JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 11, No. 2, September 2023
DOI: https://doi.org/10.35447/jitekh.v11i2.795

Analisis Pengaplikasian Linear Congruential Generator (LCG) pada Mode Cipher Block Chaining (CBC) Advanced Encryption Standard (AES)

Manovri Yeni[1], Rosyidah Siregar[2], Tommy[3*]
[1]Universitas Muhammadiyah Aceh, Banda Aceh, Indonesia
[2,3*]Fakultas Teknik dan Komputer, Universitas Harapan Medan, Medan, Indonesia
[1]manovri.yeni@unmuha.ac.id, [2]rosyidah_siregar.unhar@harapan.ac.id, [3*]tomshirakawa@gmail.com
[*)] tomshirakawa@gmail.com

Abstrak−Penggunaan Linear Congruential Generator (LCG) sebagai bagian dari metode Cipher Block Chaining (CBC) dalam Advanced Encryption Standard (AES) telah menjadi perhatian penelitian untuk meningkatkan keamanan data. Dalam percobaan ini, analisis chi-square dan analisis entropy digunakan untuk mengevaluasi keefektifan pengaplikasian LCG pada CBC-AES dibandingkan dengan CBC-AES konvensional. Analisis chi-square menunjukkan peningkatan tertinggi sebesar 15.1098 dan penurunan terendah sebesar -10.4293. Peningkatan tersebut mencerminkan perbaikan distribusi probabilitas data terenkripsi, yang mendekati distribusi acak, dan mengindikasikan penurunan kemungkinan serangan statistik terhadap data terenkripsi. Sementara itu, analisis entropy menunjukkan peningkatan tertinggi sebesar 0.3562 dan penurunan terendah sebesar -0.0942. Peningkatan ini menunjukkan bahwa data terenkripsi dengan menggunakan metode ini menjadi lebih sulit untuk diprediksi atau dianalisis oleh pihak yang tidak berwenang, meningkatkan tingkat ketidakdugaan data terenkripsi. Hasil penelitian menunjukkan peningkatan signifikan dalam keamanan data, dengan peningkatan 3.65% dalam analisis chi-square, menunjukkan distribusi probabilitas data yang lebih merata, dan peningkatan sebesar 0.066% dalam analisis entropy, mengindikasikan tingkat ketidakdugaan yang lebih tinggi dalam data terenkripsi. Hasil ini menjanjikan dan menunjukkan potensi LCG dalam meningkatkan keamanan sistem kriptografi, meskipun penelitian lebih lanjut diperlukan untuk validasi dan pengoptimalan metode ini dalam konteks keamanan informasi.

Kata Kunci: LCG; CBC; AES;Chi-Square; Entropy.

Abstract−The use of the Linear Congruential Generator (LCG) as a part of the Cipher Block Chaining (CBC) method in the Advanced Encryption Standard (AES) has been a focus of international research to enhance data security. In this experiment, chi-square analysis and entropy analysis are employed to evaluate the effectiveness of applying LCG to CBC-AES compared to conventional CBC-AES. The chi-square analysis indicates the highest improvement of 15.1098 and the lowest decrease of -10.4293. This improvement reflects an enhancement in the probability distribution of encrypted data, approaching a random distribution, and indicates a reduced likelihood of statistical attacks on the encrypted data. Meanwhile, the entropy analysis shows the highest increase of 0.3562 and the lowest decrease of -0.0942. This increase suggests that data encrypted using this method becomes more difficult to predict or analyze by unauthorized parties, increasing the unpredictability of the encrypted data. The research results demonstrate a significant improvement in data security, with a 3.65% increase in chi-square analysis, indicating a more even probability distribution of data, and a 0.066% increase in entropy analysis, indicating higher unpredictability in encrypted data. These findings are promising and indicate the potential of LCG in enhancing cryptographic system security, although further research is needed for validation and optimization of this method in the context of information security.

Keywords: LCG; CBC; AES; Chi-Square; Entropy

1. PENDAHULUAN

Cipher Block Chaining atau CBC merupakan salah satu bentuk aplikasi pada proses enkripsi dan dekripsi yang mana proses enkripsi dan dekripsi dilakukan pada blok-blok input secara berurutan dan hasil dari proses sebelumnya digunakan sebagai input pada proses blok selanjutnya sehingga ada kaitan antar blok pada saat proses enkripsi dan dekripsi yang bertujuan untuk meningkatkan keamanan hasil enkripsi. Pada beberapa metode

