**Jurnal Informasi, Sains dan Teknologi**, P-ISSN: 2621-0940 ,E-ISSN: 2829-2758 hal 72-77

# Perbandingan Kriptography Klasik Caesar Cipher Dengan Kriptography Modern Aes Dalam Tingkat Keamanan Jaringan Komputer

**Dimas Mayoni Aji Sasono, Muhlis Tahir, Fathricia Angel M. V., Mar'atul Azizah, Luluk Fariska Utami, Nurul Septiana**
Universitas Trunojoyo Madura
dimassasono2@gmail.com, muhlis.tahir@trunojoyo.ac.id, fathriciaangel@gmail.com, Izaa93390@gmail.com, Lulukfariska16@gmail.com, Nurulseptiana38@gmail.com
*korespondensi penulis dimassasono2@gmail.com*

***Abstract****. Cryptography (cryptography) is the science and art of keeping messages safe. The sender of the message will encrypt it while the recipient of the message will decrypt it. The encryption and decryption process uses keywords that have been agreed upon by the sender and recipient of the message. To better understand the development of cryptography, this journal will introduce a comparison of classical cryptography and modern cryptography at the level of computer network security. The cryptography that will be compared is Caesar Cipher and AES. This study uses the method of literature review (library research), namely research based on expert opinion and the results of previous studies.*

***Keywords***: *Comparison, Cryptography, Caesar Cipher, AES*

**Abstrak.** Kriptografi (cryptography) merupakan ilmu dan seni yang memiliki tujuan untuk menjaga pesan agar aman. Pengirim pesan akan melakukan proses enkripsi sedangkan penerima pesan melakukan proses dekripsi. Proses enkripsi dan dekripsi menggunakan kata kunci yang telah disepakati oleh pengirim dan penerima pesan. Untuk memahami perkembangan kriptografi lebih mendalam, maka di dalam jurnal ini akan diperkenalkan perbandingan kriptografi klasik dan kriptografi modern dalam tingkat keamanan jaringan komputer. Kriptografi yang akan dibandingkan yaitu Caesar Cipher dan AES. Penelitian ini menggunakan metode berupa tinjauan literatur (library research), yaitu penelitian yang didasarkan pada pendapat ahli dan hasil dari penelitian terdahulu.

**Kata kunci**: Perbandingan, Kriptografi, Caesar Cipher, AES.

## LATAR BELAKANG

Kemajuan tekonologi dalam pengelolaan dokumen saat ini telah memiliki kemudahan secara digital, hal tersebut membuat terjadinya peningkatan kejahatan di dunia maya, seperti pencurian informasi yang bersifat rahasia. Dikarenakan keamanan dokumen digital bersifat lemah dan mudah diakses secara legal ataupun ilegal oleh pihak lain. Maka dibutuhkan suatu teknik penyandian untuk menyamarkan pesan menjadi bentuk lain. Teknik tersebut akan membuat pihak

yang tidak diinginkan kesulitan dalam mencuri informasi rahasia tersebut, teknik penyandian ini akan melindungi data atau pesan digital yang bersifat pribadi atau rahasia.

