Aplikasi Teori Bilangan dalam Pseudorandom Generator

Fritz Gerald Tjie 13518065[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13518065@std.stei.itb.ac.id

***Abstract*—Makalah ini membahas tentang penggunaan teori bilangan dalam hashing untuk menghasilkan bilangan pseudorandom (pseudorandom number generator). Generator bilangan pseudorandom dapat digunakan dalam ilmu kriptografi untuk mengamankan data. Teori bilangan dapat digunakan untuk menghasilkan sebuah bilangan khusus dari sebuah bibit (seed) yang telah ditentukan. Bilangan pseudorandom adalah bilangan yang dihasilkan melalui proses tersebut dan dapat digunakan sebagai landasan atau bagian dari suatu proses enkripsi dalam ilmu kriptografi.**

***Keywords*—hashing, kriptografi, pseudorandom, pseudorandom generator, teori bilangan.**

I. PENDAHULUAN

Manusia tentu selalu ingin mengembangkan tingkat kenyamanan hidupnya. Dari alasan dasar itulah dilahirkan suatu hal bernama teknologi. Teknologi adalah suatu metode ilmiah untuk mencapai kehidupan praktis. Salah satu contoh dari hasil teknologi adalah sistem penyebaran informasi dan data. Dengan berkembangnya efektifitas dari penyebaran informasi, manusia dapat menerima dan memberikan informasi dalam skala waktu yang sangatlah singkat.

Informasi merupakan suatu asset yang sangatlah penting di zaman yang telah modern ini. Tidak jarang kita mendengar istilah "informasi lebih berharga dibandingkan uang" dan ungkapan tersebut tidaklah salah. Informasi dan data telah dianggap sebagai suatu kebutuhan yang bisa dibilang mendasar pada zaman sekarang. Informasi dibutuhkan dalam setiap aspek kehidupan, baik dalam hal-hal mendasar seperti memasak hingga hal-hal yang bisa dibilang rumit seperti cara merancang bom atom.

Tentunya seiring perkembangan teknologi, manusia mendapat banyak permasalahan baru. Berkembangnya teknologi informasi memunculkan permasalahan yaitu terancamnya keamanan dalam penyebaran informasi. Informasi yang kita terima dan kita sebarkan ke orang lain bisa saja dapat disadap dan dicuri oleh pihak-pihak tidak bertanggung jawab. Maka dari itu muncul kebutuhan baru untuk mengamankan data sehingga tidak dapat diakses oleh orang-orang yang tidak diinginkan. Salah satu cara untuk mengamankan data tersebut adalah dengan menggunakan aplikasi teori bilangan dalam menghasilkan bilangan pseudorandom.

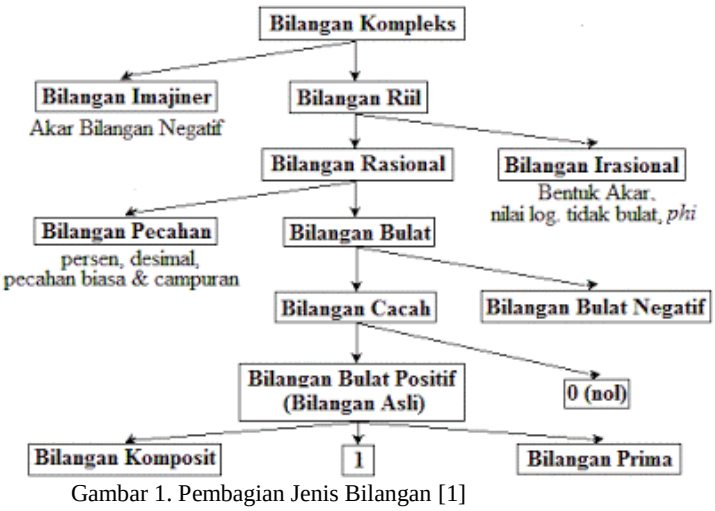
Bilangan pseudorandom adalah bilangan yang dihasilkan melalui proses randomisasi yang semu. Semu yang dimaksud disini adalah bilangan pseudorandom bukanlah bilangan yang murni dihasilkan secara acak, melainkan melalui suatu proses yang memiliki suatu bahan atau bibit (seed). Seed yang dipilih akan dijadikan parameter dari fungsi random.

