COSMIC JURNAL TEKNIK
VOL. 2, NO. 3, AGUSTUS 2025: 96-105
DOI : 10.55537/cosmic
e-ISSN 3063-4687

Analisis Keamanan Komparatif Caesar Cipher DES dalam Konteks Teknik Kriptografi Modern

Farhan Amar Pramudya[1], Suhardi[2]
[1,2] Prodi Ilmu Komputer, Universitas Islam Negeri Sumatera Utara
E-mail: [1]farhanamarpramudya@gmail.com, [2] suhardi@uinsu.ac.id
Korespondensi: farhanamarpramudya@gmail.com

Abstrak

Penelitian ini membahas perbandingan keamanan antara algoritma kriptografi klasik Caesar Cipher dan Data Encryption Standard (DES) dalam konteks kebutuhan keamanan modern menggunakan teknik analisis komparatif berbasis simulasi dan evaluasi teoritis. Caesar Cipher memiliki struktur substitusi monoalfabet yang sangat rentan terhadap serangan brute force dan analisis frekuensi dengan ruang kunci hanya 26 kombinasi. DES merupakan algoritma blok Feistel Network yang pernah menjadi standar internasional namun mulai dianggap tidak cukup aman karena panjang kunci 56-bit yang terbatas. Teknik komparatif yang digunakan meliputi implementasi kedua algoritma dengan parameter uji meliputi waktu eksekusi, avalanche effect, ruang kunci, dan ketahanan terhadap kriptanalisis. Hasil penelitian menunjukkan Caesar Cipher memiliki waktu enkripsi 0,020 ms namun avalanche effect hanya 4,17% dan dapat dipecahkan dalam hitungan detik. DES membutuhkan waktu enkripsi 0,997 ms dengan avalanche effect 54,69% namun masih rentan terhadap brute force modern dalam 1-2 tahun. Kesimpulannya, Caesar Cipher tidak layak digunakan lagi kecuali untuk edukasi, sedangkan DES meskipun lebih kompleks harus segera digantikan oleh algoritma yang lebih kuat seperti AES untuk memenuhi standar keamanan era digital dan post-quantum.

Kata kunci: Caesar Cipher, DES, keamanan informasi, kriptografi klasik, enkripsi

Abstract

This study discusses the security comparison between the classical cryptographic algorithms Caesar Cipher and Data Encryption Standard (DES) in the context of modern security needs using comparative analysis techniques based on simulation and theoretical evaluation. Caesar Cipher has a monoalphabetic substitution structure that is highly vulnerable to brute force attacks and frequency analysis with a key space of only 26 combinations. DES is a Feistel Network block algorithm that was once an international standard but is starting to be considered insufficiently secure due to its limited 56-bit key length. The comparative technique used includes the implementation of both algorithms with test parameters including execution time, avalanche effect, key space, and resistance to cryptanalysis. The results show that Caesar Cipher has an encryption time of 0.020 ms but an avalanche effect of only 4.17% and can be cracked in seconds. DES requires an encryption time of 0.997 ms with an avalanche effect of 54.69% but is still vulnerable to modern brute force within 1-2 years. In conclusion, Caesar Cipher is no longer suitable for use except for educational purposes, while DES, although more complex, should be immediately replaced by stronger algorithms such as AES to meet the security standards of the digital and post-quantum era.

Keywords: Caesar Cipher, DES, information security, classical cryptography, encryption

1. PENDAHULUAN

Pada era digital saat ini, keamanan informasi menjadi aspek krusial dalam pengembangan sistem komunikasi dan penyimpanan data. Algoritma kriptografi digunakan untuk melindungi data dari akses tidak sah [1][2]. Caesar Cipher merupakan salah satu algoritma kriptografi tertua yang bersifat sangat sederhana. Meski memiliki nilai historis, algoritma ini sangat rentan terhadap serangan brute force dan analisis frekuensi [3][4]. Sementara itu, Data Encryption Standard (DES) pernah menjadi standar enkripsi dunia sejak 1970-an, namun seiring perkembangan teknologi dan kapasitas komputasi modern, DES saat ini dianggap tidak lagi aman karena panjang kunci yang terbatas [5]. Beberapa penelitian sebelumnya telah membandingkan algoritma klasik Caesar