Kriptografi(cryptography)merupakan ilmu dan seni untuk menjaga pesan agar aman. (Cryptography is the art and science of keeping messages secure) “Crypto” berarti “secret” (rahasia) dan “graphy” berarti “writing” (tulisan). Jadi, kriptologi adalah ilmu dan seni untuk menjaga keamanan pesan yang akan dikirim ke penerima sehingga data atau pesan tersebut aman dan tidak diketahui oleh pihak ketiga (Sumandri, 2017). Kriptografi dibagi menjadi dua jenis yaitu kriptografi klasik dan kriptografi modern, kriptografi klasik digunakan sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Metode menyembunyikan pesannya adalah dengan teknik substitusi atau transposisi, bahkan bisa menggunakan keduanya secara bersamaan. Teknik substitusi adalah mengganti karakter dalam *plaintext* menjadi karakter lain yang hasilnya adalah *ciphertext*. Sedangkan transposisi adalah teknik mengubah *plaintext* menjadi *ciphertext* dengan cara melakukan permutasi pada karakternya. Kemudian, kombinasi keduanya secara kompleks adalah yang melatarbelakangi terbentuknya berbagai macam algoritma kriptografi modern. Contoh algoritma kriptografi klasik yaitu: *Caesar Cipher, Vigenere Cipher*, dan *Hill Cipher*. Kriptografi Modern merupakan suatu perbaikan dari Teknik yang digunakan pada kriptografi klasik. Algoritma di kriptografi modern ini menggunakan pengolahan dan penggunaan simbol biner yang dibentuk dari kode ASCII (*American Standard Code for Information Interchange*) karena berjalan mengikuti operasi komputer digital, sehingga membutuhkan pengetahuan dasar matematika untuk menguasainya. Algoritma ini juga memiliki tingkat kesulitan yang lebih kompleks yang menyebabkan kriptanalis sangat sulit memecahkan *ciphertext* tanpa mengetahui kuncinya. Adapun jenis kunci dalam kriptografi modern terdiri dari 3 yaitu: simetri, asimetri, dan hibrida. Pada kriptogarfi modern terdapat berbagai macam algoritma yang memiliki tujuan untuk mengamankan informasi yang dikirim melalui jaringan computer, contoh kriptografi modern yaitu MD5, RC4, AES dan lain-lain.

**KAJIAN TEORITIS**

. Caesar Chiper

Caesar Cipher, diketahui merupakan salah satu algoritma cipher tertua dalam perkembangan ilmu kriptografi. Caesar cipher juga merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada chiperteks. Teknik seperti ini disebut juga sebagai chiper abjad tunggal. Algoritma

dari kriptografi Caesar Cipher ini sangat mudah untuk digunakan siapa saja. Kunci dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama (Warnillah, et al., 2018). Adapun langkah-langkah yang dilakukan dalam membentuk chiperteks dengan Caesar Cipher adalah:

1. Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk cipherteks ke plainteks
2. Menukarkan karakter pada plainteks menjadi cipherteks dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya. Algoritma dari Caesar Cipher adalah C = E (P) = (P + K) mod 26 untuk fungsi enkripsi. Sedangkan untuk fungsi dekripsi adalah P = D (C) = (C - K) mod 26.

B. AES (Advanced Encryption Standard)

Advanced Encryption Standard (AES) adalah salah satu algoritma chiper yang digunakan untuk melindungi data atau informasi yang sifatnya rahasia. Sejak 2001, AES telah menggantikan algoritma Data Encryption Standard (DES), DES dianggap sudah kuno dan mudah dibobol atau ditembus oleh pihak yang tidak diinginkan (Andriyanto, et al., 2022). AES merupakan sistem penyandian blok yang bersifat non-Feistel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. AES menggunakan sebuah ronde untuk proses yang berulang dalam pembuatan kuncinya. Proses di dalam AES adalah sebuah transformasi terhadap state. Sebuah teks asli dalam blok (128 bit) terlebih dahulu diorganisir sebagai state. Enkripsi AES adalah transformasi terhadap state secara berulang dalam beberapa ronde. State yang menjadi keluara ronde k menjadi masukan untuk ronde ke-k +1. Pada Proses enkripsi awalnya teks asli dibentuk sebagai sebuah state. Kemudian sebelum ronde 1 dimulai blok teks asli dicampur dengan kunci ronde ke-0 (transformasi ini disebut AddRoundKey). Setelah itu, ronde ke-1 sampai dengan ronde ke-(Nr-1) dengan Nr adalah jumlah ronde (Tulloh, et al., 2016). AES menggunakan 4 jenis transformasi yaitu:

1. SubBytes, merupakan transformasi subtutusi.
2. ShiftRows, merupakan transformasi permutasi.
3. MixColumns, merupakan transformasi pengacakan.
4. AddRoundKey, merupakan transformasi penambahan kunci.

Pada ronde terakhir, yaitu ronde ke-Nr akan dilakukan transformsi serupa dengan ronde lainnya, namun tanpa transfomasi serupa dengan ronde lainnya (transformasi tanpa MixColumns). Algotirma dekripsi AES dapat diilustrasikan seperti Gambar 1. Secara ringkas algoritma deskripsi merupakan kebalikan dari algoritma enkripsi AES, yaitu algoritma dekripsi akan menggunakan Tansformasi invers terhadap semua transformasi dasar yang digunakan pada algoritma enkripsi AES. Setiap tranformasi dasar dari algoritma kriptografi AES memiliki transformasi invers, yaitu: InvSubBytes, InvShiftRows dan InvMixColumns (Tulloh, et al., 2016).

