Aplikasi Pembangkit Bilangan Acak dalam Sistem Gacha dalam Berbagai Permainan

Mahesa Gandakusuma / 13513091
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
aseham.krazzy@gmail.com

***Abstrak*—Paper ini akan membahas mengenai penggunaan pembangkit bilangan acak dalam sistem gacha dalam berbagai permainan. Dalam sistem gacha, terdapat sebuah set hadiah yang bisa didapatkan pemain setelah pemain menggunakan mata uang tertentu dalam permainan tersebut sebagai masukan. Beberapa bagian dari set tersebut lebih langka dan sulit didapatkan, sehingga kadangkala pemain perlu memasukkan mata uang yang lebih banyak. Pengembang permainan sering menggunakan sistem ini untuk mendapatkan pemasukan tambahan.**

***Kata kunci*—aplikasi permainan, gacha, pembangkit bilangan acak**

I. PENDAHULUAN

Pada zaman sekarang, permainan pada perangkat komputer, *mobile*, dan konsol semakin meningkat pesat. Pesatnya aplikasi permainan yang tersebar membuat pengembangnya bersaing untuk mendapatkan keuntungan. Salah satu cara untuk mendapatkan keuntungan adalah dengan memasukkan sistem gacha ke dalam permainan yang dibuat. Gacha dalam permainan tersebut biasanya memiliki hadiah *in-game* yang bagus atau sebuah set hadiah yang hanya bisa didapatkan dari gacha tersebut. Pemain yang membutuhkan hadiah atau set tersebut harus mengeluarkan biaya untuk mendapatkannya, namun hadiah yang didapatkan adalah hadiah acak, sehingga jika pemain belum mendapatkan hadiah yang diinginkan, pemain harus mengeluarkan biaya lebih sampai hadiah yang diinginkan telah didapatkan. Gacha dalam permainan tersebut menggunakan pembangkit bilangan acak untuk menentukan hadiah apa yang didapatkan pemain. Pembangkit bilangan acak dalam gacha akan dibahas dalam paper ini.

II. DASAR TEORI

A. Pembangkit Bilangan Acak

Pembangkit bilangan acak adalah sebuah kakas untuk menghasilkan sebuah bilangan yang bernilai acak. Bilangan acak yang dihasilkan dari sebuah pembangkit bilangan acak merupakan hasil dari perhitungan rumus matematika, sehingga tidak ada komputasi deret bilangan yang benar-benar acak seperti pada pelemparan dadu. Pembangkit bilangan acak tersebut dinamakan *pseudorandom number generator* (PRNG).

Linear Congruential Generator (LCG) adalah salah satu PRNG yang pernah ditemukan dan digunakan, dengan rumus

$$X_n = (aX_{n-1} + b) \bmod m$$

dimana X_n adalah deret angka acak ke-n, a adalah faktor pengali, b adalah elemen penjumlah, dan m adalah nilai modulus. Untuk menjalankan rumus ini, dibutuhkan sebuah kunci pembangkit X_0 yang disebut *seed*. Keunggulan dari LCG adalah operasi perhitungannya cukup sederhana sehingga dapat dijalankan dengan cepat. Namun sayangnya LCG mudah ditebak angkanya, sehingga kurang cocok untuk kriptografi.

Untuk kriptografi, salah satu pembangkit angka acak adalah *cryptographically secure pseudorandom number generator* (CSPRNG). CSPRNG memiliki dua syarat yang harus dipenuhi, yaitu lolos tes keacakan statistik sehingga angka yang didapatkan dapat lebih acak, dan tahan terhadap serangan prediksi angka yang dihasilkan.

Salah satu CSPRNG yang sederhana adalah Blum Blum Shub (BBS) yang dibuat berdasarkan teori bilangan. Algoritmanya adalah sebagai berikut:

1. Pilih dua buah bilangan prima rahasia, p dan q, yang masing-masing kongruen dengan 3 (mod 4).
2. Kalikan keduanya menjadi $n = pq$. Bilangan n ini disebut bilangan bulat Blum. Nilai n tidak perlu rahasia.
3. Pilih bilangan bulat acak lain, s, sebagai umpan sedemikian sehingga:
   (i) $2 \leq s < n$
   (ii) s dan n relatif prima
   kemudian hitung $x_0 = s^2 \bmod n$
4. Barisan bit acak dihasilkan dengan melakukan iterasi berikut sepanjang yang diinginkan:
   (i) Hitung $x_i = x_{i-1}^2 \bmod n$

(ii) z_i = bit *LSB* (*Least Significant Bit*) dari x_i

Barisan bit acak adalah $z_1, z_2, z_3, \ldots$

Keunggulan dari BBS adalah sulitnya menentukan faktor dari nilai *n* dan barisan bit yang dihasilkan tidak dapat diprediksi baik dari kanan maupun dari kiri.

