Analisa grup kurva eliptik sebagai pseudorandom number generator

Tanur Rizaldi Rahardjo - 13519214
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): tanurrizaldi@gmail.com

***Abstrak*—*Pseudorandom number generator* banyak digunakan pada bidang kriptografi yang membutuhkan keacakan. Grup kurva eliptik adalah salah satu objek yang sederhana tetapi memiliki sifat susah diprediksi sehingga banyak digunakan untuk landasan kriptosistem. Sifat susah diprediksi tersebut dapat digunakan sebagai *pseudorandom number generator*.**

Keywords—Grup; kurva eliptik; pseudorandom number generator

I. PENDAHULUAN

Pada bidang kriptografi, grup adalah objek utama yang digunakan sebagai landasan dari suatu kriptosistem. Grup adalah objek matematis sederhana yang memiliki sifat dan operasi dasar. Grup yang sering digunakan pada bidang kriptografi adalah grup berhingga atau *finite group*.

Grup berhingga yang memiliki batas atas mempermudah proses komputasi kriptografi pada komputer. Umumnya grup berhingga dibentuk menggunakan objek matematis dan operasi modulo untuk membentuk *finite group.*

Kurva eliptik adalah objek matematis yang banyak dipelajari pada bidang teori bilangan. Kurva eliptik juga dipelajari dan digunakan pada bidang kriptografi. Pada himpunan kurva eliptik dapat ditambahkan operasi sehingga menjadi suatu grup dan dapat digunakan modulo agar menjadi *finite group*.

Grup berhingga kurva eliptik memiliki sifat yang susah diprediksi untuk operasi penjumlahannya sehingga sering digunakan sebagai lanadasan kriptosistem. Perkalian skalar pada grup tersebut juga sering digunakan untuk melakukan enkripsi dan dekripsi pada kriptosistem kurva eliptik.

Pseudorandom number generator adalah fungsi yang dapat mengembalikan suatu nilai yang sekilas terlihat acak tetapi deterministik. *Pseudorandom number generator* membutuhkan suatu nilai awal yang sering disebut *seed* untuk inisiasi nilai acak. Nilai *seed* tersebut umumnya didapatkan dari suatu sumber entropi yang benar-benar acak sehingga dapat membuat *pseudorandom number generator* berfungsi layaknya *true random number generator*.

Sebagian dari himpunan *pseudorandom number generator* adalah *cryptographically secure*. *Cryptographically secure pseudorandom number generator* merupakan RNG yang aman untuk operasi kriptografi dikarenakan keacakan RNG yang cukup susah untuk melakukan analisis statistik demi melakukan prediksi nilai yang akan dikeluarkan.

Susah diprediksinya nilai pada grup kurva eliptik memungkinkan grup tersebut digunakan sebagai *pseudorandom number generator*. Titik-titik yang bergerak acak pada kurva eliptik memungkinkan mengembalikan nilai acak yang susah diprediksi yang diharapkan dapat memenuhi sifat *cryptographically secure pseudorandom number generator*.

II. DASAR TEORI

A. *Grup*

Grup adalah himpunan yang memiliki operasi sering dinamakan penjumlahan dan memenuhi sifat-sifat tertentu. Tiga sifat yang umum pada operasi grup adalah

- Asosiatif

  Untuk semua nilai a, b, dan c pada grup, (a + b) + c = a + (b + c) selalu berlaku.

- Identitas

  Terdapat suatu elemen unik 0 yang memenuhi sifat a + 0 = 0 + a = a untuk semua nilai a pada grup.

- Invers

  Untuk semua nilai a pada grup, terdapat nilai b pada grup yang memenuhi a + b = 0 dengan 0 adalah elemen identitas grup.

Salah satu sifat yang dapat dimiliki grup adalah komutatif yaitu untuk semua nilai a dan b pada grup, persamaan a + b = b + a berlaku. Grup yang memenuhi sifat komutatif dinamakan grup abelian. Grup yang memiliki himpunan berhingga sebagai dasarnya dinamakan *finite group*. Himpunan dasar grup juga mungkin himpunan tak hingga seperti unit lingkaran, interval pada bilangan real, dan sebagainya. Grup adalah salah satu

struktur paling sederhana pada matematika, terdapat struktur-struktur lain seperti ring dan medan.

