JURNAL TIMES
TECHNOLOGY INFORMATICS & COMPUTER SYSTEM

Volume XV No 1, 2026
*p*ISSN : 2337 – 3601
*e*ISSN : 2549 – 015X

Tersedia *online* di http://ejournal.stmik-time.ac.id

KOMBINASI *VIGENERE CIPHER* DAN *ONE TIME PAD* DENGAN *RANDOM KEY LINEAR CONGRUENTIAL GENERATOR* DAN *LINEAR FEEDBACK SHIFT REGISTER* UNTUK PENGAMANAN DATA TEKS

Anzas Ibezato Zalukhu[1)], Riandy Yap[2)], Irwan Jani Tarigan[3)]
Program Studi Sistem Informasi
STMIK Methodist Binjai
Jalan Jenderal Gatot Subroto, Bandar Senembah, Kecamatan Binjai Barat, Kota Binjai
e-mail: anzaszalukhu@gmail.com[1)] , rianz12junior@gmail.com[2)] , irwanjani@stmikmethodistbinjai.ac.id[3)])

Abstrak
Perkembangan teknologi informasi mempercepat proses pertukaran data digital, namun juga meningkatkan risiko keamanan seperti penyadapan dan kebocoran data pribadi. Penelitian ini bertujuan untuk meningkatkan keamanan data teks menggunakan kombinasi dua algoritma kriptografi kunci simetris klasik, yaitu *Vigenere Cipher* dan *One-Time Pad* (OTP). Kelemahan utama dari kedua metode ini terletak pada pengelolaan serta pembangkitan kunci yang mudah ditebak. Untuk mengatasi masalah tersebut, penelitian ini mengusulkan sebuah kebaruan dengan menerapkan metode pengacakan kunci secara dinamis menggunakan kombinasi dari *Linear Congruential Generator* (LCG) dan *Linear Feedback Shift Register* (LFSR) sebagai pembangkit kunci acak (*random key generator*) pada proses algoritma OTP. Pengujian sistem disimulasikan menggunakan bahasa pemrograman Python. Hasil penelitian menunjukkan bahwa integrasi metode LCG dan LFSR mampu menghasilkan kunci OTP yang sangat acak dan dinamis. Sistem berhasil melakukan proses enkripsi berlapis yang sulit diprediksi dengan hasil akhir berupa *ciphertext* yang valid, serta mampu mengembalikannya menjadi bentuk *plaintext* semula secara tepat melalui proses dekripsi.
Kata kunci : Kriptografi; *Linear Congruential Generator*; *Linear Feedback Shift Register*; *One-Time Pad*; *Vigenere Cipher.*

1. Pendahuluan

Teknologi informasi dan komunikasi diera globalisasi saat ini berlangsung sangat cepat dan canggih dan telah menjadi bagian kebutuhan penting dalam berbagai aspek kehidupan, termasuk pada bagian organisasi, Pendidikan dan pemerintahan, maupun bisnis. Pemanfaatan sistem informasi berbasis *online* memberikan kemudahan dalam proses pertukaran data dan komunikasi sehingga aktivitas pengiriman pesan dapat dilakukan dengan cepat, efektif, dan efisien [1]. Namun, di balik kemudahan tersebut muncul berbagai ancaman terhadap keamanan data, terutama pada proses pengiriman informasi melalui jaringan internet [2].

Keamanan informasi merupakan aspek sangat penting dalam pertukaran data digital. Pengiriman pesan melalui internet memiliki risiko penyadapan, pencurian data, dan manipulasi informasi oleh pihak yang tidak bertanggung jawab. Pihak ketiga dapat melakukan intersepsi terhadap pesan yang dikirim melalui internet sehingga kerahasiaan informasi tidak terjamin. Kondisi ini dapat merugikan pengirim maupun penerima, terutama jika informasi yang dikirim bersifat rahasia dan penting. Oleh karena itu, diperlukan mekanisme pengamanan data yang mampu menjaga kerahasiaan pesan selama proses transmisi berlangsung [3].

Ancaman terhadap keamanan data juga terlihat dari meningkatnya kasus pelanggaran data pribadi di Indonesia. Berdasarkan data Kementerian Komunikasi dan Digital sejak 2019 hingga 2026, tercatat sebanyak 241 kasus dugaan pelanggaran data pribadi telah ditangani, dengan puncak kasus terjadi pada tahun 2025 yang mencapai 50 kasus. Selain itu, ditemukan lebih dari seribu data pribadi diperjualbelikan secara ilegal melalui forum daring. Kondisi ini menunjukkan bahwa perlindungan data dan keamanan informasi menjadi kebutuhan yang sangat penting untuk mencegah penyalahgunaan data oleh pihak yang tidak bertanggung jawab [4].

Salah satu teknik yang digunakan untuk menjaga keamanan data adalah kriptografi [5]. Kriptografi adalah ilmu yang mempelajari teknik pengamanan data melalui proses enkripsi dan dekripsi sehingga data tidak dapat dipahami oleh pihak yang tidak memiliki hak akses [6]. Kriptografi berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, integritas data, autentikasi, dan non-repudiasi. Dalam implementasinya, proses enkripsi dilakukan dengan mengubah plainteks menjadi *ciphertext* menggunakan algoritma tertentu beserta kunci enkripsi sehingga isi pesan sulit diketahui oleh pihak lain [7].