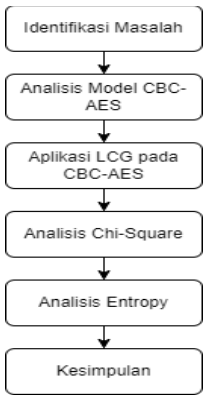
JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 11, No. 2, September 2023
DOI: https://doi.org/10.35447/jitekh.v11i2.795

kriptografi simetris seperti metode *Advanced Encryption Standard*, teknik CBC merupakan teknik yang paling umum digunakan seperti yang dapat dilihat pada beberapa penelitian terkini [1] [2].
Kelemahan utama dari mode pengoperasian Cipher Block Chaining (CBC) adalah linearitas yang melekat pada proses enkripsi dan dekripsi. Dalam CBC, setiap blok ciphertext yang dihasilkan bergantung pada ciphertext blok sebelumnya, yang menyebabkan adanya hubungan linier yang dapat dimanfaatkan oleh serangan kriptanalisis [3] [4]. Serangan terkait linear, seperti serangan differential cryptanalysis [1] [5] dan serangan plaintext-ciphertext (known-plaintext attack) [6] [7] [8], dapat memanfaatkan pola-pola linier ini untuk mengidentifikasi kunci enkripsi atau mengungkap data asli. Pada CBC, linearitas juga dapat menyebabkan kesalahan propagasi. Jika satu bit pada ciphertext mengalami gangguan, hal itu dapat menghasilkan kesalahan dalam dekripsi yang dapat menyebar ke blok-blok berikutnya [9] [10].
Selain kelemahan-kelemahan umum seperti yang telah disebutkan sebelumnya, penelitian terbaru memperkenalkan serangan yang disebut "Perturbative Bit Flip" pada mode CBC yang menunjukkan dampak dari linearitas pada keamanan enkripsi [11]. Serangan ini memanfaatkan linearitas dalam mode CBC untuk mengganti sejumlah bit tertentu dalam ciphertext tanpa pengetahuan kunci enkripsi, yang pada gilirannya dapat menyebabkan perubahan signifikan dalam dekripsi plaintext. Kelemahan linearitas pada CBC telah menjadi fokus penelitian dalam upaya untuk meningkatkan keamanan mode ini atau menggantinya dengan mode lain yang lebih tahan terhadap serangan semacam itu.
Penelitian terkait menunjukkan bahwa pengacakan urutan blok dapat digunakan untuk memperkuat keamanan enkripsi AES dalam mode CBC. Penggunaan teknik pengacakan urutan blok dalam enkripsi AES untuk mengatasi serangan known-plaintext dan chosen-plaintext. Hasil penelitian tersebut menunjukkan bahwa pengacakan urutan blok dapat memberikan tingkat perlindungan tambahan terhadap serangan tersebut [12].
penggunaan teknik permutasi blok dengan LCG untuk meningkatkan keamanan enkripsi AES dalam lingkungan cloud computing. Penelitian ini menyoroti pentingnya penggunaan pengacakan urutan blok dalam mengatasi potensi risiko keamanan data saat data disimpan atau ditransmisikan di cloud [13].
Penelitian ini bertujuan untuk menganalisis aplikasi pengacakan urutan blok pada mode pengoperasian Cipher Block Chaining (CBC) dengan Advanced Encryption Standard (AES) menggunakan Linear Congruential Generator (LCG). Analisis akan dilakukan terhadap hasil enkripsi menggunakan beberapa metrik atau pengukuran yaitu pengukuran analisis chi-square[14] dan pengukuran entropy [15]. Metriks hasil pengukuran *chi-square* dan *entropy* dari CBC-AES biasa akan dibandingkan dengan CBC-AES menggunakan pengacakan urutan blok menggunakan LCG untuk memperoleh hasil analisis pengaruh LCG terhadap CBC-AES dalam rangka meningkatkan keamanan hasil enkripsi.

2. METODE PENELITIAN

2.1 Metode Penelitian

Penelitian ini bertujuan untuk mengaplikasikan metode *Linear Congruential Generator* untuk mengacak urutan blok plainteks pada proses enkripsi pada CBC-AES. Adapun pengaplikasian pengacakan bertujuan untuk mengurangi kelemahan linearitas dari proses enkripsi pada CBC-AES. Adapun secara garis besar tahapan penelitian dapat digambarkan pada gambar 1.