Group table of D_4

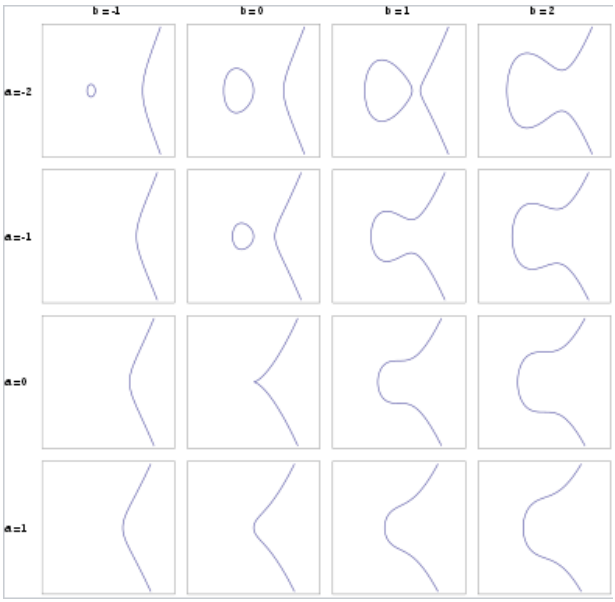
∘	id	r_1	r_2	r_3	f_v	f_h	f_d	f_c
id	id	r_1	r_2	r_3	f_v	f_h	f_d	f_c
r_1	r_1	r_2	r_3	id	f_c	f_d	f_v	f_h
r_2	r_2	r_3	id	r_1	f_h	f_v	f_c	f_d
r_3	r_3	id	r_1	r_2	f_d	f_c	f_h	f_v
f_v	f_v	f_d	f_h	f_c	id	r_2	r_1	r_3
f_h	f_h	f_c	f_v	f_d	r_2	id	r_3	r_1
f_d	f_d	f_h	f_c	f_v	r_3	r_1	id	r_2
f_c	f_c	f_v	f_d	f_h	r_1	r_3	r_2	id

Gambar 1. Grup D_4 (Sumber: en.wikipedia.org/wiki/Group_(mathematics)

Pada gambar diatas adalah contoh grup dihedral sederhana yang dinamakan D_4. Grup dihedral sering digunakan sebagai contoh grup karena grup tersebut dapat dibentuk juga oleh operasi refleksi dan rotasi yang mudah digambarkan.

B. *Kurva eliptik*

Kurva eliptik adalah kurva mulus yang sering digunakan pada bidang teori bilangan dan kriptografi. Persamaan kurva eliptik adalah $y^2 = x^3 + ax + b$ dan perlu memenuhi kondisi $4a^3 + 27b^2$ tidak sama dengan 0. Kondisi tersebut mencegah terjadinya perpotongan pada diri sendiri dan kurva mulus.

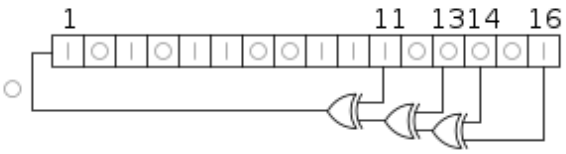


Gambar 2. Kurva elliptik (Sumber : en.wikipedia.org/wiki/Elliptic_curve)

Meskipun namanya kurva eliptik, kurva eliptik tidak memiliki banyak hubungan dengan elips. Salah satu penggunaan pada bidang kriptografi adalah faktorisasi bilangan bulat dan kriptosistem.

C. *Pseudorandom number generator*

Pseudorandom number generator adalah fungsi yang mengembalikan nilai yang sekilas terlihat acak tetapi sebenarnya deterministik. Banyak teknik pada teori *chaos* yang digunakan pada *pseudorandom number generator* dikarenakan memenuhi sifat yang terlihat acak dan sangat sensitif terhadap nilai awal. Beberapa *pseudorandom number generator* yang sering digunakan adalah peta logistik dan *linear shift feedback register*. Untuk aplikasi pada bidang kriptografi, *pseudorandom number generator* perlu memenuhi sifat-sifat yang tahan terhadap analisa statistik, *random number generator* yang memenuhi sifat tersebut dinamai *cryptographically secure pseudorandom number generator*.