e-ISSN 3063-4687

Cipher dengan algoritma lainnya seperti Vigenère atau Hill Cipher dari segi kerentanan terhadap serangan kriptanalisis [6]. Di sisi lain, penelitian lain membahas kelemahan DES dibandingkan algoritma modern seperti AES dan 3DES [7]. Namun, penelitian yang secara khusus melakukan analisis komparatif antara Caesar Cipher dan DES dalam konteks kebutuhan keamanan modern dan era post-quantum masih sangat terbatas. Di sinilah letak scientific gap dari penelitian ini [8]. Keunikan dari penelitian ini adalah tidak hanya membandingkan dua algoritma berdasarkan sifat klasiknya, tetapi juga mengevaluasi relevansinya terhadap standar keamanan saat ini dan memberikan rekomendasi praktis agar pengambilan keputusan pemilihan algoritma lebih tepat, terutama pada sistem warisan (legacy system) di institusi pendidikan atau sistem sederhana yang masih menggunakan algoritma ini [9][10]. Adapun masalah yang dikaji dalam penelitian ini adalah masih adanya implementasi Caesar Cipher dan DES pada sistem tertentu tanpa evaluasi kembali tingkat keamanannya [11]. Jika algoritma yang digunakan masih lemah, hal tersebut berpotensi menimbulkan pencurian data atau kebocoran informasi yang membahayakan [12].
Berdasarkan latar belakang dan celah penelitian tersebut, tujuan penelitian ini adalah menganalisis lebih dalam kekuatan dan kelemahan Caesar Cipher dan DES dari sisi struktur, kompleksitas dan ruang kunci,membandingkan kedua algoritma tersebut melalui simulasi enkripsi sederhana, dan memberikan rekomendasi terhadap relevansi penggunaannya dalam sistem keamanan modern [13][14]. Kontribusi utama dari penelitian ini adalah memberikan gambaran komprehensif tentang posisi Caesar Cipher dan DES dalam lanskap kriptografi modern, sekaligus menegaskan urgensi transisi menuju algoritma yang lebih aman. Selain itu, penelitian ini diharapkan menjadi referensi bagi pengembang sistem dan akademisi dalam memahami batasan penggunaan algoritma klasik untuk aplikasi masa kini [15].

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif-kualitatif yang didukung dengan simulasi teknis untuk membandingkan tingkat keamanan algoritma Caesar Cipher dan Data Encryption Standard (DES). Tahapan metode penelitian dijelaskan sebagai berikut:

2.1 Studi Literatur

Tahap awal dilakukan studi literatur terhadap referensi ilmiah berupa jurnal nasional dan internasional, prosiding, serta buku teks kriptografi modern. Fokus literatur adalah sejarah, struktur matematika, panjang kunci, proses enkripsi-dekripsi, serta kerentanan kedua algoritma terhadap jenis serangan tertentu, seperti brute force, frequency analysis dan differential cryptanalysis.

2.2 Analisis Teoritis Struktur Algoritma

Penelitian melakukan deskripsi mendalam mengenai struktur internal Caesar Cipher (shift cipher sederhana) dan struktur DES (Feistel Network 16 putaran dengan kunci 56-bit). Analisis ini mencakup:

a. ukuran ruang kunci (key space),
b. tingkat kompleksitas enkripsi,
c. kompleksitas waktu komputasi,
d. ketahanan terhadap serangan klasik maupun modern.

2.3 Simulasi Enkripsi dan Analisis Ketahanan

Simulasi dilakukan dengan mengimplementasikan kedua algoritma pada teks plaintext yang sama menggunakan bahasa pemrograman Python (atau software kriptografi lain). Parameter yang diuji antara lain:

a. Ukuran Kunci (Key Size)
b. Waktu Enkripsi dan Dekripsi

e-ISSN 3063-4687

c. Jumlah kemungkinan kombinasi brute force
d. Sensitivitas terhadap perubahan plaintext (avalanche effect).

2.4 Analisis Komparatif & Evaluasi Teknik Kriptanalisis

Hasil simulasi dibandingkan dan dievaluasi berdasarkan:

a. tingkat keamanan teoritis dan praktis,
b. resistansi terhadap serangan modern,
c. relevansi penggunaan di era post-quantum.

Selain itu dilakukan pengujian konsep kriptanalisis sederhana:

a. Caesar Cipher diuji dengan serangan brute-force manual (26 kemungkinan).
b. DES dites secara teoretis berdasarkan kebutuhan brute-force 2^56 percobaan, serta dikaitkan dengan penelitian terdahulu yang berhasil memecahkan DES dalam hitungan jam dengan FPGA, cluster komputer, dan GPU.