Berbagai algoritma kriptografi klasik masih banyak digunakan dan dikembangkan, di antaranya adalah algoritma *Vigenere Cipher* dan *One Time Pad* [8], [9]. Algoritma *Vigenère Cipher* merupakan salah satu metode kriptografi kunci simetris yang menggunakan kunci yang sama pada proses enkripsi dan dekripsi. Algoritma ini termasuk dalam teknik substitusi polialfabetik dengan memanfaatkan kata kunci untuk menentukan pola perubahan karakter plainteks [10]. *Vigenère Cipher* memiliki keunggulan dalam mengurangi kelemahan analisis frekuensi yang terdapat pada sandi monoalfabetik sehingga banyak digunakan untuk menjaga keamanan komunikasi, sedangkan *One Time Pad* dikenal memiliki tingkat keamanan yang tinggi karena menggunakan kunci acak yang panjangnya sama dengan plainteks [11], [12]. Kelemahan utama kedua algoritma tersebut terletak pada pengelolaan dan pembangkitan kunci. Penggunaan kunci

yang berulang atau mudah ditebak dapat mengurangi tingkat keamanan pesan yang dienkripsi. Oleh sebab itu, diperlukan metode pembangkitan kunci acak yang mampu meningkatkan keamanan proses enkripsi.

Salah satu metode pembangkitan kunci acak yang dapat digunakan adalah *Linear Congruential Generator* (LCG) [13], [14], [15]. Penelitian oleh Hulu dan Nadeak berhasil mengombinasikan algoritma *Vigenere Cipher* dan *One Time Pad* untuk pengamanan data teks [9]. Penelitian lain oleh Riza Maria Ulfa Br Mtd dkk. [16] juga menerapkan kombinasi kedua algoritma tersebut. Namun, kedua penelitian belum menerapkan mekanisme pengacakan kunci sehingga keamanan citra digital dan data teks masih dapat ditingkatkan, salah satu pengacakan kunci yang tepat adalah *Linear Congruential Generator* (LCG). Penelitian selanjutnya yang dilakukan oleh Anzas Zalukhu dkk. dengan judul "*Enhancing Text Messages with a Combination of Vigenère Cipher and One Time Pad Using Random Key LFSR*" berhasil mengombinasikan algoritma *Vigenere Cipher* dan *One Time Pad* dengan penerapan kunci acak menggunakan metode *Linear Feedback Shift Register* (LFSR) sehingga meningkatkan keamanan proses enkripsi pesan [17].

Berdasarkan penelitian sebelumnya, algoritma *Linear Congruential Generator* (LCG) telah banyak diterapkan pada pengacakan level *game*, pengacakan gambar *puzzle*, dan pengacakan soal, serta *quiz toefl* pembelajaran berbasis android [13], [14], [18], [19]. Namun, penelitian-penelitian tersebut hanya berfokus pada proses randomisasi data dan belum mengimplementasikan LCG sebagai pembangkit *random key* dalam sistem kriptografi. penelitian ini menawarkan kebaruan dengan mengombinasikan algoritma *Vigenere Cipher* dan One *Time Pad* dengan random key metode LCG dan LFSR untuk pengamanan data teks, sehingga menghasilkan proses enkripsi yang lebih dinamis, sulit diprediksi, dan memiliki tingkat keamanan yang lebih baik.

2. Landasan Teori

Kriptografi

Kriptografi adalah salah satu ilmu dan teknik yang digunakan dalam mengamankan data informasi dengan cara mengubah data asli (*plaintex*t) menjadi bentuk yang berbeda dengan data asli (*ciphertext*) menggunakan algoritma tertentu, sehingga hanya pihak yang memiliki kunci yang dapat mengembalikan data informasi tersebut ke bentuk semula [20].

Vigenere Cipher

Vigenère cipher adalah metode kriptografi klasik yang menggunakan teknik substitusi polialfabetik dengan memanfaatkan kata kunci untuk mengenkripsi pesan, sehingga setiap huruf pada plaintext dapat berubah menjadi huruf berbeda berdasarkan kunci yang digunakan [21].

One Time Pad (OTP)

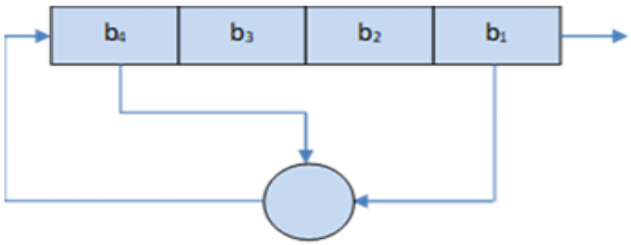
OTP adalah alah satu metode kriptografi simetri yang menggunakan kunci yang sama pada proses enkripsi dan dekripsi. Algoritma ini menggunakan deretan karakter kunci yang dibangkitkan secara acak dan memiliki panjang sama dengan pesan asli, sehingga menghasilkan tingkat keamanan yang sangat tinggi dan sering diklaim sebagai algoritma kriptografi yang sempurna apabila kunci digunakan satu kali serta dijaga kerahasiaannya [22].

Linear Congruential Generator (LCG)

Linear Congruential Generator adalah metode pembangkit bilangan acak semu (*Pseudo Random Number Generator/PRNG*) yang menghasilkan urutan angka berdasarkan persamaan matematika linear menggunakan nilai awal (*seed*), sehingga dapat digunakan untuk proses pengacakan data, pembentukan kunci, dan simulasi dalam berbagai aplikasi komputer [13], [19].

