Prosiding Seminar Nasional SAINTEK
Vol.1 No.1, 2026, Hal. 108-114
ISSN XXXX-XXXX

Implementasi Deret Aritmatika sebagai Mekanisme Pembangkitan Kunci Dinamis pada Sistem Kriptografi Simetris Berbasis *XOR*

Eriska Meiyana[1*], Annisa Nur Azizah[1]

[1]Fakultas Sains dan Teknologi, Universitas Nurul Huda
[*]E-mail: eriskameiyana12@gmail.com

Abstrak

Keamanan data menjadi aspek penting dalam pertukaran informasi digital sehingga diperlukan metode kriptografi yang mampu menjaga kerahasiaan data. Penelitian ini bertujuan untuk menganalisis implementasi deret aritmatika sebagai mekanisme pembangkitan kunci pada sistem kriptografi simetris. Metode yang digunakan meliputi penentuan parameter deret aritmatika berupa suku pertama dan beda, pembangkitan deret kunci berdasarkan rumus deret aritmatika, serta penerapan kunci tersebut pada proses enkripsi dan dekripsi menggunakan operasi *Exclusive OR (XOR)*. Kinerja sistem dianalisis melalui pengujian keberhasilan proses enkripsi dan dekripsi serta evaluasi karakteristik kunci yang dihasilkan. Hasil penelitian menunjukkan bahwa deret aritmatika mampu menghasilkan rangkaian kunci yang terstruktur dengan nilai berada pada rentang $0 - 255$ (8 bit), sehingga setiap posisi data menggunakan nilai kunci yang berbeda sesuai parameter awal yang ditentukan. Implementasi dengan parameter suku pertama 29 dan beda 5 menghasilkan deret kunci $29, 34, 39, 44, 49, 54, 59, 64, 69,$ dan 74, yang berhasil digunakan pada proses enkripsi dan dekripsi sehingga plaintext dapat dikembalikan tanpa kehilangan informasi. Dengan demikian, deret aritmatika dapat diimplementasikan sebagai alternatif mekanisme pembangkitan kunci pada sistem kriptografi simetris.

Kata kunci: Deret Aritmetika, Enkripsi, Kriptografi Simetris, Kunci Dinamis, *XOR*

Abstract

Data security has become an essential aspect of digital information exchange, creating the need for cryptographic methods capable of ensuring data confidentiality. This study aims to analyze the implementation of an arithmetic sequence as a key generation mechanism in a symmetric cryptographic system. The proposed method consists of determining the arithmetic sequence parameters, namely the first term and the common difference, generating a sequence of keys based on the arithmetic sequence formula, and applying the generated keys in the encryption and decryption processes using the Exclusive OR (XOR) operation. System performance was evaluated by testing the correctness of the encryption and decryption processes and analyzing the characteristics of the generated keys. The results indicate that the arithmetic sequence generates a structured key sequence with values ranging from 0 to 255 (8-bit), allowing each data position to use a distinct key value determined by the selected initial parameters. Using a first term of 29 and a common difference of 5, the proposed method generated the key sequence 29, 34, 39, 44, 49, 54, 59, 64, 69, and 74, which was successfully applied in the encryption and decryption processes, enabling the original plaintext to be recovered without information loss. Therefore, the arithmetic sequence can be implemented as an alternative key generation mechanism for symmetric cryptographic systems.

Keywords: *Arithmetic Sequence, Dynamic Key, Encryption, Symmetric Cryptography, XOR Operation*

PENDAHULUAN

Perkembangan teknologi informasi pada era digital telah meningkatkan kebutuhan akan keamanan data dalam berbagai aspek kehidupan. Berbagai jenis informasi, mulai dari dokumen pribadi hingga data strategis, memerlukan perlindungan agar tidak dapat diakses, dimanfaatkan, maupun dimodifikasi oleh pihak yang tidak berwenang[1]. Dalam proses pertukaran dan transmisi data, diperlukan suatu mekanisme pengamanan yang mampu menjaga kerahasiaan, integritas, dan keaslian

informasi sehingga data yang dikirimkan tetap aman dari ancaman penyadapan maupun penyalahgunaan [2],[3].

