p-ISSN: 1979-5661
e-ISSN: 2622-321X

Modifikasi Algoritma Fisher Yates Shuffle Menggunakan Linear Congruent Method Untuk Pembangkitan Bilangan Acak

Surya Darma Nasution[1], Suginam[2]

[1]Teknik Informatika, STMIK Budi Darma
Medan, Indonesia
[1]darmashadow@gmail.com

[2]Manajemen Informatika, STMIK Budi Darma
Medan, Indonesia
[2]suginam.icha@gmail.com

Abstrak

Pembangkit bilangan acak digunakan untuk menghasilkan urutan-urutan dari angka-angka sebagai hasil dari suatu perhitungan dengan komputer yang diketahui distribusinya sehingga angka-angka yang dihasilkan akan muncul secara acak. Masalah yang ada pada suatu algoritma pembangkit bilangan acak adalah apakah algoritma tersebut dapat menghasilkan angka-angka yang acak. Linear congruent method memiliki kekurangan yaitu hasil bilangan acak yang dihasilkan berpola dan algoritma fisher yates shuffle memiliki kekurangan yaitu untuk menghasilkan bilangan acak membutuhkan algoritma pembangkit bilangan acak lainnya. Dengan memodifikasi algoritma fisher yates shuffle menggunakan linear congruent method diharapkan dapat menghasilkan menghasilkan bilangan acak.

Kata Kunci: *Fisher Yates Shuffle, Linear Congruent Method, Pembangkit Bilangan Acak*

1. Pendahuluan

Pembangkit bilangan acak digunakan pada berbagai bidang, yaitu dalam simulasi, pembuatan game, dan pada bidang lainnya yang memang membutuhkan angka-angka yang acak[1][2]. Linear congruent method yang paling banyak digunakan dalam pembangkitan bilangan acak. Keuntungan pada linear congruent method yaitu kecepatan, kemudahan dalam mengimplementasikannya[3].

Algoritma fisher yates shuffle merupakan algoritma pengacakan yang proses pengacakannya dilakukan dengan permutasi acak dari suatu set bilangan. Algoritma Fisher Yates Shuffle akan terus menentukan bilangan berikutnya secara acak tanpa ketemu suatu angka yang sama[4].

Dari kedua algoritma itu memiliki kekurangan masing-masing dalam membangkitkan bilangan acak seperti pada linear congruent method kekurangannya adalah hasil pengacakannya berpola, sehingga penggunaannya kurang efektif dan mudah ditebak. Walaupun hal tersebut dapat diatasi dengan pemilihan dari nilai variabel yang digunakan, tetapi jika variabel yang digunakan tidak sesuai malah akan menghasilkan bilangan yang sama sekali tidak acak.

Kekurangan yang terdapat pada algoritma fisher yates shuffle yaitu untuk menghasilkan suatu bilangan acak memerlukan algoritma lainnya untuk mengacak (roll). Sehingga bisa dibilang algoritma tidak bisa berdiri sendiri, dan pada beberapa penelitian dapat dilihat bahwa pada saat melakukan roll maka angka yang muncul tidak dapat diketahui darimana asalnya tanpa adanya perhitungan.

Kekurangan yang terdapat pada kedua pembangkit bilangan acak tersebut dapat diatasi jika kedua algoritma itu dimodifikasi dengan cara menggunakan linear congruent method untuk roll pada algoritma fisher yates shuffle. Dimana untuk memodifikasi dengan

menggabungkan kedua algoritma tersebut tidaklah mudah karena hasil dari pembangkitan bilangan acak menggunakan linear congruent method sesekali akan mendapatkan nilai 0, sementara nilai 0 pada algoritma fisher yates shuffle tidak terdapat didalam urutan bilangan yang akan diacak.

2. Linear Congruent Method

Linear congruent method merupakan salah satu pembangkit bilangan acak yang banyak digunakan dalam program komputer. Salah satu sifat dari linear congruent method yaitu terjadi pengulangan pada periode waktu tertentu atau setelah sekian kali pembangkitan[5].