Gambar 1. Tahapan Penelitian

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 11, No. 2, September 2023
DOI: https://doi.org/10.35447/jitekh.v11i2.795

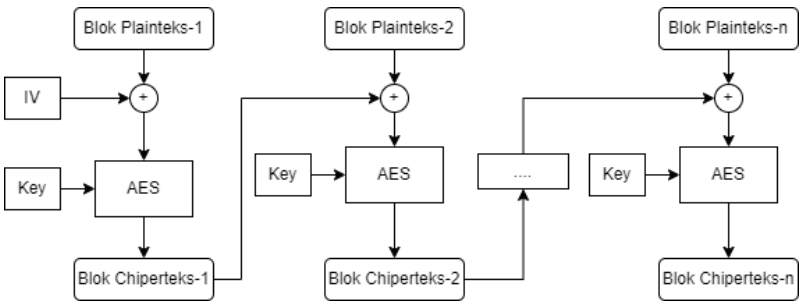
2.2 AES

AES (Advanced Encryption Standard) adalah sebuah kriptografi simetris yang banyak digunakan untuk melindungi data yang dikirimkan melalui jaringan atau disimpan dalam berbagai perangkat. AES, yang awalnya dikenal sebagai Rijndael, dikembangkan oleh Vincent Rijmen dan Joan Daemen. Ini menggunakan algoritma substitusi dan permutasi yang kuat untuk mengenkripsi data dengan cepat dan aman. AES adalah sebuah algoritma kriptografi simetris yang digunakan secara luas untuk mengamankan data dalam berbagai aplikasi. AES dirancang untuk menggantikan DES (Data Encryption Standard) karena tingkat keamanan yang lebih tinggi. AES menggunakan blok data berukuran 128 bit dan kunci enkripsi dengan panjang 128, 192, atau 256 bit.
AES memiliki beberapa langkah utama dalam proses enkripsi, termasuk substitusi byte, pergeseran baris, campuran kolom, dan penambahan kunci putaran [16]. Kombinasi dari langkah-langkah ini menghasilkan tingkat keamanan yang tinggi, bahkan terhadap serangan yang kuat. Secara umum, tahapan pada AES dapat dijabarkan sebagai berikut :

1. **Inisialisasi**: Data yang akan dienkripsi dibagi menjadi blok-blok 128-bit.
2. **Substitusi Byte (SubBytes)**: Setiap byte dalam blok diubah melalui tabel substitusi yang telah ditentukan. Ini menggantikan byte-byte asli dengan byte-byte baru.
3. **Pergeseran Baris (ShiftRows)**: Byte dalam setiap baris blok diubah dengan cara bergeser ke kiri. Baris pertama tidak diubah, baris kedua bergeser satu langkah ke kiri, baris ketiga dua langkah, dan baris keempat tiga langkah.
4. **Campuran Kolom (MixColumns)**: Kolom-kolom dalam blok diubah melalui operasi matriks. Ini mencampur byte-byte dalam kolom untuk meningkatkan keamanan.
5. **Penambahan Kunci Putaran (AddRoundKey)**: Blok hasil campuran kolom diberikan XOR dengan kunci putaran yang sesuai dengan putaran enkripsi saat ini. Kunci putaran ini berasal dari kunci utama dan kunci putaran yang dihasilkan dari kunci utama.
6. **Iterasi (Rounds)**: Proses substitusi byte, pergeseran baris, campuran kolom, dan penambahan kunci putaran diulang sejumlah putaran yang sesuai dengan panjang kunci (10 putaran untuk AES-128, 12 putaran untuk AES-192, dan 14 putaran untuk AES-256).
7. **Hasil Akhir**: Setelah putaran terakhir, blok data yang telah dienkripsi dihasilkan.

2.3 CBC-AES

Cipher Block Chaining (CBC) adalah salah satu mode pengoperasian dalam kriptografi blok yang digunakan untuk mengenkripsi data. Dalam mode CBC, setiap blok pesan plaintext di-XOR dengan blok ciphertext sebelumnya sebelum dienkripsi dengan algoritma kunci yang sama. Hal ini memungkinkan ketergantungan antar blok dalam ciphertext, yang menambah tingkat keamanan. CBC adalah salah satu mode pengoperasian yang sering digunakan dengan AES untuk mengenkripsi data [17]. Dalam konteks AES-CBC, setiap blok 128-bit plaintext di-XOR dengan blok ciphertext sebelumnya (atau dengan blok IV pertama jika ini adalah blok pertama pesan) sebelum dienkripsi dengan AES. Proses ini membuat setiap blok ciphertext tergantung pada semua blok plaintext sebelumnya dan kunci enkripsi yang sama.
Salah satu konsep unik yang perlu diperhatikan adalah "inisialisasi vektor (IV)." IV adalah nilai acak yang digunakan dalam mode CBC untuk menginisialisasi proses enkripsi pada blok pertama. IV yang berbeda akan menghasilkan ciphertext yang berbeda bahkan jika plaintextnya sama. Ini penting dalam mencegah serangan yang disebut "kedipan mata" (bit flipping attack), di mana penyerang mencoba untuk memanipulasi blok ciphertext dengan mengubah blok plaintext.



