Buletin Ilmiah Sarjana Teknik Elektro
Vol. 3, No. 3, Desember 2021, pp. 194-201
ISSN: 2685-9572, DOI: 10.12928/biste.v3i3.5546

Enkripsi Pesan Menggunakan Algoritma Linear Congruential Generator (LCG) dan Konversi Kode Morse

Deny Nugroho Triwibowo [1], Purwono [2], Imam Ahmad Ashari [3], Arif Setia Sandi [4], Yusuf Fadlila Rahman [5]
[1,3,4] Program Studi Teknologi Informasi, Universitas Harapan Bangsa, Indonesia
[2] Program Studi Informatika, Universitas Harapan Bangsa, Indonesia
[5] D3 Teknik Informatika, Sekolah Vokasi, Universitas Sebelas Maret Surakarta, Indonesia

INFORMASI ARTIKEL

Riwayat Artikel:

Dikirimkan 10 Januari 2022
Direvisi 01 Februari 2022
Diterima 14 Maret 2022

Kata Kunci:

Enkripsi;
Linear Congruential Generator (LCG);
Kode Morse

Penulis Korespondensi:

Deny Nugroho Triwibowo,
Program Studi Teknologi Informasi, Universitas Harapan Bangsa
Jalan Raden Patah No. 100, Ledug, Kembaran, Banyumas, Jawa Tengah, Indonesia.
Surel: denynugroho@uhb.ac.id

ABSTRACT / ABSTRAK

Message is an expression that is formed from a thought and feeling, reality, opinion, experience that has happened or will come, and so on. Currently, the exchange of information carried out by both the sender and the recipient has used several social media applications, such as whatsapp, telegram, line, and many more. Messages sent and received through social media applications must be connected to the internet network for the communication process in which the message can be stolen by irresponsible parties, because these parties are also connected to the same internet network. One way that can be done so that the message sent is maintained and more secure, the process of securing the data and information contained in the message is carried out. The Linear Congruential Generator (LCG) algorithm will generate a random key value and convert it into Morse code form. The results obtained from the modification of the LCG algorithm and Morse code are very helpful in the encryption process which makes the encryption results obtained quite difficult to solve because in the encryption process one plaintext character is replaced with a dot sign (.) and a minus sign (-) on the ciphertext.

Pesan merupakan ungkapan yang terbentuk dari suatu pemikiran dan perasaan, realita, opini, pengalaman yang sudah terjadi atau yang akan datang, dan lain sebagainya. Saat ini pertukaran informasi yang dilakukan baik pengirim dan penerima sudah menggunakan beberapa aplikasi media sosial, seperti *whatsapp, telegram, line*, dan masih banyak lagi. Pesan yang dikirim dan diterima melalui aplikasi media sosial harus terhubung dengan jaringan internet untuk proses komunikasinya yang di mana pesan tersebut dapat dicuri oleh pihak yang tidak bertanggungjawab, dikarenakan pihak-pihak tersebut juga terhubung pada jaringan internet yang sama. Salah satu cara yang dapat dilakukan agar pesan yang dikirimkan terjaga dan lebih aman, dilakukan proses pengamanan data dan informasi yang ada di dalam pesan tersebut. Algoritma *Linear Congruential Generator* (LCG) akan menghasilkan nilai kunci secara acak dan dikonversi ke dalam bentuk kode morse. Hasil yang didapatkan dari modifikasi algoritma LCG dan konversi kode morse dapat membantu untuk proses kriptografi yang membuat hasil enkripsi pesan cukup susah untuk dibaca karena dalam proses enkripsi pesan tiap-tiap karakter *plaintext* akan dikonversikan dengan tanda titik (.) dan tanda kurang (-) pada *cipherteks*nya.

Sitasi Dokumen ini:

D. N. Triwibowo, Purwono, I. A. Ashari, and A. S. Sandi, Y. F. Rahman, "Enkripsi Pesan Menggunakan Algoritma Linear Congruential Generator (LCG) dan Konversi Kode Morse," *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 3, no. 3, pp. 194-201, 2021. DOI: 10.12928/biste.v3i3.5546

1. PENDAHULUAN

Semakin berkembangnya teknologi informasi telah membuat komunikasi menjadi sangat penting untuk semua orang dalam bertukar informasi melalui pesan dengan mudah dan cepat [1]. Pesan merupakan ungkapan yang terbentuk dari suatu pemikiran dan perasaan, realitas, opini, pengalaman yang telah dilalui atau peristiwa yang akan terjadi, dan lain sebagainya. Pesan dapat tersampaikan dengan cara bertemu secara langsung atau dengan aplikasi media komunikasi yang tersedia. Isi dari sebuah pesan bisa saja berupa suatu informasi, hiburan, ilmu pengetahuan, nasihat ataupun semacam hasutan [2]. Untuk itu, keberhasilan dari komunikasi yang terjadi terletak pada bagaimana seorang komunikan dapat memahami konteks dari pesan yang disampaikan oleh komunikator [3].

