

Implementasi Metode Linear Congruent Method (LCM) pada Simulasi Ujian Akhir Sekolah Menengah Kejuruan Lolomatua

Senima Bulolo
STMIK Pelita Nusantara
senimanbulolo@gmail.com

Anita Sindar
STMIK Pelita Nusantara
haito_ita@yahoo.com

Abstrak

Teori pengacakan (*chaos*) merupakan materi penelitian bidang keamanan informasi. Pelaksanaan ujian secara komputerisasi memberikan dampak positif dalam hal meminimalisasi biaya dan perolehan hasil koreksi ujian yang cepat. Simulasi bidang komputer mempelajari sistem secara numerik, dilakukan pengumpulan data untuk melakukan estimasi statistik untuk mendapatkan karakteristik asli dari sistem. Simulasi penting diterapkan terutama jika diharuskan untuk melakukan eksperimen dalam rangka mencari komentar terbaik dari komponen-komponen sistem pada perangkat yang digunakan. Pelaksanaan ujian secara tertulis membutuhkan banyak peralatan, seperti alat tulis, kertas dan tenaga guru untuk mengoreksi hasil ujian. Proses ujian dapat dilakukan oleh siswa melalui komputer secara langsung terhubung pada *network*. Untuk mencegah kecurangan, maka urutan soal ujian diacak. Metode yang dapat digunakan untuk mengacak urutan soal adalah *Linear Congruential Method (LCM)*. Soal diacak sehingga setiap siswa memperoleh urutan soal yang berbeda. Penelitian menggunakan metode LCM untuk melakukan pengacakan terhadap urutan soal ujian. Pengacakan algoritma LCM dimulai dengan pemilihan nilai kunci LCM, yaitu nilai a , b dan m agar pengacakan dapat berjalan dengan sempurna. Nilai kunci digunakan berbeda-beda di dalam sistem, sehingga setiap siswa memperoleh urutan soal yang tidak sama. Penerapan simulasi menghasilkan nilai ujian yang dapat diketahui langsung setelah siswa menyelesaikan proses ujian. Aplikasi hasil rancangan dapat digunakan untuk menyelenggarakan ujian sekolah secara komputerisasi dengan pengacakan soal berdasarkan pada metode LCM.

Kata Kunci—Ujian Online, Metode LCM, Soal Acak

I. PENDAHULUAN

Proses ujian dilakukan oleh siswa menggunakan komputer yang terhubung ke jaringan *Local Area Network (LAN)*. Untuk mencegah kecurangan, maka

urutan soal ujian diacak dengan menggunakan metode *Linear Congruential Method (LCM)*, sehingga setiap siswa memperoleh urutan soal yang berbeda. LCM dipilih karena metode ini merupakan salah satu metode penghasil bilangan acak yang dapat diimplementasikan dengan cepat. *Linear*

Congruent Method (LCM) merupakan metode pembangkitkan bilangan acak yang banyak digunakan dalam program komputer [1]. Algoritma LCM mampu mengacak kemunculan soal yang akan diberikan oleh pengguna. Simulasi pengacakan algoritma LCM dengan 30 soal yang diacak dengan menentukan nilai $a = 1$, $b = 7$, $m = 30$ serta menentukan nilai $x = 6$ membuktikan bahwa tidak terdapat pengulangan pada hasil pengacakan yang dihasilkan [2]. Penelitian berjudul "Perancangan Aplikasi Quiz Menggunakan Metode Pengacakan *Linear Congruential*" (Wahyudi, Handoko dan Pasaribu, 2015) [3]. Secara teoritis mampu menghasilkan bilangan acak, namun sangat sensitif terhadap pemilihan nilai yang tidak sesuai dan dapat mempengaruhi implementasi LCM. Penelitian ini menyimpulkan bahwa penggunaan metode LCM dapat menghasilkan pengacakan yang baik dan menghasilkan urutan soal yang benar-benar acak pada aplikasi Quiz yang dirancang. Bilangan acak (random) banyak digunakan di dalam program komputer, misalnya untuk program simulasi, seperti mensimulasikan waktu kedatangan nasabah di bank, pompa bensin, dan sebaliknya), program *kriptografi*, aplikasi statistik dan sebagainya. Tidak ada komputasi yang benar-benar menghasilkan deretan bilangan acak secara sempurna. Bilangan acak yang dihasilkan dengan rumus-rumus matematika adalah bilangan acak semu (*pseudo*), karena pembangkitan bilangannya dapat diulang kembali. Pembangkitan deretan bilangan acak ini disebut pembangkit bilangan acak semu (*pseudo-random number generator* atau PRNG).