Salah satu teknologi yang banyak digunakan untuk menjamin keamanan informasi adalah kriptografi. Kriptografi berasal dari bahasa Yunani, yaitu kryptos yang berarti tersembunyi dan *graphein* yang berarti menulis. Secara umum, kriptografi merupakan ilmu dan seni yang mempelajari teknik pengamanan data dengan cara mengubah informasi menjadi bentuk yang tidak dapat dipahami oleh pihak yang tidak memiliki hak akses [4],[5]. Dalam perkembangannya ada dua jenis algoritma kriptografi, yaitu algoritma enkripsi kunci simetris (*symmetric-key encryption algorthm*) dan algoritma enkripsi kunci publik (*public-key encryption algorthm*).Melalui proses enkripsi, data asli (*plaintext*) diubah menjadi data tersandi (*ciphertext*), sedangkan proses dekripsi digunakan untuk mengembalikan data tersebut ke bentuk semula [6]. Oleh karena itu, kriptografi telah diterapkan secara luas pada berbagai bidang, seperti keamanan komputer, komunikasi digital, sistem pembayaran elektronik, dan layanan berbasis internet yang memerlukan perlindungan terhadap data sensitif [7].

Keamanan suatu sistem kriptografi tidak hanya ditentukan oleh algoritma yang digunakan, tetapi juga sangat bergantung pada kualitas kunci yang diterapkan dalam proses enkripsi dan dekripsi [8]. Berbagai mekanisme pembangkitan kunci telah dikembangkan, di antaranya menggunakan *Random Number Generator* (RNG), fungsi hash, maupun algoritma kriptografi tertentu. Meskipun metode tersebut mampu menghasilkan kunci dengan tingkat keacakan yang tinggi, sebagian di antaranya memerlukan proses komputasi yang relatif kompleks serta bergantung pada kualitas sumber bilangan acak yang digunakan. Di sisi lain, penggunaan kunci statis atau kunci yang digunakan secara berulang masih berpotensi menghasilkan pola yang dapat dimanfaatkan dalam proses kriptanalisis sehingga menurunkan tingkat keamanan sistem [9]. Oleh karena itu, diperlukan mekanisme pembangkitan kunci yang mampu menghasilkan variasi nilai kunci secara sistematis, mudah diimplementasikan, dan tidak mudah diprediksi guna mendukung keamanan proses enkripsi [10].

Salah satu operasi logika yang umum digunakan pada algoritma kriptografi simetris adalah *Exclusive OR* (*XOR*). Operasi *XOR* merupakan operasi logika biner yang menghasilkan nilai 1 apabila kedua bit masukan berbeda dan nilai 0 apabila kedua bit memiliki nilai yang sama [11]. Karakteristik tersebut menjadikan *XOR* banyak digunakan dalam berbagai algoritma kriptografi karena memiliki proses komputasi yang sederhana dan efisien [12]. Beberapa penelitian terdahulu telah mengimplementasikan metode *XOR* pada sistem kriptografi simetris melalui proses konversi *plaintext* dan kunci ke dalam representasi biner berdasarkan standar ASCII sebelum dilakukan operasi *XOR* untuk menghasilkan *ciphertext*. Proses dekripsi kemudian dilakukan menggunakan operasi *XOR* dengan kunci yang sama sehingga *ciphertext* dapat dikembalikan menjadi *plaintext* [13].

Salah satu konsep matematika yang memiliki struktur sederhana namun sistematis adalah deret aritmatika. Deret aritmatika merupakan barisan bilangan yang dibentuk berdasarkan suku pertama dan beda yang bernilai tetap sehingga menghasilkan pola bilangan yang teratur [14]. Karakteristik tersebut memungkinkan pembentukan rangkaian nilai kunci secara sistematis dengan proses perhitungan yang relatif sederhana. Selain mudah diimplementasikan, penggunaan konsep matematis dalam pembangkitan kunci juga memberikan dasar teoritis yang jelas terhadap mekanisme yang dikembangkan.

