Data Siswa 21

Gambar 3.5. Struktur Data Guru 21

Gambar 3.6. Struktur Data Soal 22

Gambar 3.7. Struktur Data Pengaturan 22

Gambar 3.8. Diagram Alir Aplikasi 23

Gambar 3.9. Rancangan Tampilan Halaman Awal 24

Gambar 3.10. Rancangan Tampilan Halaman Kerja Guru 25

Gambar 3.11. Rancangan Tampilan Halaman Kerja Siswa 26

Gambar 3.12. Rancangan Tampilan Halaman Evaluasi 27

Gambar 3.13. Diagram Alir Metode Pengacakan 28

Gambar 3.14. *Source Code* Deklarasi Variabel 29

Gambar 3.15. *Source Code* Fungsi *loadSoal()* 30

UNNES
UNIVERSITAS NEGERI SEMARANG

Gambar 3.16. *Source Code* Fungsi *clcg()* 31

Gambar 3.17. *Source Code* Fungsi *startActionPerformed()*..... 31

Gambar 3.18. *Source Code* Fungsi *viewSoal()* 32

Gambar 3.19. *Source Code* Fungsi *NextActionPerformed()*..... 33

UNNES
UNIVERSITAS NEGERI SEMARANG

BAB I

PENDAHULUAN

1.1. Latar Belakang

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. Perkembangan teknologi informasi dan komunikasi memberikan manfaat yang besar dalam dunia pendidikan. Pemanfaatan perangkat teknologi informasi dan komunikasi memudahkan pelaksanaan ujian yang tidak lagi secara konvensional melainkan sudah secara komputerisasi, dimana siswa menjawab soal ujian melalui komputer (Ichsan, 2014). Hal tersebut dilatarbelakangi oleh pelaksanaan ujian konvensional yang dirasa kurang efektif dan efisien karena membutuhkan biaya yang besar untuk mencetak soal, waktu yang lama untuk distribusi soal dan pemeriksaan jawaban masih dilakukan secara manual. Selain itu, pelaksanaan ujian konvensional rentan terhadap kecurangan dan bocornya soal-soal yang akan diajukan sebelum ujian (Nasution, 2013: 94). McCabe dan Bower dalam Shon (2006: 131) mendefinisikan beberapa parameter kecurangan yang dilakukan siswa saat ujian yaitu menyalin jawaban dari seseorang tanpa sepengetahuanya, membantu seseorang saat ujian, dan menggunakan catatan kecil. Oleh sebab itu, untuk mengatasi permasalahan tersebut dan meminimalkan segala kekurangan yang ada pada ujian konvensional maka pelu diadakannya pelaksanaan ujian berbasis komputer.

UNNES
UNIVERSITAS NEGERI SEMARANG

Pelaksanaan ujian berbasis komputer mempunyai beberapa keunggulan yaitu menghemat biaya cetak soal ujian, menghemat waktu distribusi soal dan pemeriksaan jawaban dilakukan secara otomatis sehingga hasil ujian dapat langsung dilihat oleh siswa. Keunggulan yang dimiliki ujian berbasis komputer tidak sepenuhnya sempurna tanpa celah sehingga masih terdapat kelemahan dalam pelaksanaannya yaitu siswa dapat mengakses sumber informasi pendukung secara *online* dan menggunakan alat bantu komputer yang tidak diperbolehkan saat ujian tanpa diketahui oleh pengawas untuk memperoleh jawaban (Ichsan, 2014). Kelemahan pelaksanaan ujian baik konvensional maupun berbasis komputer dapat dimanfaatkan siswa untuk melakukan tindak kecurangan, hal tersebut bertujuan untuk menghindari kegagalan akademis. Oleh karena itu, setiap pelaksanaan ujian perlu memperhatikan tindak kecurangan yang mungkin saja dilakukan oleh siswa. Untuk mengantisipasinya maka penerapan ujian berbasis komputer dilakukan secara *offline* atau tidak terkoneksi jaringan internet dan diterapkan ke dalam aplikasi desktop. Penerapan ke dalam aplikasi desktop dilakukan menggunakan bahasa pemrograman Java (*Java Programming*) karena memiliki keunggulan dibandingkan dengan bahasa pemrograman lain yaitu bersifat dapat dijalankan di platform manapun (*multiplatform*), dapat memanfaatkan kelebihan multi prosessor (*multithreaded*), dapat beradaptasi dengan lingkungan yang sedang berkembang (dinamis), berorientasi objek, dan memiliki tingkat keamaanan yang tinggi. Fungsi aplikasi desktop digunakan sebagai media untuk mengacak soal-soal yang telah disimpan guna mendapatkan paket soal yang berbeda-beda sebelum ditampilkan ke siswa.