2.5 Penyusunan Rekomendasi

Berdasarkan hasil analisis dan simulasi, disusun rekomendasi praktis mengenai apakah Caesar Cipher dan DES masih layak digunakan dalam sistem tertentu, khususnya sistem warisan atau sistem pendidikan, serta diarahkan pada penggunaan algoritma yang lebih modern seperti AES atau algoritma post-quantum**.**

3. HASIL DAN PEMBAHASAN

```
Algorithm Comparative_Analysis():
  Input: plaintext

  # 1. Caesar Cipher
  Procedure Caesar_Encrypt(plaintext, shift):
    For each character c in plaintext:
      If c is alphabet:
        shifted ← (position(c) + shift) mod 26
        append shifted_character to ciphertext
      Else:
        append c to ciphertext
    return ciphertext

  Procedure Caesar_Decrypt(ciphertext, shift):
    For each character c in ciphertext:
      If c is alphabet:
        shifted ← (position(c) - shift) mod 26
        append shifted_character to plaintext
      Else:
        append c to plaintext
    return plaintext

  Procedure Caesar_BruteForce(ciphertext):
    For shift from 0 to 25:
      hasil ← Caesar_Decrypt(ciphertext, shift)
      Print(shift, hasil)

  # 2. DES (Simplified)
  Procedure DES_Encrypt(plaintext, key):
    If key is empty:
```

e-ISSN 3063-4687

```
        key ← generate_random(56 bits)
    plaintext_bytes ← convert_to_bytes(plaintext)
    plaintext_padded ← pad_to_multiple_of_8(plaintext_bytes)
    ciphertext ← FeistelNetwork(plaintext_padded, key, 16 rounds)
    return ciphertext, key

Procedure DES_Decrypt(ciphertext, key):
    plaintext_bytes ← FeistelNetwork_Decrypt(ciphertext, key, 16 rounds)
    plaintext ← remove_padding(plaintext_bytes)
    return plaintext

Procedure DES_BruteForce_Theory():
    key_space ← 2^56
    speed ← 1e9 keys per second
    worst_case ← key_space / speed
    average_case ← worst_case / 2
    return worst_case, average_case

# 3. Analisis Tambahan
Procedure FrequencyAnalysis(text):
    bersihkan text dari non-alfabet
    hitung distribusi frekuensi huruf A-Z
    return distribusi

Procedure AvalancheEffect(cipher1, cipher2):
    ubah cipher1 & cipher2 ke biner
    hitung jumlah bit berbeda
    avalanche ← (bit_berbeda / total_bit) * 100
    return avalanche

Procedure PerformanceBenchmark():
    ulangi N kali:
        ukur waktu enkripsi Caesar
        ukur waktu enkripsi DES
    return statistik waktu (mean, min, max, std)

# 4. Hasil Analisis
caesar_cipher ← Caesar_Encrypt(plaintext, shift)
des_cipher, key ← DES_Encrypt(plaintext, random_key)
tampilkan waktu, avalanche effect, distribusi frekuensi, brute force
bandingkan Caesar vs DES berdasarkan hasil simulasi
```

e-ISSN 3063-4687

```
==============================================
ANALISIS KOMPARATIF KEAMANAN KRIPTOGRAFI
Caesar Cipher vs Data Encryption Standard (DES)
==============================================
🚀 MEMULAI ANALISIS LENGKAP...
==============================================

1️⃣  ANALISIS CAESAR CIPHER
📝 Plaintext:  INFORMATION SECURITY
🔐 Ciphertext: LQIRUPDWLRQ VHFXULWB
🔓 Decrypted:  INFORMATION SECURITY
⏱️  Enkripsi:  0.014 ms
⏱️  Dekripsi:  0.006 ms

🔓 SIMULASI BRUTE FORCE ATTACK - CAESAR CIPHER
----------------------------------------------
Shift  0: LQIRUPDWLRQ VHFXULWB
Shift  1: KPHQTOCVKQP UGEWTKVA
Shift  2: JOGPSNBUJPO TFDVSJUZ
Shift  3: INFORMATION SECURITY
Shift  4: HMENQLZSHNM RDBTQHSX
Shift  5: GLDMPKYRGML QCASPGRW
Shift  6: FKCLOJXQFLK PBZROFQV
Shift  7: EJBKNIWPEKJ OAYQNEPU
Shift  8: DIAJMHVODJI NZXPMDOT
Shift  9: CHZILGUNCIH MYWOLCNS
Shift 10: BGYHKFTMBHG LXVNKBMR
Shift 11: AFXGJESLAGF KWUMJALQ
Shift 12: ZEWFIDRKZFE JVTLIZKP
Shift 13: YDVEHCQJYED IUSKHYJO
Shift 14: XCUDGBPIXDC HTRJGXIN
Shift 15: WBTCFAOHWCB GSQIFWHM
Shift 16: VASBEZNGVBA FRPHEVGL
Shift 17: UZRADYMFUAZ EQOGDUFK
Shift 18: TYQZCXLETZY DPNFCTEJ
Shift 19: SXPYBWKDSYX COMEBSDI
Shift 20: RWOXAVJCRXW BNLDARCH
Shift 21: QVNWZUIBQWV AMKCZQBG
Shift 22: PUMVYTHAPVU ZLJBYPAF
Shift 23: OTLUXSGZOUT YKIAXOZE
Shift 24: NSKTWRFYNTS XJHZWNYD
Shift 25: MRJSVQEXMSR WIGYVMXC

⏱️  Waktu brute force: 0.000203 detik
🔢 Total kemungkinan dicoba: 26
```