Rumus dari linear congruent method yaitu :

$$Xi +1 = a.Xi + c \bmod m \quad (1)$$

Dimana :

Xi+1 = Angka acak yang baru.
Xi = Angka acak yang lama atau angka acak sebelumnya.
a = Angka konstanta pengalian.
c = Angka kenaikan.
m = Angka modulo.

Contoh penerapan Linear Congruent Method (LCM) untuk menghasilkan sebanyak empat belas (14) bilangan acak. Dengan nilai variable a=27, c=4, m=13 dan nilai x0=7. Berikut ini proses perhitungannya :

x1 = (a*x0+c) mod m
x1 = (27*7+4) mod 13
x1 = 193 mod 13
x1 = 11

x2 = (a*x1+c) mod m
x2 = (27*11+4) mod 13
x2 = 301 mod 13
x2 = 2

x3 = (a*x2+c) mod m
x3 = (27*2+4) mod 13
x3 = 58 mod 13
x3 = 6

x4 = (a*x3+c) mod m
x4 = (27*6+4) mod 13
x4 = 166 mod 13
x4 = 10

x5 = (a*x4+c) mod m
x5 = (27*10+4) mod 13
x5 = 274 mod 13
x5 = 1

x6 = (a*x5+c) mod m
x6 = (27*1+4) mod 13
x6 = 31 mod 13
x6 = 5

x7 = (a*x6+c) mod m
x7 = (27*5+4) mod 13
x7 = 139 mod 13
x7 = 9

x8 = (a*x7+c) mod m
x8 = (27*9+4) mod 13
x8 = 247 mod 13
x8 = 0

x9 = (a*x8+c) mod m
x9 = (27*0+4) mod 13
x9 = 4 mod 13

x10 = (a*x9+c) mod m
x10 = (27*4+4) mod 13
x10 = 112 mod 13

p-ISSN: 1979-5661
e-ISSN: 2622-321X

x9 = 4

x10 = 8

x11 = (a*x10+c) mod m
x11 = (27*8+4) mod 13
x11 = 220 mod 13
x11 = 12

x12 = (a*x11+c) mod m
x12 = (27*12+4) mod 13
x12 = 328 mod 13
x12 = 3

x13 = (a*x12+c) mod m
x13 = (27*3+4) mod 13
x13 = 85 mod 13
x13 = 7

x14 = (a*x13+c) mod m
x14 = (27*7+4) mod 13
x14 = 193 mod 13
x14 = 11

Dari perhitungan tersebut dapat dirangkum hasil pembangkitan bilangan acak sebanyak empat belas (14) bilangan acak dalam bentuk tabel dan dapat dilihat pada tabel 1.

Tabel 1 Hasil Pembangkitan 14 Bilangan Acak

i	xi	Xi+1
0	7	11
1	11	2
2	2	6
3	6	10
4	10	1
5	1	5
6	5	9
7	9	0
8	0	4
9	4	8
10	8	12
11	12	3
12	3	7
13	7	11

Kesimpulan yang diperoleh dari perhitungan yang dilakukan yaitu terjadi pengulangan dari bilangan acak yang dihasilkan pada nilai x13 dan x14 yaitu sama-sama bernilai 7 untuk x13 dan nilai 11 untuk x14.

Contoh lain dari penerapan Linear Congruent Method (LCM) untuk menghasilkan sepuluh (10) bilangan acak. Dengan nilai variable a=27, c=4, m=10, dan nilai x0=7. Dari contoh yang pertama, yang berubah hanya nilai variabel m yaitu 10. Berikut ini proses perhitungannya :