UNNES
UNIVERSITAS NEGERI SEMARANG

Pengacakan dilakukan dengan bantuan algoritma pembangkit bilangan acak semu *(pseudorandom number generator)* untuk menghasilkan deret bilangan acak. Metode yang paling terkenal dalam pembangkit bilangan acak semu adalah metode *Linear Congruential Generator,* tetapi hasil dari metode tersebut masih terlihat periodik sehingga harus diberikan nilai variabel yang selalu berubah-ubah untuk mengatasi keperiodikan hasil acak yang terjadi (Munthe, 2014: 114). Keperiodikan tersebut dapat menyebabkan soal yang diacak memiliki nomor yang sama terhadap siswa yang berada disekitarnya. Selain itu, metode *Linear Congruential Generator* mempunyai kelemahan yaitu jika sebuah deret bilangan acak yang dihasilkan diketahui, maka parameter dan modulus dari metode tersebut dapat diuraikan sehingga akan menyebabkan hasil acak menjadi tidak aman dan dapat diketahui hasil pola pengacakan (Katti, 2010: 203). Untuk meningkatkan dan menghasilkan deret bilangan acak yang lebih aman, maka Katti mengembangkan sebuah generasi pembangkit bilangan acak terbaru yaitu metode *Coupled Linear Congruential Generator*. Kelebihan dari metode *Coupled Linear Congruential Generator* yaitu memiliki hasil pola pengacakan yang lebih rumit dan aman dibandingkan metode *Linear Congruential Generator*. Berdasarkan hal tersebut peneliti memilih menggunakan metode *Coupled Linear Congruential Generator* untuk diterapkan ke dalam aplikasi desktop sebagai pengacak soal dengan harapan agar dapat mengatasi semua permasalahan yang terjadi pada pelaksanaan ujian.

UNNES
UNIVERSITAS NEGERI SEMARANG

1.2. Batasan Masalah

Untuk mengatasi permasalahan yang sudah diuraikan dalam latar belakang maka perlu adanya batasan masalah yang digunakan dalam melakukan penelitian ini antara lain :

a. Pelaksanaan ujian dilakukan secara komputerisasi dengan menggunakan metode *Coupled Linear Congruential Generator* sebagai pengacak soal.
b. Penerapan metode *Coupled Linear Congruential Generator* digunakan untuk memastikan tidak terdapat kesamaan soal pada nomor yang sama.
c. Pengacakan soal hanya dilakukan pada satu mata pelajaran saja dengan jumlah soal sebanyak 40.

1.3. Rumusan Masalah

Berdasarkan latar belakang permasalahan maka dapat diidentifikasi permasalahan dalam penelitian ini yaitu :

a. Bagaimana menghasilkan bilangan acak dengan pola yang rumit menggunakan kombinasi nilai pada variabel-variabel metode *Coupled Linear Congruential Generator*?
b. Bagaimana menerapkan metode *Coupled Linear Congruential Generator* untuk aplikasi pengacak soal dengan berbasis pemrograman Java?

UNNES
UNIVERSITAS NEGERI SEMARANG

1.4. Tujuan Penelitian

Berdasarkan perumusan masalah dalam penelitian ini maka tujuan dari penelitian ini adalah sebagai berikut :

a. Menghasilkan deret bilangan acak dengan pola yang rumit menggunakan metode *Coupled Linear Congruential Generator.*
b. Menerapkan metode *Coupled Linear Congruential Generator* pada aplikasi pengacak soal.

