JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 3, Juli 2020, Page 841-849
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i3.2244

Penerapan Algoritma Coupled Linear Congurential Generator (CLCG) pada Algoritma Kriptografi One Time Pad (OTP) dalam Proses Mengamankan Pesan

Deny Nugroho Triwibowo, Dony Ariyus*

Magister Teknik Informartika, Universitas Amikom Yogyakarta, Sleman, Indonesia
Email: [1]deny.15@students.amikom.ac.id, [2,*]dony.a@amikom.ac.id
Email Penulis Korespondensi: dony.a@amikom.ac.id

Abstrak−Pesan merupakan suatu gagasan, perasaan, atau pemikiran seseorang yang isinya bisa berupa ilmu pengetahuan, hiburan, informasi, nasihat, atau propaganda. Saat ini dengan perkembangan teknologi yang sangat maju seseorang dapat bertukar pesan dengan begitu mudah dan cepat tanpa ada batasan jarak dan waktu. Namun, dengan semakin mudahnya bertukar pesan ada saja masalah yang dapat terjadi, salah satunya pesan yang ingin dikirim membuka peluang bagi orang-orang yang yang ingin mencuri data dan informasi dari pesan tersebut untuk menggunakannya sebagai tindak kejahatan dan tentunya akan merugikan pihak tertentu. Maka dari itu, digunakan teknik mengamankan pesan dengan menggunakan algoritma OTP dan pembangkit bilangan acak CLCG agar pesan yang dikirim tingkat keamanannya dapat dijamin. Hasil dari penggabungan algoritma OTP dan CLCG dalam proses enkripsi dan dekripsi didapatkan pembangkit kunci acak tidak terjadi perulangan kunci yang sama dengan karakter yang sama yang saling berdekatan pada pesan. Penggunaan tabel periodik dalam proses enkripsi juga menambah kesulitan untuk memecahkan pesan karena satu karakter plaintext digantikan dengan banyak karakter pada ciphertext.

Kata Kunci: Pesan, Kriptografi, *One Time Pad* (OTP), *Coupled Linear Congruential Generator* (CLCG), Tabel Periodik

Abstract−Message is an idea, feeling, or thought of someone whose contents can be in the form of science, entertainment, information, advice, or propaganda. Nowadays, with the development of very advanced technology, one can exchange messages so easily and quickly without any limitations on distance and time. However, with the ease of exchanging messages there are problems that can occur, one of which is the message you want to send opens opportunities for people who want to steal data and information from the message to use it as a crime and will certainly harm certain parties. Therefore, the technique of securing messages is used by using the OTP algorithm and the CLCG random number generator so that messages sent to the security level can be guaranteed. The results of the merging of the OTP and CLCG algorithms in the encryption and decryption process found random key generator does not occur the same key loop with the same characters adjacent to the message. The use of periodic tables in the encryption process also increases the difficulty of deciphering messages because one plaintext character is replaced by many characters in the ciphertext.

Keywords: Message, Cryptographi, One Time Pad (OTP), Coupled Linear Congruential Generator (CLCG), Periodic Tables

1. PENDAHULUAN

Pesan merupakan suatu gagasan, perasaan, atau pemikiran yang akan di-enkripsi oleh si pengirim dan di-dekripsi oleh penerima ketika ingin saling bertukar pesan [1]. Pesan yang akan dikirimkan dan diterima isinya bisa berupa ilmu pengetahuan, hiburan, informasi, nasihat atau propaganda yang pada dasarnya bersifat konkret atau abstrak. Di mana pembuatan pesan adalah hasil dari pengalaman yang pernah dilakukan atau untuk memberitahukan kejadian yang akan datang kepada seseorang [2]. Sebuah pesan dapat disampaikan secara lisan atau tulisan dengan cara tatap muka secara langsung atau melalui media komunikasi yang saat ini sudah begitu banyak aplikasi yang dibuat.

Aplikasi media komunikasi saat ini adalah perwujudan dari perkembangan teknologi yang makin hari semakin meningkat. Sehingga membuat seseorang dengan mudahnya bertukar informasi tanpa ada batasan jarak dan waktu. Namun, keamanan yang merupakan masalah utama yang terdapat dalam jaringan yang bebas berkaitan dengan pertukaran informasi dari pengirim ke penerima begitupun sebaliknya [3], hal ini akan membuka peluang bagi orang-orang yang yang ingin mencuri data dan informasi dari pesan tersebut untuk menggunakannya sebagai tindak kejahatan dan tentunya akan merugikan pihak tertentu [4]. Untuk itu dibutuhkan teknik dalam mengamankan suatu pesan, khususnya pesan yang di dalamnya terdapat informasi yang sifatnya penting atau rahasia dengan melakukan enkripsi sebelum dikirim ke tujuan, maka tingkat keamanan informasi dari pesan tersebut dapat dijamin.