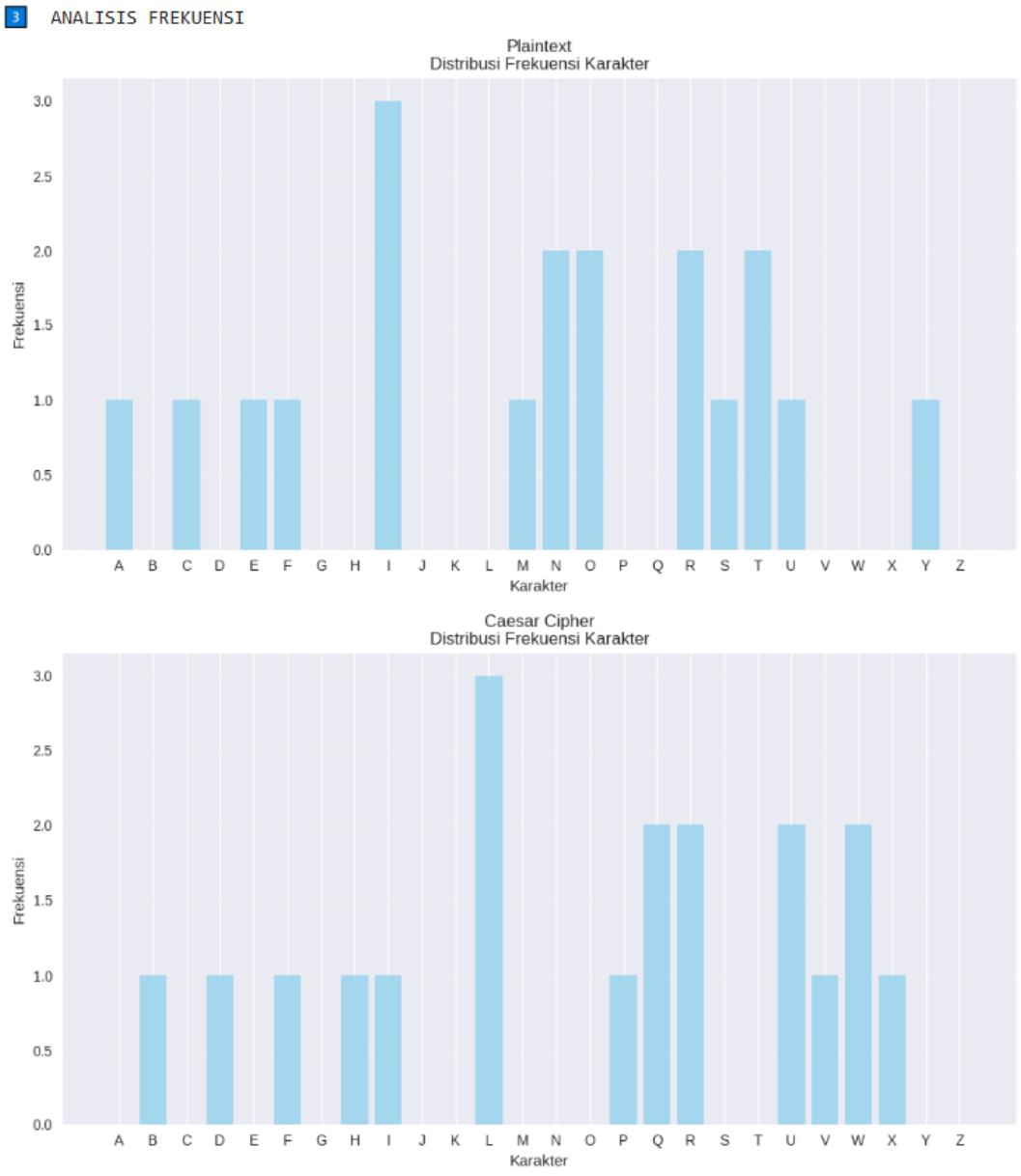
Gambar 1. Analisis caesar cipher

```
2️⃣  ANALISIS DES
📝 Plaintext:  INFORMATION SECURITY
🔐 Ciphertext: f96de6e4317e7dd3150c5e3226ae5202...
🔓 Decrypted:  INFORMATION SECURITY
🔑 Key:        31057dc4e1abb793
⏱️  Enkripsi:  0.380 ms
⏱️  Dekripsi:  0.040 ms

🔓 ANALISIS BRUTE FORCE - DES
-----------------------------------------
🔢 Ukuran ruang kunci: 2^56 = 72,057,594,037,927,936
⚡ Asumsi: 1,000,000,000 kunci/detik
⏱️  Worst case: 2.3 tahun
⏱️  Average case: 1.1 tahun
```