1.5. Manfaat Penelitian

Setelah selesainya penelitian ini diharapkan nantinya dapat mempunyai nilai manfaat antara lain sebagai berikut :

a. Dapat dijadikan sumbangan pikiran atau referensi bagi peneliti-peneliti selanjutnya yang ingin memahami, meneliti, dan mengembangkan ilmu di bidang pendidikan khususnya teknik informatika dan komputer.
b. Dapat dijadikan sebagai wahana dan wawasan dalam penerapan ilmu pengetahuan tentang pembangkit bilangan acak semu *(pseudorandom number generator).*
c. Dapat mengetahui kelebihan dan kekurangan dari metode pengacakan yang dikembangkan.

UNNES
UNIVERSITAS NEGERI SEMARANG

BAB II

LANDASAN TEORI

2.1. *Random Number Generator*

Bilangan acak adalah bilangan yang dihasilkan dari sebuah proses yang keluarannya tidak dapat diprediksi dan secara berurutan tidak bisa dihasilkan bilangan yang sama. Definisi tersebut sesuai pendapat D. H. Lehmer (1951) yang dikutip dalam Knuth (1981: 142) yaitu :

> *A random sequence is a vague notion embodying the idea of a sequence in which each term is unpredictable to the uninitiated and whose digits pass a certain number of tests, traditional with statisticians and depending somewhat on the uses to which the sequence is to be put.*

Secara komputasi untuk mendapatkan bilangan acak akan sulit dilakukan yang disebabkan bahwa komputer merupakan mesin *deterministik,* sedangkan bilangan acak muncul sebagai kejadian *probabilistic.* Satu-satunya cara untuk mendapatkan bilangan acak adalah dengan menggunakan sebuah algoritma pembangkit bilangan acak (Gaol, 2014: 45). Berdasarkan *Request For Command 1750* dalam Pardede telah ditentukan bahwa algoritma pembangkit bilangan acak harus memenuhi syarat-syarat yaitu :

a. Tidak dapat diprediksi, suatu algoritma pembangkit bilangan acak harus bersifat tidak dapat diprediksi hasil keluarannya.
b. Tahan akan pembelokan, bila perangkat keras dimanipulasi maka algoritma harus dapat bertahan terhadap manipulasi sumber bilangan hingga level tertentu yang tidak mungkin lagi dapat ditahan.

UNNES
UNIVERSITAS NEGERI SEMARANG

c. Memiliki fungsi penggabungan dan pengacakan untuk mencegah penyerangan terhadap algoritma secara keseluruhan.

Pembangkit bilangan acak biasanya digunakan untuk penerapan yang berbeda meliputi bidang *simulation, sampling, numerical analysis, computer programming, decision making,* dan *recreation* (Knuth, 1981: 1). Hal tersebut didukung dengan pendapat Kenny (2005: 6) bahwa pembangkit bilangan acak merupakan bahan-bahan penting yang skala penggunaannya meliputi *cryptography, simulation, gaming, sampling, decision making* dan *aesthetics*. Terdapat dua tipe pembangkit bilangan acak yaitu *truerandom number generator* dan *pseudorandom number generator* (Kenny, 2005: 8). *Truerandom number generator* adalah pembangkit bilangan acak nyata yang membutuhkan sumber alami keacakan yaitu entropi dan prosesnya dilakukan melalui komputer untuk menghasilkan deret bilangan acak. Pembangkit bilangan acak nyata secara definisi memiliki deret bilangan acak yang sepenuhnya tidak terduga. *Pseudorandom number generator* adalah pembangkit bilangan acak semu yang bersifat *deterministik* yang berarti bahwa proses komputasi menggunakan sebuah algoritma matematika. Hasil dari pembangkitan bilangan acak semu tidak sepenuhnya acak dan hanya mendekati beberapa dari sifat-sifat yang dimiliki bilangan acak. Bilangan acak yang dihasilkan dari pembangkit bilangan acak semu memiliki sifat periodik dan tidak memiliki sifat pada bilangan acak sesungguhnya. Sifat periodik pada pembangkit bilangan acak semu memiliki arti bahwa pada putaran tertentu setelah dijalankan akan dihasilkan deret yang berulang.