Pada dasarnya manusia adalah makhluk sosial, yang di mana setiap orang hidup dalam suatu kelompok masyarakat, dalam melakukan aktivitas kesehariannya sejak terbangun dari tidur di pagi hari sampai akan kembali tidur di malam harinya, orang - orang senantiasa terlibat dalam melakukan pertukaran informasi. Saat ini pertukaran informasi yang dilakukan baik pengirim dan penerima sudah menggunakan beberapa aplikasi media sosial, seperti *whatsapp, telegram, line*, dan masih banyak lagi [4]. Pesan yang dikirim dan diterima melalui aplikasi media sosial harus terhubung dengan jaringan internet untuk proses komunikasinya yang di mana pesan tersebut dapat dicuri oleh pihak yang tidak bertanggungjawab, dikarenakan pihak-pihak tersebut juga terhubung pada jaringan internet yang sama [5].

Salah satu cara yang dapat dilakukan agar pesan yang dikirimkan terjaga dan lebih aman, dilakukan proses pengamanan data dan informasi yang ada di dalam pesan tersebut [6]. Adapun teknik pengaman data yang banyak digunakan adalah teknik kriptografi. Kriptografi adalah teknik yang memiliki ruang lingkup untuk mempelajari tentang bagaimana cara mengamankan suatu data atau informasi agar tidak mengalami gangguan yang dilakukan oleh pihak ketiga, yang bertujuan agar dapat menjaga kerahasiaannya [7].

Ada beberapa algoritma atau metode yang digunakan dalam melakukan teknik pengamanan pesan, salah satunya algoritma *Linear Congruential Generator* (LCG). Algoritma LCG dapat menghindari penggunaan nilai kunci acak yang dilakukan secara berulang dengan menentukan nilai a, b, dan modulusnya. Lebih lanjut lagi dengan menggunakan algoritma LCG sebagai pembangkit bilangan acak semu diharapkan dapat menyulitkan pihak ketiga jika ingin memecahkan kode-kode dalam proses pengamanan data [8].

Penelitian yang dilakukan [9] dengan pengacakan nilai menggunakan algoritma LCG untuk memasukkan karakter ke dalam objek gambar dengan metode MSB didapatkan hasil nilai kompresi gambar yang berbeda yang tidak mendominasi seluruh bagian warna karena ukuran data menjadi lebih besar. Penelitian lainnya [10] dengan mengombinasikan algoritma LCG dan algoritma *The Sieve of Eratosthenes* pengujian berhasil mendapatkan kunci *public* dan *private* lebih dari satu nilai prima untuk digunakan pada algoritma RSA. Sehingga penggunaan LCG dapat membantu dalam menghasilkan nilai kunci secara acak agar data dapat terjaga kerahasiannya [11].

Berdasarkan dari beberapa penelitian sebelumnya tentang algoritma LCG, penelitian ini akan berkontribusi untuk pemilihan algoritma terbaik sebagai pembangkit bilangan acak untuk mengamankan data dan informasi dengan proses enkripsi dan deskripsi yang dilakukan. Hasil nilai yang didapatkan dari perhitungan algoritma LCG, selanjutnya akan dikonversi ke dalam bentuk kode morse, sehingga diharapkan hasil dari proses enkripsi data sulit untuk dipecahkan.

2. METODE PENELITIAN

Metode penelitian adalah langkah-langkah yang dapat digunakan untuk menyelesaikan suatu masalah yang terjadi dalam melakukan penelitian dengan mengikuti ketentuan yang dilakukan oleh peneliti agar tujuan yang diinginkan tercapai dan mendapatkan hasil pengujian atas masalah yang diangkat [12]. Berikut merupakan alur metode penelitian yang digunakan seperti pada Gambar 1.

