RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 3, No 3, Januari 2023
Hal 96-100
https://djournals.com/resolusi

Pengacakan Posisi Plaintext Menggunakan Kunci Blok Persegi pada Proses Enkripsi dengan Algoritma Arnold's Cat Map

Andysah Putera Utama Siahaan, Melva Sari Panjaitan

Fakultas Sains dan Teknologi, Universitas Pembangunan Panca Budi, Medan, Indonesia
Email: [1,*]andiesiahaan@gmail.com, [2]melva@pancabudi.ac.id
Email Penulis Korespondensi: andiesiahaan@gmail.com

Abstrak-Plaintext merupakan pesan atau informasi yang berbentuk asli yang memiliki format teks. Plaintext dapat dibuka menggunakan aplikasi text editor apapun karena sistem penyusunan informasi pada plaintext tidak menggunakan kunci keamanan. Dalam melakukan pengamanan pesan, plaintext harus diberi serangkaian perintah atau kode program untuk dapat menjadikan plaintext tersebut menjadi pesan terenkripsi. Teknik yang digunakan pada penelitian ini menggunakan skema transposisi yaitu dengan cara menyusun ulang letak karakter tersebut tanpa mengganti karakter plaintext dengan karakter lain. Tingkat kesulitan pada proses ini tergantung dari parameter nilai B dan C yang diberikan serta nilai Iterasi yang digunakan dalam menghasilkan ciphertext. Penelitian ini menggunakan penyusunan karakter dengan pola matriks 4 x 4 dimana setiap blok plaintext akan dibagi berdasarkan 16 karakter. Setiap blok akan dilakukan proses enkripsi menggunakan map yang sudah dihasilkan oleh Arnold's Cat Map. Hasil penelitian mendapatkan bahwa plaintext dapat teracak dengan baik pada proses enkripsi dan berhasil dikembalikan ke pesan asli pada saat dekripsi.

Kata Kunci: Enkripsi; Dekripsi; Arnold's Cat Map; Transposisi

Abstract-Plaintext is a message or information in the original form that has a text format. Plaintext can be opened using any text editor application because the plaintext information preparation system does not use a security key. In securing the message, the plaintext must be given a series of commands or program code to turn the plaintext into an encrypted message. The technique used in this study uses a transposition scheme, namely by rearranging the location of the characters without replacing the plaintext characters with other characters. The level of difficulty in this process depends on the parameter values B and C given and the iteration value used to generate the ciphertext. This study uses character arrangement with a 4 x 4 matrix pattern where each plaintext block will be divided based on 16 characters. Each block will be encrypted using a map that has been generated by Arnold's Cat Map. The results of the study found that the plaintext could be scrambled properly during the encryption process and was successfully returned to the original message at the time of decryption.

Keywords: Encryption; Decryption; Arnold's Cat Map; Transposition

1. PENDAHULUAN

Perkembangan teknologi telah membuat pengiriman informasi lebih cepat. Informasi dapat dikirimkan seketika melalui perangkat lunak yang sudah diprogram sedemikian rupa. Banyak aplikasi yang sudah dibangun untuk membantu pekerjaan sehari-hari [1][2]. Ada banyak perangkat lunak yang dapat membantu pengiriman pesan kepada penerima. Pesan yang dikirimkan berupa plaintext dengan format teks yang langsung dapat dibaca pada saat dibuka menggunakan text editor.

Pesan dapat berupa informasi penting yang tidak boleh diketahui oleh orang lain [3]. Pesan tersebut dapat disalahgunakan apabila jatuh ke orang yang tidak bertanggung jawab. Kelemahan informasi berbentuk plaintext adalah informasi tersebut tidak memiliki keamanan yang dapat melindungi isi atau konten dari pesan tersebut [4]. Kebutuhan akan pengamanan sangat penting dilakukan untuk menjaga agar pesan tersebut tidak dapat dibaca secara sembarangan [5].