UNNES
UNIVERSITAS NEGERI SEMARANG

2.2. Matrik

Definisi matrik menurut Kaufman (2011: 589) adalah jajaran bilangan yang disusun dalam baris dan kolom diantara tanda kurung, sedangkan menurut Stroud (1996: 354) matrik adalah sekumpulan bilangan kompleks yang disusun menurut baris dan kolom sehingga membentuk jajaran persegi panjang. Selain itu, Anton (1987) menjelaskan bahwa matrik adalah susunan segi empat siku-siku dari bilangan yang disusun berdasarkan baris dan kolom. Berdasarkan ketiga definisi matrik tersebut dapat disimpulkan bahwa matrik merupakan sekumpulan bilangan komplek yang disusun berdasarkan baris dan kolom diantara tanda kurung siku. Suatu matrik ditunjukkan dengan menuliskan jajarannya di antara kurung siku, misalnya :

$$\begin{array}{cc} & \text{Kolom} \\ & \downarrow \\ \text{Baris} \rightarrow & \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \end{array}$$

Gambar 2.1. Matrik 2 × 3

Berdasarkan gambar 2.1 dijelaskan bahwa matrik tersebut memiliki 2 baris dan 3 kolom yang disebut matrik 2 × 3. Setiap bilangan dalam matrik disebut elemen atau unsur. Pada umumnya, matrik memiliki i baris dan j kolom yang disebut matrik $i \times j$ atau matrik berorde $i \times j$. Matrik hanyalah sekedar kumpulan jajaran bilangan yang tidak memiliki hubungan aritmetis antar elemen-elemennya (Stroud, 1996: 355). Matrik A akan memiliki notasi alamat baris dan kolom yang berbeda-beda ditunjukkan pada gambar berikut :

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

Gambar 2.2. Notasi Matrik

Sebuah matrik yang hanya memiliki satu baris disebut vektor baris atau matrik baris, dan sebuah matrik yang hanya memiliki satu kolom disebut vektor kolom atau matrik kolom. Sebagai contoh matrik 2 × 1 adalah vektor kolom, matrik 1 × 4 adalah vektor baris, dan matrik 1 × 1 adalah keduanya vektor baris dan vektor kolom.

2.3. *Linear Congruential Generator*

Metode *Linear Congruential Generator* adalah sebuah metode untuk membangkitkan bilangan acak semu x_0, $x_1, x_2, \ldots x_n$ yang diajukan oleh D. H. Lehmer (Fuller, 1975: 173). Metode ini merupakan salah satu jenis pembangkit bilangan acak semu *(pseudorandom number generator)* yang paling terkenal dan banyak digunakan dalam aplikasi komputer modern. Metode *Linear Congruential Generator* memanfaatkan persamaan linier untuk membangkitkan bilangan acak dalam jumlah besar dan waktu yang cepat (Munthe, 2014: 112). Li (2005) menjelaskan bahwa kualitas dari metode *Linear Congruential Generator* sangat bergantung pada pemilihan parameter-parameternya. Parameter tersebut meliputi variabel a, b, m, dan x_n yang mana nilai dari a, b dan m diketahui dan memiliki nilai yang konstan sedangkan nilai dari x_n bersifat rahasia. Setiap anggota dari deret bilangan acak akan menghasilkan penggantinya dengan cara integer x_n dikalikan dengan bilangan bulat a dan ditambahkan dengan bilangan bulat b.