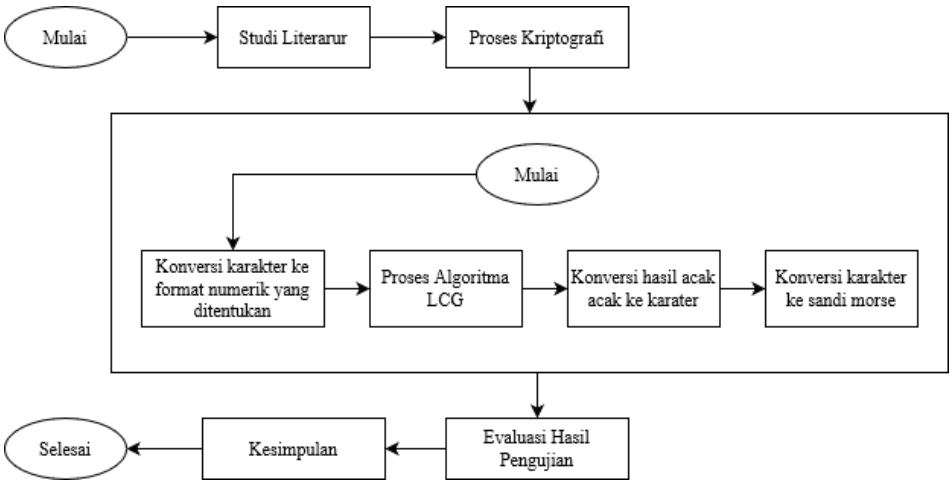
2.1. Studi Literatur

Menurut Arikunto [13] "studi literatur merupakan cara pandang dalam membentuk suatu kajian teoritis dan referensi lain yang memiliki kaitannya dengan nilai, budaya dan norma yang berkembang pada situasi sosial yang sedang diteliti secara menggeneralisasi. Selain itu, studi literatur sangat penting dalam melakukan suatu penelitian, hal ini dikarenakan teori – teori tentang penelitian yang dilakukan diperoleh melalui serangkaian proses ilmiah dan teori tersebut harus dapat diuji keasliannya."

2.2. Proses Kriptografi

Kriptografi merupakan penamaan dari bahasa Yunani yang terdiri dari kata *kryptós* yang memiliki arti rahasia, dan *graphein* yang memiliki arti tulisan. Maka dari itu dapat dikatakan secara sederhananya bahwa proses Kriptografi merupakan suatu bidang ilmu atau seni yang mempelajari tentang cara bagaimana merahasiakan sebuah pesan atau tulisan yang berisi data dan informasi secara aman dan rahasia [14]. Proses

Kriptografi sendiri memiliki dua teknik, yaitu teknik enkripsi dan teknik deskripsi. Teknik enkripsi merupakan proses bagaimana mengubah pesan asli dari suatu data atau informasi (*plaintext*) menjadi pesan yang susah untuk dibaca (*ciphertext*), sedangkan teknik deskripsi merupakan kebalikan teknik enkripsi yaitu mengubah pesan yang sulit untuk dibaca (*ciphertext*) menjadi pesan asli (*plaintext*). Untuk saat ini proses kriptografi menjadi bagian terpenting untuk keamanan dan jaringan komputer karena yang menjadi keistimewaan dari teknik keduanya adalah bagaimana menyediakan data ataupun informasi yang dibutuhkan tanpa mendapat gangguan dari pihak ketiga [15].



Gambar 1. Alur Metode Penelitian

Menurut Long dan Chen [16] protokol kriptografi dapat dikelompokkan ke dalam empat bidang, antara lain:

- Enkripsi Simetrik: Enkripsi ini digunakan untuk menyembunyikan suatu aliran data dari berbagai macam ukuran, termasuk pesan, file, kunci enkripsi, dan kata sandi.
- Enkripsi asimetris: Enkripsi ini digunakan untuk menyembunyikan blok data kecil, seperti kunci enkripsi dan nilai fungsi hash, yang digunakan dalam tanda tangan digital.
- Algoritma integritas data: Digunakan untuk melindungi blok data, seperti pesan, dari perubahan.
- Protokol otentikasi: Ini adalah skema berdasarkan penggunaan algoritma kriptografi yang dirancang untuk mengotentikasi identitas pihak yang memiliki wewenang.

2.2.1 Konversi Karakter ke Numerik

Dalam tahap ini akan ditentukan karakter – karakter yang dapat dimasukkan ke dalam pesan plaintext yang selanjutnya akan dikonversikan ke dalam numerik atau nilai untuk merepresentasikan karakter – karakter tersebut seperti pada Tabel 1.