II. METODE

A. Teori Pengacakan (Chaos)

Karakteristik yang menarik dari chaos adalah sensitifitasnya terhadap nilai awal (initial value). Jika nilai awal sistem chaos diubah sedikit saja, misalnya sebesar 10-10, maka bila sistem chaos tersebut diiterasikan sejumlah kali, hasil iterasinya berbeda signifikan dengan sebelumnya. Sensitivitas ini sangat berguna di dalam kriptografi karena bersesuaian dengan prinsip *diffusion* dari Shannon dalam merancang sebuah *algoritma kriptografi*. Prinsip *diffusion* ini, maka pengubahan satu bit nilai awal *chaos* dapat menyebabkan *cipherteks* tetap tidak berhasil didekripsi [4]. Bilangan acak adalah deretan nilai yang acak dan tidak dapat diprediksi secara keseluruhan. Untuk menghasilkan bilangan acak merupakan hal yang sulit, kebanyakan pembangkit bilangan acak (random bit / random number generator) mempunyai beberapa bagian

yang dapat diprediksi dan berhubungan. Kebanyakan RNG mengulang *string* yang sama setelah melakukan n putaran, sedangkan ada beberapa RNG lainnya menghasilkan nilai acak dengan berfokus pada suatu area tertentu dan mendistribusikannya secara seragam [5].

B. Linear Congruential Method (LCM)

Metode yang paling umum digunakan untuk membangkitkan bilangan acak adalah dengan pembangkit bilangan acak kongruen-lanjar (*linear congruential method* atau LCM) [6]. Metode LCM diimplementasikan dalam bentuk rumus umum [7]:

$$x_n = (a \cdot x_{n-1} + b) \bmod m \quad (1)$$

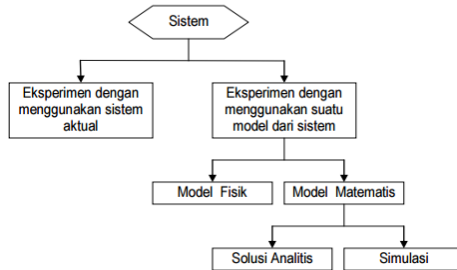
dalam hal ini, x_n = bilangan acak ke- n dari deretan. x_{n-1} = bilangan acak sebelumnya. a = faktor pengali; b = faktor penambah (increment); m = modulus. Keuntungan dari LCM adalah operasinya dapat berjalan dengan sangat cepat. Kunci pembangkit adalah x_0 yang disebut sebagai umpan (seed). LCG mempunyai periode tidak lebih besar dari m . Jika a , b dan m dipilih secara tepat (misalnya b relatif prima terhadap m dan $a-1$ habis dibagi oleh semua faktor prima dari m), maka LCG akan mempunyai periode maksimal, yaitu sebesar $m-1$. Misalkan $a = 2791$, $b = 7879$, $m = 15$ dan $x_0 = 0$, maka perhitungan untuk $x_1 = (2791 \cdot 0 + 7879) \bmod 15$, sehingga $x_1 = 4$.

C. Random Number Generator (RNG)

Bilangan acak yang dihasilkan oleh komputer sekalipun tidak benar-benar acak dan kebanyakan bilangan acak yang diterapkan dalam kriptografi juga tidak benar-benar acak, tetapi hanya berupa acak semu. Ini berarti bahwa bilangan acak yang dihasilkan itu dapat ditebak susunan atau urutan nilainya. *Random number generator* (RNG) adalah suatu peralatan komputasional yang dirancang untuk menghasilkan suatu urutan nilai yang tidak dapat ditebak polanya dengan mudah, sehingga urutan nilai tersebut dapat dianggap sebagai suatu keadaan acak (random). Dalam kriptografi, bilangan acak sering dibangkitkan dengan menggunakan pembangkit bilangan acak semu (*pseudo random number generator*). *Random number generator* (RNG) adalah suatu peralatan komputasional yang dirancang untuk menghasilkan suatu urutan nilai yang tidak dapat ditebak polanya dengan mudah, sehingga urutan nilai tersebut dapat dianggap sebagai suatu keadaan acak (random) [8]. *Random number generator* merupakan pembangkit bilangan acak secara nulerik/aritmatika menggunakan komputer yang sering digunakan untuk proses perhitungan.