Bilangan pseudorandom dapat dihasilkan dengan berbagai macam algoritma dan program yang dinamakan pseudorandom number generator (PRNG). Tetapi tidak semua pseudorandom number generator dapat memberikan hasil yang sesuai untuk mengamankan informasi. Karena hasil bilangan yang diberikan random atau acak tetapi bisa saja pola yang diberikan mudah ditebak. Maka dari itu, suatu pseudorandom number generator harus memenuhi standar tertentu sehingga dapat digunakan untuk tujuan kriptografi, dalam hal ini untuk mengenkripsi data.

Cryptographically secure pseudorandom number generator (CSPRNG) atau cryptographic pseudorandom number generator (CPRNG) adalah sebuah pseudorandom number generator yang memiliki sifat-sifat yang cocok dan memenuhi standar yang membuat hasil yang diperoleh dapat digunakan untuk tujuan kriptografi.

II. TEORI BILANGAN

Bilangan dapat dibedakan menjadi beberapa jenis yaitu bilangan riil, bilangan bulat, bilangan cacah, dst. Pembagian jenis bilangan ini dapat digambarkan dalam bentuk diagram seperti dibawah ini.



Gambar 1. Pembagian Jenis Bilangan [1]

Berikut adalah beberapa contoh dari bilangan-bilangan yang telah disebutkan di Gambar 1.

- Bilangan riil : $\sqrt{15}$, 8.0, -21.0, 1
- Bilangan imajiner : $\sqrt{-1}$
- Bilangan irasional : $\sqrt{2}$
- Bilangan prima : 2, 3, 5
- Bilangan bulat : -1, 0, 1, 2, 3

Teori bilangan adalah suatu cabang dari ilmu matematika murni yang mempelajari tentang bilangan bilangan bulat dan fungsi matematis yang mengaplikasikan bilangan bulat. Teori bilangan umumnya memiliki fokus studi yaitu bilangan prima xdan sifat-sifatnya.

Bilangan-bilangan bulat tersebut memiliki sebuah sifat umum, yaitu sifat pembagian pada bilangan bulat. Misalkan *a* dan *b* merupakan bilangan bulat dan $a \neq 0$, maka *a* habis membagi *b* jika terdapat bilangan bulat *c* sedemikian sehinga *b = ac*. Sebagai contoh, *4 | 12* karena *12/4 = 3* atau *12 = 4 × 3*. Hal ini dapat dinotasikan sebagai berikut

$$a|\, b \text{ jika } b = ac, c \in \mathbb{Z} \text{ dan } a \neq 0$$

Secara umum, suatu bilangan bulat jika dibagi dengan bilangan bulat lainnya dapat dituliskan dalam sebuah persamaan dengan menggunakan bilangan bulat. Misalkan terdapat sebuah bilangan bulat *m* dan *n* dimana *n > 0*. Jika bilangan *m* dibagi dengan bilangan bulat *n* maka akan terdapat bilangan bulat unik *q* (quotient) dan *r* (remainder). Hal ini dapat dinotasikan sebagai berikut

$$m = nq + r$$
$$n > 0, 0 \leq n < r$$

Persamaan diatas merupakan Teorema Eucledian yang ditemukan oleh Euclid, seorang matematikawan asal Yunani dalam bukunya *Element*. Sebagai contoh dari teorema ini adalah

$$15/7 = 2\text{ , sisa } 1$$
$$15 = 7 \times 2 + 1$$

Bilangan bulat juga mempunyai sifat lain yaitu pembagi bersama terbesar (PBB). Misalkan *a* dan *b* adalah suatu bilangan bulat yang tidak nol. Maka PBB dari *a* dan *b* adalah bilangan bulat terbesar, dalam hal ini dapat diumpamakan dengan *d* sedemikian rupa sehingga *d | a* dan *d | b*. Sehingga dapat dinyatakan bahwa PBB(*a*, *b*) = *d*. Sebagai contoh

$$\text{PBB}(12, 15) = 3$$
$$\text{PBB}(27, 54) = 9$$

Sifat PBB dan Teorema Eucledian ini dapat dihubungkan dengan teorema. Misalkan *m* dan *n* bilangan bulat, dengan syarat $n > 0$ dan $0 \leq r < n$ sedemikian sehingga