Berdasarkan uraian permasalahan tersebut, penelitian ini berfokus pada pengembangan mekanisme pembangkitan kunci berbasis deret aritmatika pada sistem kriptografi simetris. Kajian dilakukan untuk menganalisis karakteristik matematis dari kunci yang dihasilkan serta mengevaluasi potensi penerapannya dalam mendukung proses enkripsi dan dekripsi data. Kontribusi penelitian ini diharapkan dapat memperkaya alternatif metode pembangkitan kunci yang efisien, mudah diterapkan, dan memiliki landasan matematis yang terstruktur dalam pengembangan sistem keamanan data digital.

METODE PENELITIAN

Penelitian ini merupakan penelitian eksperimental yang bertujuan untuk mengembangkan mekanisme pembangkitan kunci berbasis deret aritmatika pada sistem kriptografi simetris. Metode yang digunakan memanfaatkan konsep matematis deret aritmatika untuk menghasilkan rangkaian kunci yang digunakan dalam proses enkripsi dan dekripsi data. Seluruh tahapan penelitian dilakukan secara sistematis mulai dari perancangan algoritma, implementasi proses enkripsi dan dekripsi, hingga analisis terhadap kinerja metode yang dikembangkan.

Tahap awal penelitian dilakukan dengan merancang mekanisme pembangkitan kunci berdasarkan konsep deret aritmatika. Pada tahap ini, parameter berupa suku pertama (a) dan beda (b) ditetapkan sebagai dasar pembentukan deret kunci yang disepakati oleh pihak pengirim dan penerima. Agar setiap nilai kunci dapat direpresentasikan dalam format 8-bit, nilai a dan seluruh suku yang dihasilkan harus berada pada rentang 0–255. Selain itu, nilai b tidak disarankan bernilai terlalu kecil atau sama dengan nol karena dapat menghasilkan perubahan nilai kunci yang relatif kecil atau bahkan menghasilkan kunci yang sama pada setiap posisi. Kondisi tersebut berpotensi membentuk pola kunci yang lebih teratur sehingga lebih mudah diprediksi. Oleh karena itu, pemilihan nilai a dan b perlu mempertimbangkan variasi kunci yang dihasilkan agar mekanisme pembangkitan kunci mampu menghasilkan deret yang lebih beragam. Deret kunci dibangkitkan menggunakan persamaan berikut:

$$a_n = (a + (n-1)b) \quad (1)$$

dengan:

a_n = suku ke-n dengan $(0 \leq a_n \leq 255)$
a = suku pertama dengan $(0 \leq a \leq 255)$
b = beda dengan $(0 \leq b \leq 255)$[14].

Setiap nilai kunci dipetakan ke rentang $0 - 255$ menggunakan operasi modulo 256.

Prosedur penelitian terdiri atas beberapa tahapan sebagai berikut.

(1) Menentukan Parameter

Tahap pertama dalam mekanisme pembangkitan kunci adalah penentuan parameter deret aritmatika, yaitu suku pertama (a) dan beda (b). Nilai kedua parameter tersebut disepakati oleh pihak pengirim dan penerima, kemudian digunakan untuk membangkitkan deret kunci yang berfungsi sebagai kunci simetris pada proses enkripsi dan dekripsi.

(2) Menentuan Deret Kunci

Berdasarkan nilai suku pertama (a) dan beda (b) yang telah ditentukan, dibentuk deret aritmatika sebagai sumber pembangkitan kunci. Nilai setiap suku pada deret digunakan sebagai kunci dinamis yang diterapkan secara berurutan dalam proses pengamanan data.

(3) Proses Enkripsi

Setiap karakter atau piksel dienkripsi menggunakan operasi *XOR* dengan persamaan berikut:

$$C_i = P_i \oplus K_i \quad (2)$$

dengan:
C_i menyatakan nilai *ciphertext* (data hasil enkripsi) pada posisi ke-i
P_i menyatakan nilai *plaintext* (data asli) pada posisi ke-i
K_i menyatakan nilai kunci pada posisi ke-i yang dibangkitkan dari deret aritmatika
i menyatakan indeks atau urutan data ke-i
$\oplus$ menyatakan operasi *XOR*