Ada dua teknik yang telah populer dan banyak digunakan dalam proses keamanan pesan, yaitu, steganografi dan kriptografi [5]. Steganografi adalah teknik menyembunyikan pesan pada suatu objek untuk mengelabui indra penglihatan manusia [6]. Sedangkan kriptografi adalah teknik untuk mengubah bentuk pesan menjadi bentuk lain yang memiliki arti berbeda dengan pesan itu sendiri, bahkan memungkin membuatnya seperti file yang rusak, sehingga sulit dibaca atau dimengerti oleh pihak lain [7] [8] [9]. Teknik kriptografi merupakan teknik yang dapat digunakan untuk mengenkripsi naskah asli (*plaintext*) yang diacak menggunakan suatu kunci enkripsi menjadi naskah acak yang Ada begitu banyak metode yang digunakan dalam proses mengamankan pesan, salah satunya metode OTP (*One Time Pad*). *One Time Pad* sendiri bergantung pada kunci acak yang digunakan. Semakin tinggi jumlah kunci acak yang digunakan dan tidak menggunakannya kembali, maka keamanan chipertext dari *One Time Pad* akan semakin tinggi yang membuatnya sangat aman dan sulit dipecahkan [10]. Penggunaan pembangkit

Submitted: **02/06/2020**; Accepted: **09/07/2020**; Published: **20/07/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 3, Juli 2020, Page 841-849
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i3.2244

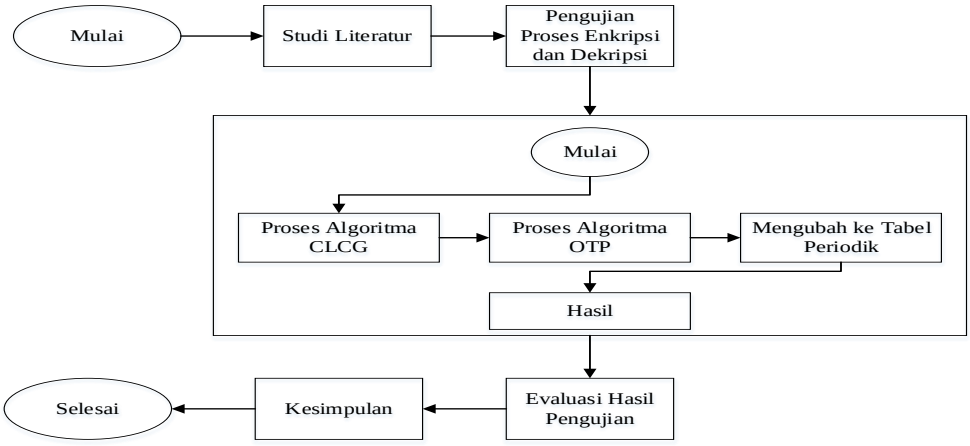
bilangan acak untuk mendapatkan kebutuhan kunci yang ingin digunakan pada proses OTP. Salah satunya dengan metode *Linear Congruential Generator* (LCG) yang mampu menghindari penggunaan kunci yang rekursif dengan menentukan rentang nilai a, nilai c, dan nilai m pada metode LCG [11]. Lebih lanjut lagi dengan penggunaan pembangkit bilangan acak diharapkan akan lebih menyulitkan kriptanalis atau orang yang ingin memecahkan kode untuk kepentingan pribadi dan merugikan orang lain dalam memecakan data [4].

Penelitian yang dilakukan Kwasi Boakye-Boateng dan Arash Habibi Lashkari [12] menjelaskan tentang penggunaan OTP untuk mengamankan protokol GOOSE sangat memungkinkan karena kunci generasi dari PRNG (pseudo-random number generator) tampak benar benar acak. Akan tetapi, implementasi PRNG terlihat bersifat deterministik atau menghasilkan output yang sama. Oleh karena itu membutuhkan penyegaran / pembaharuan terutama fokus pada pembaharuan inputan PRNG. Penelitian yang dilakukan N. Khairina, M. Harahap, A. Husein et al [13] menghasilkan kunci acak dengan menggunakan algoritma Rivest Shamir Adleman (RSA) dan mengkombinasikan dengan algoritma Quadratic Congruential Generator (QCG) yang menunjukkan bahwa setiap plaintext masing – masing memiliki nilai p, q, kunci private, dan kunci pribadi yang sangat unik. Namun, hasil dari penggunaan nilai unik tersebut dapat mencegah terhadap serangan cryptanalyst sebesar 64%. Selanjutnya, penelitian yang dilakukan Rachmat Aulia, A. Zakir, dan Muhammad Zulhafiz [14] melakukan kombinasi OTP dan LCG untuk mengamankan pesan teks sebelum dikirim ke target yang dituju. Hasil dari kombinasi algoritma ini didapatkan kunci acak yang berbeda setiap karakter teks pada pesan. Namun, konversi dari plaintext ke ciphertext cukup rentan untuk dilakukan cryptanalyst karena satu karakter terkonversi dengan satu karakter juga.

Untuk itu dalam penelitian ini akan dikembangkan metode penggabungan LCG atau *Coupled Linear Congruential Generator* untuk pembangkitan nilai acak yang sulit untuk dipecahkan. Nilai dari hasil perhitungan OTP dan CLCG, selanjutnya akan dikonversi ke dalam bentuk tabel periodik dengan menyesuaikan nomor atom yang telah didefinisikan terlebih dahulu dan mengambil variabel simbol dan konfigurasi elektronnya.