## HASIL DAN PEMBAHASAN

AES merupakan metode enkripsi yang lebih aman dan kompleks dibandingkan dengan Caesar Cipher. AES menggunakan kunci enkripsi yang lebih panjang, algoritma kriptografi simetris yang lebih kuat, dan telah terbukti efektif dalam melindungi data penting di seluruh dunia. Di sisi lain, Caesar Cipher merupakan metode enkripsi yang sangat sederhana dan mudah ditebak, karena hanya menggeser huruf dalam pesan sebanyak tiga posisi. Meskipun Caesar Cipher lebih mudah dipahami dan digunakan untuk tujuan pendidikan, namun dalam konteks keamanan jaringan modern, metode ini tidak lagi dianggap sebagai metode kriptografi yang aman.

AES memberikan tingkat keamanan yang lebih tinggi dalam melindungi data dari akses yang tidak sah dan modifikasi, sedangkan Caesar Cipher memberikan tingkat keamanan yang rendah dan mudah ditembus oleh penyerang. AES lebih tahan terhadap serangan kriptografi modern seperti serangan brute force dan serangan side-channel, sementara Caesar Cipher lebih rentan terhadap serangan brute force. AES membutuhkan waktu lebih lama untuk melakukan enkripsi dan dekripsi dibandingkan dengan Caesar Cipher, karena kompleksitas algoritma yang lebih tinggi. Namun, keamanan data yang dihasilkan jauh lebih tinggi daripada Caesar Cipher.

Penggunaannya, AES sering digunakan dalam keamanan jaringan modern, seperti mengamankan data transaksi finansial online, email, dan data militer. Sedangkan Caesar Cipher lebih cocok digunakan untuk tujuan pendidikan dan pemahaman dasar tentang konsep enkripsi. Dalam jangka panjang, AES memberikan tingkat keamanan yang lebih baik karena kompleksitas algoritma dan kunci yang digunakan lebih sulit untuk ditembus oleh penyerang. Dengan demikian, dalam konteks keamanan jaringan modern, AES merupakan metode enkripsi yang lebih direkomendasikan dibandingkan dengan Caesar Cipher.

Tingkat kompleksitas AES menggunakan kunci enkripsi 128-bit, 192-bit, atau 256-bit. Kunci enkripsi tersebut digunakan untuk mengacak data dan menjadikannya tidak dapat dibaca oleh orang yang tidak memiliki kunci enkripsi yang benar. Di sisi lain, Caesar Cipher merupakan metode enkripsi yang sangat sederhana dan mudah ditebak, karena hanya menggeser huruf dalam pesan sebanyak tiga posisi.

Kecepatan, AES membutuhkan waktu lebih lama untuk melakukan enkripsi dan dekripsi dibandingkan dengan Caesar Cipher. Hal tersebut disebabkan karena kompleksitas algoritma pada AES lebih tinggi. Namun, meskipun AES membutuhkan waktu lebih lama, keamanan data yang dihasilkan jauh lebih tinggi daripada Caesar Cipher.

Jenis algoritma dan Jenis serangan, AES menggunakan algoritma kriptografi simetris yang lebih kompleks, sedangkan Caesar Cipher hanya menggunakan algoritma penggeseran sederhana. Dalam AES, enkripsi dan dekripsi menggunakan algoritma yang sama, sementara Caesar Cipher menggunakan algoritma yang berbeda untuk enkripsi dan dekripsi. AES lebih tahan terhadap serangan kriptografi modern, seperti serangan brute force dan serangan side-channel. Sedangkan Caesar Cipher lebih rentan terhadap serangan brute force, di mana penyerang dapat mencoba semua kemungkinan kombinasi huruf dan angka hingga menemukan pesan asli.