(4) Proses Dekripsi

Setiap karakter atau piksel didekripsi menggunakan operasi *XOR* dengan persamaan berikut:

$$P_i = C_i \oplus K_i \quad (3)$$

dengan:
C_i menyatakan nilai *ciphertext* (data hasil enkripsi) pada posisi ke-i
P_i menyatakan nilai *plaintext* (data asli) pada posisi ke-i
K_i menyatakan nilai kunci pada posisi ke-i yang dibangkitkan dari deret aritmatika
i menyatakan indeks atau urutan data ke-i

⊕ menyatakan operasi *XOR*

HASIL DAN PEMBAHASAN

Pada bagian ini disajikan hasil implementasi mekanisme pembangkitan kunci menggunakan deret aritmatika pada sistem kriptografi simetris. Pembahasan diawali dengan penentuan parameter pembangkitan kunci, kemudian dilanjutkan dengan proses pembangkitan kunci, enkripsi, serta dekripsi.

(1) Menentukan Parameter

Pembangkitan kunci dilakukan menggunakan deret aritmatika dengan nilai suku pertama sebesar 29 dan beda sebesar 5.

(2) Menentukan Deret Kunci

Kunci dibangkitkan menggunakan persamaan (1):

$$K_n = (a + (n-1)b)\ mod\ 256$$
$$K_n = (29 + (n-1)5)\ mod\ 256$$

Berdasarkan persamaan tersebut diperoleh deret kunci:

$$29, 34, 39, 44, 49, 54, 59, 64, 69, 74, 79, 84, 89, 94, \cdots$$

Pada penelitian ini digunakan *plaintext* "MATEMATIKA" yang terdiri atas empat karakter sehingga hanya sepuluh nilai kunci pertama yang digunakan, yaitu 29, 34, 39, 44, 49, 54, 59, 64, 69, dan 74. Hasil pembangkitan kunci ditunjukkan pada Tabel 1.

Table 1 Hasil Pembangkitan Kunci

Posisi	K_i	Biner
1	29	00011101
2	34	00100010
3	39	00100111
4	44	00101100
5	49	00110001
6	54	00110110
7	59	00111011
8	64	01000000
9	69	01000101
10	74	01001010

Hasil tersebut menunjukkan bahwa setiap posisi data memperoleh nilai kunci yang berbeda sehingga proses enkripsi tidak menggunakan kunci yang sama secara berulang.

(3) Proses Enkripsi

Sebelum proses enkripsi dilakukan, *plaintext* dikonversi ke dalam representasi ASCII[15]. Hasil konversi ditunjukkan pada Tabel 2, sebagai berikut.

Tabel 2 Konversi *Plaintext* ke ASCII

Plaintext	ASCII (P_i)	Biner
M	77	01001101
A	65	01000001
T	84	01010100
E	69	01000101
M	77	01001101
A	65	01000001
T	84	01010100
I	73	01001001
K	75	01001011

A	65	01000001

Proses enkripsi dilakukan menggunakan operasi *XOR* antara nilai *plaintext* dan kunci yang bersesuaian. Hasil enkripsi ditunjukkan pada Tabel 3, sebagai berikut.

Tabel 3 Hasil Enkripsi Menggunakan *XOR*

Posisi	ASCII (P_i)	K_i	$C_i = P_i \oplus K_i$	ASCII (C_i)
1	01001101 (77)	00011101 (29)	01010000 (80)	P
2	01000001 (65)	00100010 (34)	01100011 (99)	c
3	01010100 (84)	00100111 (39)	01110011 (115)	s
4	01000101 (69)	00101100 (44)	01101001 (105)	i
5	01001101 (77)	00110001 (49)	01111100 (124)	|
6	01000001 (65)	00110110 (54)	01110111 (119)	w
7	01010100 (84)	00111011 (59)	01101111 (111)	o
8	01001001 (73)	01000000 (64)	00001001 (9)	TAB
9	01001011 (75)	01000101 (69)	00001110 (14)	SO
10	01000001 (65)	01001010 (74)	00001011 (11)	VT

Nilai biner hasil enkripsi tersebut kemudian dikonversi berdasarkan tabel ASCII sehingga diperoleh *ciphertext* Pcsi|woTABSOVT.

