KETIK : Jurnal Informatika
ISSN: 3026-183X (Media Online)
Vol. 02, No. 05, Mei 2025 Hal. 41-46
Publisher: Faatuatua Media Karya
jurnal.faatuatua.com/index.php/KETIK
DOI: doi.org/10.70404/ketik.v2i05.209

Implementasi Permuted Congruential Generator pada Proses Pembangkitan Kunci Algoritma One Time Pad

Taronisokhi Zebua
[1]*Universitas Budidarma Medan, Indonesia, e-mail: taronizeb@gmail.com*

Info Artikel

Diajukan: *24-04-2025*
Diterima: *17-05-2025*
Diterbitkan: *30-05-2025*

Kata Kunci:
Keamanan;
Kriptografi;
OTP;
RNG;
PCG.

Keywords:
security;
criptography;
OTP;
RNG;
PCG.

Abstrak

Keoptimalan kunci yang digunakan oleh algoritma pengamanan data merupakan salah satu elemen penting yang sangat berpengaruh dalam mewujudkan tujuan teknik kriptografi dalam mengamankan data. Umumnya, algoritma kriptografi klasik masih menggunakan kunci yang lemah dan memiliki pola berulang, misalnya algoritma one time pad sehingga mudah dipecahkan oleh penyerang. Salah satu teknik yang dapat digunakan untuk mengoptimalkan kunci yang digunakan oleh algoritma kriptografi adalah penggunaan teknik pembangkitan kunci secara acak, sehingga tidak terjadi pengulangan kata kunci. Hal ini dapat dilakukan dengan memanfaatkan teknik pembangkitan bilangan secara acak (random number generation). Teknik permuted congruential generator merupakan salah satu teknik pembangkitan bilang secara acak dan tidak berulang. Nilai acak yang dihasilkan dari teknik ini akan direpresentasikan sebagai nilai-nilai kunci yang digunakan oleh algoritma pengamanan data. Penelitian ini mencoba memadukan teknik permuted congruential generator untuk membangkitkan nilai-nilai kunci yang digunakan oleh algoritma one time pad untuk mengamankan data teks, sehingga diperoleh nilai-nilai kunci yang jauh lebih optimal dan sulit ditemukan polanya dibandingkan dengan kunci yang dibentuk berdasarkan aturan one time pad sendiri.

Abstract

The effectiveness of the key used by data security algorithms is a crucial element that significantly influences the achievement of cryptographic objectives in securing information. In general, classical cryptographic algorithms still rely on weak keys with repetitive patterns, such as the one-time pad algorithm, making them vulnerable to attacks. One technique that can be employed to enhance the quality of keys used in cryptographic algorithms is the application of random key generation, which prevents repetition of key values. This can be achieved by utilizing random number generation techniques. The Permuted Congruential Generator (PCG) is one such technique that produces non-repetitive and randomly distributed values. The random outputs generated through this method can be represented as key values used by data encryption algorithms. This study seeks to integrate the Permuted Congruential Generator technique for generating key values used by the one-time pad algorithm to secure textual data, thereby producing more optimal keys with patterns that are significantly harder to detect compared to keys generated by the standard one-time pad method.

1. PENDAHULUAN

Peningkatan pemanfaataan media online dan media-media sosial dalam kegiatan berdistribusi data dan informasi yang sifatnya rahasia saat ini telah memicu perhatian terhadap penanganan dan usaha pengoptimalan keamanan data tersebut. Data penting atau informasi yang bersifat rahasia yang didistribusikan melalui media online sangat rentang terhadap tindakan pencurian atau tindakan lain yang dapat merugikan pihak pemilik data. Tentu hal ini dilakukan oleh pihak-pihak yang tidak diberikan akses untuk data tersebut (penyerang). Berdasarkan penelian terdahulu, mengatakan bahawa dibutuhkan sebuah tindakan pengamanan terhadap data penting atau informasi yang bersifat rahasia agar data tersebut tetap terjaga serta terhindar dari tindakan-tindakan pencurian data tersebut [1].