UNNES
UNIVERSITAS NEGERI SEMARANG

Selanjutnya, hasil tersebut dibagi dengan bilangan bulat m dan sisa hasil bagi diambil sebagai x_{n+1}. Dengan demikian dari algoritma tersebut didapatkan sebuah model matematis yaitu (Knuth, 1981: 9) :

$$x_{n+1} = ((a \times x_n) + b) \ mod \ m \qquad (2.1)$$

Keterangan :

x_{n+1} = bilangan acak ke-n dari deretnya

x_n = bilangan acak sebelumnya

a = faktor pengali

b = penambah

m = modulus

n = 0, 1, 2, 3, . . . dan seterusnya

Syarat yang dimiliki oleh *Linear Congruential Generator* untuk menghasilkan periode penuh yaitu jika dan hanya jika (Knuth, 1981: 16) :

a. b relatif prima terhadap m.

b. $a - 1$ dapat dibagi dengan setiap faktor prima dari m.

c. $a - 1$ adalah kelipatan 4 jika m adalah kelipatan 4.

Deret bilangan acak yang dihasilkan oleh metode *Linear Congruential Generator* paling besar adalah m atau periode penuh dan akan berulang setelah n tertentu, bahkan pada kebanyakan kasus periodenya kurang dari m. Untuk mengatasi keperiodikan nilai acak maka harus diberikan nilai variabel yang selalu berubah-ubah (Munthe, 2014: 113). Penentuan nilai pada variabel a, b dan m sangat menentukan baik tidaknya bilangan acak dan suatu pola yang diperoleh.

2.4. *Coupled Linear Congruential Generator*

Katti (2010: 203) menjelaskan bahwa metode *Linear Congruential Generator* sudah lama diketahui tidak aman yang disebabkan jika hasil sebuah deret bilangan diketahui, maka parameter dan modulus dapat diuraikan. Metode *Coupled Linear Congruential Generator* adalah sebuah metode pembangkit bilangan acak semu yang memanfaatkan penggabungan dua persamaan *linear* berbasis metode *Linear Congruential Generator* sebagai generasi baru pembangkit bilangan acak. Metode *Coupled Linear Congruential Generator* didefinisikan dengan persamaan :

$$x_{n+1} = ((a_1 \times x_n) + b_1) \ mod\ m$$

$$y_{n+1} = ((a_2 \times y_n) + b_2) \ mod\ m \qquad (2.2)$$

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

Pengembangan metode *Coupled Linear Congruential Generator* yang dilakukan oleh Katti digunakan untuk menghasilkan enkripsi deret bit B_n dengan kondisi :

UNNES
UNIVERSITAS NEGERI SEMARANG

$$B_n = \begin{cases} 1, & x_{n+1} > y_{n+1} \\ 0, & y_{n+1} \geq x_{n+1} \end{cases} \quad (2.3)$$

Metode *Coupled Linear Congruential Generator* dimodifikasi dengan matrik. Berdasarkan hasil persamaan x_{n+1} dan y_{n+1} maka akan didapatkan deret bilangan acak yang akan dirubah ke dalam bilangan orde matrik. Orde x didapatkan dari modulus x_{n+1} terhadap jumlah baris dengan persamaan :

$$M_{(x,0)} = x_{n+1} \; mod \; i \quad (2.4)$$

Orde y didapatkan dari modulus y_{n+1} terhadap jumlah kolom dengan persamaan :

$$M_{(0,y)} = y_{n+1} \; mod \; j \quad (2.5)$$

Hasil akhir didapatkan dengan menggunakan matrik baru dari persamaan :

$$M_n = M[x_{n+1} \; mod \; i][y_{n+1} \; mod \; j] \quad (2.6)$$

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 $A_{(4,5)}$.