(4) Proses Dekripsi

Proses dekripsi dilakukan menggunakan kunci yang sama dengan proses enkripsi. *Ciphertext* didekripsi menggunakan persamaan:

$$P_i = C_i \oplus K_i$$

Hasil dekripsi ditunjukkan pada Tabel 4, sebagai berikut.

Tabel 4 Hasil Dekripsi Menggunakan *XOR*

Posisi	$C_i = P_i \oplus K_i$	K_i	$P_i = C_i \oplus K_i$	ASCII (P_i)
1	01010000 (80)	00011101 (29)	01001101 (77)	M
2	01100011 (99)	00100010 (34)	01000001 (65)	A
3	01110011 (115)	00100111 (39)	01010100 (84)	T
4	01101001 (105)	00101100 (44)	01000101 (69)	E
5	01111100 (124)	00110001 (49)	01001101 (77)	M
6	01110111 (119)	00110110 (54)	01000001 (65)	A
7	01101111 (111)	00111011 (59)	01010100 (84)	T
8	00001001 (9)	01000000 (64)	01001001 (73)	I
9	00001110 (14)	01000101 (69)	01001011 (75)	K
10	00001011 (11)	01001010 (74)	01000001 (65)	A

Nilai ASCII hasil dekripsi kemudian dikonversi kembali menjadi karakter sehingga diperoleh *plaintext* MATEMATIKA. Hasil ini menunjukkan bahwa metode yang diusulkan mampu mengembalikan data ke bentuk semula tanpa kehilangan informasi.

Berdasarkan hasil implementasi pada Tabel 3 dan Tabel 4, mekanisme pembangkitan kunci menggunakan deret aritmatika berhasil diterapkan pada sistem kriptografi simetris berbasis operasi *Exclusive OR* (*XOR*). Pada proses enkripsi, setiap karakter *plaintext* terlebih dahulu dikonversi ke dalam representasi ASCII dan biner, kemudian dilakukan operasi *XOR* dengan nilai kunci yang dibangkitkan menggunakan deret aritmatika. Hasil enkripsi menunjukkan bahwa setiap posisi data menggunakan nilai kunci yang berbeda sehingga karakter *plaintext* yang sama dapat menghasilkan nilai *ciphertext* yang berbeda. Kondisi ini menunjukkan bahwa variasi kunci yang dihasilkan mampu mengurangi penggunaan kunci yang sama secara berulang dan menghasilkan *ciphertext* yang lebih bervariasi. Selanjutnya, proses dekripsi menggunakan operasi *XOR* dengan kunci yang sama berhasil

mengembalikan seluruh *ciphertext* menjadi *plaintext* semula, yaitu "MATEMATIKA", tanpa mengalami perubahan data. Hasil tersebut membuktikan bahwa mekanisme pembangkitan kunci berbasis deret aritmatika dapat diterapkan secara konsisten pada proses enkripsi dan dekripsi. Dengan demikian, metode yang diusulkan mampu menghasilkan rangkaian kunci yang sistematis, mudah diimplementasikan, serta berpotensi mendukung peningkatan keamanan data pada sistem kriptografi simetris berbasis operasi *XOR*.

SIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa deret aritmatika dapat dimanfaatkan sebagai mekanisme pembangkitan kunci pada sistem kriptografi simetris. Kunci yang dibangkitkan menggunakan parameter suku pertama dan beda menghasilkan rangkaian nilai yang berbeda pada setiap posisi data sehingga dapat digunakan dalam proses enkripsi dan dekripsi menggunakan operasi *XOR*. Hasil implementasi menunjukkan bahwa *plaintext* berhasil diubah menjadi *ciphertext* yang berbeda dari data asli, sedangkan proses dekripsi mampu mengembalikan *ciphertext* menjadi *plaintext* secara tepat. Dengan demikian, metode yang diusulkan dapat diterapkan sebagai alternatif pembangkitan kunci yang sederhana, mudah diimplementasikan, dan memiliki dasar matematis yang jelas dalam sistem kriptografi simetris.