Teknik kriprografi merupakan salah satu teknik yang dapat digunakan dalam mengamankan data atau informasi yang bersifat penting dan rahasia. Teknik ini mengamankan data penting dengan

menyandikan data penting menjadi data yang sulit dipahami oleh orang lain, sehingga dapat meminimalkan tindakan-tindakan para pihak yang tidak berhak untuk itu. Teknik ini dapat diimplementasikan dengan memanfaatkan berbagai algoritma yang dimiliki oleh teknik ini, sehingga kerahasiaan, integritas dan otentikasi data dapat tetap terjaga. Berdarkan penelitian terdahulu, mengatakan bahwa teknik kriptografi menjadi salah satu teknik yang dapat dimanfaatkan untuk mengatasi masalah keamanan data, sehingga data tetap terjadi dan terhindar dari tindakan manipulasi data yang dilakukan oleh pihak lain [1] [2].

Teknik kriptografi ini memiliki berbagai algoritma untuk mengimplementasikannya dalam mengamankan data. Salah satunya adalah algoritma *One Time Pad* (OTP). Selain elemen algoritma, maka elemen penting yang diperlukan dalam penerapan teknik kriptografi ini adalah kunci. Peranan kunci dalam penerapan algoritma kriptografi sangat penting, karena dengan pemanfaatan kunci yang kuat, maka keoptimalan keamanan terhadap data yang diamankan tentu lebih optimal pula. Kunci ini harus dijaga kerahasiaannya sehingga tidak mudah didapatkan oleh orang lain yang tidak memiliki hak untuk mengakses data. Namun dari beberapa algoritma teknik kriptografi khususnya yang masih tergolong klasik, masih menggunakan komposisi pembentukan kunci yang kurang optimal, sehingga masih mudah dipecahkan atau diketahui oleh para penyerang. Penelitian terdahulu mengatakan bahwa kunci dalam algoritma kriptografi sangat memiliki pengaruh yang kuat untuk mewujudkan tujuan pengamanan data [3].

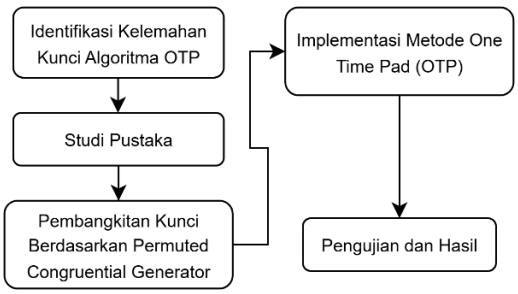
Salah satu algoritma kriptografi yang tergolong klasik adalah algoritma *One Time Pad* (OTP). Algoritma ini mengamankan data penting dengan kunci yang memiliki panjang sama dengan jumlah panjang data yang diamankan. Umumnya algoritma ini dikatakan bahwa termasuk salah satu algoritma yang rumit dipecahkan, namun dilihat dari sisi kunci yang memiliki jumlah yang sama dengan jumlah datanya, maka akan sangat sulit dibentuk dan diingat oleh pengguna. Selain hal itu, kunci yang panjang dapat mengakibatkan penggunaan kata kunci yang berulang secara periodik untuk mencapai jumlah yang sama dengan jumlah data yang akan diamanakan. Penelitian terdahulu mengatakan bahwa salah satu kelemahan dari algoritma ini adalah nilai kunci yang dibangkitkan pada proses enkripsi akan sulit mendapatkan nilai dan periodik yang sama pada saat pembangkitan kunci pada proses dekripsi [4].

Pembangkitan bilangan acak merupakan salah satu teknik yang umum digunakan untuk mendapakan deret bilangan yang acak. Teknik ini juga banyak digunakan dalam mendukung kinerja algoritma kriptografi. Salah satu algoritma yang dapat digunakan dalam menghasilkan bilangan acak adalah algoritma *permuted congruential generator*. Algoritma ini merupakan generalisasi dari bentuk barisan bilangan acak yang sangat acak dengan memanfaatkan beberapa nilai awal untuk menghasilkan rangkaian nilai bilangan acak [5] [6].