Linear Feedback Shift Register (LFSR)

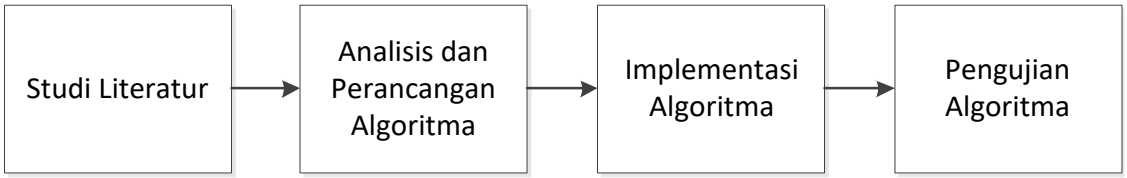
Linear Feedback Shift Register atau disingkat LFSR adalah metode pembangkit bilangan atau bit acak semu (*pseudo-random*) yang bekerja menggunakan mekanisme pergeseran bit (*shift register*) dan operasi logika XOR (Exclusive OR) [17].



Gambar 1. LFSR - 4bit. [23]

3. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimen untuk menguji efektivitas keamanan dari kombinasi algoritma kriptografi.



Gambar 2. Tahapan Penelitian.

a) Studi Literatur

Tahap ini merupakan tahap awal penelitian dengan mengumpulkan referensi dari berbagai jurnal dan sumber lain yang berkaitan dengan kriptografi, algoritma *Vigenere Cipher, One Time Pad*, serta metode pembangkit kunci acak *Linear Congruential Generator* (LCG) dan *Linear Feedback Shift Register* (LFSR). Selain itu, dilakukan juga pengumpulan data terkait kasus-kasus keamanan data.

b) Analisis dan Perancangan Sistem

Pada tahap ini dilakukan pengolahan dan analisis terhadap data yang telah dikumpulkan, meliputi proses kriptografi berupa enkripsi, pembangkitan kunci, dan dekripsi. Proses analisis dilakukan dengan mengombinasikan dua algoritma, yaitu *Vigenere Cipher* dan *One Time Pad* (OTP), sedangkan proses pembangkitan kunci OTP menggunakan metode *Linear Congruential Generator* (LCG) dan *Linear Feedback Shift Register* (LFSR) hingga menghasilkan *ciphertext* akhir. Selanjutnya dilakukan perancangan sistem berdasarkan literatur yang telah didapat.

c) Implementasi Sistem

Tahap implementasi sistem merupakan tahap penerapan hasil perancangan ke dalam bentuk aplikasi atau program menggunakan bahasa pemrograman *Python*. Pada tahap ini dilakukan pembangunan sistem kriptografi dengan mengimplementasikan kombinasi algoritma *Vigenere Cipher* dan *One Time Pad* (OTP), serta metode pembangkit kunci *Linear Congruential Generator* (LCG) dan *Linear Feedback Shift Register* (LFSR). Implementasi meliputi proses input *plaintext*, kunci *Veigenere cipher* pembangkitan kunci acak, proses enkripsi, pembentukan *ciphertext*, hingga proses dekripsi untuk mengembalikan *ciphertext* menjadi *plaintext* semula. Selain itu, dilakukan pengujian fungsi sistem untuk memastikan seluruh proses berjalan sesuai dengan rancangan dan menghasilkan output yang benar.

d) Pengujian Algoritma

Tahap pengujian sistem dilakukan untuk menguji kinerja sistem kriptografi yang telah dibangun, meliputi proses enkripsi dan dekripsi menggunakan kombinasi algoritma *Vigenere Cipher, One Time Pad* (OTP), LCG, dan LFSR. Pengujian dilakukan untuk memastikan sistem berjalan sesuai rancangan dan menghasilkan output yang valid.

Algoritma Vigenere Cipher dan *One Time Pad* (OTP)

Algoritma *Vigenere Cipher* adalah algoritma kriptografi klasik berbasis substitusi polialfabetik yang menggunakan kunci berulang untuk mengenkripsi plainteks menjadi cipherteks sedangan OTP adalah metode kriptografi simetris yang menggunakan kunci acak sekali pakai dengan panjang kunci sama dengan panjang plaintext untuk menghasilkan ciphertext yang sangat aman. Rumus Enkripsi Vigene Cipher dan OTP:

$$C_i = P_i + K_i \; mod \; 26 \text{ atau } C_i = (P_i + K_i) - 26 \qquad (1)$$

Rumus Deskripsi Vigenere Cipher dan OTP:

$$P_i = C_i - K_i \; mod \; 26 \text{ atau } P_i = (C_i - K_i) + 26 \qquad (2)$$

Keterangan:
P_i = Plainteks
C_i = Cipherteks
K_i = Kunci

Pembangkit Kunci LCG dan LFSR

Linear Congruential Generator adalah metode pembangkit bilangan acak semu menggunakan operasi aritmatika modulo untuk menghasilkan deret angka acak sedangkan *Linear Feedback Shift Register* adalah metode pembangkit bilangan acak berbasis pergeseran bit dan operasi XOR pada register.

Rumus LCG:

$$X_{n+1} = (\mathrm{a}.\mathrm{X_n} + \mathrm{c})\ mod\ m \qquad (3)$$

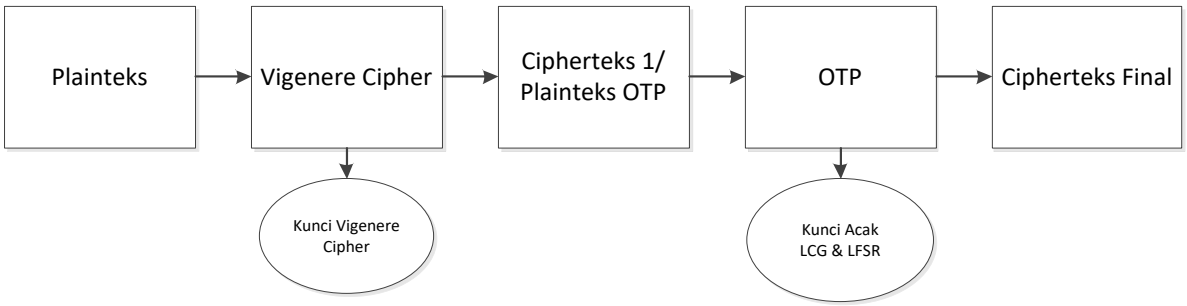
X_n = seed/bilangan sebelumnya
a = multiplier
c = increment
m = modulus