Tabel 1. Karakter ke Numerik

Karakter	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Numerik	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Karakter	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0
Numerik	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

2.2.2 Algoritma *Linear Congruential Generator* (LCG)

Algoritma LCG merupakan metode *Pseudo Random Number Generator* (PRNG) atau pembangkit bilangan acak semu yang tertua dan paling popular [17]. Algoritma LCG diperkenalkan pertama kali oleh seorang peneliti bernama D. H. Lehmer pada tahun 1951 [18]. Sederhananya rumus algoritma LCG sebagai berikut:

$$X_{n+1} = (aX_n + b) mod\ m \quad (1)$$

Dengan

X_{n+1} = nilai acak ke- (n+1) dari urutannya
X_n = nilai acak ke-n dari urutannya
a = faktor pengali
b = increment
m = modulus

Algoritma LCG memiliki deretan penuh (m - 1) jika semua syarat di bawah ini terpenuhi, antara lain :

- b relatif prima terhadap m.
- a dapat dibagi dengan semua faktor prima dari m.
- a merupakan kelipatan 4 jika m merupakan kelipatan 4.
- m > maksimal (a, b, $X0$).
- $m > 0$, $b > 0$.

Contoh hasil perhitungan pembangkit bilangan acak semu dengan LCG sebanyak 36 kali dengan menggunakan persamaan 1 sebagai berikut.
Diketahui:
$a = 1$, $b = 19$, $m = 36$, $X0 = 0$

Tabel 2. Perhitungan LCG

Xn	X0	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10	X11	X12	X13	X14
Nilai Acak Semu	19	2	21	4	23	6	25	8	27	10	29	12	31	14	33
Xn	X15	X16	X17	X18	X19	X20	X21	X22	X23	X24	X25	X26	X27	X28	X29
Nilai Acak Semu	16	35	18	1	20	3	22	5	24	7	26	9	28	11	30
Xn	X30	X31	X32	X33	X34	X35									
Nilai Acak Semu	13	32	15	34	17	0									

2.2.3 Konversi Karakter ke Kode Morse

Kode Morse merupakan suatu teknik pengiriman informasi berupa teks dalam deretan nada *on-off*, cahaya, atau klik yang secara langsung dapat dipahami oleh pendengar atau pengawas yang berpengalaman tanpa menggunakan alat yang khusus [19]. Dinamakan kode morse berdasarkan oleh penemunya, yaitu Samuel F. B. Morse [20]. Kode morse internasional akan menyandikan huruf latin dasar, beberapa huruf latin spesial, angka *Arabic*, dan *prosigns* yang memiliki standarisasi deretan signal pendek dan panjang yang dinamai sebagai titik dan garis (*dots and dashes*). Setiap simbol pada kode morse akan menggambarkan sebuah huruf karakter (teks atau angka) atau *prosigns*. Jangka waktu lamanya suatu signal panjang yang berbentuk *dashes*/garis merupakan tiga kalinya dari jangka waktu *dots*/titik. Jarak antar *dashes/ dots* adalah satu garis [21]. Dalam menulis kode morse untuk memisahkan setiap huruf diberi tanda garis miring satu (/) dan saat spasi kata diberi tanda garis miring dua (//). Adapun kode morse yang digunakan akan ditunjukkan pada Tabel 3.

Tabel 3. Kode Morse

Karakter	Kode Morse	Karakter	Kode Morse	Karakter	Kode Morse
A	.-	M	--	Y	-.--
B	-…	N	-.	Z	--..
C	-.-.	O	---	1	.----
D	-..	P	.--.	2	..---
E	.	Q	--.-	3	…--
F	..-.	R	.-.	4	….-
G	--.	S	…	5	…..
H	….	T	-	6	-….
I	..	U	..-	7	--…
J	.---	V	…-	8	---..
K	-.-	W	.--	9	----.
L	.-..	X	-..-	0	-----

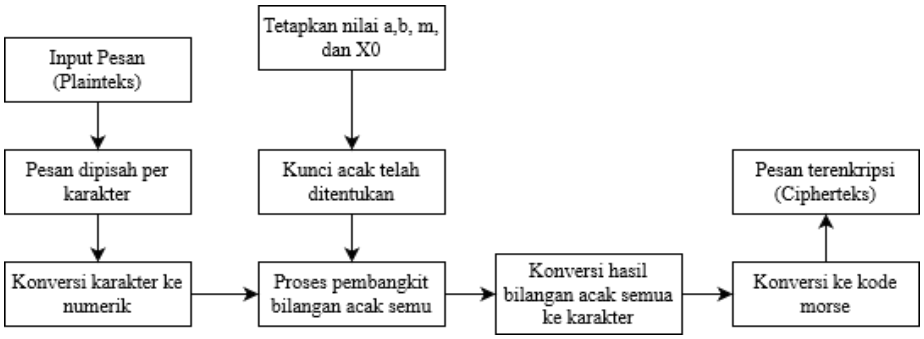
Berikut ini akan diberikan contoh bagaimana cara mengonversi kata dengan menggunakan kode morse, seperti kata:
KAMPUS MERDEKA = -.-/.-/--/.--./..-/…//--/./.-./-.././-.-/.-