Kriptografi adalah salah satu yang digunakan untuk melakukan transformasi plaintext menjadi ciphertext [6][7]. Plaintext dapat diamankan menggunakan teknik kriptografi dengan algoritma tertentu. Penelitian ini menggunakan algoritma Arnold's Cat Map dalam melakukan pengamanan pada plaintext. Pada dasarnya, algoritma ini digunakan terhadap pengacakan piksel pada gambar tetapi tidak menutup kemungkinan dapat digunakan dalam melakukan pengacakan plaintext [8].

Kelemahan dari plaintext akan dapat diatasi dengan memanfaatkan algoritma ini dalam melakukan penukaran posisi karakter. Algoritma Arnold's Cat Map bekerja dengan skema transposisi [9]. Teknik transposisi bekerja dengan menukar letak karakter atau nomor indeks pada masing-masing karakter [10].

Pembentukan letak karakter ditentukan berdasarkan pola atau map yang dibangkitkan oleh algoritma menggunakan nilai parameter tertentu. Hasil transposisi karakter akan bergantung pada kunci yang digunakan terhadap blok plaintext tersebut.

Plaintext akan dibagi berdasarkan matriks persegi yang menghasilkan blok plaintext. Setiap blok plaintext akan dibentuk dengan pola N x N dengan nilai N adalah 4. Blok plaintext dan blok kunci yang dihasilkan harus berbentuk bujur sangkar untuk memudahkan pertukaran posisi karakter menggunakan algoritma Arnold's Cat Map. Algoritma ini bekerja berdasarkan nilai Iterasi, B dan C yang digunakan.

Nilai iterasi tidak wajib digunakan. Iterasi merupakan perulangan yang dilakukan untuk meningkatkan keamanan dan menjauhkan plaintext dari usaha pengembalian paksa yang dilakukan menggunakan brute force attack.

ISSN 2745-7966 (Media Online)
Vol 3, No 3, Januari 2023
Hal 96-100
https://djournals.com/resolusi

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi merupakan ilmu komputer yang berfungsi untuk melakukan penyandian pesan sehingga pesan tersebut terhindar kebocoran informasi [11]. Proses kriptografi terdiri dari proses enkripsi dan dekripsi [12]. Setiap proses memiliki kunci yang akan digunakan untuk melindungi plaintext sehingga menghasilkan ciphertext. Ciphertext akan dibentuk sesuai dengan algoritma yang digunakan pada proses enkripsi pesan [13]. Penggunaan algoritma yang sama harus dilakukan untuk melakukan proses dekripsi agar menghasilkan pesan asli kembali.

2.2 Arnold's Cat Map

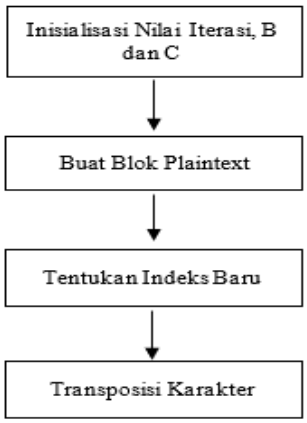
Arnold's Cat Map adalah transformasi yang dilakukan untuk melakukan pertukaran posisi piksel yang dapat diterapkan pada gambar [14]. Piksel gambar disusun ulang sehingga mengaburkan gambar aslinya. Tata letak piksel diatur ulang secara acak sesuai dengan nilai parameter yang digunakan, tetapi algoritma ini memiliki kelemahan dimana ketika transformasi diulang cukup lama, gambar asli akan ditampilkan kembali [15]. Berikut ini adalah formula yang digunakan pada algoritma Arnold's Cat Map.

$$\begin{bmatrix} y^1 \\ x^1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ c & bc+1 \end{bmatrix} \begin{bmatrix} y \\ x \end{bmatrix} \text{Mod N} \quad (1)$$

Keterangan:
y1 = posisi vertikal piksel yang baru
x1 = posisi horizontal piksel yang baru
y = posisi vertikal piksel yang lama
x = posisi horizonal piksel yang lama
b = nilai parameter 1
c = nilai parameter 2

2.3 Tahapan Penelitian

Penelitian ini memiliki beberapa tahapan yang akan digunakan dalam melakukan proses enkripsi menggunakan algoritma Arnold's Cat Map. Dalam proses transformasi plaintext ke ciphertext ada beberapa langkah yang harus dilakukan agar posisi karakter dapat dipindahkan ke posisi baru seperti yang dijelaskan pada gambar 1.