Penelitian ini menguraikan bagaimana prosedur yang dilakukan untuk membangkitkan kunci dari algoritma one time pad berdasarkan pembangkit bilangan acak *permuted congruential generator* yang akan diimplementasikan dalam proses enkripsi dan dekripsi data teks, sehingga diharapkan kinerja dari algorima *one time pad* lebih meningkat dalam menjamin kemanan data atau informasi penting.

2. METODE PENELITIAN

Penelitian ini dilakukan berdasarkan pendekatan kualitatif eksperimental karena melibatkan penerapan teknik *permuted congruential generator* untuk membangkitkan nilai-nilai kunci pada algoritma *one time pad*. Objek dalam penelitian ini adalah data yang berbentuk teks yang nantinya dienkripsi berdasarkan algoritma *one time pad* dengan kunci yang dibangkitkan berdasarkan teknik *permuted congruential generato*r. Alur penelitian disajikan pada diagaram di bawah ini :



Gambar 1. Alur Penelitian

2.1 Kriptografi

Teknik kriptografi merupakan salah satu teknik yang dapat digunakan dalam upaya pengamanan data penting atau data yang bersifat rahasia. Teknik ini mempelajari bagaimana agar data penting atau data rahasia yang disitribusikan kepada pihak lain dapat sampaikan dengan aman [7]. Teknik ini bekerja dengan merubah data menjadi data yang tidak lagi dapat dengan mudah dipahami oleh orang lain, sehingga kerahasiaan informasi penting yang terkandung di dalam sebuah data dapat terjaga dengan baik. Beberapa hal yang menjadi tujuan utama dari pemanfaatan teknik kriptografi [3] [8], adalah:

1. Kerahasiaan (*confidentiality*)
   Aspek ini merupakan sebuah hal yang harus dicapai agar data yang diamankan harus dapat dirahasiakan makanya agar orang lain tidak mengetahuinya.
2. Integritas data (data *integrity*)
   Aspek ini bertujuan agar data yang diamankan tidak dapat diakses oleh pihak lain selain penerima yang sah.
3. Autentikasi (*authentication*)
   Aspek ini bertujuan untuk mengindentifikasi pihak-pihak yang mengakses data yang diamankan.
4. Ketiadaan penyangkalan (*nonrepudiation*)
   Aspek ini bertujuan untuk mencegah aksi penyangkalan terhadap aksi yang dilakukan oleh pengirim maupun penerima informasi.

Teknik kriptografi mengamankan data dengan proses pengubahan data asli menjadi simbol-simbol yang tidak dapat dimengerti lagi. Hal ini dilakukan berdasarkan algoritma-algoritma kriptografi yang telah ada. Ada tiga fungsi utama dari teknik kriptografi [9], yaitu :

1. Enkripsi, merupakan istilah lain dari proses menyandikan data penting ke dalam bentuk simbol-simbol yang tidak dapat dimengerti lagi oleh pihak lain sehinggan keaslian dan keamanan data dapat terjaga.
2. Dekripsi adalah proses untuk merubah atau mengembalikan data tersandi kebentuk aslinya agar arti data dapat dimengerti oleh penerima.
3. Kunci, merupakan elemen yang paling penting dalam mengimplementasikan proses enkripsi dan dekripsi. Keamanan kunci di dalam kriptografi menjadi prioritas karena serumit apapun algoritma yang digunakan akan dapat dipecahkan bila kunci yang digunakan berhasil ditemukan. Kunci terbagi menjadi dua bagian, kunci rahasia (*private key*) dan kunci umum (*public key*).

Beberapa kekuatan yang dimiliki oleh algoritma kriptografi dalam proses mengenkripsi data [10], yaitu:

1. Konfusi/pembingungan (*confusion*), yaitu suatu proses dimana teks sulit dikembalikan pada bentuk awal secara tanpa melalui proses dekripsi.
2. Difusi/peleburan *(difusion*), yaitu suatu proses dimana karakteristik suatu teks dihilangkan sehingga mengamankan suatu informasi.