Gambar 2. CBC-AES

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 11, No. 2, September 2023
DOI: https://doi.org/10.35447/jitekh.v11i2.795

Keunikan dari mode pengoperasian CBC dalam aplikasinya pada AES terletak pada penggunaan IV [18], proses XOR, dan ketergantungan blok ciphertext yang menjadikannya salah satu pilihan yang kuat untuk mengamankan komunikasi data.

2.4 *Linear Congruential Generator*

LCG (Linear Congruential Generator) adalah salah satu jenis generator angka acak yang digunakan dalam dunia komputer dan statistik [19]. LCG adalah algoritma sederhana yang menghasilkan urutan bilangan pseudo-random (angka yang terlihat acak, tetapi sebenarnya dihasilkan dari formula matematika). LCG adalah metode sederhana untuk menghasilkan angka pseudo-random dengan menggunakan hubungan linear sederhana dalam bilangan bulat. Generator ini memanfaatkan hubungan rekursif untuk menghasilkan angka-angka berikutnya dalam urutan. Umumnya, sebuah LCG didefinisikan oleh tiga parameter :

1. **Seed (X0):** Nilai awal yang digunakan untuk memulai generator.
2. **Multiplier (a):** Konstanta yang mengontrol periode dan distribusi angka yang dihasilkan.
3. **Increment (c):** Konstanta lain yang dapat digunakan untuk menggeser nilai yang dihasilkan.

LCG menghasilkan angka-angka pseudo-random dengan menggunakan rumus berikut:

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

Dimana X_n adalah angka yang dihasilkan pada iterasi ke-n, a adalah multiplier, c adalah increment dan m adalah modulus, yaitu nilai tertentu yang menentukan periode generator. LCG sangat sederhana dalam implementasinya dan dapat menghasilkan deret angka yang tampaknya acak jika parameter-parameter (seperti a, c, m, dan seed awal) dipilih dengan tepat. Namun, penting untuk dicatat bahwa LCG memiliki beberapa kelemahan, seperti pola yang dapat diidentifikasi dalam deret angka yang dihasilkan jika parameter-parameternya tidak dipilih secara hati-hati. Oleh karena itu, dalam aplikasi yang memerlukan tingkat keamanan yang tinggi, seperti kriptografi, LCG biasanya tidak digunakan.

2.5 Analisis Chi-square

Analisis Chi-Square adalah salah satu teknik statistik yang digunakan dalam kriptanalisis untuk mengevaluasi sejauh mana hasil enkripsi dari sebuah algoritma kriptografi terdistribusi secara acak atau apakah terdapat pola yang dapat diidentifikasi. Teknik ini sering digunakan untuk mengidentifikasi kerentanan dalam implementasi kriptografi. Analisis Chi-Square didasarkan pada uji Chi-Square, yang adalah sebuah teknik statistik yang digunakan untuk mengukur kesesuaian antara hasil observasi dan hasil yang diharapkan. Dalam konteks kriptografi, hasil observasi adalah serangkaian blok ciphertext atau bit dalam ciphertext, sedangkan hasil yang diharapkan adalah distribusi acak atau homogen [20]. Pada penelitian ini adapun persamaan chi-square yang digunakan adalah:

$$Chi - Square(X^2) = \sum\left[\frac{(O-E)^2}{E}\right] \quad (2)$$

Dimana X^2 adalah nilai chi-square yang dihitung, O adalah frekuensi observasi (frekuensi kemunculan dalam data chiperteks) dalam kelompok tertentu dan E adalah frekuensi yang diharapkan (jumlah yang diharapkan atau frekuensi yang seharusnya muncul dalam kelompok tertentu jika data terdistribusi secara acak). Dalam konteks analisis hasil enkripsi, frekuensi observasi adalah berapa kali sebuah pola, nilai, atau blok ciphertext tertentu muncul dalam data yang dienkripsi. Frekuensi yang diharapkan adalah berapa kali pola, nilai, atau blok ciphertext tersebut diharapkan muncul jika data tersebut terdistribusi secara acak.

Nilai Chi-Square yang dihasilkan dari perhitungan ini kemudian dapat dibandingkan dengan nilai ambang batas Chi-Square yang sesuai dengan tingkat signifikansi tertentu dan derajat kebebasan. Jika nilai Chi-Square yang dihitung melebihi nilai ambang batas, maka dapat disimpulkan bahwa hasil enkripsi tidak terdistribusi secara acak atau ada pola yang dapat diidentifikasi dalam ciphertext, yang dapat menjadi indikasi potensi kerentanan atau masalah dalam algoritma enkripsi.