3. HASIL DAN PEMBAHASAN

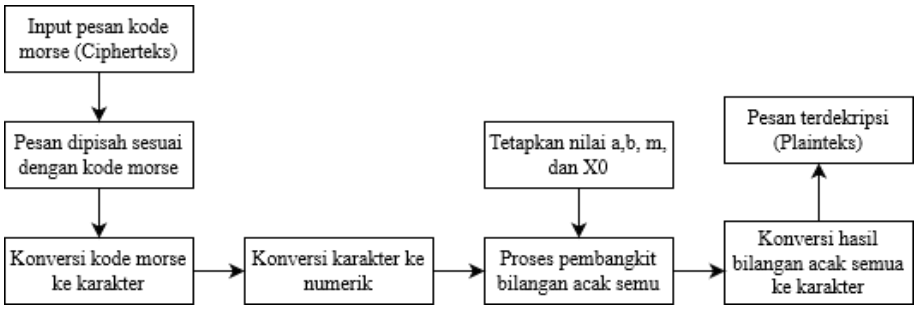
Pada tahap ini akan melakukan pengujian untuk mendapatkan hasil penelitian yang sesuai dengan alur penelitian dari proses teknik enkripsi dan deskripsi yang akan ditunjukkan pada Gambar 2 dan Gambar 3.

Pada Gambar 2. Akan menjelaskan bagaimana proses enkripsi terjadi, dari pesan yang dapat dibaca atau *plaintext* menjadi sebuah pesan yang susah untuk dibaca atau *ciphertext*. Pertama – tama melakukan inputan pesan dan menentukan nilai kunci yang akan menjadi pembangkit bilangan acak. Pesan yang telah diinputkan akan dipisah per karakternya, lalu akan dikonversikan ke bentuk numerik yang selanjutnya akan diolah menggunakan rumus algoritma LCG sesuai dengan persamaan 1. Ketika hasil perhitungan telah didapatkan,

hasilnya akan kembali dikonversikan ke dalam bentuk karakter. Langkah terakhir adalah hasil dari konversi karakter tersebut akan dikonversikan kembali ke dalam bentuk kode morse yang akan menjadi sebuah pesan ciphertext.



Gambar 2. Alur Enkripsi Pesan



Gambar 3. Alur Deskripsi Pesan

Sedangkan Pada Gambar 2. Akan menjelaskan bagaimana proses deskripsi terjadi, dari pesan yang tidak susah dibaca atau ciphertext menjadi sebuah pesan yang dapat dibaca atau palintext. Pertama – tama melakukan inputan kode morse *ciphertext* dan menentukan nilai kunci yang sama pada proses enkripsi yang di mana akan menjadi pembangkit bilangan acak. Kode morse yang telah diinputkan akan dipisah per karakternya dengan tanda garis miring (/), lalu kode morse akan dikonversikan ke bentuk numerik yang selanjutnya akan diolah menggunakan rumus algoritma LCG sesuai dengan persamaan 1. Langkah terakhir adalah hasil dari perhitungan yang didapatkan akan dikonversikan ke dalam bentuk karakter, sehingga pesan akan kembali menjadi pesan yang dibaca oleh penerima pesan.

3.1. Proses Enkripsi Pesan

Pada tahap ini akan dilakukan proses enkripsi pesan (*plaintext*) yaitu "WASPADA JAM 9 MALAM", di mana terlebih dahulu pesan dipisah per karakter dan diubah ke dalam bentuk numerik yang terdapat pada Tabel 1 untuk ditemukan nilai acaknya menggunakan algoritma LCG. Proses untuk melakukan enkripsi pesan dengan perhitungan yang terdapat di Tabel 2 dan hasilnya dapat dilihat pada Tabel 4.

Tabel 4. Hasil Enkripsi Pesan

Plainteks	Numerik	Nilai LCG	Karakter	Kode Morse
W	22	5	F	..-.
A	0	19	T	-
S	18	1	B	-...
P	15	16	Q	--.-
A	0	19	T	-
D	3	4	E	.
A	0	19	T	-
Spasi	//	//	//	//
J	9	10	K	-.-
A	0	19	T	-
M	12	31	6	-....
Spasi	//	//	//	//
9	34	17	R	.-.
Spasi	//	//	//	//
M	12	31	6	-....
A	0	19	T	-

Plainteks	Numerik	Nilai LCG	Karakter	Kode Morse
L	11	12	L	.-..
A	0	19	T	-
M	12	31	6	-….