D. Simulasi

Simulasi adalah suatu teknik meniru operasi-operasi atau proses-proses yang terjadi dalam suatu sistem dengan bantuan perangkat komputer dan dilandasi oleh beberapa asumsi tertentu sehingga sistem dapat dipelajari secara ilmiah, Gambar 1.

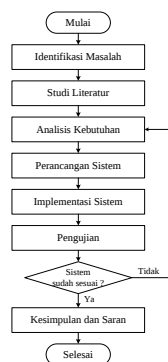


Gambar 1. Salah Satu Cara Mempelajari Sistem

Ruang lingkup permasalahan sebagai berikut :

1. Soal ujian dipersiapkan untuk sekolah menengah Kejuruan berjumlah 60 soal yang terdiri dari mata pelajaran Bahasa Indonesia, Bahasa Inggris, Matematika, dengan masing-masing bidang studi berjumlah 20 soal.
2. Pengguna sistem adalah administrator, guru (pembuat soal) dan siswa/siswi sebagai user yang mengikuti ujian.
3. Soal dibatasi pada bentuk pilihan berganda dan dapat berisi teks dan gambar.
4. Soal ujian ditampilkan secara acak dengan menggunakan *Linear Congruent Method* (LCM).

Data penelitian berupa soal ujian dipersiapkan untuk sekolah menengah Kejuruan berjumlah 60 soal yang terdiri dari mata pelajaran Bahasa Indonesia, Bahasa Inggris, Matematika, dengan masing-masing bidang studi berjumlah 20 soal. Tahapan dari penelitian mengenai aplikasi implementasi metode *Linear Congruent Method* (LCM) pada simulasi, Gambar 2.



Gambar 2. Alur Penelitian

III. HASIL

A. Analisa Metode Linear Congruent Method

Pengacakan algoritma LCM didahului dengan pemilihan nilai kunci LCM (a, b dan m) agar pengacakan dapat berjalan dengan sempurna. Pemilihan nilai kunci ini dilakukan secara acak di dalam sistem dan proses pengacakan tidak ditampilkan kepada user.

Nilai m = 60, karena jumlah soal ujian adalah 60 soal. Pilih nilai b secara acak, sehingga nilai Faktor Persekutuan Terbesar (FPB) atau nilai GCD antara b dan m harus sama dengan 1, atau kedua bilangan tidak mempunyai faktor yang sama kecuali angka 1. m = 60 = 2 x 2 x 3 x 5 x 1; Pilih b = 707 = 7 x 101 x 1; Nilai b dan m tidak memiliki faktor yang sama kecuali angka 1. Oleh karena itu nilai b = 707 dapat dipilih. Pilih nilai a secara acak, sehingga nilai (a-1) dapat dibagi oleh semua faktor prima dari m. Pilih a = 601; a-1 = 600 dapat dibagi habis oleh faktor prima m, yaitu 2, 3 dan 5. Oleh karena itu, nilai a = 601 dapat dipilih. Dengan demikian, kunci yang digunakan untuk pengacakan adalah: a = 601, b = 707 dan m = 60. Proses menghasilkan bilangan acak dengan rumus LCM dilakukan dengan menggunakan persamaan 2.

$$x_n = (a \cdot x_{n-1} + b) \bmod m \quad (2)$$

Proses menghasilkan bilangan acak dengan algoritma LCM dengan nilai a = 601, b = 707 dan m = 60 adalah sebagai berikut:

0. $x(0) = 0$
1. $x(1) = (a \cdot x(0) + b) \bmod m; x(1) = 47$
2. $x(2) = (a \cdot x(1) + b) \bmod m; x(2) = 34$
3. $x(3) = (a \cdot x(2) + b) \bmod m; x(3) = 21$
4. $x(4) = (a \cdot x(3) + b) \bmod m; x(4) = 8$
5. $x(5) = (a \cdot x(4) + b) \bmod m; x(5) = 55$
6. $x(6) = (a \cdot x(5) + b) \bmod m; x(6) = 42$
7. $x(7) = (a \cdot x(6) + b) \bmod m; x(7) = 29$
8. $x(8) = (a \cdot x(7) + b) \bmod m; x(8) = 16$
9. $x(9) = (a \cdot x(8) + b) \bmod m; x(9) = 3$
10. $x(10) = (a \cdot x(9) + b) \bmod m; x(10) = 50$
11. $x(11) = (a \cdot x(10) + b) \bmod m; x(11) = 37$
12. $x(12) = (a \cdot x(11) + b) \bmod m; x(12) = 24$
13. $x(13) = (a \cdot x(12) + b) \bmod m; x(13) = 11$
14. $x(14) = (a \cdot x(13) + b) \bmod m; x(14) = 58$
15. $x(15) = (a \cdot x(14) + b) \bmod m; x(15) = 45$
16. $x(16) = (a \cdot x(15) + b) \bmod m; x(16) = 32$
17. $x(17) = (a \cdot x(16) + b) \bmod m; x(17) = 19$
18. $x(18) = (a \cdot x(17) + b) \bmod m; x(18) = 6$
19. $x(19) = (a \cdot x(18) + b) \bmod m; x(19) = 53$
20. $x(20) = (a \cdot x(19) + b) \bmod m; x(20) = 40$
21. $x(21) = (a \cdot x(20) + b) \bmod m; x(21) = 27$
22. $x(22) = (a \cdot x(21) + b) \bmod m; x(22) = 14$
23. $x(23) = (a \cdot x(22) + b) \bmod m; x(23) = 1$
24. $x(24) = (a \cdot x(23) + b) \bmod m; x(24) = 48$
25. $x(25) = (a \cdot x(24) + b) \bmod m; x(25) = 35$