$$m = nq + r$$

$$\text{PBB}(\text{m}, \text{n}) = \text{PBB}(\text{n}, \text{r})$$

Sebagai contoh dari teorema ini adalah misalkan $m = 60$ dan $n = 18$, maka

$$60 = 18 \times 3 + 6$$
$$\text{PBB}(60, 18) = \text{PBB}(18, 6) = 6$$

PBB dapat dicari dengan menggunakan algortima Eucledian. Algoritma Eucledian bertujuan untuk mencari PBB dari 2 buah bilangan bulat. Algoritma ini mengatakan bahwa misalkan *m* dan *n* adalah bilangan bulat tidak negative dengan $m \geq n$. Misalkan $r_0 = m \text{ dan } \text{r}_1 = \text{n}$. Lakukan pembagian secara terus-menerus sehingga dapat diperoleh

$$r_0 = r_1 q_1 + r_2\text{ , } 0 \leq r_2 \leq r_1$$
$$r_0 = r_2 q_2 + r_3\text{ , } 0 \leq r_3 \leq r_2$$
$$\ldots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n\text{ , } 0 \leq r_n \leq r_{n-1}$$
$$r_{n-1} = r_n q_n + 0$$

Algoritma diatas dapat dihubungkan dengan PBB sebagai berikut

$$\text{PBB}(m, n) = \text{PBB}(\text{r}_0, \text{r}_1) = \text{PBB}(r_1, r_2) = \cdots =$$
$$PBB(r_{n-1}, r_n) = \text{PBB}(\text{r}_\text{n}, 0) = r_n$$

Maka, PBB dari *m* dan *n* adalah sisa terakhir yang tidak nol dari pembagian tersebut. Unutk memperjelas, maka dapat dilihat dari contoh berikut

$$m = 80, n = 12$$
$$80 = 6 \times 12 + 8$$
$$12 = 1 \times 8 + 4$$
$$8 = 2 \times 4 + 0$$

Sehingga didapatkan melalui algoritma Eucledian

$$FPB(80, 12) = 4$$

Bilangan bulat juga memiliki sebuah sifat unik yang sangatlah sering digunakan dalam teori bilangan, yaitu sisa hasil bagi atau modulo

$$a \bmod m = r \leftrightarrow a = mq + r$$

Dimana *a* dan *m* adalah bilangan bulat dan *q* merupakan hasil bagi dari *a* dan *m* serta *r* merupakan sisa hasil bagi dari *a* dan *m* Sebagai contoh

$$7 \bmod 3 = 1$$
$$5 \bmod 3 = 2$$
$$23 \bmod 5 = 3$$

Persamaan diatas dinamakan Aritmetika Modulo

Bilangan memiliki suatu sifat yang bernama kongruen, seperti contoh

$$38 \bmod 5 = 3$$
$$13 \bmod 5 = 3$$
$$\text{maka } 38 \equiv 13 \pmod 5$$

Persamaan diatas dapat dibaca 38 kongruen dengan 13 dalam modulo 5. Misalkan a dan b adalah bilangan bulat dan $m > 0$, maka

$$a \equiv b \ (mod\ m) \text{ jika dan hanya jika } m \mid (a - b)$$

Jika a tidak kongruen dengan b dalam modulus m, maka ditulis sebagaia berikut

$$a \not\equiv b \ (mod\ m)$$

Misalkan m adalah bilang bulat positif, maka berlaku

- Jika $a \equiv b \ (mod\ m)$ dan c adalah sembarang bilangan bulat maka
  - $(a + c) \equiv (b + c) \ (mod\ m)$
  - $ac \equiv bc \ (mod\ m)$
  - $a^p \equiv b^p \ (mod\ m), p \geq 0$
- Jika $a \equiv b \ (mod\ m)$ dan $c \equiv d \ (mod\ m)$, maka
  - $(a + c) \equiv (b + d\ ) (mod\ m)$
  - $ac \equiv bd \ (mod\ m)$

Dalam prinsip modulo terdapat istilah invers atau balikan. Misalkan x adalah invers dari $a \ (mod\ m)$, maka

$$ax \equiv 1 \ (mod\ m)$$

Atau dalam notasi "sama dengan"

$$ax = 1 + km$$

Atau

$$x = \frac{1 + km}{a}$$

Dimana k adalah bilangan bulat dan solusi dari persamaan tersebut adalah semua bilangan bulat yang memenuhi. Bentuk kongruen dari sebuah bilangan bulat dapat dikembangkan lagi menjadi kekongruenan lanjar (linear congruential). Kekongruenan lanjar berbentuk

$$ax \equiv b \ (mod\ m)$$

Dimana $m > 0$, a dan b merupakan sembarang bilangan bulat, dan x adalah peubah bilangan bulat. Sehingga bentuk diatas dapat diubah menjadi