Dari teknik kriptografi yang dilakukan, maka hasil proses enkripsi dari pesan *plaintext* "WASPADA JAM 9 MALAM" yaitu = **..-./-/-…/--.-/-/./-//-.-/-/-….//.-.//-….-/-/.-../-/-….**

Selain dari pengujian yang dilakukan pada percobaan contoh kasus di Tabel 4. Pengujian juga dilakukan untuk beberapa pesan *plaintext* untuk mengetahui hasil proses enkripsi pesannya yang terdapat di Tabel 5.

Tabel 5. Teknik Enkripsi Pesan

No.	Plainteks	Cipherteks (Kode Morse)
1	JANGAN PERGI DULU	-.-/-/---/--../-/---//--.-/-..-/…/--../..---//./-../--/-..
2	1 JAM LAGI PINTU DIBUKA	.---//-.-/-/-….//--/-/--../..---//--.-/..---/---/..-/-..//./..---/-.-/-../….-/-
3	HATI HATI PENYERGAPAN DIARAH JAM 12	../-/..-/..---//../-/..-/..---//--.-/-..-/---/…/-..-/…/--../-/--.-/-/---//./..---/-/…/-/..//-.-/-/-….//.---/…--
4	CARI 36 PASUKAN TAMBAHAN	…-/-/…/..---//.-../--…//--.-/-/-…/-../….-/-/---//..-/-/-….-/-.-./-/../-/---
5	9 KG BERAT DAGING ITU	.-.//….-/--..//-.-./-..-/…/-/..-//./-/--../..---/---/--..//..---/../-/-..

3.2. Proses Deskripsi

Pada tahap ini akan dilakukan proses pengembalian dari pesan *ciphertext* (kode morse) menjadi sebuah pesan yang dapat terbaca oleh pengguna (*plaintext*) dengan menggunakan algoritma LCG yang terdapat pada Tabel 2, di mana *ciphertext* akan dipisah – pisah terlebih dahulu dan akan dikonversi ke karakter lalu ke numerik sesuai yang ditunjukkan di Tabel 1. Berikut ini merupakan hasil proses deskripsi pesan yang terdapat di Tabel 6.

Tabel 6. Hasil Dekripsi Pesan

Kode Morse	Karakter	LCG	Numerik	Plainteks
..-.	F	5	22	W
-	T	19	0	A
-…	B	1	18	S
--.-	Q	16	15	P
-	T	19	0	A
.	E	4	3	D
-	T	19	0	A
//	//	//	//	Spasi
-.-	K	10	9	J
-	T	19	0	A
-….	6	31	12	M
//	//	//	//	Spasi
.-.	R	17	34	9
//	//	//	//	Spasi
-….	6	31	12	M
-	T	19	0	A
.-..	L	12	11	L
-	T	19	0	A
-….	6	31	12	M

Dari teknik kriptografi yang dilakukan, maka hasil proses deskripsi dari pesan *ciphertext* **..-./-/-…/--.-/-/./-//-.-/-/-….//.-.//-….-/-/.-../-/-….** yaitu = "WASPADA JAM 9 MALAM"

Selain pengujian dari proses dekripsi yang dilakukan terhadap contoh kasus di Tabel 6. Pengujian juga dilakukan terhadap pesan *ciphertext* yang terdapat pada Tabel 5. untuk membuktikan bahwa *ciphertext*nya akan kembali seperti semula (*plaintext*) yang ditunjukkan di Tabel 7.

Tabel 7. Teknik Deskripsi Pesan

No.	Cipherteks (Kode Morse)	Plainteks
1	-.-/-/---/--../-/---//--.-/-..-/…/--../..---//./-../--/-..	JANGAN PERGI DULU
2	.---//-.-/-/-….//--/-/--../..---//--.-/..---/---/..-/-..//./..---/-.-/-../….-/-	1 JAM LAGI PINTU DIBUKA
3	../-/..-/..---//../-/..-/..---//--.-/-..-/---/…/-..-/…/--../-/--.-/-/---//./..---/-/…/-/..//-.-/-/-….//.---/…--	HATI HATI PENYERGAPAN DIARAH JAM 12
4	…-/-/…/..---//.-../--…//--.-/-/-…/-../….-/-/---//..-/-/-….-/-.-./-/../-/---	CARI 36 PASUKAN TAMBAHAN
5	.-.//….-/--..//-.-./-..-/…/-/..-//./-/--../..---/---/--..//..---/../-/-..	9 KG BERAT DAGING ITU