2.6 Analisis Entropy

Entropi digunakan untuk mengukur tingkat ketidakdugaan dalam ciphertext. Jika semua nilai dalam ciphertext memiliki probabilitas kemunculan yang sama, maka entropinya akan maksimum, menunjukkan tingkat keacakan yang tinggi. Analisis entropi pada hasil ciphertext adalah metode yang digunakan untuk mengukur tingkat keacakan atau ketidakdugaan dari teks terenkripsi. Entropi adalah ukuran yang digunakan untuk mengevaluasi

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 11, No. 2, September 2023
DOI: https://doi.org/10.35447/jitekh.v11i2.795

sejauh mana informasi yang terkandung dalam data terdistribusi secara merata atau acak. Semakin tinggi entropi, semakin acak atau kompleks data tersebut.
Adapun persamaan Entropy yang digunakan pada penelitian ini adalah:

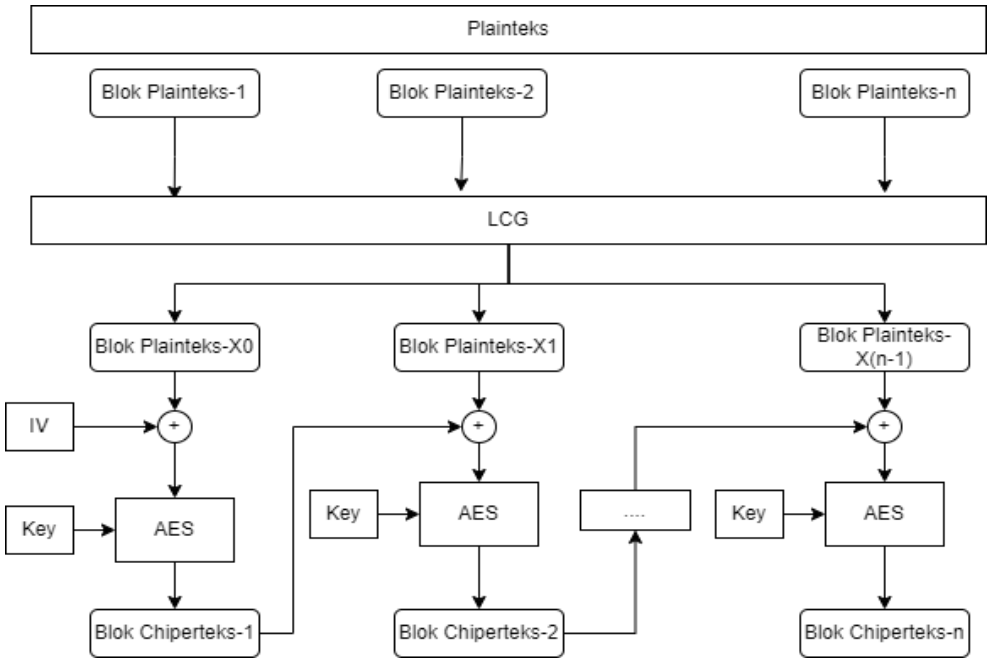
$$H = -\sum(p_i . log_2(p_i)) \quad (3)$$

Dimana H adalah nilai entropi, p_i adalah probabilitas kemunculan nilai i dalam ciphertext. Analisis entropi dapat membantu mendeteksi potensi masalah dalam algoritma enkripsi atau penggunaan kunci yang tidak aman. Jika ciphertext memiliki entropi yang rendah, ini mungkin menunjukkan adanya masalah dalam penghasilan ciphertext, seperti penggunaan kunci yang lemah atau pola yang dapat diidentifikasi.

2.7 Model LCG-CBC-AES

Aplikasi LCG pada CBC-AES adalah dengan mengacak urutan dari blok yang diproses oleh CBC-AES. Pada CBC-AES 128-bit, plainteks akan dibagi kedalam beberapa blok berukuran 128-bit yang kemudian akan diproses secara linear. Adapun pada penelitian ini, blok – blok plainteks akan diacak terlebih dahulu urutannya menggunakan LCG sehingga menghilangkan linearitas dari CBC- AES biasa. Adapun tahapan aplikasi LCG pada CBC-AES dapat dijabarkan sebagai berikut:

1. Menghitung jumlah blok (n) yang dapat terbentuk dari input plainteks dan jadikan jumlah blok menjadi nilai modulo pada LCG (m).
2. Membangkitkan bilangan acak LCG (X_i) mulai dari X_0 sampai X_{n-1}.
3. Mengurutkan urutan blok berdasarkan nilai X_i yang dihasilkan oleh LCG.
4. Melakukan proses enkripsi CBC-AES menggunakan blok yang telah diacak.