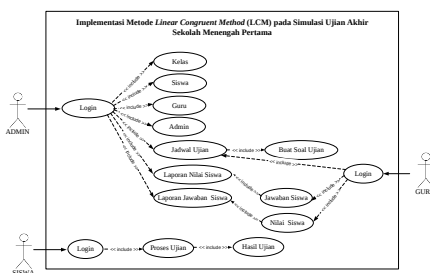
TABEL 1. HASIL BILANGAN ACAK

<i>i</i>	Bilangan acak ke- <i>i</i>	<i>i</i>	Bilangan acak ke- <i>i</i>	<i>i</i>	Bilangan acak ke- <i>i</i>
1	47	21	27	41	7
2	34	22	14	42	54
3	21	23	1	43	41
4	8	24	48	44	28
5	55	25	35	45	15
6	42	26	22	46	2
7	29	27	9	47	49
8	16	28	56	48	36
9	3	29	43	49	23
10	50	30	30	50	10
11	37	31	17	51	57
12	24	32	4	52	44
13	11	33	51	53	31
14	58	34	38	54	18
15	45	35	25	55	5
16	32	36	12	56	52
17	19	37	59	57	39
18	6	38	46	58	26
19	53	39	33	59	13
20	40	40	20	60	0

Sesuai dengan tabel 1 maka semua soal ujian akan ditempatkan pada urutan yang sesuai dengan bilangan acak yang dihasilkan. Soal ujian ke-1 akan ditempatkan pada urutan ke-47, soal ujian ke-2 akan akan ditempatkan pada urutan ke-34, soal ujian ke-3 akan akan ditempatkan pada urutan ke-21, soal ujian ke-4 akan akan ditempatkan pada urutan ke-8, soal ujian ke-5 akan akan ditempatkan pada urutan ke-55, dan seterusnya hingga soal ujian ke-60 akan akan ditempatkan pada urutan ke-0 (urutan pertama).

B. Hasil Perancangan

Use case merupakan salah satu diagram *Unified Modeling Language (UML)*, Gambar 3.



Gambar 3. Use Case Diagram

Pengguna dapat memilih menu [Data Utama] – [Kelas] untuk membuka *form* Kelas. Fungsi dari *form* ini adalah untuk memasukkan kelas yang terdapat pada sekolah. Tampilan *Form* Kelas Gambar 4. Pengguna dapat memilih menu [Data Utama] – [Siswa] untuk membuka *form* Siswa. Fungsi dari *form* untuk memasukkan data siswa sekolah. Tampilan *Form* Siswa, Gambar 5.

Gambar 4. Form Kelas

Gambar 5. Form Siswa

Gambar 6. Form Guru

Gambar 7. Form Bidang Studi

Pengguna dapat memilih menu [Data Utama] – [Guru] untuk membuka *form* Guru. Fungsi dari *form* ini adalah untuk memasukkan data guru yang mengajar di sekolah. Tampilan *form* Guru, Gambar 6. Pengguna dapat memilih menu [Data Utama] – [Bidang Studi] untuk membuka *form* Bidang Studi. Fungsi dari *form* ini adalah untuk memasukkan bidang studi yang dipelajari, Gambar 7. Guru dapat memilih salah satu jadwal ujian dan menekan tombol "Edit Soal Ujian" untuk mulai memasukkan soal ujian pada jadwal ujian yang telah ditentukan. Tampilan *form* Edit Soal Ujian, Gambar 8.