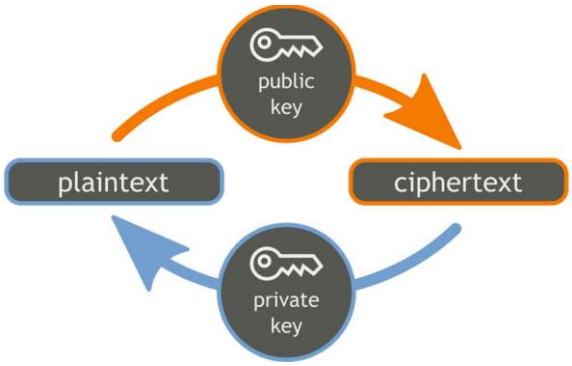
$$ax = b + km$$
$$x = \frac{b + km}{a}$$

Sama seperti mencari invers dari modulo, k adalah bilangan bulat dan solusi dari persamaan tersebut adalah k yang menghasilkan x sebagai bilangan bulat.

III. KRIPTOGRAFI

Kriptografi atau kriptologia berasal dari Bahasa Yunani yaitu "kryptos" yang berarti tersembunyi, rahasia dan "graphein" yang berarti menulis atau "logia" yang berarti ilmu pengetahuan. Berarti secara harafiah, kriptografi berarti suatu cabang ilmu pengetahuan yang mempelajari tentang cara mengamankan komunikasi dari pihak-pihak yang tidak diinginkan. Tujuan dari kriptografi adalah untuk menjamin pesan yang akan dikirimkan bersifat rahasia dan tidak dapat diidentifikasi oleh pihak yang tidak berhak.

Komponen dari kriptografi terdiri dari 3 bagian, yaitu plainteks (pesan yang ingin dienkripsi), cipherteks (pesan yang ingin didekripsi), dan key (kunci yang digunakan untuk enkripsi dan dekripsi).

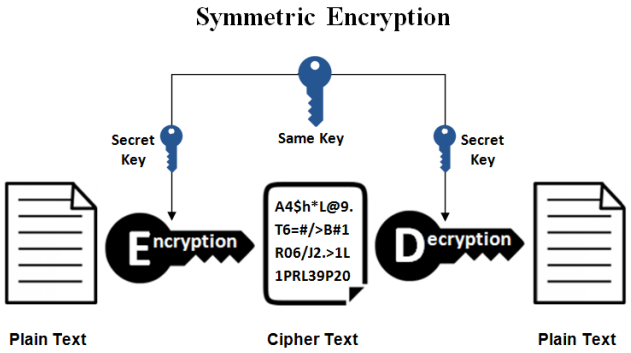


Gambar 2. Ilustrasi Kriptografi [2]

Kriptografi sendiri sebenarnya dapat dibagi menjadi 2 berdasarkan perbedaan cara penggunaan key dalam proses enkripsi dan dekripsi. Kedua jenis kriptografi tersebut adalah

- Symmetric Encryption
- Asymmetric Encryption

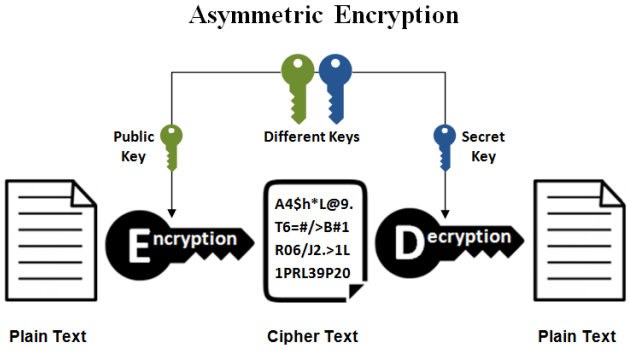
Symmetric Encryption (enkripsi simetris) adalah sistem enkripsi yang menggunakan key yang sama dalam proses enkripsi dan dekripsi. Contoh Symmetric Encryption yang terkenal adalah AES-129, AES-192, dan AES-256.