Gambar 3. Skema Aplikasi LCG pada CBC-AES

3. HASIL DAN PEMBAHASAN

Model aplikasi LCG dan CBC-AES yang dibangun pada penelitian ini kemudian di-uji menggunakan plainteks dengan tipe teks yang diperoleh dari sumber dataset Kaggle. Adapun dataset yang digunakan pada penelitian ini dapat dilihat pada tabel 1. Teks yang terdapat pada setiap berkas dataset akan di-enkripsi menggunakan model CBC-AES yang telah dilengkapi dengan LCG.

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 11, No. 2, September 2023
DOI: https://doi.org/10.35447/jitekh.v11i2.795

Tabel 1. Dataset

No.	Filename	Ukuran
1	business_1.txt	849 byte
2	entertainment_1.txt	1.9 kb
3	food_1.txt	1.71 kb
4	graphics_1.txt	2.14 kb
5	historical_1.txt	5.67 kb
6	medical_1.txt	1.28 kb
7	politics_1.txt	2.54 kb
8	space_1.txt	1.45 kb
9	sport_1.txt	1.2 kb
10	technologie_1.txt	3.75 kb

Menggunakan dataset yang dapat dilihat pada tabel 1, model yang dikembangkan di-uji untuk menghasilkan chiperteks yang kemudian dianalisis menggunakan analisis *chi-square*, proses analisis kemudian akan membandingkan hasil analisis *chi-square* dari model CBC-AES biasa dengan model CBC-AES menggunakan LCG yang dapat dilihat pada tabel 2.

Tabel 2. Hasil Analisis Chi-Square

No.	Filename	chi-square (CBC-AES)	chi-square (LCG-CBC-AES)
1	business_1.txt	277.9259	249.4815
2	entertainment_1.txt	254.8293	216.3252
3	food_1.txt	256.1441	250.955
4	graphics_1.txt	250.3597	228.259
5	historical_1.txt	235.4286	249.6703
6	medical_1.txt	266.2857	276.1905
7	politics_1.txt	264.7805	230.439
8	space_1.txt	262.9053	231.9158
9	sport_1.txt	266.7342	278.0759
10	technologie_1.txt	252.3485	278.6667

Dalam uji chi-square, tujuannya adalah untuk membandingkan distribusi frekuensi data yang diamati dengan distribusi yang diharapkan (biasanya distribusi acak). Jika hasil chi-square mendekati 0, itu menunjukkan bahwa data memiliki tingkat keacakan yang tinggi dan mendekati distribusi acak yang diharapkan. Ini sering dianggap sebagai indikator kualitas dalam konteks kriptografi. Berdasarkan hal tersebut, maka peningkatan yang diperoleh dapat dilihat dari semakin rendah skor positif yang diperoleh maka model memberikan hasil yang lebih baik, sehingga peningkatan dapat dihitung dalam satuan persen seperti yang terlihat pada tabel 3.

Tabel 3. Kinerja Model Analisis Chi-Square

No.	Filename	chi-square (CBC-AES)	chi-square (LCG-CBC-AES)	Peningkatan (%)
1	business_1.txt	277.9259	249.4815	10.2345
2	entertainment_1.txt	254.8293	216.3252	15.1098
3	food_1.txt	256.1441	250.955	2.0259
4	graphics_1.txt	250.3597	228.259	8.8276
5	historical_1.txt	235.4286	249.6703	-6.0493
6	medical_1.txt	266.2857	276.1905	-3.7196
7	politics_1.txt	264.7805	230.439	12.9698
8	space_1.txt	262.9053	231.9158	11.7873
9	sport_1.txt	266.7342	278.0759	-4.2521
10	technologie_1.txt	252.3485	278.6667	-10.4293

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 11, No. 2, September 2023
DOI: https://doi.org/10.35447/jitekh.v11i2.795

Berdasarkan analisis kinerja model dapat dilihat bahwa secara rata – rata model LCG-CBC-AES memberikan peningkatan sebesar 3.65%, walaupun tidak semua file mengalami peningkatan dari sisi analisis *chi-square*. Dari pengujian yang dilakukan, diperoleh chi-square tertinggi yaitu 15.1098 dan terendah adalah -10.4293. Analisis selanjutnya dilakukan menggunakan analisis entropy yang dapat dilihat pada tabel 4.