2.2 One Time Pad (OTP)

Algoritma ini termasuk salah satu algoritma teknik kriptografi simetri yag ditemukan pada tahuan 1917 pada perang dunia kedua. Sebagai algoritma yang tergolong simetri, maka algoritma ini menggunakan kunci yang sama baik pada proses enkripsi maupun dekripsi. Hingga saat ini, algoritma *one time pad* dinyatakan tidak dapat dipecahkan meskipun diberikan sumber daya yang tidak terbatas [4] [11].

Prosedur untuk melakukan proses enkripsi maupun dekripsi berdasarkan algoritma ini hampir sama dengan prosedur yang digunakan oleh algoritma *vegenere cipher*. Perbedaan keduanya terletak pada penggunaan kunci. Bila pada algoritma *vegenere cipher* kunci yang digunakan akan diulang, namun pada algoritma OTP jumlah kunci yang digunakan harus sama dengan jumlah data yang diamankan. Adapun formula yang digunakan dalam proses enkripsi maupun dekripsi, adalah [12]:

Formula proses enkripsi :

$$Ci = (Pi + Ki) \bmod 26 \quad \ldots\ldots (1)$$

Formula proses dekripsi :

$$Pi = ((Ci - Ki)) \bmod 26 \quad \ldots\ldots (2)$$

dimana :

Pi = Data yang diamankan
Ci = Cipher
Ki = Kunci

Agar seluruh nilai ASCI dapat diakses, maka nilai modulus dapat diganti dengan 256.

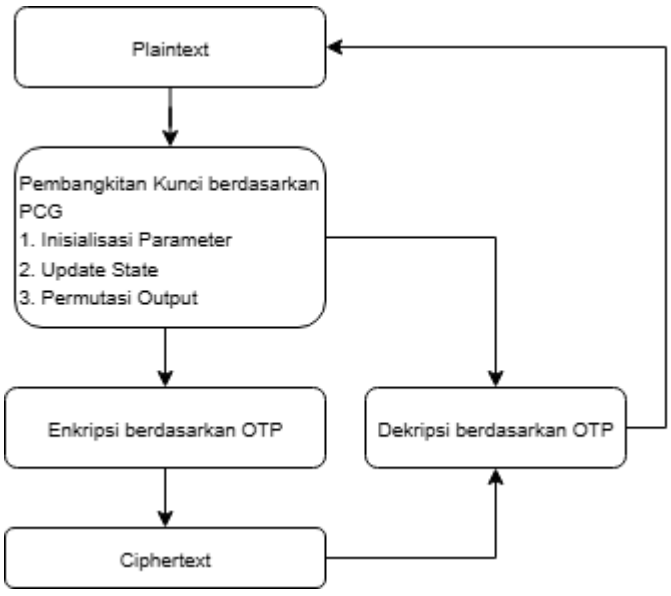
2.3 Permuted Congruential Generator (PCG)

Permuted Congruential Generator (PCG) adalah algoritma pembangkit bilangan acak (PRNG) yang ringan, cepat, dan memiliki kualitas distribusi acak tinggi, lebih baik daripada *Linear Congruential Generator* (LCG) biasa. PCG ditemukan oleh Melissa E. O'Neill (2014) dan dirancang untuk efisiensi serta kemudahan implementasi di perangkat modern. Algortima ini menggabungkan dua komponen utama, yaitu *Linear Congruential Generator* (LCG) sebagai *state progression* dan Permutation function sebagai *output transformation* [13].
Beberapa kelebihan dari PCG, yaitu distribusi acak bagus (tidak berpola), cepat dan ringan untuk implementasi, cocok untuk sistem *embedded*, game, dan simulasi.
Adapun langkah-langkah dari PCG [6] [13], adalah :