Rumus LFSR:

$$f = b_4 \oplus b_1 \qquad (4)$$

f = *feedback*
b_4 = Bit-4
$\oplus$ = XOR
b_1 = Bit-1

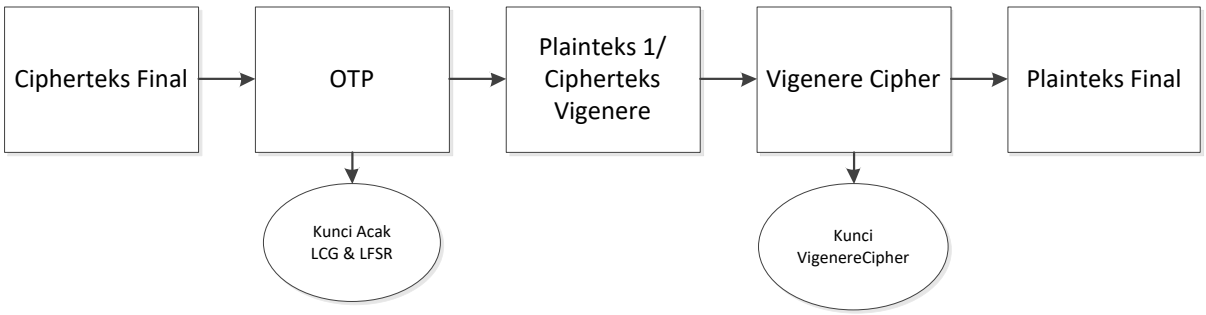
***Flowchart* Proses Enkripsi:**



Gambar 3. Proses Tahapan Enkripsi

Proses enkripsi diawali dengan memasukkan plaintext dan kunci *Vigenere Cipher*, kemudian plaintext dienkripsi menggunakan algoritma *Vigenere Cipher*. Selanjutnya, sistem membangkitkan *random key* menggunakan metode *Linear Congruential Generator* dan bit acak menggunakan *Linear Feedback Shift Register* untuk memperkuat kunci enkripsi. Hasil enkripsi *Vigenere* kemudian dienkripsi kembali menggunakan algoritma *One-Time Pad* hingga menghasilkan *ciphertext* akhir yang lebih aman.

***Flowchart* Proses Deskripsi:**



Gambar 4. Proses Tahapan Deskripsi

Proses dekripsi dimulai dengan memasukkan *ciphertext* akhir (final) yang telah diterima oleh penerima pesan. Sistem kemudian menggunakan kunci OTP acak yang dibangkitkan melalui metode *Linear Congruential Generator (LCG) dan Linear Feedback Shift Register* (LFSR) yang sama seperti pada proses enkripsi. *Ciphertext* akhir terlebih dahulu didekripsi menggunakan algoritma *One-Time Pad* (OTP) sehingga menghasilkan *ciphertext* sementara berupa hasil enkripsi *Vigenere Cipher*. Selanjutnya, *ciphertext* sementara tersebut didekripsi menggunakan algoritma *Vigenere Cipher* dengan menggunakan kunci *Vigenere cipher* yang sesuai. Pada tahap ini setiap karakter *ciphertext* dikembalikan ke bentuk semula berdasarkan proses pergeseran karakter sesuai kunci. Setelah seluruh proses dekripsi selesai dilakukan, sistem menghasilkan kembali plaintext asli sehingga pesan dapat dibaca dan dipahami oleh penerima dengan benar.

4. Hasil Penelitian

Implementasi Algoritma

Pada tahap implementasi algoritma, sistem melakukan proses pengamanan data teks menggunakan kombinasi algoritma *Vigenere Cipher*, *Linear Congruential Generator*, *Linear Feedback Shift Register*, dan *One-Time Pad*. Proses implementasi dilakukan menggunakan plaintext "ANZAS" dengan kunci Vigenere "12345".

Proses Enkripsi *Vigenere Cipher*:

$$C_i = P_i + K_i \ mod\ 26$$

Plainteks	A	N	Z	A	S
Numerik Plainteks	**0**	**13**	**25**	**0**	**18**
Kunci	**1**	**2**	**3**	**4**	**5**

Tabel 1. Hasil Enkripsi *Vigenere Cipher*

Plainteks P_i	**Kunci** K_i	**Rumus Enkripsi Vigenere Cipher** $\boldsymbol{C_i = P_i + K_i\ mod\ 26}$	**Cipherteks 1** C_i	**Kode Karekter**
0	1	(0+1) mod 26	1	B
13	2	(13+2) mod 26	15	P
25	3	(25+3) mod 26	2	C
0	4	(0+4) mod 26	4	E
18	5	(18+5) mod 26	23	X

Hasil dari proses enkripsi *Vigenère Cipher* tersebut adalah *ciphertext* "**BPCEX**", dengan representasi numerik **[1, 15, 2, 4, 23].**

Pembangkitan Kunci OTP (LCG & LFSR)

Panjang *plaintext* terdiri dari 5 karakter, maka panjang kunci pada algoritma *One-Time Pad* juga harus berjumlah 5 karakter. Oleh karena itu, sistem membangkitkan sebanyak 5 kunci acak untuk digunakan pada proses enkripsi OTP.