Gambar 1. Tahapan penelitian

Penelitian ini menggunakan blok plaintext yang berukuran 4 x 4 sehingga berjumlah 16 karakter dalam setiap proses enkripsi. Berikut ini akan digambarkan secara lengkap pembentukan blok pada plaintext dan ciphertext.

Tabel 1. Susunan plaintext

	0	**1**	**2**	**3**
0	a	b	c	d
1	e	f	g	h
2	i	j	k	l
3	m	n	o	p

Tabel 2. Susunan ciphertext

	0	**1**	**2**	**3**
0	a	j	c	l
1	e	n	g	p

ISSN 2745-7966 (Media Online)
Vol 3, No 3, Januari 2023
Hal 96-100
https://djournals.com/resolusi

	0	1	2	3
2	i	b	k	d
3	m	f	o	h

Tabel 1 adalah huruf a hingga p adalah karakter plaintext yang disusun secara horizontal dan berurutan. Apabila ruang sudah tidak mencukupi, maka karakter tersebut akan disusun di kolom pertama pada baris berikutnya dan begitu seterusnya hingga semua karakter tersusun dengan baik. Tabel 2 adalah hasil proses enkripsi yang akan menyusun ulang posisi karakter pada plaintext. Tabel 3 adalah posisi kolom dan baris dari masing-masing karakter sebelum dan sesudah enkripsi.

Tabel 3. Posisi karakter sebelum dan sesudah enkripsi

No.	Karakter	Y	X	Yi	Xi
1	a	0	0	0	0
2	b	0	1	2	1
3	c	0	2	0	2
4	d	0	3	2	3
5	e	1	0	1	0
6	f	1	1	3	1
7	g	1	2	1	2
8	h	1	3	3	3
9	i	2	0	2	0
10	j	2	1	0	1
11	k	2	2	2	2
12	l	2	3	0	3
13	m	3	0	3	0
14	n	3	1	1	1
15	o	3	2	3	2
16	p	3	3	1	3

3. HASIL DAN PEMBAHASAN

Bagian ini akan menyajikan perhitungan dan pembahasan tentang proses enkripsi dari algoritma Arnold's Cat Map. Perhitungan akan menggunakan beberapa parameter yang akan digunakan dalam pembentukan posisi karakter pada ciphertext. Berikut ini adalah gambaran dan penjelasan lengkap dari percobaan proses enkripsi menggunakan algoritma Arnold's Cat Map.

Parameter:

Iterasi = 1
N = 4
B = 3
C = 5
Plaintext= CRYPTO IS BETTER

Tabel 4. Posisi karakter sebelum enkripsi

	0	1	2	3
0	C	R	Y	P
1	T	O		I
2	S		B	E
3	T	T	E	R

Hasil perhitungan posisi baru berdasarkan algoritma Arnold's Cat Map dapat dilihat pada penjelasan berikut ini.

$$\begin{bmatrix} y^0 \\ x^0 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \end{bmatrix} Mod\ 16 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} y^0 \\ x^1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} Mod\ 16 = \begin{bmatrix} 3 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} y^0 \\ x^2 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \end{bmatrix} Mod\ 16 = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} y^0 \\ x^3 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 0 \\ 3 \end{bmatrix} Mod\ 16 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} y^1 \\ x^0 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} Mod\ 16 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} y^1 \\ x^1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} Mod\ 16 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