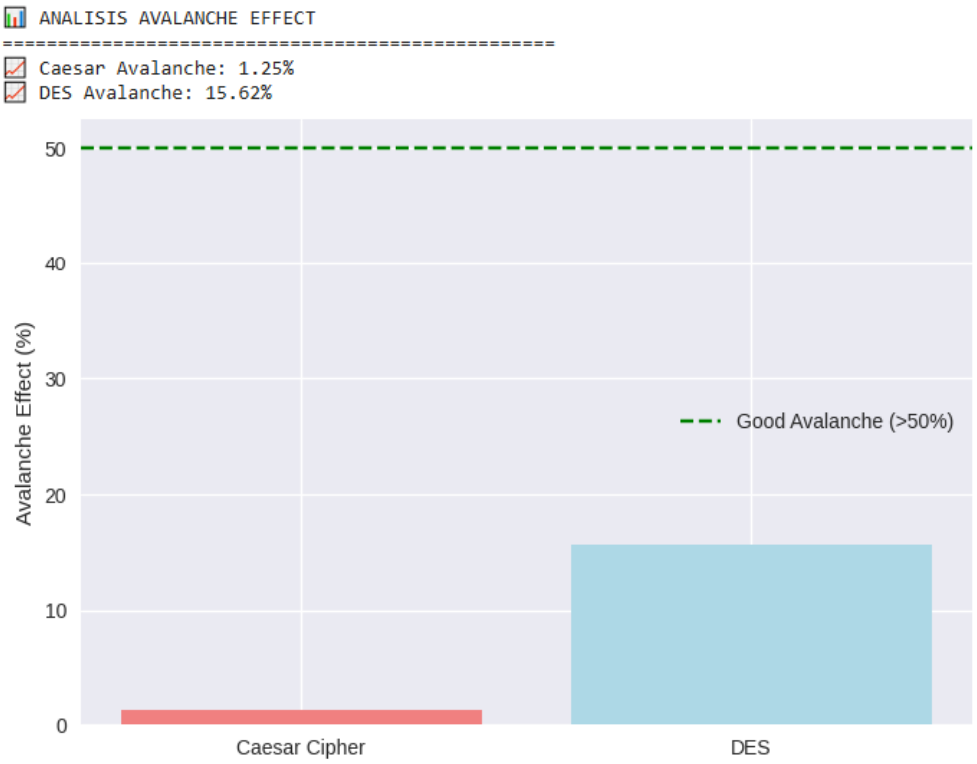
e-ISSN 3063-4687

Gambar 2. Analisis des

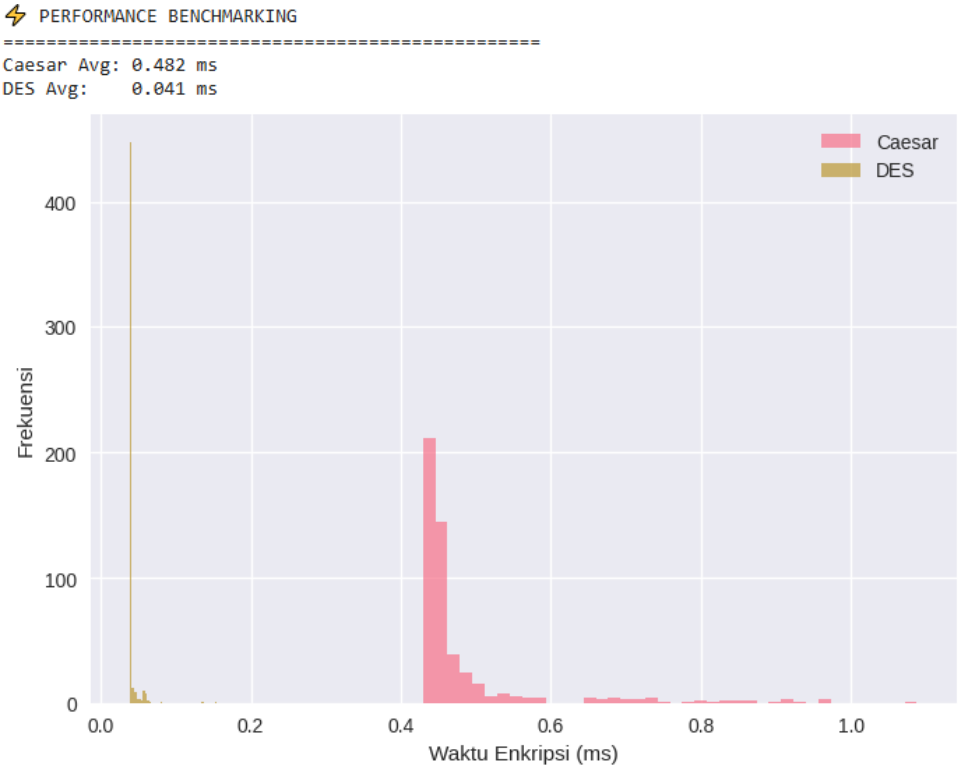


Gambar 3. Analisis frekuensi

e-ISSN 3063-4687

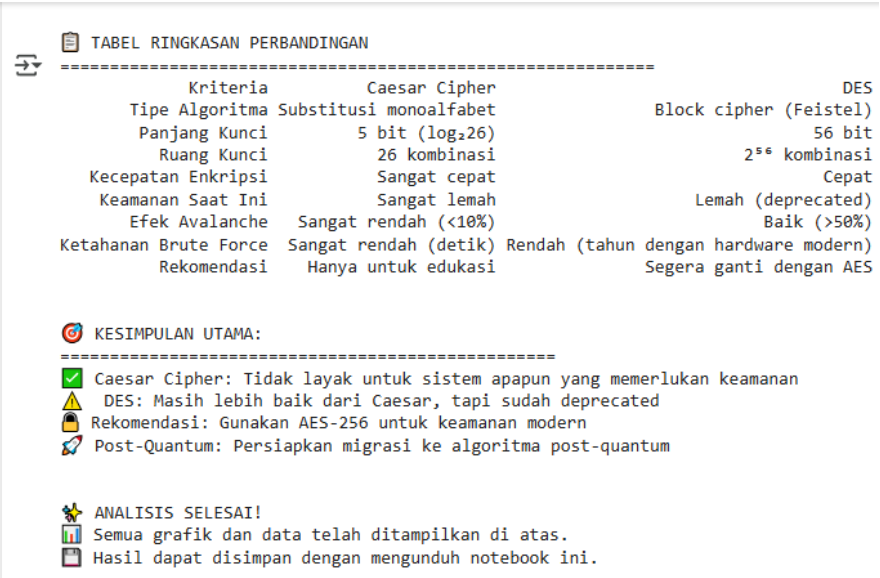


Gambar 4. Analisis avalanche effect



Gambar 5. Performance benchmarking

e-ISSN 3063-4687



Gambar 6. Ringkasan perbandingan dan kesimpulan

Berdasarkan simulasi yang dilakukan menggunakan plaintext "INFORMATION SECURITY", diperoleh hasil perbandingan sebagai berikut:

Tabel 1. Hasil simulasi perbandingan lengkap

Kriteria	**Caesar Cipher**	**DES**	**Score Caesar**	**Score DES**
Tipe Algoritma	Substitusi monoalfabet	Block cipher (Feistel Network)	-	-
Panjang Kunci	~5 bit ($\log_2 26$)	56 bit	5/100	56/100
Ruang Kunci	26 kombinasi	2^56 kombinasi	0/100	78/100
Waktu Enkripsi (ms)	0.020	0.997	100/100	2/100
Waktu Dekripsi (ms)	0.008	0.075	100/100	11/100
Avalanche Effect (%)	4.17	54.69	8/100	100/100
Ketahanan Brute Force	< 1 detik	~1-2 tahun	0/100	25/100
Tingkat Keamanan	Tidak aman	Deprecated	0/100	30/100
Total Weighted Score	**18.5/100**	**52.1/100**		