## KESIMPULAN DAN SARAN

### KESIMPULAN

Berdasarkan perbandingan caesar cipher dan AES dapat disimpulkan bahwa metode AES lebih unggul dari caesar cipher. AES merupakan metode enkripsi yang lebih aman dan kompleks dibandingkan dengan caesar cipher. AES menggunakan kunci enkripsi yang lebih panjang, algoritma kriptografi simetris yang lebih kuat, dan telah terbukti efektif dalam melindungi data penting di seluruh dunia. Selanjutnya pada jenis algoritma dan jenis serangan, AES menggunakan algoritma kriptografi simetris yang lebih kompleks, sedangkan caesar cipher hanya menggunakan algoritma penggeseran sederhana. AES lebih tahan terhadap serangan kriptografi modern, seperti serangan brute force dan serangan side-channel, sedangkan caesar cipher lebih rentan terhadap serangan brute force, di mana penyerang dapat mencoba semua kemungkinan kombinasi huruf dan angka hingga menemukan pesan asli.

## SARAN

Berdasarkan kesimpulan yang telah dijelaskan sebelumnya, penulis memilikii harapan dimasa yang akan datang dengan ditemukan atau diteliti lebih lanjut mengenai perbandingan caesar cipher dan AES sehingga bisa di kaji lebih mendalam terkait keamanan dalam menggunakan caesar cipher atau AES. Selanjutnya, bagaimana AES selalu memperbarui kunci enkripsi secara teratur dan menggunakan kunci yang kuat dengan panjang yang lebih besar, sehingga lebih sulit ditembus oleh penyerang. Selain itu, pastikan juga untuk melindungi kunci enkripsi dari akses yang tidak sah dan menggunakan mode enkripsi yang tepat untuk kebutuhan spesifik. Sementara caesar cipher tidak digunakan untuk tujuan keamanan jaringan modern karena mudah ditebak dan tidak aman. Namun, metode ini dapat digunakan untuk tujuan pendidikan dan pemahaman dasar tentang konsep enkripsi.

## DAFTAR PUSTAKA


Aisyah, A., & Ariyanto, H. (2017). Perbandingan antara algoritma AES dan Caesar Cipher dalam pengamanan data berbasis web. Jurnal Informatika, 6(2), 143-148.

Andriyanto, M. R., & Sukmasetya, P. (2022). Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Keamanan Data Transaksi Pada Sistem E-Marketplace. Journal of Computer System and Informatics (JoSYC), 4(1), 179-187.

Gumelar, D. B., & Pramusinto, W. (2018). Implementasi Algoritma Kriptografi Dengan Algoritma Caesar Cipher, Advanced Encryption Standard 256, Dan Rc6 Untuk Aplikasi Chatting Berbasis Android. Skanika, 1(2), 711-717.

Irianto, R. P., & Kusumadewi, S. (2019). Analisis perbandingan AES, Blowfish, dan Caesar Cipher dalam keamanan file teks. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 3(12), 5183-5188.

Maulana, I., & Kristiawan, M. (2020). Analisis perbandingan algoritma Caesar Cipher dan AES pada sistem keamanan data. Jurnal Teknologi dan Sistem Komputer, 8(4), 212-219.

Nugroho, A. S. (2019). Penerapan Algoritma AES dan Caesar Cipher pada Sistem Pengamanan Email. Jurnal Teknologi dan Sistem Komputer, 7(1), 25-30.

Nurhadiyanto, P., & Kurniawan, A. (2021). Perbandingan algoritma kriptografi Caesar Cipher dan AES dalam pengamanan data di aplikasi smartphone. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 5(2), 1852-1859.

Raharjo, B., & Yuliani, R. (2017). Analisis Keamanan AES dan Caesar Cipher pada Aplikasi Instant Messaging. Jurnal Ilmiah Komputer dan Informatika, 10(1), 11-20.

Sumandri. (2017). Studi Model Algoritma Kriptografi Klasik dan Modern. Yogyakarta.

Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen. Matematika: Jurnal Teori dan Terapan Matematika, 15(1).

Warnilah, A. I., & Nugraha, S. N. (2018). Komparasi Algoritma Kriptografi Elgamal Dan Caesar Cipher Untuk Enkripsi Dan Dekripsi Pesan. IJCIT (Indonesian Journal on Computer and Information Technology) Vol, 3.