Gambar 3. *Linear Shift Feedback Register (Sumber : en.wikipedia.org/wiki/Linear-feedback_shift_register)*

Gambar diatas merupakan contoh *pseudorandom number generator* sederhana yang sangat mudah untuk diimplementasikan pada sirkuit sederhana karena hanya menggunakan operasi *shift* dan *xor*. Namun *linear shift feedback register* sendiri bukanlah *cryptographically secure pseudorandom number generator* karena mudahnya melakukan serangan statistik. Untuk mencapai *cryptographically secure pseudorandom number generator*, diperlukan gabungan beberapa *linear shift feedback register* agar fungsi yang dihasilkan non-linear yang susah untuk dilakukan analisa statistik.

III. Rencana Implementasi

Untuk melakukan analisa statistik dan pengujian sifat-sifat *cryptographically secure pseudorandom number generator*, grup kurva eliptik akan diimplementasikan pada bahasa python. Implementasi akan menggunakan kurva eliptik dengan modulo yang ditentukan. Karena pada kurva eliptik hasil operasi merupakan titik, konversi titik ke angka akan dilakukan dengan penjumlahan absis dan ordinat. Titik identitas pada grup akan diimplementasikan menggunakan *library math* pada python.

IV. Implementasi

Berikut adalah *pseudocode* sederhana untuk melakukan analisis *cryptographically secure pseudorandom number generator* pada grup kurva eliptik

```
function add(a, b)
        if a.x = b.x and – a.y = b.y then
                return O
        else if a.x = b.x then
                return O
        else if a = O then
                return b
        else if b = O then
                return a
        else
                m ← ((a.x – b.x) *
modinv(a.x – b.x, p)) % p
                result.x ← (m**2 – a.x – b.x)
% p
                result.y ← (m * (a.x – b.x) –
a.y) % p
```

Fungsi diatas digunakan untuk operasi penjumlahan pada grup kurva eliptik yang memenuhi definisi pada grup kurva eliptik. Pada fungsi tersebut diasumsikan terdapat fungsi modinv yang menerima dua bilangan bulat dan mengembalikan hasil invers perkalian pada aritmatika modulo.

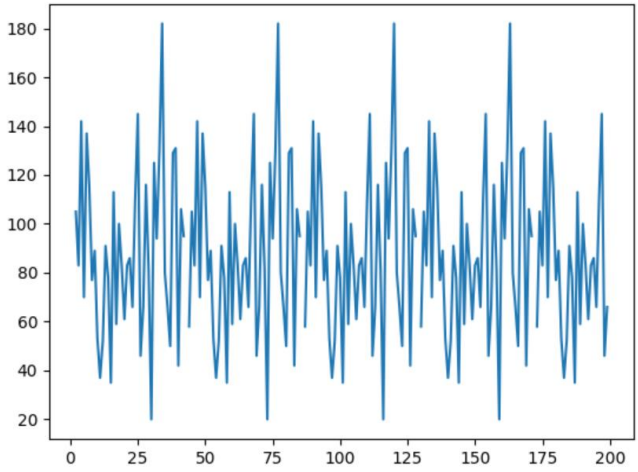
```
function multiply(a, k)
        result ← a
        i ← 0
        repeat
                result ← add(result, a)
                i ← i + 1
        until i = k - 2
```

Fungsi diatas digunakan untuk operasi perkalian skalar pada grup kurva eliptik. Fungsi tersebut menggunakan fungsi penjumlahan yang dibuat sebelumnya untuk melakukan perkalian skalar titik pada grup kurva eliptik.