Berdasarkan hasil penelitian tersebut, penulis menyarankan kepada peneliti selanjutnya untuk mengembangkan metode pembangkitan kunci berbasis deret aritmatika dengan mengombinasikannya bersama metode lain, seperti fungsi hash, bilangan acak, atau algoritma berbasis chaos, guna meningkatkan tingkat keamanan kunci yang dihasilkan. Selain itu, metode ini juga dapat diimplementasikan dan diuji pada berbagai jenis data, seperti citra digital, audio, maupun dokumen teks berukuran besar untuk mengetahui kinerja dan tingkat keamanannya pada skenario yang lebih kompleks. Bagi pengembang sistem keamanan data, hasil penelitian ini dapat dijadikan sebagai referensi dalam merancang mekanisme pembangkitan kunci yang sederhana dan efisien sebagai bagian dari proses enkripsi pada sistem kriptografi simetris.

DAFTAR PUSTAKA

[1] K. B. Ziliwu, A. Maslan, and H. Kremer, “Implementasi Caesar Cipher Pada Algoritma Kriptografi Dalam Penyandian Pesan Whatsapp,” *J. COMASIE*, 2022.

[2] W. Utomo, R. Latifah, And R. D. Risanty, “Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Caesar Cipher Dan Vigenere Cipher,” Teknologi Informasi dan Komputer. [Online]. Available: https://jurnal.umj.ac.id

[3] L. N. Hidayati, G. F. Fitriana, I. F. Adam, and F. Informatika, “Perbandingan Keacakan Citra Enkripsi Algoritma AES dan Camelia Uji NPCR dan UACI,” Vol. 8, No. 6, pp. 274–283, 2021, doi: 10.30865/jurikom.v8i6.3624.

[4] A. H. Kridalaksana and Z. Arifin, “Kriptografi Aes Mode Cbc Pada Citra Digital Berbasis Android,” Vol. 1, No. 1, pp. 45–52, 2016.

[5] C. Danuputri, N. Santosa, and F. D. Samuel, “Pengujian Pengembangan Terhadap Algoritma Vigenere Key Kriptografi”, [Online]. Available: https://s.id/jurnalresistor

[6] L. D. Simatupang, D. Bengkulu, J. Meranti, R. No, and S. Lebar Bengkulu, “Pengamanan Dokumen Teks Dengan Menerapkan Kombinasi Algoritma Kriptografi Klasik,” 2022.

[7] M. Rivaldi, I. Zarkasih Harahap, H. Isdianto, R. Amanda Putri, and F. Sains, “Positif : Jurnal Sistem dan Teknologi Informasi Implementasi Algoritma Kriptografi Vigenere Cipher Pada Pengamanan Pesan Text Berbasis Web”.

[8] J. Sasongko, “Pengamanan Data Informasi menggunakan Kriptografi Klasik,” vol. X, no. 3, pp. 160–167, 2005.

[9] R. Maulana and R. M. Simanjorang, “Implementasi Kriptografi Untuk Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4,” *J. Nas. Komputasi dan*

Teknol. Inf., vol. 4, no. 6, 2021.

[10] D. Ramalinda and A. R. Raharja, "Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi," 2024.

[11] I. F. Kriptografi, "Kriptografi Modern Pendahuluan," 2019.

[12] W. F. Senjaya, B. Rahardjo, T. Informatika, and U. K. Maranatha, "Implementasi dan Pengukuran Kinerja Operasi Aritmatika Finite Field Berbasis Polinomial Biner," vol. 1, pp. 183–193, 2015.

[13] Y. N. Tetik, F. E. Neno, D. Ariyus, J. Ring, and R. Utara, "Combination Of Xor Binary Algorithm And Steganography Using Least Significant Bit (LSB)," vol. 3839, pp. 187–196.

[14] Y. Safari and S. M. Putri, "Studi Komprehensif Tentang Barisan Dan Deret Aritmatika : Teori Dan Aplikasi," vol. 4, pp. 4445–4452, 2025.

[15] ASCII Code, "ASCII Table - Table of ASCII Codes, Characters and Symbols." Accessed: Jun. 14, 2026. [Online]. Available: https://www.ascii-code.com/