Proses LCG:

$$X_{n+1} = (\mathrm{a}.\mathrm{X_n} + \mathrm{c}) \bmod \mathrm{m}$$

Parameter: m = 256, a = 11, c = 37, **Seed (X_n) = 7.**

Tabel 2. Hasil Pembangkitan Kunci LCG

Iterasi	**Rumus LCG** $X_{n+1} = (\mathrm{a}.\mathrm{X_n} + \mathrm{c}) \bmod 256$	**Kunci LCG**	**Biner**
X_1	(11 x 7 + 37) mod 256	114	01110010
X_2	(11 x 114 + 37) mod 256	11	00001011
X_3	(11 x 11 + 37) mod 26	158	10011110
X_4	(11 x 158 + 37) mod 26	239	11101111
X_5	(11 x 239 + 37) mod 26	106	01101010

Proses LFSR (4-bit):

Rumus yang digunakan:

$$f = b_4 \oplus b_1$$

Seed Awal $S_0 = \mathbf{1001} \rightarrow [\mathbf{9}]$

Struktur Pergeseran Register [$b_4\ b_3\ b_2\ b_1$]

Panjang plainteks yang digunakan adalah 5 karakter, maka proses pembangkitan kunci dilakukan sebanyak 5 kali iterasi.

Pembangkitan **Kunci 1**:

Tabel 3. Hasil Pembangkitan Kunci-1

Iterasi	**Rumus** $f = b_4 \oplus b_1$	**Output**	**Hasil**
Kondisi Awal		1 0 0 1	
Shift-1	$1 \oplus 1$	0	0 1 0 0
Shift-2	$0 \oplus 0$	0	0 0 1 0
Shift-3	$0 \oplus 0$	0	0 0 0 1
Shift-4	$0 \oplus 1$	1	1 0 0 0
Hasil Y_1		**1 0 0 0 → 8**	

Pembangkitan **Kunci 2**:

Tabel 4. Hasil Pembangkitan Kunci-2

Iterasi	Rumus $f = b_4 \oplus b_1$	Output	Hasil
Kondisi Awal	1 0 0 0		
Shift-1	$1 \oplus 0$	1	1 1 0 0
Shift-2	$1 \oplus 0$	1	1 1 1 0
Shift-3	$1 \oplus 0$	1	1 1 1 1
Shift-4	$1 \oplus 1$	0	0 1 1 1
Hasil Y_2	**0 1 1 1→ 7**		

Pembangkitan **Kunci 3**:

Tabel 5. Hasil Pembangkitan Kunci-3

Iterasi	Rumus $f = b_4 \oplus b_1$	Output	Hasil
Kondisi Awal	**0 1 1 1**		
Shift-1	$0 \oplus 1$	1	1 0 1 1
Shift-2	$1 \oplus 1$	0	0 1 0 1
Shift-3	$0 \oplus 1$	1	1 0 1 0
Shift-4	$1 \oplus 0$	1	1 1 0 1
Hasil Y_3	**1 1 0 1→ 13**		

Pembangkitan **Kunci 4**:

Tabel 6. Hasil Pembangkitan Kunci-4

Iterasi	Rumus $f = b_4 \oplus b_1$	Output	Hasil
Kondisi Awal	**1 1 0 1**		
Shift-1	$1 \oplus 1$	0	0 1 1 0
Shift-2	$0 \oplus 0$	0	0 0 1 1
Shift-3	$0 \oplus 1$	1	1 0 0 1
Shift-4	$1 \oplus 1$	0	0 1 0 0
Hasil Y_4	**0 1 0 0→ 4**		

Pembangkitan **Kunci 5**:

Tabel 7. Hasil Pembangkitan Kunci-5

Iterasi	Rumus $f = b_4 \oplus b_1$	Output	Hasil
Kondisi Awal	**0 1 0 0**		
Shift-1	$0 \oplus 0$	0	0 0 1 0
Shift-2	$0 \oplus 0$	0	0 0 0 1
Shift-3	$0 \oplus 1$	1	1 0 0 0
Shift-4	$1 \oplus 0$	1	1 1 0 0
Hasil Y_5	**1 1 0 0→ 12**		

Kombinasi LCG & LFSR

Pembangkitan kunci *One-Time Pad* (OTP) dilakukan dengan menggabungkan dua metode pembangkit bilangan acak semu, yaitu *Linear Congruential Generator* (LCG) dan *Linear Feedback Shift Register* (LFSR). LCG menghasilkan deret bilangan acak *X*, sedangkan LFSR menghasilkan deret bit acak *Y*. Kedua nilai tersebut dikonversi ke bentuk biner, kemudian dilakukan operasi XOR (*exclusive OR*) untuk menghasilkan nilai acak gabungan sebagai dasar pembentukan kunci OTP.

Tabel 8. Hasil Pembangkitan Kunci LCG ⊕ LFSR

LCG (X)	LFSR (Y)	Proses XOR (X⊕Y)	Modulo 26	Kunci OTP
114 → 01110010	8 → 00001000	01111010 = 122	122 mod 26	**18**
11 → 00001011	7 → 00000111	00001100 = 12	12 mod 26	**12**
158 → 10011110	13 → 00001101	10010011 = 147	147 mod 26	**17**
239 → 11101111	4 → 00000100	11101011 = 235	235 mod 26	**1**
106→ 01101010	12 → 00001100	01100110 = 102	102 mod 26	**24**

Hasil pembangkitan kunci *One-Time Pad* (OTP) menggunakan kombinasi metode *Linear Congruential Generator* dan *Linear Feedback Shift Register* diperoleh deret kunci sebagai berikut: **K = [18, 12, 17, 1, 24]** Deret ini kemudian digunakan sebagai kunci pada proses enkripsi One-Time Pad.