x1 = (a*x0+c) mod m
x1 = (27*7+4) mod 10
x1 = 193 mod 10
x1 = 3

x2 = (a*x1+c) mod m
x2 = (27*3+4) mod 10
x2 = 85 mod 10
x2 = 5

x3 = (a*x2+c) mod m
x3 = (27*5+4) mod 10
x3 = 139 mod 10
x3 = 9

x4 = (a*x3+c) mod m
x4 = (27*9+4) mod 10
x4 = 247 mod 10
x4 = 7

x5 = (a*x4+c) mod m
x5 = (27*7+4) mod 10
x5 = 193 mod 10
x5 = 3

x6 = (a*x5+c) mod m
x6 = (27*3+4) mod 10
x6 = 85 mod 10
x6 = 5

x7 = (a*x6+c) mod m
x7 = (27*5+4) mod 10
x7 = 139 mod 10
x7 = 9

x8 = (a*x7+c) mod m
x8 = (27*9+4) mod 10
x8 = 247 mod 10
x8 = 7

x9 = (a*x8+c) mod m
x9 = (27*7+4) mod 10
x9 = 193 mod 10
x9 = 3

x10 = (a*x9+c) mod m
x10 = (27*3+4) mod 10
x10 = 85 mod 10
x10 = 5

Dari perhitungan tersebut dapat dirangkum hasil pembangkitan bilangan acak sebanyak sepuluh (10) bilangan acak dalam bentuk tabel dan dapat dilihat pada tabel 2.

Tabel 2 Hasil Pembangkitan 10 Bilangan Acak

i	xi	Xi+1
0	7	3
1	3	5
2	5	9
3	9	7
4	7	3
5	3	5
6	5	9
7	9	7
8	7	3
9	3	5

Kesimpulan yang diperoleh dari perhitungan yang dilakukan yaitu terjadi pengulangan terus menerus yaitu 3,5,9,7, sehingga dapat disimpulkan dengan merubah nilai variabel m, maka hasilnya akan berbeda dan bilangan yang dihasilkan tidak benar-benar random.

p-ISSN: 1979-5661
e-ISSN: 2622-321X

3. Algoritma Fisher Yates Shuffle

Algoritma Fisher Yates Shuffle merupakan algoritma pangacakan yang lebih baik dan sesuai untuk mengacak angka, dengan waktu proses yang cepat dan tidak memerlukan waktu yang lama untuk melakukan proses pengacakan. Algoritma Fisher Yates Shuffle terdiri dari dua metode yaitu, orisinal dan modern. Dalam penelitian ini dipilih metode yang modern karena metode ini khusus digunakan untuk proses pengacakan dengan sistem yang komputerisasi, dikarenakan hasil pengacakan bisa lebih variatif.

Metode modern yang digunakan untuk menghasilkan suatu permutasi acak untuk angka 1 sampai N adalah sebagai berikut :

1. Tuliskan angka dari 1 sampai N.
2. Pilih sebuah angka acak K diantara 1 sampai dengan jumlah angka yang belum dicoret.
3. Dihitung dari bawah, coret angka K yang belum dicoret, dan tuliskan angka tersebut di lain tempat.
4. Ulangi langkah 2 dan langkah 3 sampai semua angka sudah tercoret.
5. Urutan angka yang dituliskan pada langkah 3 adalah permutasi acak dari angka awal.

Contoh penerapan algoritma fisher yates shuffle untuk menghasilkan sepuluh (10) bilangan acak dapat dilihat pada tabel 3.

Tabel 3 Hasil Pengacakan Algoritma Fisher Yates Shuffle

Range	Acak	Dicoret	Hasil
		1,2,3,4,5,6,7,8,9,10	
1-10	6	1,2,3,4,5,10,7,8,9	6
1-9	2	1,9,3,4,5,10,7,8	2,6
1-8	2	1,8,3,4,5,10,7	9,2,6
1-7	7	1,8,3,4,5,10	7,9,2,6
1-6	3	1,8,10,4,5	3,7,9,2,6
1-5	1	5,8,10,4	1,3,7,9,2,6
1-4	2	5,4,10	8,1,3,7,9,2,6
1-3	1	10,4	5,8,1,3,7,9,2,6
1-2	1	4	10,5,8,1,3,7,9,2,6
Hasil Pengacakan			4,10,5,8,1,3,7,9,2,6

Kesimpulan yang diperoleh dari proses yang telah dilakukan yaitu tidak terjadi pengulangan seperti pada Linear Congruent Method, tidak ada angka yang muncul 2 (dua) kali, sehingga angka yang muncul memang benar-benar acak. Dan kelemahannya yaitu diperlukan algoritma lainnya untuk mengacak angka pada proses acak.