ISSN 2745-7966 (Media Online)
Vol 3, No 3, Januari 2023
Hal 96-100
https://djournals.com/resolusi

$$\begin{bmatrix} y^1 \\ x^2 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} Mod\ 16 = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$$
$$\begin{bmatrix} y^1 \\ x^3 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \end{bmatrix} Mod\ 16 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$
$$\begin{bmatrix} y^2 \\ x^0 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \end{bmatrix} Mod\ 16 = \begin{bmatrix} 2 \\ 2 \end{bmatrix}$$
$$\begin{bmatrix} y^2 \\ x^1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} Mod\ 16 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$$
$$\begin{bmatrix} y^2 \\ x^2 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 2 \\ 2 \end{bmatrix} \text{Mod } 16 = \begin{bmatrix} 0 \\ 2 \end{bmatrix}$$
$$\begin{bmatrix} y^2 \\ x^3 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} \text{Mod } 16 = \begin{bmatrix} 3 \\ 2 \end{bmatrix}$$
$$\begin{bmatrix} y^3 \\ x^0 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 3 \\ 0 \end{bmatrix} \text{Mod } 16 = \begin{bmatrix} 3 \\ 3 \end{bmatrix}$$
$$\begin{bmatrix} y^3 \\ x^1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} \text{Mod } 16 = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$$
$$\begin{bmatrix} y^3 \\ x^2 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} \text{Mod } 16 = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$$
$$\begin{bmatrix} y^3 \\ x^3 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 5 & 3*5+1 \end{bmatrix} \begin{bmatrix} 3 \\ 3 \end{bmatrix} \text{Mod } 16 = \begin{bmatrix} 0 \\ 3 \end{bmatrix}$$

Tabel 5. Hasil perubahan tata letak karakter

	0	**1**	**2**	**3**		**0**	**1**	**2**	**3**
0	(0,0)	(0,1)	(0,2)	(0,3)	0	(0,0)	(3,0)	(2,0)	(1,0)
1	(1,0)	(1,1)	(1,2)	(1,3)	1	(1,1)	(0,1)	(3,1)	(2,1)
2	(2,0)	(2,1)	(2,2)	(2,3)	2	(2,2)	(1,2)	(0,2)	(3,2)
3	(3,0)	(3,1)	(3,2)	(3,3)	3	(3,3)	(2,3)	(1,3)	(0,3)

Tabel 5 menjelaskan perubahan tata letak pada karakter yang akan ditransposisikan menggunakan algoritma Arnold's Cat Map. Terlihat pemetaan dilakukan secara sistem yang melibatkan parameter Iterasi, B dan C. Percobaan ini menggunakan iterasi sebanyak satu kali. Hasil transposisi karakter atau ciphertext dapat dilihat secara lengkap pada Tabel 6.

Tabel 6. Hasil transposisi karakter

	0	**1**	**2**	**3**		**0**	**1**	**2**	**3**
0	C	R	Y	P	0	C	T	S	T
1	T	O		I	1	O	R	T	
2	S		B	E	2	B		Y	E
3	T	T	E	R	3	R	E	I	P

Pada tabel tersebut, dapat dilihat perubahan yang significant dari plaintext ke ciphertext. Baris 0 kolom 0 tidak mengalami perubahan karena nilai ini mengalami perkalian terhadap angka 0 sehingga hasil posisi X dan Y dari ciphertext juga tidak mengalami perubahan sama sekali. Tetapi tidak menutup kemungkinan ada karakter pada plaintext di baris dan kolom tertentu tidak mengalami perubahan juga. Hasil ciphertext yang diperoleh adalah "CTSTORT B YEREIP".

4. KESIMPULAN

Algoritma Arnold's Cat Map digunakan dalam menentukan transposisi karakter plaintext berdasarkan nilai Iterasi, B dan C pada parameter input. Karakter pada plaintext akan ditempatkan pada posisi baru dari perhitungan yang dilakukan oleh algoritma Arnold's Cat Map. Dari perhitungan dapat dilihat bahwa nilai modulo akan membatasi agar hasil transposisi tidak melewati batas kolom dan baris yang sudah ditentukan. Kombinasi nilai Iterasi, B dan C harus tepat agar hasil ciphertext tidak mudah untuk ditebak. Tingkat kesulitan ditentukan oleh seberapa baik kombinasi dari ketiga nilai tersebut. Algoritma ini akan lebih efektif pada jumlah nilai N yang besar karena peluang untuk terjadinya pertukaran karakter antar tetangga lebih kecil.