Gambar 3. Ilustrasi Symmetric Encryption [3]

Asymmetric Encryption (enkripsi asimetris) adalah sistem enkripsi yang menggunakan key yang berbeda dalam proses

enkripsi dan dekripsi. Contoh Asymmetric Encryption yang terkenal adalah RSA, DSA, dan Elliptic curve techniques.



Ganbar 4. Ilustrasi Asymmetric Encryption [4]

Kriptografi dapat diaplikasikan untuk pengiriman data melalui saluran komunkasi (pesan dikirimkan dalam bentuk cipherteks) dan penyimpanan data di dalam disk storage (data disimpan dalam memori disk dalam bentuk cipherteks)

Beberapa algoritma yang sering digunakan dalam kriptografi adalah

- Caesar Cipher
- Substitution Cipher
- Vigenere Cipher
- Algoritma RSA
- Pseudorandom Number Generator
- Hashing
- XOR Cryptography

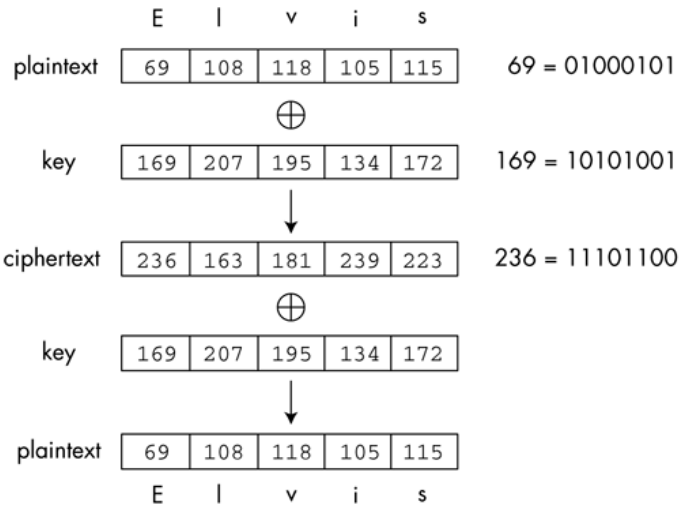
$$M1 = message1$$

$$M2 = message2$$

$$k = mask$$

$$M1 \oplus k \oplus M2 \oplus k = M1 \oplus M2$$

Gambar 5. Metode XOR Cryptography [5]



Gambar 6. Hasil Enkripsi dari XOR Cryptography [6]

IV. PSEUDORANDOM

Bilangan pseudorandom, sesuai dengan namanya "pseudorandom" yang diambil dari kata "pseudo" yang berarti semu atau tidak terlihat seperti sebenarnya dan kata "random" yang berarti acak, adalah suatu bilangan yang terlihat seperti bilangan acak tetapi sebenarnya tidak. Bilangan pseudorandom didapatkan melalui suatu algoritma yang mengaplikasikan formula matematika, terkhususnya teori bilangan. Formula matematika ini disebut pseudorandom number generator (PRNG).

Pseudorandom number generator akan menghasilkan sebuah sekuen bilangan dari suatu bibit (seed). Bilangan yang dihasilkan terlihat random dan dapat digenerasikan dalam waktu yang singkat dan dalam jumlah yang banyak, sehingga pseudorandom number generator dinilai lebih menguntungkan dibandingkan beberapa random number generator lainnya seperti, hardware number generator.

Random number (bilangan acak) merupakan suatu hal yang dibutuhkan dalam sistem enkripsi dalam bidang ilmu kriptografi. Sebagai contoh, random number digunakan untuk menghasilkan key dalam berbagai algoritma enkripsi, seperti

- SHA
- Public dan private key RSA
- Salt

Tidak semua bilangan yang dihasilkan oleh pseudorandom number generator dapat digunakan untuk metode enkripsi karena bilangan tersebut dapat mudah ditebak tergantung dengan algoritma yang digunakan untuk mendapatkan bilangan tersebut. Maka dari itu pseudorandom number generator harus memenuhi standar dan kualitas tertentu sehingga dapat digunakan untuk kepentingan kriptografi.

Cryptographically secure pseudorandom number generator (CSPRNG) atau cryptographic pseudorandom number generator (CPRNG) adalah sebuah pseudorandom number generator yang memiliki sifat-sifat yang cocok dan memenuhi standar yang membuat hasil yang diperoleh dapat digunakan untuk tujuan kriptografi.