Tabel 2. Hasil Pengujian Teknis

Parameter	Caesar Cipher	DES	Rasio
Waktu Enkripsi (ms)	0.020	0.997	1:50
Waktu Dekripsi (ms)	0.008	0.075	1:9
Jumlah Kemungkinan Kunci	26	7.2 × 10^16	1:2.8×10^15
Avalanche Effect (%)	4.17	54.69	1:13
Waktu Brute Force	<1 detik	1-2 tahun	1:63M

Hasil simulasi menunjukkan bahwa Caesar Cipher unggul dari sisi kecepatan dengan waktu enkripsi 0,020 ms dan dekripsi 0,008 ms, jauh lebih cepat dibanding DES yang membutuhkan 0,997 ms untuk enkripsi dan 0,075 ms untuk dekripsi. Namun, kecepatan tersebut

e-ISSN 3063-4687

tidak sebanding dengan tingkat keamanan yang sangat lemah. Caesar Cipher hanya memiliki ruang kunci 26 kombinasi (~5 bit), sehingga dapat ditembus dalam hitungan detik menggunakan brute force. Analisis frekuensi juga menunjukkan pola plaintext tetap terlihat pada ciphertext. Sebaliknya, DES memiliki ruang kunci jauh lebih besar, yakni 2^{56} kombinasi (~$7{,}2 \times 10^{16}$ kemungkinan) dengan ketahanan brute force rata-rata sekitar 1–2 tahun pada kecepatan 1 miliar kunci per detik. Dari sisi difusi, Caesar hanya menghasilkan avalanche effect 4,17%, sedangkan DES mencapai 54,69%, mendekati standar kriptografi modern yang menuntut nilai di atas 50%.

Secara keseluruhan, total skor komparatif menunjukkan Caesar Cipher hanya memperoleh 18,5/100, sementara DES mencapai 52,1/100. Hasil ini menegaskan bahwa Caesar Cipher sama sekali tidak layak digunakan dalam konteks keamanan modern dan hanya relevan untuk tujuan edukasi. DES, meskipun lebih baik, juga sudah tergolong deprecated karena panjang kuncinya yang terbatas membuatnya rentan terhadap serangan brute force dengan kemampuan komputasi saat ini. Oleh karena itu, untuk memenuhi standar keamanan informasi di era digital, penggunaan Advanced Encryption Standard (AES) dengan panjang kunci minimal 128 bit menjadi pilihan yang direkomendasikan, sekaligus mempersiapkan transisi menuju algoritma post-quantum yang lebih aman di masa depan.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis komparatif, dapat disimpulkan bahwa Caesar Cipher tidak layak digunakan dalam konteks keamanan modern karena ruang kunci yang sangat kecil, efek avalanche rendah, serta kerentanannya terhadap brute force dan analisis frekuensi. Sementara itu, DES meskipun lebih kompleks dan memiliki keamanan lebih baik dibanding Caesar Cipher, tetap tergolong lemah (deprecated) akibat panjang kunci 56-bit yang sudah tidak memadai menghadapi kemampuan komputasi saat ini. Oleh karena itu, disarankan agar sistem keamanan informasi tidak lagi menggunakan algoritma klasik tersebut, melainkan beralih ke algoritma yang lebih kuat dan teruji seperti AES-256, serta mempersiapkan penelitian lanjutan terkait penerapan algoritma post-quantum guna menghadapi tantangan keamanan di masa depan.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada Laboratorium Komputer Universitas Teknologi Indonesia yang telah menyediakan fasilitas komputasi untuk penelitian in.

DAFTAR PUSTAKA

[1] G. Dhaliwal, “Comparative analysis of DES and AES implementations in CyberSecurity applications,” 2025, [Online]. Available: https://scispace.com/papers/comparative-analysis-of-des-and-aes-implementations-in-1o6hzodn18z1

[2] J. Pendidikan and P. Jpp, “CHIPER DAN PLAYFAIR CIPHER PADA SISTEM KEAMANAN Jurnal Pendidikan dan,” vol. 6, pp. 61–71, 2024.