Proses One Time Pad (OTP)
Rumus Enkripsi:

$$C_i = P_i + K_i \ mod\ 26$$

Cipherteks hasil *Vigenere Cipher* "**BPCEX" → [1, 15, 2, 4, 23]**

Plainteks	1	15	2	4	23
Kunci	18	12	17	1	24

Tabel 9. Hasil Enkripsi OTP (final)

Plainteks OTP P_i	**Kunci OTP** K_i	**Rumus OTP** $C_i = P_i + K_i \ mod\ 26$	**Cipherteks Final** C_i	**Karakter**
1	18	(1+18) mod 26	19	**T**
15	12	(15+12) mod 26	1	**B**
2	17	(2+17) mod 26	19	**T**
4	1	(4+1) mod 26	5	**F**
23	24	(23+24) mod 26	21	**V**

Hasil akhir *ciphertext* diperoleh dari proses enkripsi berlapis menggunakan algoritma *Vigenere Cipher* dan *One-Time Pad* dengan kunci acak hasil pembangkitan Linear Congruential Generator serta Linear Feedback Shift Register. Hasil ciphertext final yang diperoleh adalah: C_i **= "T B T F V" → 19 1 19 5 21**

Proses Deskripsi:

Proses dekripsi dimulai dengan memasukkan *ciphertext* akhir ke dalam sistem. *Ciphertext* tersebut terlebih dahulu didekripsi menggunakan algoritma *One-Time Pad* (OTP) dengan kunci acak hasil pembangkitan metode LCG dan LFSR sehingga menghasilkan *ciphertext Vigenere cipher*. Selanjutnya, *ciphertext Vigenere cipher* didekripsi menggunakan kunci *Vigenere cipher* untuk memperoleh kembali *plaintext* asli. Setelah seluruh proses selesai, pesan asli dapat dibaca oleh penerima dengan benar.

Proses Deskripsi OTP:

$$P_i = C_i - K_i \ mod\ 26 \text{ atau } P_i = (C_i - K_i) + 26$$

Tabel 10. Hasil Deskripsi OTP dengan Kunci Acak LCG & LFSR

Cipherteks OTP C_i	**Kunci OTP (LCG & LFSR)** K_i	**Rumus Deskripsi OTP** $P_i = C_i - K_i \ mod\ 26$	**Plainteks 1** P_i	**Karakter**
19	18	(19−18) mod 26	1	**B**
1	12	(1−12) mod 26	15	**P**
19	17	(19−17) mod 26	2	**C**
5	1	(5−1) mod 26	4	**E**
21	24	(21−24) mod 26	23	**X**

Proses Deskripsi Vigenere Cipher:

$$P_i = C_i - K_i \ mod\ 26 \text{ atau } P_i = (C_i - K_i) + 26$$

Tabel 11. Hasil Deskripsi Vigenere Cipher (Final)

Plainteks 1 (C_i)	**Kunci Vigenere Cipher** K_i	**Rumus Deskripsi Vigenere Cipher** $P_i = C_i - K_i \ mod\ 26$	**Plainteks** P_i	**Karakter**
1	1	(1−1) mod 26	0	**A**
15	2	(15−2) mod 26	13	**N**
2	3	(2−3) mod 26	25	**Z**
4	4	(4−4) mod 26	0	**A**
23	5	(23−5) mod 26	18	**S**

Hasil proses dekripsi menunjukkan bahwa kombinasi algoritma *Vigenere Cipher* dan *One-Time Pad* dengan random key LCG & LFSR berhasil mengembalikan *ciphertext* ke bentuk plainteks awal secara tepat. Hasil dari kombinasi proses

deskripsi menghasilkan plainteks dari awal yaitu P_i **= [A N Z A S] → 0 13 25 0 18**

Implementasi Sistem

Implementasi sistem dilakukan melalui proses simulasi dan pengujian menggunakan bahasa pemrograman *Python*. Sistem yang dirancang berhasil diimplementasikan dan mampu menjalankan proses enkripsi serta dekripsi sesuai dengan algoritma yang digunakan.

Gambar 5. Hasil Enkripsi

Gambar 6. Hasil Deskripsi

Pengujian Sistem

Pengujian sistem dilakukan dengan beberapa data teks yang berbeda untuk memastikan proses enkripsi dan dekripsi berjalan dengan baik. Hasil pengujian menunjukkan bahwa sistem berhasil menghasilkan *ciphertext* serta mengembalikannya kembali menjadi *plainteks* awal secara tepat sesuai dengan rancangan sistem.