2. METODOLOGI PENELITIAN

Metode penelitian merupakan suatu proses atau cara yang digunakan untuk menyelesaikan masalah yang diajukan dalam sebuah penelitian dengan sekumpulan prosedur yang dilakukan oleh peneliti untuk untuk mencapai tujuan dan menentukan jawaban atas masalah yang diajukan. Adapun metode penelitian yang digunakan dapat dilihat pada gambar 1.



Gambar 1. Metode Penelitian

2.1 Studi Literatur

Menurut Sugiyono [15] "studi literatur merupakan kajian teoritis dan referensi lain yang berkaitan dengan nilai, budaya dan norma yang berkembang pada situasi sosial yang diteliti, selain itu studi kepustakaan sangat penting dalam melakukan penelitian, hal ini dikarenakan penelitian tidak akan lepas dari literatur-literatur Ilmiah."

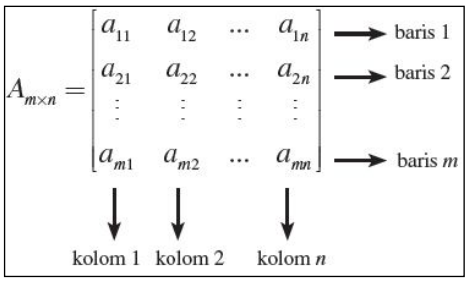
2.3 Pengujian Proses Enkripsi dan Dekripsi

2.3.1 Matrik

Definisi matrik menurut Kaufman [16] adalah jajaran bilangan yang disusun dalam baris dan kolom diantara tanda kurung yang disusun menurut m baris dan n kolom sehingga membentuk jajaran (*array*) persegi maupun persegi panjang. Matrik yang memiliki baris dan kolom disebut matrik $m \times n$ atau matrik berorde $m \times n$. Suatu matrik ditunjukkan dengan menuliskan jajarannya di antara kurung siku, misalnya:

Submitted: **02/06/2020**; Accepted: **09/07/2020**; Published: **20/07/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 3, Juli 2020, Page 841-849
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i3.2244



Gambar 2. Matrik

Sebuah matrik yang hanya memiliki satu baris disebut vektor baris atau matrik baris, dan sebuah matrik yang hanya memiliki satu kolom disebut vektor kolom atau matrik kolom. Sebagai contoh matrik yang akan digunakan pada penelitian ini adalah matrik 9 x 14 dengan jumlah keseluruhan 126.

Tabel 1. Matrik Ordo 9 x 14

Indeks	0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	15	16	17	18	19	20	21	22	23	24	25	26	27	28
2	29	30	31	32	33	34	35	36	37	38	39	40	41	42
3	43	44	45	46	47	48	49	50	51	52	53	54	55	56
4	57	58	59	60	61	62	63	64	65	66	67	68	69	70
5	71	72	73	74	75	76	77	78	79	80	81	82	83	84
6	85	86	87	88	89	90	91	92	93	94	95	96	97	98
7	99	100	101	102	103	104	105	106	107	108	109	110	111	112
8	113	114	115	116	117	118	119	120	121	122	123	124	125	126

2.3.2 Coupled Linear Congruential (CLCG)

Metode *Coupled Linear Congruential Generator* adalah sebuah metode pembangkit bilangan acak semu yang memanfaatkan penggabungan dua persamaan linear berbasis metode *Linear Congruential Generator* sebagai generasi baru pembangkit bilangan acak [17]. Metode *Coupled Linear Congruential Generator* didefinisikan dengan persamaan :

$$x_{i+1} = a_1 x_i + b_1 \ (mod\ m) \quad (1)$$

$$y_{i+1} = a_2 y_i + b_2 \ (mod\ m) \quad (2)$$

Keterangan :

x_{i+1} = bilangan acak x ke- n dari deret nya
y_{i+1} = bilangan acak y ke- n dari deretnya
x_n = bilangan acak x dari sebelumnya
y_n = bilangan acak y dari sebelumnya
a = faktor pengali
b = increment
m = modulus
i = 0,1,2,3,… dan seterunya.

Pengembangan metode *Coupled Linear Congruential Generator* yang dilakukan oleh Katti digunakan untuk menghasilkan enkripsi deret bit B_i dengan kondisi :

$$B_{i+1} = \begin{cases} 1, & jika\ x_{i+1} > y_{i+1} \\ 0, & sebaliknya \end{cases} \quad (3)$$

Metode *Coupled Linear Congruential Generator* dimodifikasi dengan matrik. Berdasarkan hasil persamaan x_{i+1} dan y_{i+1} maka akan didapatkan deret bilangan acak yang akan dirubah ke dalam bilangan orde matrik. Orde x didapatkan dari modulus x_{i+1}terhadap jumlah baris dengan persamaan :

$$M_{(x,0)} = x_{i+1}\ mod\ i \quad (4)$$

Orde y didapatkan dari modulus y_{i+1} terhadap jumlah kolom dengan persamaan :

$$M_{(0,y)} = y_{i+1}\ mod\ j \quad (5)$$

Hasil akhir didapatkan dengan menggunakan matrik baru dari persamaan :

$$M_n = M[x_{i+1}\ mod\ i][y_{i+1}\ mod\ j] \quad (6)$$

Keterangan :