CSPRNG yang lain adalah dengan menggunakan Teori Chaos. Teori Chaos adalah teori yang menyatakan bahwa terdapat kekacauan secara sains yang membuat sesuatu menjadi tak dapat diprediksi. Teori ini lebih ditujukan terhadap sesuatu yang non-linear yang tidak mungkin untuk diprediksi atau dikontrol, seperti keadaan cuaca, harga pasar, dan sebagainya. Salah satu karakteristiknya adalah peka terhadap nilai awal, sehingga sistem akan menghasilkan sesuatu yang acak meskipun sistem *chaos* sendiri bersifat deterministik.

Berikut adalah salah satu fungsi chaos:

$$x_{i+1} = r\, x_i\, (1 - x_i)$$

dimana x adalah nilai-nilai chaos ($0 \leq x \leq 1$) dan r adalah laju pertumbuhan yang bernilai ($0 \leq r \leq 4$). Nilai x_0 digunakan sebagai nilai awal untuk pembangkitan bilangan acak.

B. Gacha

Gacha adalah mesin permainan dimana pemain harus memasukkan koin atau alat lainnya untuk mendapatkan hadiah acak yang terbungkus dalam sebuah kapsul yang terdapat di dalam mesin tersebut. Hadiah yang terdapat dalam sebuah mesin gacha biasanya merupakan bagian dari set hadiah keseluruhan. Dalam beberapa mesin gacha, terdapat beberapa hadiah yang lebih sulit untuk didapatkan dari hadiah yang lain, sehingga pemain yang mengincar hadiah tersebut harus mengeluarkan lebih banyak koin lagi jika tidak kunjung mendapatkannya. Tak jarang pula pemain mendapatkan hadiah yang telah didapatkan sebelumnya atau duplikat dari mesin yang sama.

Gacha yang akan dibahas dalam paper ini hanyalah gacha yang terdapat dalam berbagai permainan dalam perangkat komputer, *mobile*, atau konsol. Gacha dalam permainan dalam perangkat tersebut tentu saja tidak menggunakan mesin fisik yang berisikan berbagai hadiah dengan banyak yang berbeda tiap hadiah, namun berupa hadiah yang tidak terbatas dengan kemungkinan untuk mendapatkannya berbeda-beda, biasanya semakin kecil kemungkinannya semakin bagus hadiah yang didapatkan. Sebuah hadiah dikatakan langka (*rare*) jika banyaknya hadiah tersebut lebih sedikit dari barang-barang lainnya, atau kemungkinan mendapatkannya lebih kecil. Ada lagi hadiah yang dikatakan *super-rare* (SR) dan *super-super-rare* (SSR), yaitu hadiah yang lebih sulit didapatkan daripada hadiah *rare*. Hadiah SR atau SSR biasanya sangat bagus dan paling banyak diincar oleh pemain.

Gacha dapat digolongkan sebagai perjudian, karena biasanya untuk memainkannya, pemain membutuhkan sebuah mata uang dalam permainan ataupun uang asli yang telah dikonversi menjadi mata uang yang dibutuhkan. Selain itu, hadiah yang didapatkan adalah secara acak sehingga pemain yang kurang beruntung harus mengeluarkan biaya lebih jika ingin mendapatkan hadiah yang diinginkan. Oleh karena itu, pembuat atau pengembang aplikasi permainan seringkali mengaplikasikan sistem gacha untuk mendapatkan keuntungan dari pemainnya.

III. ANALISIS

A. Kaitan Gacha dan Pembangkit Bilangan Acak

Sistem gacha masih sering digunakan oleh para pembuat atau pengembang aplikasi permainan untuk mengambil keuntungan, karena untuk mendapatkan barang-barang *in-game* yang langka dari gacha tersebut pemain perlu mengeluarkan biaya. Biaya yang dimaksud dapat berupa mata uang permainan tersebut, atau uang asli yang telah dikonversi.