4. KESIMPULAN

Berdasarkan dari hasil pengujian teknik kriptografi mulai dari enkripsi dan dekripsi pesan yang dilakukan dengan menggunakan algoritma LCG sebagai pembangkit bilangan acak semu, menghasilkan nilai acak deret yang berbeda. Hal ini disebabkan oleh masukan bilangan a, b, dan m sesuai dengan ketentuan atau syarat-syarat perhitungan algoritma LCG, sehingga deret nilai acak yang dihasilkan tidak ada yang berurutan atau berulang sampai dengan nilai maksimal modulus yang dimasukkan. Penambahan metode dengan mengkonversi hasil dari nilai acak ke kode morse sangat membantu dalam proses enkripsi yang dilakukan. Sehingga membuat hasil enkripsi yang didapatkan menyulitkan pihak-pihak yang tidak berwenang untuk membacanya karena dalam proses enkripsi pesan, tiap-tiap karakter dari plaintext akan dikonversikan dengan hanya tanda titik (.) dan/atau tanda kurang (-) pada cipherteksnya.

REFERENSI

[1] A. I. Warnilah and S. N. Nugraha, "Komparasi Algoritma Kriptografi Elgamal Dan Caesar Cipher Untuk Enkripsi Dan Dekripsi Pesan," *IJCIT (Indonesian Journal on Computer and Information Technology)*, vol. 3, no. 2, pp. 243–252, 2018, https://ejournal.bsi.ac.id/ejurnal/index.php/ijcit/article/view/4671.

[2] A. Liliweri, *Komunikasi Serba Ada Serba Makna*. Jakarta: Kencana Predana Media, 2011.

[3] S. N. Paramasari and A. Nugroho, "Strategi Komunikasi Kesehatan dalam Upaya Membangun Partisipasi Publik pada Masa Pandemi Covid-19," *J. Lensa Mutiara Komun.*, vol. 5, no. 1, pp. 123–132, 2021, https://doi.org/10.51544/jlmk.v5i1.2036.

[4] Z. F. Nurhadi and A. W. Kurniawan, "Kajian Tentang Efektivitas Pesan Dalam Komunikasi," *J. Komun. Has. Pemikir. dan Penelit.*, vol. 3, no. 1, pp. 90–91, 2017, https://journal.uniga.ac.id/index.php/JK/article/view/253.

[5] M. Agung, R. Roslina, and R. E. Sari, "Implementasi Aplikasi Pembuatan Chat," *Jurnal Mahasiswa Fakultas Teknik Dan Ilmu Komputer*, vol. 1, no. 1, pp. 293–306, 2019, https://www.e-journal.potensi-utama.ac.id/ojs/index.php/FTIK/article/view/866.

[6] D. N. Triwibowo and D. Ariyus, "Penerapan Algoritma Coupled Linear Congurential Generator (CLCG) pada Algortima Kriptografi One Time Pad (OTP) dalam Proses Mengamankan Pesan," *J. Media Inform. Budidarma*, vol. 4, no. 3, p. 841, 2020, https://doi.org/10.30865/mib.v4i3.2244.

[7] H. Mukhtar, *Kriptografi untuk Keamanan Data*. Yogyakarta: Deepublish, 2018.

[8] G. K. Sodhi, G. S. Gaba, L. Kansal, M. El Bakkali, and F. E. Tubbal, "Implementation of message authentication code using DNA-LCG key and a novel hash algorithm," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 1, p. 352, 2019, https://doi.org/10.11591/ijece.v9i1.pp352-358.

[9] M. Elveny, R. Syah, I. Jaya, and I. Affandi, "Implementation of Linear Congruential Generator (LCG) Algorithm, Most Significant Bit (MSB) and Fibonacci Code in Compression and Security Messages Using Images," *J. Phys. Conf. Ser.*, vol. 1566, no. 1, 2020. https://doi.org/10.1088/1742-6596/1566/1/012015

[10] D. Apdilah and H. Swanda, "Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP," *J. Teknol. Inf.*, vol. 2, no. 1, p. 45, 2018. https://doi.org/10.36294/jurti.v2i1.407

[11] O. Dakhi, M. Masril, R. Novalinda, J. Jufrinaldi, and A. Ambiyar, "Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher," *INVOTEK J. Inov. Vokasional dan Teknol.*, vol. 20, no. 1, pp. 27–36, 2020. https://doi.org/10.24036/invotek.v20i1.647

[12] A. M. Yusuf, *Metode Penelitian : Kuantitatif, Kualitatif, dan Penelitian Gabungan*. Jakarta: Kencana Predana Media, 2016.