German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI) telah menentukan 4 kriteria untuk menjamin kualitas dari deterministic pseudorandom number generator. Keempat kriteria tersebut adalah

- K1 – Harus ada kemungkinan tinggi bahwa sekuen bilangan acak yang dihasilkan harus berbeda satu dengan yang lain.
- K2 – Bilangan yang dihasilkan harus lulus tes monobit, tes poker, tes runs, tes longruns, dan tes autocorrection.
- K3 – Penyerang (pihak yang akan memecahkan enkripsi) harus tidak mungkin bisa untuk menghitung atau menebak nilai sebelum atau sesudah dari sekuen bilangan, atau bilangan apapun yang terkandung dalam sekuen tersebut.
- K4 – Seharusnya tidak mungkin untuk siapapun untuk menghitung atau menebak nilai sebelum atau sesudah dari sekuen bilangan, atau bilangan apapun yang terkandung dalam sekuen tersebut.

Untuk tujuan kriptografik, hanya pseudorandom number generator yang telah memenuhi kriteria K3 atau K4 yang dapat digunakan.

V. Aplikasi Teori Bilangan dalam Pseudorandom Generator

Seperti yang telah dikemukakan dalam Bab IV, aplikasi dan kegunaan dari random number sangatlah besar dalam ilmu kriptografi dan keamanan data. Random number dapat digunakan sebagai landasan dari suatu algoritma untuk proses enkripsi dan dekripsi. Bayangkan jika proses enkripsi dilakukan dengan bilangan asal yang mudah ditebak sebagai seednya. Tentu keamaan informasi dapat terancam dan informasi yang seharusnya bersifat rahasia dapat diketahui oleh orang banyak. Bagaimana akibatnya jika misalnya, suatu pesan rahasia yang memuat keselamatan suatu negara dapat dengan mudah dirampas oleh orang-orang yang tidak bertanggung jawab. Tentu keselamatan negara tersebut terancam dan bisa saja perdamaian dunia juga terancam.

Untuk itu, dibutuhkan sebuah algoritma yang dapat menghasilkan bilangan yang dapat digunakan untuk proses enkripsi dan tidak mudah ditebak, mudah untuk dihasilkan tetapi keamanannya tetap terjamin.

Berdasarkan kebutuhan itulah pseudorandom number generator dibutuhkan, khususnya pseudorandom number generator yang telah melewati standar untuk dapat disebut cryptographically secure pseudorandom number generator (CSPRNG) atau cryptographic pseudorandom number generator (CPRNG).

Salah satu metode atau algoritma untuk menghasilkan bilangan pseudorandom yang sederhana adalah dengan menggunakan metode kekongrueanan lanjar yang telah dijelaskan pada Bab II.

Metode kekongurenan lanjar yang akan diterapkan adalah sebagai berikut

Pilih 4 buah bilangan bulat

$$m, sebagai\ modulus$$
$$a, sebagai\ multiplier$$
$$c, sebagai\ increment$$
$$x_0, sebagai\ seed$$

Dengan ketentuan

$$2 \leq a < m$$
$$0 \leq c < m$$
$$0 \leq x_0 < m$$

Tujuan dari pseudorandom number generator adalah untuk menghasilkan sekuen bilangan acak yang dinotasika sebagai berikut

$$\{x_n\}_{n=1}^{\infty}$$

Dengan ketentuan

$$0 \leq x_n < m$$

Maka didapat kongruensi

$$x_n + 1 = (ax_n + c)\ mod\ m$$

Dengan persamaan diatas, pada m, a, c, x_0 tertentu hasil sekuen dari $\{x_n\}$ akan berulang, yang berarti setelah generasi kesekian, sekuen akan berulang dari awal. Semakin cepat hal itu terjadi (semakin kecil jumlah bilangan unik) maka hasil generator makin buruk. Untuk mengatasi hal ini, maka digunakan bilangan besar (big number). Untuk kemudahan, penulis menggunakan kombinasi sebagai berikut

$$m = 17, a = 5, c = 2, x_0 = 3$$

Maka akan didapat hasil iterasi dari persamaan diatas

$$x_1 = (5 \times x_0 + 2)\ mod\ 17 = 0$$
$$x_2 = (5 \times x_1 + 2)\ mod\ 17 = 2$$
$$x_3 = (5 \times x_2 + 2)\ mod\ 17 = 12$$
$$x_4 = (5 \times x_3 + 2)\ mod\ 17 = 11$$
$$x_5 = (5 \times x_4 + 2)\ mod\ 17 = 6$$
$$x_6 = (5 \times x_5 + 2)\ mod\ 17 = 15$$
$$x_7 = (5 \times x_6 + 2)\ mod\ 17 = 9$$
$$x_8 = (5 \times x_7 + 2)\ mod\ 17 = 13$$

Dst.