1. Inisialisasi Parameter
   Tahap ini merupakan penentuan nilai-nilai utama yang digunakan dalam fomulasi PCG :
   a. state awal (seed), misal dari waktu (time()) atau input *user*.
   b. multiplier (a) → bilangan ganjil besar, misalnya 6364136223846793005
   c. increment (c) → bilangan ganjil, misalnya 1442695040888963407
   d. modulus (m) → biasanya 2^64, dipakai implisit karena menggunakan *integer overflow*.
   e. Ukuran output → 32-bit, 64-bit, dan sebagainya.
2. Update State (LCG Step)
   proses ini merupakan proses untuk membangkitkan bilangan acak berdasarkan state awal dengan formula :
   $X_{n+1} = (aX_n + c) \bmod 2^k$ .....(3)
   Keterangan :
   X_n : *state* ke-n
   a : *multiplier* (bilangan ganjil besar)
   c : *increment* (biasanya ganjil, untuk keacakan penuh)
   k : ukuran bit dari *state* (umumnya 8, 16, 32, 64 atau 128 bit)
3. Perutasi *Output*
   output = $((Xn \gg 1) \oplus Xn) \bmod m$ .....(4)
   umumnya nilai pergeseran ditentukan sendiri oleh pengguna.

3. HASIL DAN ANALISIS

Pengoptimalan kunci yang digunakan pada algoritma one time pad, diharapkan dapat meningkatkan ketahanan algoritma ini terhadap kemudahan unutk mengetahui nilai dan pola kunci yang digunakan. Pemanfaatan nilai kunci yang panjang (sama dengan jumlah karakter data) pada one time pad menjadi salah satu kerumitan bagi pengguna untuk menghafal kata kunci. Namun hal tersebut dapat diatasi dengan melakukan proses pembangkitan kunci secara otomatis berdasarkan teknik pembangkitan bilangan acak. Proses ini menggunakan teknik *permuted congruential generator*, sehingga proses pembangkitan nilai kunci jauh lebih cepat.



Gambar 1. Skema Penerapan PCG dalam OTP

Implementasi proses pembangkitan kunci dalam penelitian ini dicontohkan untuk menfamankan sebuah data teks.

Plaintext : RAHASIA
Inisialisasi nilai variabel PCG :
a. *state* awal (X0) = 42
b. multiplier (a) = 1664525
c. increment (c) = 1013904223
d. modulus (m) = 256
e. Ukuran *output* = 8 bit
f. Permutasi output 2 bit kanan ke kiri
Proses untuk interaksi 1 :
X_1 = ((1664525 x 42) +1013904223) mod 256
= 1083814273 mod 256
= 129, dirubah ke biner menjadi 10000001
Permutasi 2 bit kiri ke kanan menjadi : 01100000 (96 decimal)
Hasil permutasi kemudian di XOR dengan Xn :
menjadi 10000001
01100000 XOR
11100001 (256 decimal)
X_1 = 256
Sehingga diperoleh 5 bilangan acak dari yang dilakukan berdasarkan proses di atas :

Tabel 1. Hasil Pembangkitan Kunci berdasarkan PCG

Iterasi	Nilai LCG	Biner	Shif Right 2 to Left	Hasil Shift XOR Xn	Output (Decimal)
1	129	10000001	01100000	11100001	225
2	132	10000100	00100001	10100101	165
3	195	11000011	11110000	00110011	51
4	122	01111010	10011110	11100100	228
5	65	01000001	01010000	00010001	17
6	64	01000000	00010000	01010000	88
7	195	11000011	11110000	00110011	51

Nilai *output* pada tabel 1 di atas akan digunakan sebagai nilai kunci pada proses enkripsi maupun dekripsi berdasarkan algoritma *one time pad*.

Prosen enkripsi :

Plaintext	=	R	A	H	A	S	I	A
Kunci	=	225	165	51	228	17	88	51
DecimalPlaintext	=	82	65	72	65	83	73	65
DecimalKunci	=	225	165	51	228	17	88	51
(P + K) mod 256	=	51	230	123	37	100	161	116
Cipher	=	3	æ	{	%	d	¡	t

Proses dekripsi tentu dilakukan oleh penerima ciphertext yang diawali dengan pembangkitan kata kunci berdasarkan teknik PCG, kemudian melakukan proses dekripsi. Proses dekripsi ini dilakukan dengan mengurangi nilai decimal cipher dengan nilai kunci yang dihasilkan dari PCG kemudian dimoduluskan dengan nilai m, sehingga diperoleh nilai *plaintext* awal.