REFERENCES

[1] M. Zen, Supiyandi, C. Rizal, and M. Eka, "Rancang Bangun Aplikasi Absensi Siswa (Studi Kasus Lkp Karya Prima Kursus)," J. Ilmu Komput. dan Inform., vol. 5, no. 2, pp. 80–87, 2021, doi: 10.30829/algoritma.v5i2.10507.

[2] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," Inform. Mulawarman J. Ilm. Ilmu Komput., vol. 10, no. 1, p. 20, Jun. 2016, doi: 10.30872/jim.v10i1.23.

[3] J. H. Lubis, "Implementasi Keamanan Data Dengan Metode Kriptografi XOR," J. Sist. Inf. Kaputama, vol. 2, no. 2, pp. 2–4, 2018.
[4] Sukriadi Shafar, "Pengertian Dan Contoh Kriptografi dengan Proses Enkripsi dan Dekripsi," On Digital Forensics, 2016. http://ondigitalforensics.weebly.com/cryptography/pengertian-dan-contoh-kriptografi-dengan-proses-enkripsi-dan-dekripsi#.W7w6mxMzZZ0
[5] S. Supiyandi, H. Hermansyah, and K. A. P. Sembiring, "Implementasi dan Penggunaan Algoritma Base64 dalam Pengamanan File Video," J. MEDIA Inform. BUDIDARMA, vol. 4, no. 2, p. 340, Apr. 2020, doi: 10.30865/mib.v4i2.2042.
[6] J. R. Paragas, A. M. Sison, and R. P. Medina, "A New Variant of Hill Cipher Algorithm using Modified S-Box," Int. J. Sci. Technol. Res., vol. 8, no. 10, pp. 615–619, 2019.
[7] A. Rohmanu, "Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File," J. Inform. SIMANTIK, vol. 2, no. 1, pp. 1–11, 2017.
[8] R. Purba, A. Halim, and I. Syahputra, "Enkripsi Citra Digital Menggunakan Arnold's Cat Map dan Nonlinear Chaotic Algorithm," JSM STMIK Mikroskil, vol. 15, no. 2, pp. 61–68, 2014.
[9] W. M. Rahmawati and F. Liantoni, "Penggunaan Arnold Cat's Map dan Beta Chaotic Map Pada Enkripsi Data Citra," J. ELTIKOM, vol. 2, no. 2, pp. 50–57, 2018, doi: 10.31961/eltikom.v2i2.85.
[10] A. P. U. Siahaan, "Data Security Techniques Using Square Block Keys in Text Format," Int. J. Res. Rev., vol. 10, no. 2, pp. 354–358, 2023, doi: 10.52403/ijrr.20230244.
[11] R. Munir, "Pengantar Kriptografi," KRIPTOGRAFI, 2006.
[12] F. Diani and Y. Widhiyasana, "Enkripsi SMS dengan Menggunakan One Time Pad (OTP) dan Kompresi Lempel-Ziv-Welch (LZW)," J. Nas. Tek. Elektro dan Teknol. Inf., vol. 7, no. 3, pp. 3–8, 2018, doi: 10.22146/jnteti.v7i3.436.
[13] A. P. U. Siahaan, "Three-Pass Protocol Concept in Hill Cipher Encryption Technique," Int. J. Sci. Res., vol. 5, no. 7, pp. 1149–1152, 2016.
[14] E. Hariyanto and R. Rahim, "Arnold's Cat Map Algorithm in Digital ImageEncryption," Int. J. Sci. Res., vol. 5, no. 10, pp. 1363–1365, 2016.
[15] T. A. Putra, I. Ruslianto, and S. Bahri, "Application of Arnold Cat Map and Logistic Map Methods for Securing Citizens' Data Image," J. Comput. Eng. Syst. Sci., vol. 7, no. 2, pp. 470–481, 2022, doi: 10.24114/cess.v7i2.36302.