M_n = hasil bilangan acak ke- n dari deretnya
x_{i+1} = bilangan acak x ke- n dari deretnya

Submitted: **02/06/2020**; Accepted: **09/07/2020**; Published: **20/07/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 3, Juli 2020, Page 841-849
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i3.2244

y_{i+1} = bilangan acak y ke- n dari deretnya
i = baris matriks
j = baris kolom
n = 0,1,2,3,… dan seterusnya

Contoh hasil perhitungan pembangkitan bilangan acak dengan CLCG sebanyak 10 kali sebagai berikut :
Diketahui
$Matrik\ baris = 9$
$Matrik\ kolom = 14$
$X0\ (baris) = 4$
$Y0\ (kolom) = 5$
$a = 64$
$b = 17$
$m = 126$

Tabel 2. Perhitungan CLCG sebanyak 10 kali

X	Nilai	Y	Nilai	Baris	Kolom	Hasil
X1	21	Y1	85	3	1	44
X2	101	Y2	39	2	11	40
X3	55	Y3	119	1	7	22
X4	9	Y4	73	0	3	4
X5	89	Y5	27	8	13	126
X6	43	Y6	107	7	9	108
X7	123	Y7	61	6	5	90
X8	77	Y8	15	5	1	72
X9	31	Y9	95	4	11	68
X10	111	Y10	49	3	7	50

2.3.3 One Time Pad (OTP)

Algortima OTP pertama kali ditemukan oleh Gilbert Vernam di tahun 1917 menggunakan karakter-karakter kunci yang berisi huruf-huruf yang tersusun secara acak. OTP merupakan salah satu algoritma yang populer dan sering digunakan dalam teknik kriptografi di jaman modern saat ini. Algoritma OTP termasuk kelompok algoritma simetris dalam teknik kriptografi dimana kunci enkripsi dan dekripsi dalam bentuk dan panjang yang sama dengan *plaintext* atau teks aslinya, serta menggunakan operasi XOR dalam proses enkripsi dan dekripsinya [18]. Keunggulan dari algoritma OTP adalah sangat sulit dan rumit untuk dipecahkan tapi memiliki kekurangan dimana kunci yang digunakan kadang terlalu panjang karena harus menyesuaikan jumlah karakter *plaintext* yang akan dienkripsi [19]. Dari semua algoritma kriptografi yang telah dirancang, algoritma OTP adalah metode yang telah terbukti benar-benar aman secara matematis. Algoritma OTP bisa dikatakan algoritma yang 'sempurna' jika memenuhi kondisi seperti berikut [20] kunci harus sepanjang dengan *plainteks*, kunci harus tersusun secara acak seluruhnya atau sepenuhnya berbeda, kunci hanya sekali digunakan pada setiap melakukan proses enkripsi, dan hanya terdapat dua salinan dari kunci: satu untuk pengirim dan satu untuk penerima [21]. Rumus enkripsi dan dekripsi OTP dalam dijabarkan melalui Persamaan 7 dan Persamaan 8 [22].

$$Ci = (Pi + Ki)\ mod\ X \quad (7)$$
$$Pi = (Ci - Ki)\ mod\ X \quad (8)$$

dimana:
$Ci = Ciphertext$
$Pi = Plaintext$
$Ki = Kunci$
$mod\ X = nilai\ maksimal\ kunci$

2.3.4 Tabel Periodik

Tabel periodik unsur berisi unsur-unsur kimia yang tersusun sesuai ketetapan nomor atom dan konfigurasi elektron. Unsur tersebut disusun berdasarkan nomer atomnya dan dibagi menjadi 2 susunan, susunan baris terdiri dari 7 periode, susunan kolom terbagi menjadi 8 golongan. Setiap unsur didaftarkan berdasarkan nomor atom dan lambang unsur [23]. Dalam tabel periodik hanya 2 kategori yang akan digunakan untuk meng-enkripsi pesan yaitu simbol dan konfigurasi elektron. Dalam penelitian ini Tabel Periodik ditambahkan 8 karakter untuk melengkapi Tabel ASCII sebanyak 126 yang akan digunakan. Adapun tabel yang akan digunakan akan ditunjukan pada Tabel 3. sebagai berikut:

Submitted: **02/06/2020**; Accepted: **09/07/2020**; Published: **20/07/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 3, Juli 2020, Page 841-849
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i3.2244