4. KESIMPULAN

Berdasarkan hasil dan analisa penerapan teknik PCG pada proses pembangkitan kunci enkripsi maupun dekripsi one time pad di atas, maka disimpulkan bahwa kunci yang digunakan lebih bervariasi dan sulit ditebak oleh penyerang. Nilai kunci yang dihasilkan akan berubah setiap iterasi yang dilakukan karena proses pembangkitan kunci selalu bergantung pada nilai state sebelumnya. Pengguna tidak perlu lagi menghafal kata kunci yang digunakan karena akan dibangkitkan secara otomatis berdasarkan teknik PCG, hanya saja perlu dirahasiakan dan diketahui oleh kedua belah pihak baik pengirim maupun penerima nilai-nilai inisialisasi variabel PCG yang telah disepakati bersama.

REFERENSI

[1] D. A. Fauzan, A. Fathurrozi and S. , "Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma RSA (Rivest Shamir Adleman) dan AES (Advanced Encryption Standard) Berbasis Web," *Journal of Information and Information Security (JIFORTY),* vol. 4, no. 1, pp. 91-104, 2023.

[2] S. A. Talib, "The Importance of Cryptography in Cloud Computing," *AL-ESRAA UNIVERSITY COLLEGE JOURNAL OF ENGINEERING SCIENCES,* vol. 6, no. 10, pp. 59-80, 2024.

[3] M. Sianturi and T. Zebua, "Modifikasi Pembangkit Kunci Algoritma Vigenere Cipher Berdasarkan Pembangkit Bilangan Acak CSPRNG Untuk Mengamankan Citra Digital," *JUSSI: Jurnal Sains Dan Teknologi Informasi,* vol. 2, no. 4, pp. 136-142, 2023.

[4] H. Alam, A. K. Habibi and H. Widya, "Penggunaan Algoritma Vegenere Cipher dan One Time Pad untuk Keamanan Pesan Teks," in *SEMNASTEK - UISU*, Medan, 2022.

[5] I. Sunni, "Aplikasi Lagged Fibonacci Generator dan Bilangan Irrasional dalam Stream Cipher," Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Bandung, 2011.

[6] C. Bouillaguet, F. Martinez and J. Sauvage, "Practical seed-recovery for the PCG Pseudo-Random Number Generator," *IACR Transactions on Symmetric Cryptology,* no. 3, p. 175–196, 2020.

[7] N. M. S. Sianturi, N. B. Nugroho and W. R. Maya, "Implementasi Kriptografi Untuk Pengamanan Data Aset Perusahaan Pada PT.PLN (Persero) Dengan Menggunakan Metode Algoritma AES 192," *Jurnal CyberTech,* 2020.

[8] D. H. Pane, "IMPLEMENTASI KRIPTOGRAFI KEAMANAN DATA RESI PADA PT JNE PERBAUNGAN MENGGUNAKAN METODE MERKLE HELLMAN," *Device : Journal of Information System, Computer Science and Information Technology,* vol. 1, no. 1, pp. 6-10, 2020.

[9] T. Zebua, "Penerapan Multiply With Carry Generator pada Proses Pembangkitan Kunci Algoritma Beaufort Cipher," *Journal of Information System Research (JOSH),* vol. 4, no. 2, p. 607−613, 2023.

[10] M. Z. Solihin and K. A. M., "IMPLEMENTASI KRIPTOGRAFI MENGGUNAKAN METODE ALGORITMA RSA PADA APLIKASI PENGAMANAN DATA BERBASIS JAVA DESKTOP UNTUK UD TIRTA SOEPER TELOER," in *Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*, Jakarta, 2022.

[11] M. K. Harahap and N. Khairina, "Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks," *Sinkron Jurnal & PenelitianTeknik Informatika,* vol. 1, no. 2, pp. 58-62, 2017.

[12] S. A. Saputri and N. , "Penerapan Algoritma One Time Pad Pada Pesan Rahasia Menggunakan QR Code Berbasis Android," *Jurnal FTIK,* vol. 1, no. 1, pp. 1193-1206.

[13] Z. B. METİN and F. ÖZKAYNAK, "PCG-Generated Randomness: A NIST Analysis of 100-Million Bits," *Turkish Journal of Science & Technology,* vol. 20, no. 1, pp. 55-61, 2025.