4. Modifikasi Algoritma

Proses memodifikasi algoritma fisher yates shuffle dengan menggunakan linear congruent method agar kekurangan yang terdapat pada kedua algoritma tersebut saling menutupi satu sama lain. Alasan yang dimodifikasi bukanlah algoritma linear congruent method karena kekurangan linear congruent method yang berpola dan berulang-ulang tidak dapat diselesaikan dengan algoritma fisher yates shuffle. Tetapi algoritma fisher yates shuffles dapat dimodifikasi untuk menutupi kekurangannya dengan menambahkan algoritma pembangkit bilangan acak lainnya.

Modifikasi dilakukan dengan membuat aturan baru dalam penetapan pada nilai dari variabel linear congruent method, yaitu :

a = Jumlah bilangan acak dibagi 2
c = Jumlah range tertinggi
m = Jumlah range tertinggi
xi = Jumlah bilangan acak dibagi 2 ditambah 1.

Contoh penerapan hasil modifikasi algoritma fisher yates shuffle menggunakan linear congruent method untuk menghasilkan sepuluh (10) bilangan acak dapat dilihat pada tabel 4.

Tabel 4 Hasil Pengacakan Dari Proses Modifikasi

Range	a	c	m	Roll (xi)	Scratch	Result
1-10	5	10	10	6	1,2,3,4,5,10,7,8,9	6
1-9	5	9	9	4	1,2,3,9,5,10,7,8	4,6
1-8	5	8	8	5	1,2,3,9,8,10,7	5,4,6
1-7	5	7	7	5	1,2,3,9,7,10	8,5,4,6
1-6	5	6	6	2	1,10,3,9,7	2,8,5,4,6
1-5	5	5	5	1	7,10,3,9	1,2,8,5,4,6
1-4	5	4	4	2	7,9,3	10,1,2,8,5,4,6
1-3	5	3	3	2	7,3	9,10,1,2,8,5,4,6
1-2	5	2	2	1	3	7,9,10,1,2,8,5,4,6
1	5	1	1	1		3,7,9,10,1,2,8,5,4,6

5. Kesimpulan

Hasil dari proses modifikasi yang dilakukan dapat menghasilkan bilangan yang benar-benar acak dan tidak berpola seperti pada linear congruent method. Serta Kecepatan dan kemudahan untuk membangkitkan bilangan acak masih sama seperti sebelum dilakukannya modifikasi.

Daftar Pustaka

[1] C. R. Selian, “PERANCANGAN APLIKASI GAME TEBAK WAJAH ATLET BULU TANGKIS DENGAN MENGGUNAKAN LINEAR CONGRUENT METHODS (LCM),” *Pelita Inform. Inf. dan Inform.*, vol. 4, no. 3, Aug. 2013.

[2] M. A. Hasan, Supriadi, and Zamzami, “Implementasi Algoritma Fisher-Yates Untuk Mengacak Soal Ujian Online Penerimaan Mahasiswa Baru (Studi Kasus : Universitas Lancang Kuning Riau),” *J. Teknol. dan Sist. Inf.*, vol. 3, no. 2, 2017.

[3] S. D. Nasution, “Penerapan Metode Linier Kongruen dan Algoritma Vigenère Chiper Pada Aplikasi Sistem Ujian Berbasis Lan,” *Pelita Inform.*, vol. 4, no. 1, pp. 94–102, 2013.

[4] R. Nugraha, E. EXRIDORES, and H. Sopryadi, “Penerapan Algoritma Fisher-Yates Pada Aplikasi The Lost Insect Untuk Pengenalan Jenis Serangga Berbasis Unity 3D,” *STMIK Glob. Inform. MDP, Palembang*, 2015.

[5] Sulindawaty, “PEMBUATAN PERANGKAT LUNAK PENYIMPANAN DATA RAHASIA DENGAN MENGGUNAKAN TEKNIK STEGANOGRAPHY UNTUK MEDIA CITRA DIGITAL,” *J. SAINTIKOM*, vol. 10, no. 3, pp. 155–173, 2011.