Tabel 3. Tabel Periodik

Atomic Number	Symbol	† Electron Configuration	Atomic Number	Symbol	† Electron Configuration
1	H	1s1	64	Gd	[Xe] 4f7 5d1 6s2
2	He	1s2	65	Tb	[Xe] 4f9 6s2
3	Li	[He] 2s1	66	Dy	[Xe] 4f10 6s2
4	Be	[He] 2s2	67	Ho	[Xe] 4f11 6s2
5	B	[He] 2s2 2p1	68	Er	[Xe] 4f12 6s2
6	C	[He] 2s2 2p2	69	Tm	[Xe] 4f13 6s2
7	N	[He] 2s2 2p3	70	Yb	[Xe] 4f14 6s2
8	O	[He] 2s2 2p4	71	Lu	[Xe] 4f14 5d1 6s2
9	F	[He] 2s2 2p5	72	Hf	[Xe] 4f14 5d2 6s2
10	Ne	[He] 2s2 2p6	73	Ta	[Xe] 4f14 5d3 6s2
11	Na	[Ne] 3s1	74	W	[Xe] 4f14 5d4 6s2
12	Mg	[Ne] 3s2	75	Re	[Xe] 4f14 5d5 6s2
13	Al	[Ne] 3s2 3p1	76	Os	[Xe] 4f14 5d6 6s2
14	Si	[Ne] 3s2 3p2	77	Ir	[Xe] 4f14 5d7 6s2
15	P	[Ne] 3s2 3p3	78	Pt	[Xe] 4f14 5d9 6s1
16	S	[Ne] 3s2 3p4	79	Au	[Xe] 4f14 5d10 6s1
17	Cl	[Ne] 3s2 3p5	80	Hg	[Xe] 4f14 5d10 6s2
18	Ar	[Ne] 3s2 3p6	81	Tl	[Hg] 6p1
19	K	[Ar] 4s1	82	Pb	[Hg] 6p2
20	Ca	[Ar] 4s2	83	Bi	[Hg] 6p3
21	Sc	[Ar] 3d1 4s2	84	Po	[Hg] 6p4
22	Ti	[Ar] 3d2 4s2	85	At	[Hg] 6p5
23	V	[Ar] 3d3 4s2	86	Rn	[Hg] 6p6
24	Cr	[Ar] 3d5 4s1	87	Fr	[Rn] 7s1
25	Mn	[Ar] 3d5 4s2	88	Ra	[Rn] 7s2
26	Fe	[Ar] 3d6 4s2	89	Ac	[Rn] 6d1 7s2
27	Co	[Ar] 3d7 4s2	90	Th	[Rn] 6d2 7s2
28	Ni	[Ar] 3d8 4s2	91	Pa	[Rn] 5f2 6d1 7s2
29	Cu	[Ar] 3d10 4s1	92	U	[Rn] 5f3 6d1 7s2
30	Zn	[Ar] 3d10 4s2	93	Np	[Rn] 5f4 6d1 7s2
31	Ga	[Ar] 3d10 4s2 4p1	94	Pu	[Rn] 5f6 7s2
32	Ge	[Ar] 3d10 4s2 4p2	95	Am	[Rn] 5f7 7s2
33	As	[Ar] 3d10 4s2 4p3	96	Cm	[Rn] 5f7 6d 7s2
34	Se	[Ar] 3d10 4s2 4p4	97	Bk	[Rn] 5f9 7s2
35	Br	[Ar] 3d10 4s2 4p5	98	Cf	[Rn] 5f10 7s2
36	Kr	[Ar] 3d10 4s2 4p6	99	Es	[Rn] 5f11 7s2
37	Rb	[Kr] 5s1	100	Fm	[Rn] 5f12 7s2
38	Sr	[Kr] 5s2	101	Md	[Rn] 5f13 7s2
39	Y	[Kr] 4d1 5s2	102	No	[Rn] 5f14 7s2
40	Zr	[Kr] 4d2 5s2	103	Lr	[Rn] 5f14 7s2 7p ?
41	Nb	[Kr] 4d4 5s1	104	Rf	[Rn] 5f14 6d2 7s2 ?
42	Mo	[Kr] 4d5 5s1	105	Db	
43	Tc	[Kr] 4d5 5s2	106	Sg	
44	Ru	[Kr] 4d7 5s1	107	Bh	
45	Rh	[Kr] 4d8 5s1	108	Hs	
46	Pd	[Kr] 4d10	109	Mt	
47	Ag	[Kr] 4d10 5s1	110	Ds	
48	Cd	[Kr] 4d10 5s2	111	Rg	
49	In	[Kr] 4d10 5s2 5p1	112	Cn	
50	Sn	[Kr] 4d10 5s2 5p2	113	Uut	
51	Sb	[Kr] 4d10 5s2 5p3	114	Uuq	
52	Te	[Kr] 4d10 5s2 5p4	115	Uup	
53	I	[Kr] 4d10 5s2 5p5	116	Uuh	
54	Xe	[Kr] 4d10 5s2 5p6	117	Uus	
55	Cs	[Xe] 6s1	118	Uuo	
56	Ba	[Xe] 6s2	119	!	
57	La	[Xe] 5d1 6s2	120	@	
58	Ce	[Xe] 4f1 5d1 6s2	121	#	

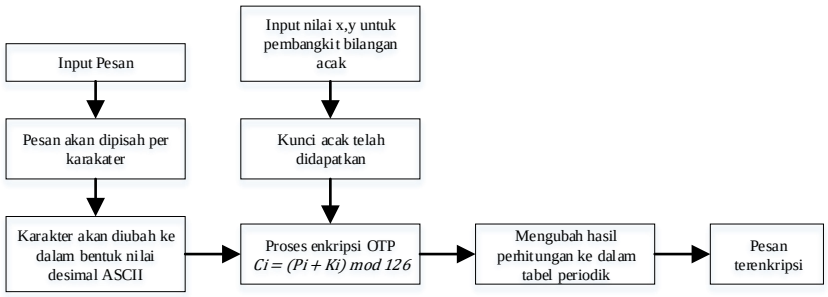
Submitted: **02/06/2020**; Accepted: **09/07/2020**; Published: **20/07/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 3, Juli 2020, Page 841-849
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i3.2244