2.5. Pemrograman Java

Bahasa pemrograman Java dikembangkan oleh Sun Microsystems yang digagas oleh James Gosling pada Juni 1991. Java pertama kalinya dirilis untuk umum pada tahun 1995 sebagai komponen pendukung dari Sun Microsystems. Pada Desember 2008, Sun Microsystems merilis Java SE *(Standard Edition)* dan membangun beberapa konfigurasi tipe platform lainnya yaitu Java EE (*Enterprise Application*) dan Java ME (*Mobile Application*) yang diberikan secara gratis dan *open-source*. Java memiliki tujuan yaitu *Write Once Run Anywhere* (WORA) yang berarti bahwa sebuah project Java hanya cukup ditulis satu kali dan dapat dijalankan di manapun. Adapun beberapa hal yang menjadi kelebihan dari Java yaitu :

a. Sederhana, bersifat ringkas dengan pengaturan fitur yang kohesif membuat lebih mudah untuk dipelajari dan digunakan.
b. Aman, menyediakan sarana yang aman untuk menciptakan aplikasi internet.
c. Portabel, dapat dieksekusi dalam lingkungan yang memiliki sistem *run-time*.
d. Berorientasi objek, berwujud modern dengan pemrograman berorientasi objek.
e. Kuat, mendorong pemrograman yang bebas dari kesalahan dengan mengidentifikasi penulisan (*syntax*) dan melakukan pemeriksaan *run-time*.

UNNES
UNIVERSITAS NEGERI SEMARANG

f. Multithreaded, memberikan dukungan terintegrasi untuk pemrograman dengan memanfaatkan kelebihan muti prosessor.

g. Multiplatform, tidak terikat pada suatu mesin atau arsitektur sistem operasi.

h. Interpreted, mendukung lintas platform melalui penggunaan b*ytecode*.

i. Kinerja tinggi, memiliki *bytecode* yang digunakan untuk mengoptimalikan kecepatan proses eksekusi.

j. Terdistribusi, dirancang dengan lingkungan yang terdistribusi dari internet.

k. Dinamis, dapat membawa sejumlah besar jenis informasi *run-time* secara bersama yang digunakan untuk memverifikasi akses ke objek.

2.6. Penelitian Terdahulu

Penelitian sebelumnya yang relevan dan menjadi acuan pustaka terhadap teori-teori yang digunakan tentang penggunan metode *Linear Congruential Generator* dan *Coupled Linear Congruential Generator* pada penelitian ini dengan judul "Implementasi Metode *Coupled Linear Congruential Generator* (CLCG) Pada Aplikasi Pengacak Soal" adalah sebagai berikut :