Tabel 12. Hasil Pengujian Enkripsi

Plainteks	Key Vigenere Cipher	Seed LCG	Seed LFSR	Key OTP (LCG & LFSR)	Cipherteks 1 (Vigenere)	Cipherteks Final

METHODIST	3 2 1 6 5 4 9 8 7	7	9	18 12 17 1 24 2 0 7 2	PGUNTHRAA	HSLORJRHC
BINJAI	4 5 6 1 2 2	7	9	18 12 17 1 24 2	FNTKCK	XZKLAM
BINJAI	4 5 6 1 2 2	5	7	3 3 0 4 24 21	FNTKCK	IQTOAF
STMIK METHODIST BINJAI	3 2 1	7	9	18 12 17 1 24 2 0 7 2 14 11 10 5 7 25 19 7 10 18 1	VVNLMNHVIRFJVVCLPKDK	NHEMKPHCKFQTACBEWUVL
SUMATERAUTARA	1 2 3 4 5	7	9	18 12 17 1 24 2 0 7 2 14 11 10 5	TWPEYFTDYYBTD	LIGFWHTKAMMDI
SUMATERAUTARA	1 2 3 4 5	5	10	7 17 11 24 22 5 13 17 12 13 3 4 23	TWPEYFTDYYBTD	ANACUKGUKLEXA

Tabel 13. Hasil Pengujian Deskripsi

Cipher teks Final	**Key Vigenere Cipher**	**Seed LCG**	**Seed LFSR**	**Key OTP (LCG & LFSR)**	**Plainteks 1 (OTP)**	**Plainteks Final**
HSLORJRHC	3 2 1 6 5 4 9 8 7	7	9	18 12 17 1 24 2 0 7 2	PGUNTHRAA	METHODIST
XZKLAM	4 5 6 1 2 2	7	9	18 12 17 1 24 2	FNTKCK	BINJAI
IQTOAF	4 5 6 1 2 2	5	7	3 3 0 4 24 21	FNTKCK	BINJAI
NHEMKPHCKFQTACBEWUVL	3 2 1	7	9	18 12 17 1 24 2 0 7 2 14 11 10 5 7 25 19 7 10 18 1	VVNLMNHVIRFJVVCLPKDK	STMIKMETHODISTBINJAI
LIGFWHTKAMMDI	1 2 3 4 5	7	9	18 12 17 1 24 2 0 7 2 14 11 10 5	TWPEYFTDYYBTD	SUMATERAUTARA
ANACUKGUKLEXA	1 2 3 4 5	5	10	7 17 11 24 22 5 13 17 12 13 3 4 23	TWPEYFTDYYBTD	SUMATERAUTARA

5. Kesimpulan

Penelitian ini berhasil mengimplementasikan sistem pengamanan data teks berlapis melalui kombinasi algoritma *Vigenere Cipher* dan *One-Time Pad* (OTP) menggunakan bahasa pemrograman Python. Penerapan metode *Linear Congruential Generator* (LCG) dan *Linear Feedback Shift Register* (LFSR) yang diintegrasikan melalui operasi *XOR* terbukti efektif mengatasi kelemahan kunci klasik dengan menghasilkan deret kunci OTP yang acak, dinamis, dan sulit diprediksi. Berdasarkan hasil pengujian sistem, kombinasi ini memiliki tingkat akurasi yang tinggi karena mampu melakukan proses enkripsi dengan aman sekaligus mengembalikan *ciphertext* menjadi *plaintext* semula secara tepat tanpa adanya kesalahan karakter. Dengan demikian, integrasi kedua metode pembangkit bilangan acak semu ini berhasil meningkatkan kualitas dinamisme dan keamanan pada sistem kriptografi simetris.

Daftar Pustaka

[1] A. Junaedy Abu Huraerah, A. Wahid Abdullah, and A. Rivai, “Pengaruh Teknologi Informasi Dan Komunikasi Terhadap Pendidikan Indonesia,” Dec. 2023, Accessed: May 26, 2026. [Online]. Available: https://journal.iain-manado.ac.id/index.php/jiep/article/download/2715/1541

[2] M. Alfian and R. Rahman, "Keamanan Jaringan Pada Perguruan Tinggi," *JURNAL RISET SISTEM INFORMASI*, vol. 1, pp. 59–64, Jul. 2024, doi: 10.69714/qgnbgv11.

[3] A. Khairunnisa Ramadhani Saidiman, S. Salwa Huwaidah Sugianto, and R. Rahman, "Analisis Penerapan SSL/TLS Dalam Menjaga Keamanan Transmisi Data Pada Aplikasi Web," *Jurnal Ilmiah Multidisiplin Terpadu*, vol. 10, no. 1, pp. 2246–6111, Jan. 2026, Accessed: May 26, 2026. [Online]. Available: https://sejurnal.com/pub/index.php/jimt/article/download/699/675/718

[4] H. Kemenko Polhukam RI, "Kemenko Polkam Dorong Percepatan Regulasi Pelindungan Data di Masa Transisi," Kementerian Koordinator Bidang Politik dan Keamanan. Accessed: May 26, 2026. [Online]. Available: https://polkam.go.id/kemenko-polkam-dorong-percepatan-regulasi-pelindungan-data-di-masa-transisi/

[5] M. Akbar, I. Kanedi, and O. Jey FhiterW, "Implementasi Kriptografi Metode Elgamal Untuk Keamanan Data Teks," *Universitas Dehasen Bengkulu Jl. Meranti Raya No. 32 Kota Bengkulu*, vol. 21, no. 2, p. 341139, Oct. 2695, Accessed: May 26, 2026. [Online]. Available: https://jurnal.unived.ac.id/index.php/jmi/article/download/9376/6650/

[6] 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," *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, vol. 10, no. 1, p. 20, Feb. 2016, doi: 10.30872/jim.v10i1.23.

[7] A. A. Siagian and Z. Indra, "Analisis Teknik Playfair Dan Shift Cipher Sebagai Metode Kriptografi Klasik Untuk Keamanan Data," *JUKOMTEK (Jurnal Komputer dan Teknologi)*, vol. Vol. 04, No. 01, pp. 13–19, Jan. 2025, Accessed: May 26, 2026. [Online]. Available: https://jurnal-cahayapatriot.org/index.php/jukomtek/article/view/315

[8] A. A. Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," *JURNAL Al-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, vol. 4, No.3, no. 3, pp. 110–115, Mar. 2018, doi: 10.36722/sst.v4i3.280.