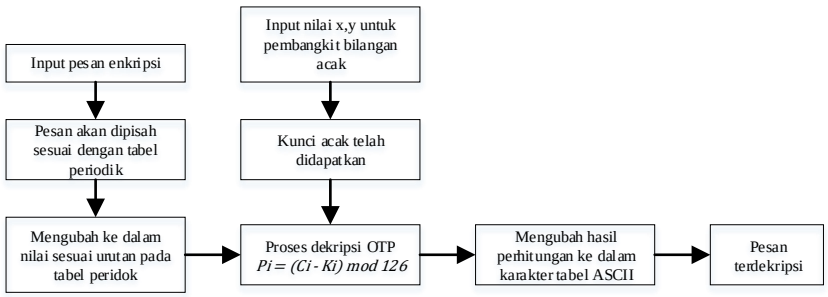
Atomic Number	Symbol	† Electron Configuration	Atomic Number	Symbol	† Electron Configuration
59	Pr	[Xe] 4f3 6s2	122	$	
60	Nd	[Xe] 4f4 6s2	123	%	
61	Pm	[Xe] 4f5 6s2	124	?	
62	Sm	[Xe] 4f6 6s2	125	&	
63	Eu	[Xe] 4f7 6s2	126	)	

3. HASIL DAN PEMBAHASAN

Pada penelitan ini alur untuk proses enkripsi dan dekripsi akan ditunjukkan pada Gambar 3. dan Gambar 4.



Gambar 3. Alur proses enkripsi pesan



Gambar 4. Alur proses dekripsi pesan

3.1 Proses Enkripsi

Berikut ini proses enkripsi dari sebuah pesan (*plaintext*) yaitu "Saya Pergi", dimana akan terlebih dahulu dibangkitkan kunci acak sepanjang *plaintext*-nya menggunakan CLCG. Proses dalam melakukan penyandian dengan menggunakan metode OTP pada Persamaan (7) dan kunci acak pada Tabel 2 akan ditunjukkan pada Tabel 4. berikut ini :

Contoh perhitungan OTP pada proses enkripsi pesan :

Diketahui karakter "S" memiliki nilai ASCII 83, dengan kunci CLCG 44, maka hasil enkripsinya adalah :

$= (83 + 44) Mod\ 126,$

$= 127\ Mod\ 126,$

$= 1, karena\ sisa\ bagi\ 127 : 126\ adalah\ 1$

Sehingga nilai 1 pada Tabel Periodik adalah He1s2

Tabel 4. Proses Enkripsi Pesan

Plaintext	ASCII	Kunci CLCG	Tabel Periodik	Enkripsi
S	83	44	1	He1s2
a	97	40	11	Mg3s2
y	121	22	17	Ar3s23p6
a	97	4	101	No5f147s2
spasi	32	126	32	As3d104s24p3
p	112	108	94	Am5f77s2
e	101	90	65	Dy4f106s2
r	114	72	60	Pm4f56s2
g	103	68	45	Pd4d10
i	105	50	29	Zn3d104s2

Submitted: **02/06/2020**; Accepted: **09/07/2020**; Published: **20/07/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 3, Juli 2020, Page 841-849
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i3.2244

Maka hasil enkripsinya adalah =
He1s2Mg3s2Ar3s23p6No5f147s2As3d104s24p3Am5f77s2Dy4f106s2Pm4f56s2Pd4d10Zn3d104s2

Adapun pengujian proses enkripsi tidak hanya dilakukan pada contoh kasus pada Tabel 4. Namun, pengujian dilakukan pada beberapa plaintext yang ditunjukkan pada Tabel 5. sebagai berikut :

Tabel 5. Proses Enkripsi

No.	Plaintext	Kunci x dan y	Ciphertext
1	Hati-Hati Akan Ada Perkumpulan Jam 12.00 Tengah Malam	X= 10 Y= 14	**Ir4f145d76s2Cf5f107s2Es5f117s2Yb4f146s2UuoP3s23p3Ti3d24s2V3d34s2O2s22p4Tc4d55s2Ce4f15d16s2Pb6p2Er4f126s2Eu4f76s2Np5f46d17s2$Al3s23p1UuoBr3d104s24p5Au4f145d106s1Pb6p2Ir4f145d76s2Dy4f106s2Ce4f15d16s2Ge3d104s24p2Cl3s23p5Ar3s23p6UusRa7s2Bk5f97s2H1s1Ga3d104s24p1Zn3d104s2Cu3d104s1O2s22p4Sb4d105s25p3Ac6d17s2Pu5f67s2Ra7s2!C2s22p2UupNp5f46d17s2Pa5f26d17s2Ta4f145d36s2Y4d15s2Ta4f145d36s2Rn6p6Ir4f145d76s2Te4d105s25p4Mo4d55s1Ga3d104s24p1Ho4f116s2Pu5f67s2DsLr5f147s27p?W4f145d46s2Pb6p2**
2	Terima Kasih	X=25 Y=20	**I4d105s25p5Te4d105s25p4Ag4d105s1Se3d104s24p4Ca4s2UuhAg4d105s1Hf4f145d26s2Os4f145d66s2Os4f145d66s2Sm4f66s2Tc4d55s2**
3	Awas!	X=2 Y=27	**Th6d27s2)Rn6p6Fm5f127s2)**