Gambar 8. Tampilan Form Edit Soal Ujian

Setelah menjawab semua pertanyaan soal ujian dan tekan tombol "Selesai" dan *form* Hasil Ujian,

Gambar 9. Pengguna dapat memilih menu [Laporan] – [Laporan Jawaban Siswa] untuk menampilkan laporan jawaban siswa. Tampilan *form* Filter Laporan Jawaban Siswa, Gambar 10.

No	Soal	Jawaban Benar	Jawaban Siswa	Nilai
1	Soal No-1. Jawaban = A (BENAR)	A	A	20
2	Soal No-2. Jawaban = D (SALAH)	D	C	0
3	Soal No-3. Jawaban = C (BENAR)	C	C	20
4	Soal No-4. Jawaban = A (SALAH)	A	B	0
5	Soal No-5. Jawaban = B (BENAR)	B	B	20
TOTAL NILAI = 60				

Gambar 9. Form Hasil Ujian

Gambar 10. Form Laporan Siswa

V. KESIMPULAN

1. Aplikasi dapat digunakan untuk menyelenggarakan ujian sekolah secara komputerisasi dengan pengacakan soal berdasarkan pada metode *Linear Congruential Generator*.
2. Metode LCG dapat diimplementasikan dengan sangat cepat untuk mengacak urutan soal tanpa adanya jeda atau waktu tunggu yang mempengaruhi lamanya proses ujian.
3. Aplikasi dapat menampilkan hasil ujian setelah proses ujian selesai, sehingga siswa dapat langsung mengetahui nilai ujian dan guru tidak perlu melakukan koreksi secara manual.
4. Aplikasi menyediakan laporan jawaban siswa sebagai hasil koreksi atas proses ujian siswa, dan laporan nilai siswa untuk menampilkan laporan nilai ujian per kelas.

REFERENCES

- [1] Gunawan, Dedy Agung Prabowo, Mahasiswa Baru Dengan Pengacakan Soal Menggunakan Linear Congruent Method (Studi Kasus di Universitas Muhammadiyah Bengkulu), Jurnal Informatika Upgris Vol. 3, No. 2, 2017, hal 143-151.
- [2] Rian Laksana Putra, Arris Maulana, Tuti Iriani, Evaluasi Program Pelaksanaan Ujian Online Dengan Menggunakan Learning Management System Moodle Berbasis Android Di SMK Negeri 1 Jakarta, Jurnal Pendidikan Teknik Sipil Volume 8, No 1, Februari 2019 hal : 48-54.
- [3] Anita Sinder Sinaga, Implementasi OLAP Menggunakan Dashboard Holistics Software Pada LPPM STMIK Pelita Nusantara, Jutikomp, Vol. 2 No. 1 Tahun 2019, hal : 55-59.
- [4] Joko Wicaksono, M Dharmawan A, Erwin Azhari W, Yoannita, Penerapan Algoritma Linear Congruent Method Untuk Pengacakan Soal pada Pengenalan Kampus Berbasis Virtual Reality, 2018.
- [5] Sistem Ujian Online Seleksi Penerimaan Mahasiswa Baru Dengan Pengacakan Soal Menggunakan Linear Congruent Method (Studi Kasus di Universitas Muhammadiyah Bengkulu), Jurnal Informatika UPGRIS Vol. 3, No. 2, December 2017
- [6] M. Rifqi Tsani, Nurhadianto, Sistem Informasi Ujian Berbasis Web Server SMK Bina Islam Mandiri (Bisma) Kersana Brebes Tegal , Cogito Smart Journal, Vol. 1/No. 1/Desember 2015, Hal: 45-55.
- [7] A Sinder RMS, Sistem Bilangan Digital, Penerbit CV. AA. Rizky Serang Banten Oktober 2019.
- [8] Sugeng Supriyadi, Dadang Hamdani, Yoyon Mohamad Furqon, Rancang Bangun Alfabet Memory Game Menggunakan Linear Congruent Method (LCM), Unikus Journal 2018.
- [9] Niria Laila, Anita Sinder RMS, Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra, ScientiCO : Computer Science Informatics Journal Vol. 1, No. 2, 2018, 47-58.
- [10] Susilowati, Taufik Hidayat, Rancang Bangun Sistem Informasi Ujian Online (Studi Kasus Pada SMAN 58 Jakarta), Jurnal Teknik Komputer, Vol 4, No. 1, Februari 2018.