Tabel 2.1. Penelitian Terdahulu

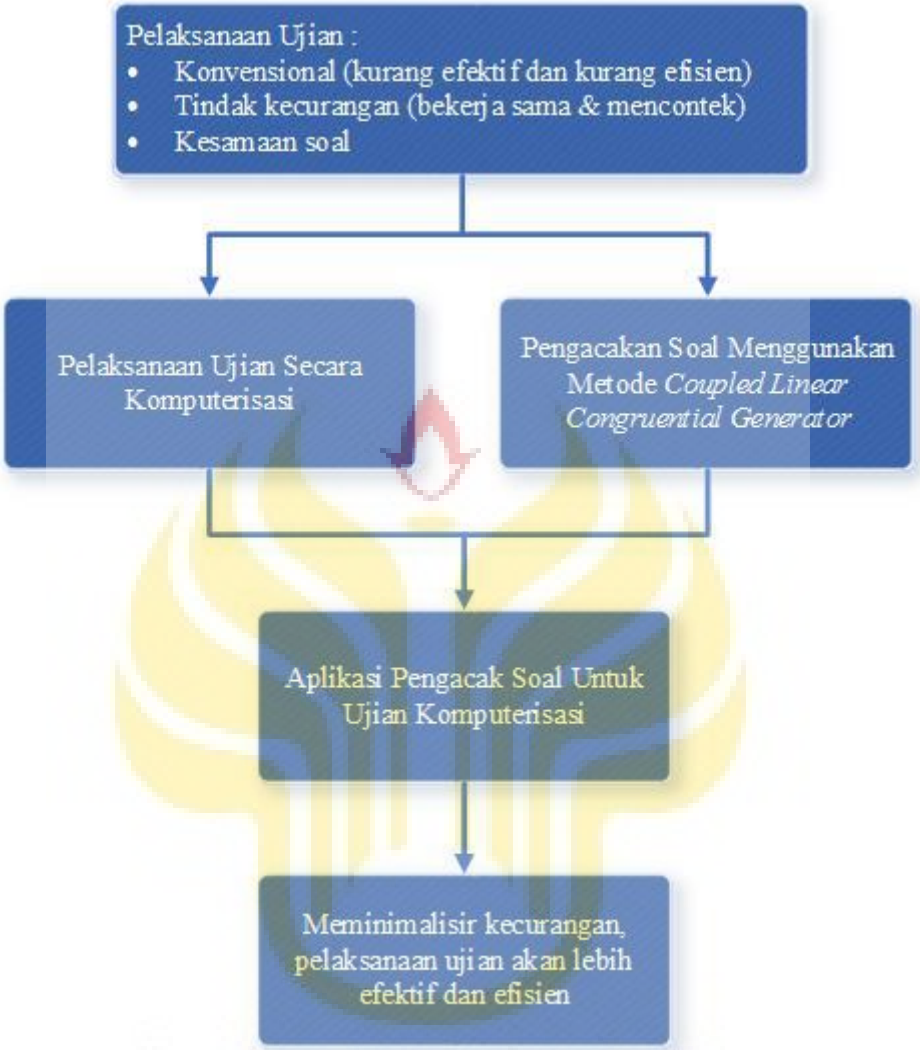
No	Judul Penelitian	Peneliti
1	Implementasi *Linier Congruent Method* (LCM) Pada Aplikasi *Tryout* SNMPTN	Daniel Munthe
2	Perancangan Aplikasi Ujian *Try Out* Menggunakan Metode *Linear Congruent Methods* (LCM)	Diana Lumban Gaol
3	Penerapan Metode Linier Kongruendan Algoritma *Vigenere Chiper* Pada Aplikasi Sistem Ujian Berbasis LAN	Surya Dama Nasution
4	*Pseudorandom Bit Generation Using Coupled Congruential Generators*	Raj S. Katti, Rajesh G. Kavasseri, dan Sai V.

Dari penelitian-penelitian tersebut dapat disimpulkan bahwa penggunaan algoritma pembangkit bilangan acak semu dapat diterapkan ke dalam masalah simulasi yang berkaitan dengan pengacakan soal. Algoritma pembangkit bilangan acak semu yang sering digunakan dalam pelaksanaa ujian untuk mengacak soal adalah metode *Linear Congruential Generator*, akan tetapi metode tersebut dianggap kurang aman sehingga Katti mengembangkan sebuah metode *Coupled Linear Congruential Generator*.

2.7. Kerangka Berfikir

Pelaksanaan ujian konvensional dirasa kurang efektif dan efisien sehingga perlu perbaikan dengan diadakannya pelaksanaan ujian berbasis komputer yang dapat menutup kekurangan pada ujian konvensional. Akan tetapi, pelaksanaan ujian berbasis komputer juga memiliki kekurangan yaitu siswa dapat mengakses sumber informasi pendukung dan menggunakan alat bantu komputer untuk mendapatkan jawaban. Selain itu, soal dengan nomor yang sama dapat memberikan siswa peluang untuk bekerja sama dan saling mencontek baik pada pelaksanaan ujian secara konvensional maupun berbasis komputer sehingga perlu adanya pengacakan soal. Pengacakan soal dilakukan dengan menggunakan metode *Coupled Linear Congruential Generator* yang diterapkan ke dalam pelaksanaan ujian berbasis komputer dengan harapan agar dapat meminimalisir tindak kecurangan yang dilakukan siswa dan pelaksanaan ujian dapat lebih efektif dan efisien. Dari berbagai masalah dan solusi yang telah dijelaskan maka dapat digambarkan kerangka berfikir sebagai berikut :

UNNES
UNIVERSITAS NEGERI SEMARANG



Gambar 2.3. Kerangka Berfikir

UNNES
UNIVERSITAS NEGERI SEMARANG

BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan penelitian yang telah dilakukan terhadap suatu metode pengacakan untuk diterapkan dalam aplikasi pengacak soal dapat disimpulkan bahwa :

a. Metode *Coupled Linear Congruential Generator* menghasilkan deret bilangan acak dengan pola yang banyak dan rumit.
b. Aplikasi dapat mengacak soal dengan menerapkan metode *Coupled Linear Congruential Generator*.