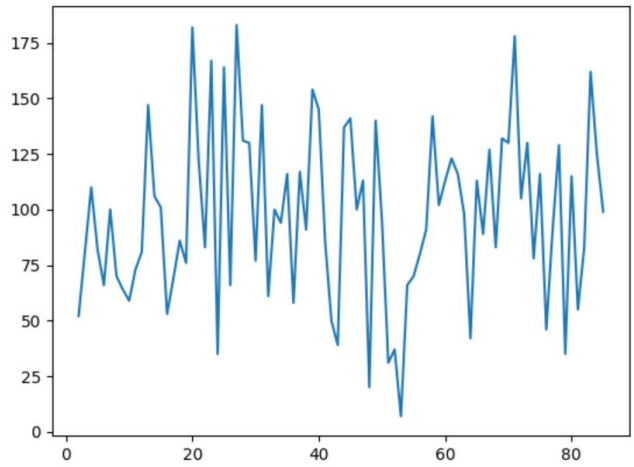
Untuk kebutuhan visualisasi akan digunakan *library matplotlib* yang didapatkan pada repository *library* python. Persamaan kurva eliptik yang digunakan adalah $y^2 = (x^3 + ax + b) \pmod p$

V. Analisis

Berikut adalah salah satu hasil operasi perkalian yang diiterasikan berulang, parameter yang digunakan adalah a = 22, b = 60, p = 97 dan titik awal adalah (28, 30)

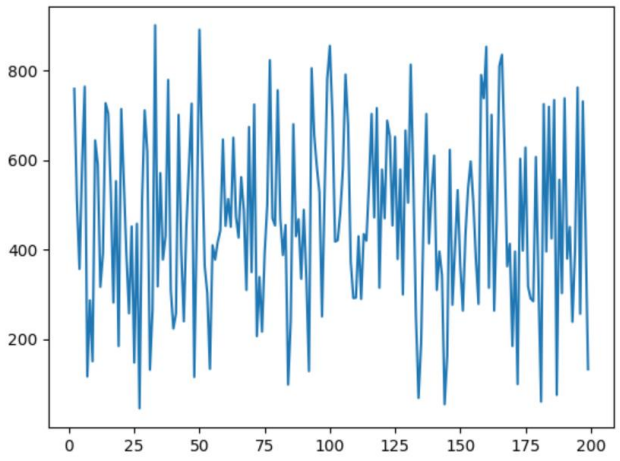


Pada grafik terlihat bahwa terdapat beberapa kali pengulangan dan periode pengulangan adalah 85. Berikut adalah hasil perbesaran grafik.

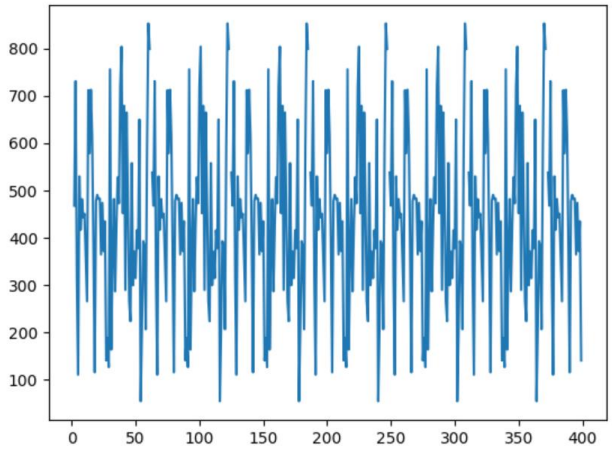


Distribusi angka pada *pseudorandom number generator* cukup acak jika dilihat sekilas pada grafik.

Berikut adalah operasi perkalian pada parameter yang lebih besar dibandingkan sebelumnya

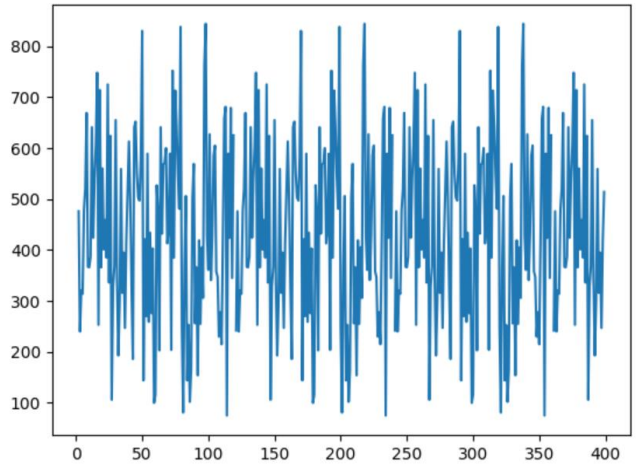


Gambar diatas menggunakan nilai a = 941, b = 937, p = 461, dan titik awal (420, 159). Meskipun terlihat acak sekilas, fungsi tersebut hanya memiliki periode 62.