Dari contoh di atas dapat terlihat bahwa bilangan yang dihasilkan terlihat acak dan tidak memiliki pola sama-sekali. Jika ingin mendapatkan bilangan dengan rentang acak yang makin besar, dapat digunakan bilangan yang bernilai lebih besar.

Selain algoritma kekongruenan lanjar, terdapat algoritma lain yang dapat digunakan untuk membentuk pseudorandom number generator, seperti

- Linear-feedback shift register
- Lagged Fibonacci generator
- Blum Blum Shub

Sekuen bilangan acak yang telah dihasilkan nantinya dapat digunakan sebagai seed atau key untuk metode enkripsi lainnya yang memerlukan sekuen bilangan acak seperti yang telah dijelaskan di Bab IV.

VI. Kesimpulan

Dalam makalah ini, penulis telah membahas tentang aplikasi teori bilangan dalam kehidupan praktis manusia, yaitu dalam mengamankan persebaran informasi lewat pseudorandom number generator. Berdasarkan percobaan dan penelitian yang dilakukan oleh penulis, ternyata sistem enkripsi dan dekripsi dapat dilakukan dengan teori bilangan dasar melalui aritmatika modulo, kekongruenan lanjar, dsb.

Algoritma untuk membangun pseudorandom rumber generator yang telah dibahas di makalah ini hanyalah contoh sederhana dari begitu banyaknya metode untuk membangun pseudorandom number generator yang tentu saja bisa kebih efektif dan efisien. Tetapi alasan penulis memilih metode

kekongruenan lanjar adalah untuk menunjukkan bahwa teorema dasar yang ada di teori bilangan dapat digunakan untuk menghasilkan pseudorandom number generator.

VII. Ucapan Terima Kasih

Makalah ini tidak mungkin dapat diselesaikan tanpa bantuan Tuhan Yang Maha Esa. Penulis ingin mengucapkan terima kasih kepada Ibu Harlili selaku pengajar pada mata kuliah IF2120 Matematika Diskrit Kelas 2. Penulis juga ingin mengucapkan terima kasih kepada keluarga, sahabat, dan orang-orang yang menolong penulis dalam menyelesaikan makalah ini. Penulis juga tidak lupa untuk mengucapkan terima kasih keapda Institut Teknologi Bandung yang telah memberikan penulis kesempatan untuk belajar dan mengembangkan diri.

Referensi

http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Teori%20Bilangan.pdf diakses 1 Desember 2019 pukul 04.35

https://www.geeksforgeeks.org/pseudo-random-number-generator-prng/ diakses 1 Desember 2019 pukul 06.35

Liddell, Henry George; Scott, Robert; Jones, Henry Stuart; McKenzie, Roderick (1984). A Greek-English Lexicon. Oxford University Press.

https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences diakses 2 Desember 2019 pukul 13.00

https://cse.unl.edu/~choueiry/F07-235/files/NumberTheoryApplications.pdf diakses 3 Desember 2019 pukul 07.10

Schindler, Werner (2 December 1999). "Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators" (PDF). Anwendungshinweise und Interpretationen (AIS). Bundesamt für Sicherheit in der Informationstechnik. pp. 5–11.

[1] https://3.bp.blogspot.com/-r_mrs93-9CE/WAbtTjHho4I/AAAAAAAABG4/f4MBPpUE5y4ciS4H54hjCQHL59YEV-qYQCLcB/s1600/sketsa%2Bbilangan.gif
[2] http://media.factmyth.com/2015/11/cryptography.jpg
[3] https://www.ssl2buy.com/wiki/wp-content/uploads/2015/12/Symmetric-Encryption.png
[4] https://www.ssl2buy.com/wiki/wp-content/uploads/2015/12/Asymmetric-Encryption.png
[5] https://www.quora.com/Why-are-true-random-number-generators-more-secure-than-pseudo-random-number-generators
[6] https://qph.fs.quoracdn.net/main-qimg-ebedf431c26489398e4e20fb943f88d0

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, 6 Desember 2019

Fritz Gerald Tjie
13518065