Tabel 4. Hasil Analisis Entropy

No.	Filename	entropy (CBC-AES)	entropy (LCG-CBC-AES)
1	business_1.txt	7.7492	7.7768
2	entertainment_1.txt	7.9035	7.9184
3	food_1.txt	7.8938	7.8965
4	graphics_1.txt	7.9182	7.9241
5	historical_1.txt	7.9704	7.9688
6	medical_1.txt	7.8546	7.8472
7	politics_1.txt	7.9246	7.9359
8	space_1.txt	7.8681	7.8873
9	sport_1.txt	7.8436	7.8276
10	technologie_1.txt	7.9522	7.9478

Ketika ciphertext memiliki entropi tinggi, artinya serangkaian ciphertext memiliki variasi yang tinggi, dan prediksi terhadap nilai-nilai individu dalam ciphertext menjadi sulit. Sebaliknya, jika ciphertext memiliki entropi rendah, maka kemungkinan kemunculan nilai-nilai tertentu lebih besar daripada yang lain. Ini bisa menjadi indikasi adanya pola atau kerentanan dalam enkripsi. Berdasarkan hal tersebut, maka peningkatan yang diperoleh dapat dilihat dari semakin tinggi skor positif yang diperoleh maka model memberikan hasil yang lebih baik, sehingga peningkatan dapat dihitung dalam satuan persen seperti yang terlihat pada tabel 5.

Tabel 5. Kinerja Model Analisis Entropy

No.	Filename	entropy (CBC-AES)	entropy (LCG-CBC-AES)	Peningkatan (%)
1	business_1.txt	7.7492	7.7768	0.3562
2	entertainment_1.txt	7.9035	7.9184	0.1885
3	food_1.txt	7.8938	7.8965	0.0342
4	graphics_1.txt	7.9182	7.9241	0.0745
5	historical_1.txt	7.9704	7.9688	-0.0201
6	medical_1.txt	7.8546	7.8472	-0.0942
7	politics_1.txt	7.9246	7.9359	0.1426
8	space_1.txt	7.8681	7.8873	0.244
9	sport_1.txt	7.8436	7.8276	-0.204
10	technologie_1.txt	7.9522	7.9478	-0.0553

Dari tabel 5 diperoleh peningkatan rata-rata dari pengukuran entropy sebesar 0.066% yang mana sama dengan pengukuran *chi-square*, tidak semua file mengalami peningkatan. Dari hasil pengujian yang dilakukan, diperoleh peningkatan tertinggi yaitu 0.3562 dan terendah adalah -0.0942. Namun, berdasarkan kedua pengukuran tersebut dapat diperoleh peningkatan tingkat keamanan dimana hasil enkripsi menjadi lebih merata dan acak.

4. KESIMPULAN

Berdasarkan hasil percobaan pengaplikasian Linear Congruential Generator (LCG) pada mode Cipher Block Chaining (CBC) Advanced Encryption Standard (AES), terdapat peningkatan yang signifikan dalam keamanan data dibandingkan dengan penggunaan CBC-AES biasa. Analisis chi-square menunjukkan peningkatan sebesar 3.65%, sedangkan analisis entropy mengindikasikan peningkatan sebesar 0.066%. Hasil peningkatan ini

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 11, No. 2, September 2023
DOI: https://doi.org/10.35447/jitekh.v11i2.795

menunjukkan bahwa penggunaan LCG pada mode CBC-AES mampu meningkatkan kekuatan enkripsi data secara signifikan. Peningkatan 3.65% dalam analisis chi-square menunjukkan bahwa distribusi probabilitas dari data terenkripsi menjadi lebih merata dan mendekati distribusi acak. Hal ini mengindikasikan bahwa kemungkinan serangan statistik terhadap data terenkripsi telah berkurang secara signifikan. Selain itu, peningkatan sebesar 0.066% dalam analisis entropy menunjukkan bahwa data terenkripsi dengan metode ini lebih sulit untuk diprediksi atau dianalisis oleh pihak yang tidak berwenang. Dengan demikian, penggunaan LCG pada CBC-AES telah berhasil menguatkan lapisan keamanan dalam proses enkripsi data, sehingga data menjadi lebih aman dari serangan potensial. Hasil ini sangat menjanjikan dalam konteks keamanan informasi, karena mereka menunjukkan bahwa metode ini dapat menjadi pilihan yang lebih kuat untuk melindungi data sensitif dari ancaman potensial. Namun, perlu diingat bahwa keamanan sistem kriptografi sangat bergantung pada faktor-faktor lainnya seperti panjang kunci, pengelolaan kunci, dan implementasi yang tepat. Oleh karena itu, pengembangan lebih lanjut dan pengujian lebih lanjut mungkin diperlukan untuk memastikan keamanan yang optimal.

REFERENSI

[1] M. E. Hameed, M. M. Ibrahim, N. Abd Manap dan A. A. Mohammed, "A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES," *Future generation computer systems,* vol. 111, pp. 829-840, 2020.

[2] S. W. Lee dan K. B. Sim, "Design and hardware implementation of a simplified DAG-based blockchain and new AES-CBC algorithm for IoT security," *Electronics,* vol. 10, no. 9, p. 1127, 2021.