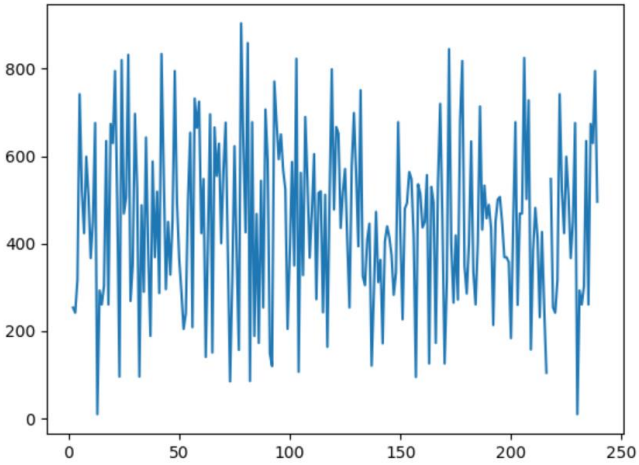


Gambar diatas menggunakan parameter a, b, p dan titik awal yang sama tetapi iterasi yang lebih panjang untuk menggambarkan periodisitas fungsi. Terlihat bahwa perkalian grup kurva eliptik sebagai *pseudorandom number generator* tidak menjamin parameter yang besar akan menghasilkan periode yang lebih besar.

Berikut adalah parameter yang lebih kecil tetapi memiliki periode yang jauh lebih panjang dibandingkan sebelumnya, a = 95, b = 94, p = 461, titik awal = (160, 49).



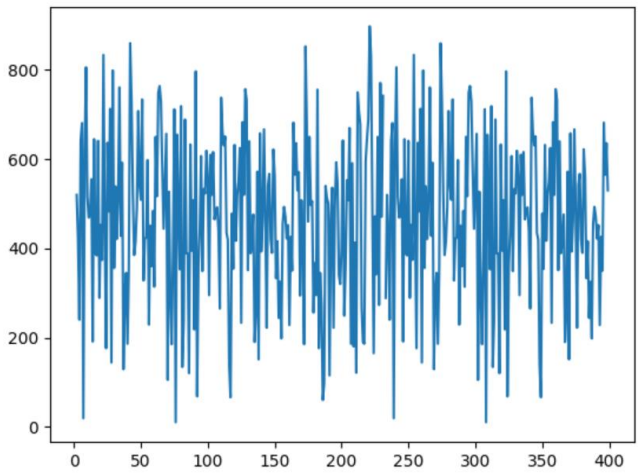
Parameter tersebut menyebabkan periode fungsi lebih dari 300 dengan angka yang lebih kecil dibandingkan sebelumnya.



Fungsi tersebut berjalan dengan lebih cepat dan menghasilkan hasil yang cukup acak dengan angka yang kecil.

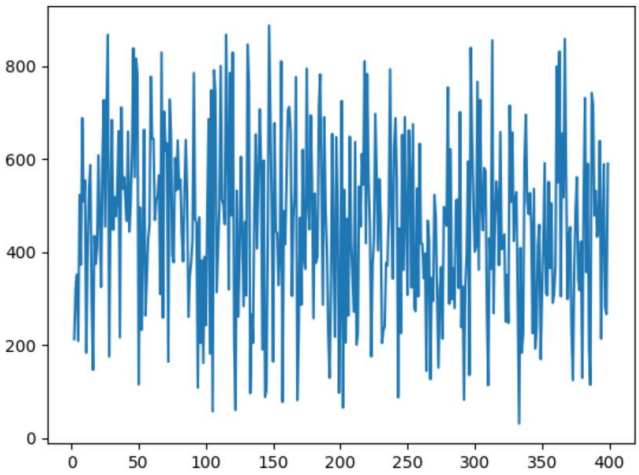
Berikut adalah beberapa hasil tambahan

a = 21, b = 14, p = 461, titik awal = (285, 4)