Dalam gacha dalam aplikasi permainan, telah disebutkan bahwa sistem yang digunakan bukanlah berbagai barang dengan banyak tertentu, namun berupa hadiah dengan kemungkinan mendapatkannya berbeda-beda. Pembangkit bilangan acak digunakan untuk menentukan hadiah tersebut dengan cara mencocokkan bilangan yang dihasilkan dengan jangkauan nilai tertentu dan mencocokkan jangkauan tersebut dengan hadiah yang didapat. Misalkan sebuah hadiah memiliki kemungkinan untuk mendapatkannya 5%, maka jika bilangan acak yang dihasilkan termasuk dalam jangkauan 5% tersebut dari jangkauan keseluruhan bilangan acak yang dihasilkan, pemain mendapatkan hadiahnya. Berikut adalah pseudocode untuk melakukan pencocokan hadiah:

```
function Random(n : integer) : integer
    // n berfungsi sebagai jangkauan nilai random yang dihasilkan
    x : integer
    x ← RandomGenerator() mod n
    //  memanggil algoritma pembangkit bilangan acak dan mengisi nilai x dengan hasil pembangkitan, kemudian lakukan modulus n
    return x

function GetPrize() : integer
    x : integer
    hadiah : array[m] of integer
    //  nilai m menyatakan banyak jenis hadiah yang bisa didapatkan pemain
    x ← Random(n)
    //  nilai n dapat berupa apapun, sesuai banyak kemungkinan yang ada
    hadiah ← [p1, p2, p3, ... , pm]
```

```
// nilai elemen array hadiah berisi kemungkinan mendapatkannya, yang totalnya harus sama dengan jangkauan total
i : integer
i ← 0
while (x>=0)
   x ← x - hadiah[i]
   if (x<0)
      break
   else
      i ← i + 1
   end if
end while
return i // pemain mendapat hadiah ke-i
```

Berdasarkan algoritma di atas, fungsi Random(n) adalah pembangkit angka acak yang menghasilkan sebuah angka acak dengan memanggil RandomGenerator(). Fungsi RandomGenerator() inilah yang berisi sebuah algoritma pembangkit bilangan acak. Sementara itu, fungsi GetPrize() diperlukan untuk melakukan pencocokan hadiah dengan total $p_1 + p_2 + p_3 + ... + p_m$ harus sama dengan n dan kemungkinan tiap hadiah adalah p_i/n. Pemain mendapatkan hadiah sesuai dengan hasil angka acak yang dihasilkan oleh fungsi Random(n).

B. Keamanan Pembangkit Bilangan Acak dalam Sistem Gacha

Pembangkit bilangan acak dalam gacha dibuat sedemikian rupa sehingga kemunculan hadiah benar-benar acak dan tidak dapat diprediksi oleh pemain. Adalah sebuah kerugian bagi pengembang aplikasi permainan jika hadiah acak yang didapatkan dapat diprediksi oleh pemain dengan mudah, karena hadiah SR atau SSR yang seharusnya sangat sulit didapatkan jika pemain kurang beruntung akan menjadi lebih mudah didapatkan.

Berdasarkan teori yang telah disampaikan pada Bab II, LCG tidak dapat digunakan untuk membuat sistem gacha, karena kelemahan LCG adalah bilangan yang dihasilkan dapat diprediksi dengan cara mengetahui nilai *a*, *b*, dan *m*, kemudian mengatur nilai *seed* sedemikian rupa sehingga hadiah SR atau SSR bisa didapatkan dengan mudah.

Apabila pembangkit bilangan acak yang digunakan adalah CSPRNG, keamanan dari serangan prediksi akan lebih terjamin karena lebih sulit untuk dilakukan kriptanalisis dengan cara mengetahui nilai parameter dalam persamaan pada CSPRNG. Misalnya pada BBS, pola bit yang dihasilkan tidak dapat diprediksi dari kanan maupun dari kiri, dan pada teori chaos pola yang dihasilkan benar-benar acak.

IV. KESIMPULAN

Pada sistem gacha dalam aplikasi permainan, dibutuhkan pembangkit bilangan acak yang aman, layaknya pembangkit bilangan acak yang digunakan dalam kriptografi. Pembangkit bilangan acak yang aman dari serangan prediksi akan menguntungkan pembuat aplikasi permainan yang menerapkan sistem gacha.

V. UCAPAN TERIMA KASIH

Pertama-tama saya mengucapkan syukur kepada Tuhan Yang Maha Esa yang telah melimpahkan berkatnya selama pengerjaan makalah ini sampai selesai. Saya juga mengucapkan terima kasih kepada bapak Rinaldi Munir sebagai dosen pengajar IF4020 Kriptografi yang telah memberikan materi mata kuliah kriptografi yang membantu dalam proses penyelesaian paper ini.

REFERENSI

[1] https://bothgunsblazingblog.wordpress.com/2013/08/07/gacha/ Diakses pada 14 Desember 2016, pukul 16.45 WIB.
[2] Slide kuliah IF4020 dengan judul Pembangkit Angka Acak.
[3] http://fractalfoundation.org/resources/what-is-chaos-theory/ Diakses pada 14 Desember 2016, pukul 23.08 WIB.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

.

Bandung, 20 Desember 2016

ttd

Mahesa Gandakusuma / 13513091