[3] M. Gjorgjievska Perusheska, H. Mihajloska Trpcheska dan V. Dimitrova, "Deep Learning-based Cryptanalysis of Different AES Modes of Operation," dalam *Future of Information and Communication Conference,* 2022.

[4] A. Al-Sabaawi, "Cryptanalysis of Block Cipher: Method Implementation," dalam *2022 International Conference for Advancement in Technology (ICONAT),* 2022.

[5] Qiao, K., Cheng, J. dan Ou, C., "A New Mixture Differential Cryptanalysis on Round-Reduced AES," *Mathematics,* vol. 10, no. 24, p. 4736, 2022.

[6] Fujita, R., Isobe, T. dan Minematsu, K., "ACE in Chains: How Risky Is CBC Encryption of Binary Executable Files?," dalam *Applied Cryptography and Network Security: 18th International Conference, ACNS 2020,* Rome, Italy, 2020.

[7] Hameed, M. E., Ibrahim, M. M., Abd Manap, N. dan Attiah, M. L., "Comparative study of several operation modes of AES algorithm for encryption ECG biomedical signal," *International Journal of Electrical and Computer Engineering,* vol. 9, no. 6, p. 4850, 2019.

[8] El Hanouti, I., El Fadili, H. dan Zenkouar, K., "Cryptanalysis of an embedded systems' image encryption," *Multimedia Tools and Applications,* vol. 80, no. 9, pp. 13801-13820, 2021.

[9] O. S. Faragallah, El-sayed, H. S., Afifi, A. dan El-Zoghdy, S. F., "Small details gray scale image encryption using RC6 block cipher," *Wireless Personal Communications,* vol. 118, pp. 1559-1589, 2021.

[10] Boke, A. K., Nakhate, S. dan Rajawat, A., "Efficient key generation techniques for securing IoT communication protocols," *IETE Technical Review,* vol. 38, no. 3, pp. 282-293, 2021.

[11] Chen, R. W., Hong, Y. Y. dan Hsu, C. Y., "Perturbative Bit Flip: A New Twist to CBC Mode Attacks," *Proceedings of the 26th ACM Conference on Computer and Communications Security (CCS),* pp. 107-119, 2019.

[12] Moniruzzaman, A. B. M. dan Razzaque, M. A., "Enhancing the Security of AES-128 with Block Shuffling," *Proceedings of the 2nd International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT),* pp. 1-6, 2020.

[13] Alshaikh, S., Almesaeed, M. H. dan Aljoumaa, H. A., "Enhancing Data Security in Cloud Computing Using Block Shuffling Technique," *International Journal of Computer Applications,* vol. 975, p. 8887, 2019.

[14] Chakraborty, R. dan Mandal, J. K., "An FPGA based cascaded CBC block cipher through RPSPNC and TE," *Microsystem Technologies,* vol. 25, no. 5, pp. 1669-1677, 2019.

JITEKH
Jurnal Ilmiah Teknologi Harapan
P-ISSN: 2338-5677 || E-ISSN 2549-6646
Vol. 11, No. 2, September 2023
DOI: https://doi.org/10.35447/jitekh.v11i2.795

[15] G. Thoms, R. Muresan dan A. Al-Dweik, "Design of chaotic block cipher operation mode for intelligent transportation systems," dalam *2019 IEEE International Conference on Consumer Electronics (ICCE)*, 2019.

[16] Muttaqin, K. dan Rahmadoni, J., "Analysis and design of file security system AES (advanced encryption standard) cryptography based," *Journal of Applied Engineering and Technological Science (JAETS)*, vol. 1, no. 2, pp. 113-123, 2020.

[17] Sudrajat, A., Prasetyo, Y. H. dan Kusumawardani, M., "Implementasi Enkripsi Advanced Encryption Standard (AES-128) Mode Cipher Block Chaining (CBC) sebagai Keamanan Komunikasi Pergerakan Robot Humanoid KRSBI," *Journal of Telecommunication Network (Jurnal Jaringan Telekomunikasi)*, vol. 11, no. 1, pp. 6-11, 2021.

[18] Assafli, H. T. dan Hashim, I. A., "Security enhancement of AES-CBC and its performance evaluation using the Avalanche effect," dalam *2020 3rd International Conference on Engineering Technology and its Applications (IICETA)*, 2020.

[19] Makmur, F., Daniawan, B. dan Wijaya, A., "The Analysis and Design Computerized Semester Exams by Randomization Order of The Questions with Linear Congruential Generator Methods (Study Case: Agathos Vocational High School)," *bit-Tech*, vol. 1, no. 3, pp. 161-204, 2019.

[20] Pradhan, D., Som, S. dan Rana, A., "Cryptography encryption technique using circular bit rotation in binary field," dalam *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, 2020.