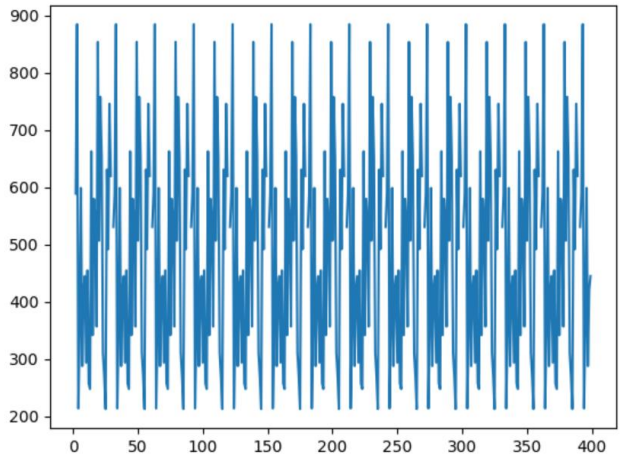
Titik awal = (19, 279)

a = 92, b = 84, p = 461



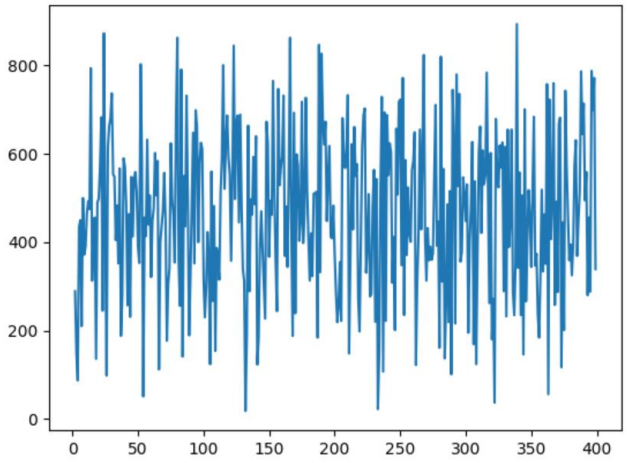
Titik awal = (345, 186)

a = 76, b = 28, p = 461



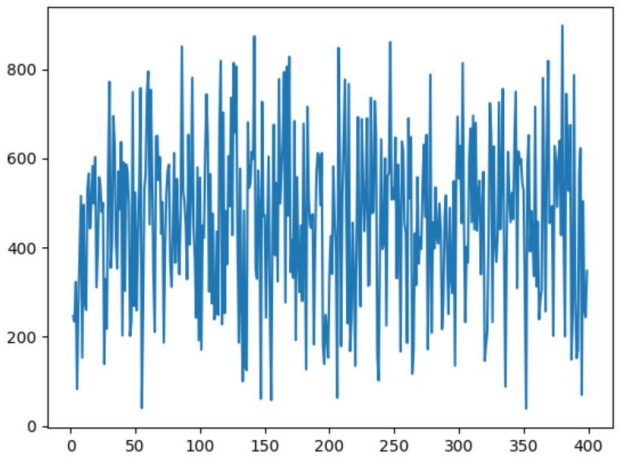
Titik awal = (337, 165)

a = 60, b = 18, p = 461



Titik awal = (281, 417)

a = 21, b = 73, p = 461



VI. KESIMPULAN

Dengan analisa sederhana untuk parameter kecil dan implementasi yang sederhana, grup kurva eliptik dapat digunakan untuk *pseudorandom number generator*. Namun untuk keperluan kriptografi, operasi perkalian pada grup kurva eliptik tanpa modifikasi tidak cocok untuk *CRPRNG*.

ACKNOWLEDGMENT

Penulis berterima kasih kepada pak Rinaldi Munir selaku tim pengajar mata kuliah IF4020 Kriptografi yang telah mengajarkan mata kuliah dengan baik.

REFERENCES

[1] Munir, Rinaldi. (2021). Bahan Kuliah IF4020 Kriptografi program Studi Informatika STEI-ITB.

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 2021

Tanur Rizaldi Rahardjo
13519214