[13] S. Arikunto, *Metode Penelitian Kuantitatif, Kualitatif, dan Kombinasi (Mixed Methods)*. Bandung: Alfabeta, 2014.

[14] C. A. Haris and D. Ariyus, "Kombinasi dan Modifikasi Vigenere Cipher dan Hill Cipher Menggunakan Metode Hybrid Kode Pos, Trigonometri, dan Konversi Suhu Sebagai Pengamanan Pesan," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 15, no. 2, p. 90, 2020, https://doi.org/10.30872/jim.v15i2.3746.

[15] R. Prabowo and W. Pramusinto, "Implementasi Kriptografi dengan Algoritma Vigenere Cipher, AES 128 dan RC 4 untuk Aplikasi Pesan Instan Berbasis Android," *J. Skanika*, vol. 1, no. 3, pp. 931–937, 2018, https://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/2508.

[16] L. Dong and K. Chen, *Cryptographic Protocol : Security Analysis Based on Trusted Freshness*. Beijing: Higher Education Press.

[17] S. Hallgren, *Linear Congruential Generators Over Elliptic Curves*, Pittsburgh: Carnegie Mellon University, 1994.

[18] D. H. Lehmer, *Random Number Generation on the BRL Highspeed Computing Machines*, London: Math. Rev 15, 1954.

[19] A. Wijaya, E. Kwok, and H. Agung, "Aplikasi Morse Code Translator Metode Klasifikasi Euclidean Distance dengan Algoritma Ocrchie untuk Menerjemahkan Kode Morse," *KALBISCIENTIA J. Sains dan Teknol.*, vol. 5, no. 1, pp. 30–34, 2018, http://research.kalbis.ac.id/Research/Files/Article/Full/5GJT98A5SN6NP8S131Z5HQAM3.pdf.

[20] S. F. B. Morse, *Samuel F. B. Morse : His Letters and Journals (Volume 1)*, London: Cambridge University Press, 2014, https://doi.org/10.1017/CBO9781107449923.

[21] N. Chafid and A. Saputra, "Penerapan Metode Binary Search Tree Untuk Deskirpsi Sandi Morse berbasis Android," *J. Univ. Satya Negara Indones.*, vol. 10, no. 1, pp. 1–10, 2017, https://lppm.usni.ac.id/jurnal/chafid.pdf.

BIOGRAFI PENULIS

Deny Nugroho Triwibowo menyelesaikan pendidikan magister di Program Studi Teknik Informatika Universitas Amikom Yogyakarta pada tahun 2021. Saat ini penulis 1 adalah dosen tetap di Program Studi Teknologi Informasi Universitas Harapan Bangsa, Purwokerto. Bidang penelitiannya adalah Computer Vision, Cryptography, dan Data Science.

Purwono lahir pada 16 Mei 1989 di Banyumas Indonesia. Ia adalah lulusan Sistem Informasi Sekolah Tinggi Ilmu Komputer (STIKOM) Yos Sudarso tahun 2019. Pendidikan pasca sarjananya adalah program magister di Teknik Informatika Univeristas Ahmad Dahlan (UAD). Saat ini ia sebagai dosen program studi informatika di Universitas Harapan Bangsa (UHB) Purwokerto. Bidang yang diminati adalah Data Science, Blockchain, Internet of Things

Imam Ahmad Ashari menyelesaikan pendidikan magister di Program Studi Sistem Informasi Universitas Diponegoro pada tahun 2019. Saat ini penulis 3 adalah dosen tetap di Program Studi Teknologi Informasi Universitas Harapan Bangsa, Purwokerto. Bidang penelitiannya adalah IoT, Data Science, Interpolation dan Metaheuristic.

Arif Setia Sandi menyelesaikan pendidikan magister di Program Studi Teknik Informatika Universitas Amikom Yogyakarta pada tahun 2021. Saat ini penulis 4 adalah dosen tetap Di Program Studi Teknologi Informasi Universitas Harapan Bangsa, Purwokerto. Bidang penelitiannya adalah Internet of Things.

Yusuf Fadlila Rahman menyelesaikan pendidikan magister di Program Studi Teknik Informatika Universitas Amikom Yogyakarta pada tahun 2021. Saat ini penulis 5 adalah dosen tetap Di Program Studi D3 Teknik D3 Informatika, Sekolah Vokasi, Universitas Sebelas Maret Surakarta. Bidang penelitiannya adalah Decision Support System dan Data Mining.