3.2 Proses Dekripsi

Dalam melakukan proses pengembalian *ciphertext* menjadi *plaintext* dapat dilihat pada Persamaan 2.8, kunci yang akan digunakan sama dengan proses enkripsi dengan menggunakan CLCG yang terdapat pada Tabel 2. Cara memisahkan *ciphertext* untuk 1 (satu) karakter yang selanjutnya akan diubah menjadi nilai, dengan cara memotong akhir nilai sebelum huruf kapital dalam ciphertext. Berikut ini pada Tabel 6. merupakan proses dekripsi nya.

Diketahui Ciphertext He1s2 memiliki nilai 1 pada Tabel Periodik dengan kunci yang sama seperti proses enkripsi 44, maka perhitungan proses dekripsinya sebagai berikut :

$= (1 - 44)\ Mod\ 126,$
$= -43\ Mod\ 126,$
$= 83, karena\ sisa\ bagi - 43{:}\ 126\ adalah\ 83$

Sehingga nilai ASCII 83 adalah karakter “S”

Tabel 6. Proses Dekripsi Pesan

Ciphertext	Tabel Periodik	Kunci CLCG	ASCII	Plaintext
He1s2	1	44	83	S
Mg3s2	11	40	97	a
Ar3s23p6	17	22	121	y
No5f147s2	101	4	97	a
As3d104s24p3	32	126	32	spasi
Am5f77s2	94	108	112	p
Dy4f106s2	65	90	101	e
Pm4f56s2	60	72	114	r
Pd4d10	45	68	103	g
Zn3d104s2	29	50	105	i

Maka hasil enkripsinya adalah = Saya pergi.

Adapun proses dekripsi yang dilakukan dari Tabel 5. akan ditunjukkan pada Tabel 7.

Tabel 7. Proses Dekripsi

No.	Ciphertext	Kunci x dan y	Plaintext
1	**Ir4f145d76s2Cf5f107s2Es5f117s2Yb4f146s2UuoP3s23p3Ti3d24s2V3d34s2O2s22p4Tc4d55s2Ce4f15d16s2Pb6p2Er4f126s2Eu4f76s2Np5f46d17s2$Al3s23p1UuoBr3d104s24p5Au4f145d106s1Pb6p2Ir4f145d76s2Dy4f106s2Ce4f15d16s2Ge3d104s24p2Cl3s23p5Ar3s23p6UusRa7s2Bk5f97s2H1s1Ga3d104s24p1Zn3d104s2Cu3d10**	X= 10 Y= 14	Hati-Hati Akan Ada Perkumpulan Jam 12.00

Submitted: **02/06/2020**; Accepted: **09/07/2020**; Published: **20/07/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 3, Juli 2020, Page 841-849
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i3.2244

	4s1O2s22p4Sb4d105s25p3Ac6d17s2Pu5f67s2Ra7s2!C2s22p2Up Np5f46d17s2Pa5f26d17s2Ta4f145d36s2Y4d15s2Ta4f145d36s2R n6p6Ir4f145d76s2Te4d105s25p4Mo4d55s1Ga3d104s24p1Ho4f11 6s2Pu5f67s2DsLr5f147s27p?W4f145d46s2Pb6p2		Tengah Malam
2	**I4d105s25p5Te4d105s25p4Ag4d105s1Se3d104s24p4Ca4s2UuhA g4d105s1Hf4f145d26s2Os4f145d66s2Os4f145d66s2Sm4f66s2Tc4 d55s2**	X=25 Y=20	Terima Kasih
3	**Th6d27s2)Rn6p6Fm5f127s2)**	X=2 Y=27	Awas!

4. KESIMPULAN

Bedasarkan dari perhitungan proses enkripsi dan dekripsi, penggunaan algoritma OTP tidak perlu memasukkan banyak kunci untuk proses tersebut. Adapun jumlah kunci yang dimasukkan hanya nilai x dan y sebagai nilai untuk membangkitkan bilangan acak menggunakan algoritma CLCG. Implementasi algoritma CLCG pada proses pembangkitan kunci acak terbukti tidak terjadi perulangan nilai yang sama pada karakter yang sama yang berdekatan, hal ini dikarenakan penentuan nilai a, b, dan m dan juga dalam penggunaan matrik. Modifikasi dengan menggunakan tabel periodik sangat membantu untuk dalam proses enkripsi, sehingga hasil enkripsi yang didapatkan cukup sulit untuk dipecahkan karena dalam proses enkripsi satu karakter plaintext digantikan dengan beberapa karakter pada ciphertext.