[9] V. Hulu and B. Nadeak, "Kombinasi Algoritma Vigenere Cipher dan One Time Pad untuk Mengamankan Data Teks," *KAKIFIKOM (Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer)*, vol. 02, no. 01, pp. 49–57, Apr. 2020.

[10] S. A. ALABADY, T. F. SHAWKAT, and A. W. ADREES, "Enhanced Vigenere Cipher Algorithm For Improved Cryptographic Security," *Quantum Journal of Engineering, Science and Technology*, vol. 6, no. 1, pp. 1–12, Dec. 2024, doi: 10.55197/QJOEST.V6I1.194.

[11] M. D. Asrofa, S. Bahri, and K. Kasliono, "One-Time Pad Cryptography for Secure Data Transmission in IoT Smart Door Using QR Code," *Jurnal Media Informasi Teknologi*, vol. 2, no. 2, pp. 133–148, Oct. 2025, doi: 10.69616/MIT.V2I2.248.

[12] Vignesh, N. P. Deepa, T. Srinivasan, R. S. Somesh, and V. Mendonca, "Quantum Cipher Exchange with BB84 Protocol and Cryptography Using the One-Time Pad Algorithm," *Proceedings of the 3rd International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics, IITCEE 2025*, 2025, doi: 10.1109/IITCEE64140.2025.10915391.

[13] H. Eka Putra and K. Harianto, "Implementasi Linear Congruential Generator untuk Pengacakan Gambar pada Permainan Puzzle," *Sains dan Teknologi Informasi*, vol. 4, no. 1, pp. 89–96, Jun. 2018, doi: 10.33372/STN.V4I1.302.

[14] A. M. Siahaan and J. Hendrik, "Perancangan Aplikasi Edukasi Pembelajaran Alfabet dan Angka Berbasis Android dengan Metode Linear Congruential Generator (LCG)," *Bulletin of Computer Science Research*, vol. 3, no. 1, pp. 170–176, Dec. 2022, doi: 10.47065/BULLETINCSR.V3I1.223.

[15] I. T. Kurniawan, H. Haryanto, E. Dolphina, and E. Z. Astuti, "Pseudo Random Number Generator Menggunakan Algoritma Linear Congruential Generator untuk Variasi Level dan Ketersediaan Konten pada Game Hyper Casual," *TECHNO CREATIVE*, vol. 3, no. 2, pp. 84–90, Feb. 2026, doi: 10.62411/TCV.V3I2.3246.

[16] M. Rizaludin and F. Fikriah, "Prediksi Prediksi Perilaku Pelanggan Pada Produk UMKM Batik Dengan Menggunakan Algoritma Decision Tree," *Teknomatika*, vol. 13, no. 02, pp. 8–16, Nov. 2023, doi: 10.61423/TEKNOMATIKA.V13I02.622.

[17] A. I. Zalukhu, Z. Sitorus, S. Suhardiansyah, and N. Septiani, "Enhancing Text Messages with a Combination of Vigenère Cipher and One Time Pad Using Random Key LFSR," *Jurnal Sains dan Teknologi*, vol. 6, no. 1, pp. 52–57, May 2024, doi: 10.55338/SAINTEK.V6I1.3190.

[18] T. Mhd Zulfikar, L. Tanti, P. Utama, and J. K. Yos Sudarso KM, "Rancang Bangun Aplikasi Quiz Simulasi TOEFL Memanfaatkan Algoritma Linear Congruential Generator (LCG) Berbasis Android," *Jurnal Info Digit (JID)*, vol. 2, no. 1, pp. 18–31, Jan. 2024, Accessed: May 26, 2026. [Online]. Available: https://kti.potensi-utama.org/index.php/JID/article/view/1260

[19] dwita deslianti and A. Fahry, "APLIKASI PEMBELAJARAN BAHASA INGGRIS DENGAN MENGGUNAKAN ALGORITMA LINEAR CONGRUENT GENERATOR BERBASIS ANDROID," *JUSIBI (Jurnal Sistem Informasi dan E-Bisnis)*, vol. 5, no. 1, pp. 9–15, Jan. 2023, doi: 10.54650/JUSIBI.V5I1.496.

[20] N. S. Harahap and M. Iqbal, "METODE PEMBAYARAN ELEKTRONIK BERDASARKAN PADA KRIPTOGRAFI," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 10, no. 2, pp. 2167–2173, Mar. 2026, doi: 10.36040/JATI.V10I2.17316.

[21] P. Pazri and A. H. Hasugian, "Implementasi Algoritma Vigenere Cipher Untuk Keamanan Data Bantuan Sosial Di Desa," *Bulletin of Computer Science Research*, vol. 5, no. 4, pp. 317–328, Jun. 2025, doi: 10.47065/BULLETINCSR.V5I4.544.

[22] S. Sarifah, I. Faisal, and I. Lubis, "Metode One Time Pad sebagai Verifikasi Akun E-Wallet dalam Pencegahan Cybercrime," *Explorer (Hayward).*, vol. 5, no. 1, pp. 59–72, Jan. 2025, doi: 10.47065/EXPLORER.V5I1.1817.

[23] O. Krianto Sulaiman, "Generate Pseudo-Random Numbers Linear-Feedback Shift Register (LSFR) Pada Kunci Algoritma One Time Pad (OTP)," *Seminar Nasional Teknologi Komputer & Sains (SAINTEKS)*, pp. 171–175, Feb. 2020, Accessed: May 28, 2026. [Online]. Available: https://prosiding.seminar-id.com/index.php/sainteks