5.2. Saran

Dalam penelitian ini jumlah nilai yang dapat diacak terbatas oleh kondisi tertentu dengan syarat-syarat yang telah ditentukan. Selain itu, algoritma pada modifikasi metode *Coupled Linear Congruential Generator* masih menggunakan dasar operasi aritmatika dan logika pemrograman yang sederhana. Oleh karena itu, disarankan penelitian selanjutnya dapat mengembangkan metode modifikasi *Coupled Linear Congruential Generator* untuk dapat mengacak bilangan sesuai dengan jumlah yang diinginkan dan pengembangan sistem pengambil keputusan untuk menentukan variabel-variabel dan ukuran matrik yang digunakan dalam pengacakan.

UNNES
UNIVERSITAS NEGERI SEMARANG

DAFTAR PUSTAKA

Anton, H., dan C. Rorres. 2010. *Elementary Linear Algebra: Applications Version.* 10th Edition. John Wiley & Sons, Inc.

Fuller, A.T. 1975. The Period of Pseudorandom Number Generated by Lehmer's Congruential Method. *The Computer Journal* 19(2): 173-177.

Gaol, D. L. 2014. Perancangan Aplikasi Ujian Try Out Menggunakan Metode Linear Congruent Methods (LCM). *Jurnal Pelita Informatika Budi Darma* 6(3): 44-48.

Ichsan, M. 2014. Menutup Celah Ujian Online. *http://www.bppk.kemenkeu.go.id/publikasi/artikel/419-artikel-teknologi-informasi/20318-menutup-celah-ujian-online*. 25 Juli 2015 (23:14).

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.

Katti, R. S., Kavasseri, R. G., & Sai, V. 2010. Pseudorandom Bit Generation Using Coupled Congruential Generators. *Circuits and Systems II: Express Briefs, IEEE Transactions* 57(3), 203-207.

Kaufman, J. E., dan K. L. Schwitters. *Algebra For College Students*. 9th Edition. Nelson Education, Ltd. Canada.

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

Kenny, C. dan K. Mosurski. 2005. Random Number Generators: An Evaluation and Comparison of Random.org and Some Commonly Used Generators. Computer Science Department, TCD.

Li, C. C., dan B. Sun. 2005. Using Linear Congruential Generators for Cryptographic Purposes. *Computers and Their Applications*: 13-19.

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

Pardede, Jasman. Implementasi Random Numbers Java untuk Menciptakan Missing Value dari suatu Tabel. *http://lib.itenas.ac.id/kti/wp-content/uploads/2013/06/04.-Implementasi-Random-Numbers-Java-Untuk-Menciptakan-Missing-Value-dari-suatu-Tabel-Jasman-Pardede.pdf.* 7 Maret 2015 (14:13).

Shon, P. C. H. 2006. How College Students Cheat On In-Class Examinations: Creativity, Strain, and Techniques of Innovation. *Plagiary: Cross-Disciplinary Studies in Plagiarism, Fabrication, and Falsification,* 130-148.

Stroud, K. A. 1987. *Engineering Mathematics.* 4th Edition Keempat. The Mcmillan Press, Ltd. Terjemahan E. Sucipto. *Matematika Untuk Teknik.* Cetakan 1. Erlangga. Jakarta.

Sugiyono. 2013. *Metode Penelitian Pendidikan (Pendekatan Kuantitatif, Kualitatif, dan R & D).* Alfabeta. Jakarta.

UNNES
UNIVERSITAS NEGERI SEMARANG