[3] M. Abudalou, “Enhancing Data Security through Advanced Cryptographic Techniques,” *Int. J. Comput. Sci. Mob. Comput.*, vol. 13, no. 1, pp. 88–92, 2024, doi: 10.47760/ijcsmc.2024.v13i01.007.

[4] A. Scrivano, “A Comparative Study of Classical and Post-Quantum Cryptographic Algorithms in the Era of Quantum Computing,” pp. 1–16, 2025, [Online]. Available: http://arxiv.org/abs/2508.00832

[5] E. Fathalla and M. Azab, “Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-Based Signature Schemes, Security, and Optimizations,” *IEEE Access*, vol. 12, no. September, pp. 175969–175987, 2024, doi: 10.1109/ACCESS.2024.3485602.

[6] F. R. Ghashghaei, Y. Ahmed, N. Elmrabit, and M. Yousefi, “Enhancing the Security of Classical Communication with Post-Quantum Authenticated-Encryption Schemes for the

e-ISSN 3063-4687

Quantum Key Distribution," *Computers*, vol. 13, no. 7, 2024, doi: 10.3390/computers13070163.

[7] I. A. Abdulmunem and M. M. Hoobi, "Enhanced DES Algorithm Using Efficient Classical Algorithm," *Iraqi J. Sci.*, vol. 65, no. 12, pp. 7251–7275, 2024, doi: 10.24996/ijs.2024.65.12.37.

[8] R. A. Manurung, Sutarman, and S. Efendi, "Comparative Analysis of the Performance of Four Symmetric Algoritms on Digital File Security," *JITE (Journal Informatics Telecommun. Eng.*, vol. 8, no. 2, pp. 152–164, 2023, [Online]. Available: https://www.researchgate.net/publication/335117624_Malang_City_Polytechnic_Web_Based_Student_Attendance_Information_System_Telecommunications_Engineering_Study_Program_Using_Fingerprint/fulltext/5d515fe34585153e594ef214/Malang-City-Polytechnic-Web-Based-S

[9] A. A. Siagian and Z. Indra, "Analisis Teknik Playfair Dan Shift Cipher Sebagai Metode Kriptografi Klasik Untuk Keamanan Data," *J. Komput. dan Teknol.*, vol. 4, no. 1, pp. 13–19, 2025, doi: 10.58290/jukomtek.v4i1.315.

[10] Dimas Mayoni Aji Sasono, Muhlis Tahir, Fathricia Angel M. V., Mar'atul Azizah, Luluk Fariska Utami, and Nurul Septiana, "Perbandingan Kriptography Klasik Caesar Cipher Dengan Kriptography Modern Aes Dalam Tingkat Keamanan Jaringan Komputer," *J. Informasi, Sains dan Teknol.*, vol. 6, no. 1, pp. 72–77, 2023, doi: 10.55606/isaintek.v6i1.93.

[11] A. Zuhri, H. R. Putra, A. Fazri, and M. Miftahurrahmah, "Aplikasi Pesan Instan Accessible Di Era Komunikasi Kontemporer Tahun 2022 Bagi Digital Natives Indonesia," *Komuniti J. Komun. dan Teknol. Inf.*, vol. 14, no. 2, pp. 165–189, 2022, doi: 10.23917/komuniti.v14i2.17729.

[12] M. H. M. Baig, H. B. Ul Haq, and W. Habib, "A Comparative Analysis of AES, RSA, and 3DES Encryption Standards based on Speed and Performance," *Manag. Sci. Adv.*, vol. 1, no. 1, pp. 20–30, 2024, doi: 10.31181/msa1120244.

[13] V. Zuliani Erikasari, W. Zahra Mulqiya, T. Firli Maharani, and A. Turmudi Zy, "Studi Efektivitas Metode Hybrid Caesar-Vigenere Cipher dalam Keamanan Teks Effectiveness Study of Hybrid Caesar-Vigenere Cipher Method in Text Security," vol. 15, no. 1, pp. 33–42, 2025, [Online]. Available: https://stmikpontianak.org/ojs/index.php/sisfotenika

[14] Uci Julya Ningsih, Sophia Salsabila, Isniar Hutapea, Dewi Santika, and Indra Gunawan, "Pendekripsian Caesar Chiper Dengan Menggunakan Teknik-Teknik Kriptanalisis," *J. Ilmu Komput. dan Multimed.*, vol. 1, no. 1, pp. 11–15, 2024, doi: 10.46510/ilkomedia.v1i1.10.

[15] M. Rahmawati, SH., *Hukum Bisnis Di Era Digital*, vol. 3, no. maret. 2024.