REFERENCES

[1] A. Liliwer, Komunikasi Serba Ada Serba Makna, Kencana, 2010.
[2] S. M. Suryanto, Pengantar Ilmu Komunikasi, Bandung: CV. Pustaka Setia, 2015.
[3] R. Aulia, "Pemanfaatan Website Sebagai Sarana Managing Data Dalam Suatu Organisasi (Studi Kasus: Pertemuan Ilmiah Nasional (Pin) Perhimpunan Dokter Spesialis Saraf Indonesia (Perdossi) 2013 Medan)," InfoTekJar: Jurnal Nasional Informatika dan Teknolologi Jaringan, vol. I, no. 1, pp. 1-6, 2016.
[4] P. Utomo, Sapriadi dan M. Zarlis, "Algoritma Split-Merge One Time Pad Dalam Peningkatan Enkripsi Data," dalam Seminar Nasional Teknologi Informatika (SEMANTIKA), 2017.
[5] E. H. Houssein, A. A. Mona dan A. E. Hassanien, "An image steganography algorithm using haar discrete wavelet transform with advanced encryption system," dalam Federated Conference on Computer Science and Information Systems (FedCSIS)., 2016.
[6] E. H. Rachmawanto dan C. A. Sari, "A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size," dalam International Seminar on Application for Technology of Information and Communication (iSemantic), 2017.
[7] H. A. Elsayed, Y. K. Jadaan dan S. K. Guirguis, "Image security using quantum Rivest-Shamir-Adleman cryptosystem algorithm and digital watermarking.," dalam Progress in Electromagnetic Research Symposium (PIERS)., 2016.
[8] D. Ariyus, Kriptografi Keamanan Data dan Komunikasi, Yogyakarta: Graha Ilmu, 2006.
[9] I. Wibowo, Susanto dan J. Karel, "Penerapan Algoritma Kriptografi Asimetris RSA untuk Keamanan Data di Oracle," Jurnal Informatika, vol. 1, no. 5, 2011.
[10] Saha, B. Jyoti, K. K. Kabi dan C. Pradhan, "Non blind watermarking technique using enhanced one time pad in DWT domain," dalam Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2014.
[11] J. Clawdia, N. Khairina dan M. K. Harahap, "Implementasi Algoritma Kriptografi One Time Pad (OTP) Dengan Dynamic Key Linear Congruential Generator (LCG)," dalam KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), 2017.
[12] K. B. Boateng dan A. H. Lashkari, "Securing GOOSE : The Return of One-Time Pads," dalam International Carnahan Conference on Security Technology (ICCST), Chennai, 2019.
[13] N. Khairina, M. K. Harahap, A. M. Husein, Muhathir dan R. Muliono, "Secure Data Encryption Through Combination of RSA Cryptography Random Key Algorithm and Quadratic Congruential Generator," dalam Journal of Physics: Conference Series, 2019.
[14] R. Aulia, A. Zakir dan M. Zulhafiz, "Penerapan Algoritma One Time Pad & Linear Congruential Generator Untuk Keamanan Pesan Teks," InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan, vol. 4, no. 1, 2019.
[15] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif, dan Kombinasi, Bandung: Alfa Beta, 2012.
[16] J. E. kaufmann dan K. L. Schwitters, Algebra for college students., Cengage Learning, 2014.
[17] I. M. D. Biantara, I. M. Sudana, A. F. Suni, Suyono dan A. Hangga, "Modifikasi Metode Linear Congruential Generator Untuk Optimalisasi Hasil Acak.," dalam Seminar Nasional Informatika (SEMNASIF), Yogyakarta, 2015.
[18] E. H. Rachmawanto dan C. A. Sari, "Secure image steganography algorithm based on dct with otp encryption.," Journal of Applied Intelligent System, vol. II, no. 1, pp. 1-11, 2017.
[19] O. Tornea, M. E. Borda, V. Pileczki dan R. Malutan, "DNA Vernam cipher.","," dalam E-Health and Bioengineering Conference (EHB), 2011.
[20] C. A. Sari dan E. H. Rachmawanto, "Gabungan Algoritma Vernam Chiper dan End of File Untuk Keamanan Data.," Jurnal Teknologi Informasi, vol. XIII, no. 3, pp. 150-157, 2014.

Submitted: **02/06/2020**; Accepted: **09/07/2020**; Published: **20/07/2020**

JURNAL MEDIA INFORMATIKA BUDIDARMA
Volume 4, Nomor 3, Juli 2020, Page 841-849
ISSN 2614-5278 (media cetak), ISSN 2548-8368 (media online)
Available Online at https://ejurnal.stmik-budidarma.ac.id/index.php/mib
DOI 10.30865/mib.v4i3.2244

[21] R. Shukla, H. O. Prakash, R. P. Bhushan, S. Venkataraman dan G. Varadan, "Sampurna Suraksha: unconditionally secure and authenticated one time pad cryptosystem.," dalam International Conference on Machine Intelligence and Research Advancement, India, 2013.
[22] D. R. I. M. Setiadi, E. H. Rachmawanto dan C. A. Sari, "Implementasi One Time Pad Kriptografi Pada Gambar Grayscale Dan Gambar Berwarna.," dalam Proceeding SENDI_U, Semarang, 2017.
[23] R. Chang, Kimia Dasar : Konsep - Konsep Inti, Jakarta: Erlangga, 2005.

Submitted: **02/06/2020**; Accepted: **09/07/2020**; Published: **20/07/2020**