ALGORITMA DES

Adam Anwar[1], Meilisa Kesia M[2], Octavia Christyanti S[3], Rizky Andi K[4], Alvendo Wahyu Aranski[5]
Institut Teknologi Batam
2021046@student.iteba.ac.id

Abstrak

Keamanan data menjadi hal yang sangat penting menghadapi peningkatan kasus pencurian data untuk tujuan kriminal. Kriptografi menjadi solusi kunci dalam menjaga informasi melalui teknik enkripsi yang menjamin kerahasiaan dan integritas data. Algoritma Data Encryption Standard (DES), yang diadopsi oleh NIST sebagai Standar Pengolahan Informasi Federal, telah menjadi algoritma kriptografi yang terkemuka secara global. Jurnal ini menyajikan tinjauan komprehensif tentang Algoritma DES, mencakup prinsip-prinsipnya, metode enkripsi, dan relevansinya dalam mengamankan data elektronik. Dengan menggunakan metode analisis deskriptif dengan pendekatan literatur, penelitian ini mengkaji Algoritma DES secara kritis, mempertimbangkan prinsip kerjanya, proses enkripsi, dan aplikasinya dalam keamanan data. Meskipun digunakan secara luas, kekhawatiran tentang keamanan DES muncul karena panjang kunci yang relatif pendek (56 bit), membuatnya rentan terhadap serangan brute-force. Para peneliti telah mengusulkan algoritma yang lebih kuat dengan panjang kunci yang lebih besar untuk mengatasi tantangan keamanan yang terus berkembang di era digital ini. Kesimpulannya, DES telah menjadi penting dalam kriptografi modern, namun penelitian yang berkelanjutan diperlukan untuk mengatasi ancaman keamanan yang terus berkembang. Pertimbangan terhadap kebutuhan aplikasi khusus menjadi penting saat menggunakan algoritma DES.

Key Words: Keamanan data, Pencurian data, Kriptografi, Enkripsi.

1. PENDAHULUAN

Pengamanan data menjadi isu yang semakin mendesak dalam era digital saat ini, terutama dengan maraknya kasus pencurian data untuk tindakan kejahatan, termasuk penyalahgunaan data untuk kegiatan kriminal. Pencurian data ini menyebabkan

kekhawatiran tentang kerahasiaan, integritas, dan keutuhan data pengguna. Oleh karena itu, kriptografi, sebagai ilmu yang mempelajari teknik enkripsi untuk menjaga kerahasiaan data, menjadi sangat penting dalam upaya mengamankan data elektronik. Salah satu algoritma kriptografi yang telah memainkan peran penting dalam kemajuan kriptografi modern adalah Algoritma DES (Data Encryption Standard). Algoritma ini diadopsi oleh NIST sebagai standar pengolah informasi Federal AS dan telah menjadi algoritma enkripsi yang paling banyak digunakan di dunia.

Dalam konteks ini, jurnal ini bertujuan untuk mengulas secara mendalam tentang Algoritma DES. Akan dijelaskan prinsip kerja algoritma ini, metode enkripsi yang digunakan, serta relevansi dan peran Algoritma DES dalam mengamankan data elektronik. Dalam pembahasan ini, jurnal juga akan mengutip sumber-sumber yang relevan yang berkaitan dengan Algoritma DES, termasuk penjelasan dari Tampubolon (2021), Ariska & Wahyuddin (2022), Primartha (2011), dan Asmara et al. (2012).

2. METODELOGI PENELITIAN

Studi ini menggunakan metode analisis deskriptif dengan pendekatan literatur untuk mengumpulkan informasi tentang Algoritma DES. Sumber data yang digunakan meliputi jurnal ilmiah, artikel, dan buku yang berhubungan dengan kriptografi, khususnya tentang Algoritma DES. Data yang diperoleh dari berbagai sumber tersebut kemudian dianalisis secara kritis untuk memahami prinsip kerja, metode enkripsi, dan aplikasi Algoritma DES dalam pengamanan data elektronik.

3. ANALISA DAN PERANCANGAN

Algoritma DES, juga dikenal sebagai Data Encryption Standard, adalah algoritma kriptografi yang sangat berpengaruh dalam dunia keamanan informasi. Algoritma ini menggunakan metode enkripsi blok, di mana data plaintext berukuran 64 bit diubah menjadi data ciphertext berukuran 64 bit menggunakan kunci internal 56 bit. Proses enkripsi melibatkan beberapa tahapan transformasi data, termasuk substitusi, permutasi, dan fungsi XOR, untuk menghasilkan output ciphertext.

Seperti yang dikutip oleh Tampubolon (2021), peran kriptografi dalam mengamankan dokumen adalah dengan menggunakan teknik enkripsi sehingga dokumen tidak dapat dibaca oleh kriptanalis, yaitu orang yang memecahkan chipertext

menjadi plaintext tanpa mengetahui kunci dan algoritma yang digunakan. Algoritma DES diadopsi oleh NIST sebagai standar pengolah informasi Federal AS dan telah menjadi algoritma enkripsi yang paling banyak digunakan di dunia (Primartha, 2011).

Keunikan Algoritma DES terletak pada penggunaan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah K1, K2, ..., K16, maka pada proses dekripsi urutan kunci yang digunakan adalah K16, K15, ..., K1. Dengan kata lain, algoritma yang digunakan untuk enkripsi dan dekripsi sebenarnya sama, hanya perbedaannya pada penggunaan urutan dengan kemajuan teknologi, panjang kunci yang relatif pendek (56 bit) menjadi rentan terhadap serangan brute-force kunci internal yang terbalik (Asmara et al., 2012).

4. KESIMPULAN

Algoritma DES telah menjadi salah satu tonggak penting dalam perkembangan kriptografi modern dan telah digunakan secara luas dalam mengamankan data elektronik. Namun, dengan perkembangan teknologi dan meningkatnya kekuatan komputasi, keamanan Algoritma DES telah menjadi pertanyaan. Penelitian dan pengembangan lanjutan dalam bidang kriptografi diperlukan untuk menghadapi tantangan keamanan yang semakin kompleks di era digital ini. Meskipun demikian, penggunaan Algoritma DES dapat dipertimbangkan dengan bijaksana dengan memperhatikan lingkungan dan tingkat keamanan yang dibutuhkan dalam masing-masing aplikasi.

REFERENSI

Ariska, & Wahyuddin. (2022). PENERAPAN KRIPTOGRAFI MENGGUNAKAN ALGORITMA DES (DATA ENCRYPTION STANDARD) (Vol. 2, Issue 2). https://jurnal.umpar.ac.id/index.php/sylogghttps://jurnal.umpar.ac.id/index.php/syl og

Asmara, D. I. W., Kesiman, A. W. M., & Agustini, K. (2012). PENGEMBANGAN APLIKASI KRIPTOGRAFI FILE AUDIO DENGAN ALGORITMA DATA ENCRYPTION STANDARD (DES). Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI), 1, 130–147. https://ejournal.undiksha.ac.id/index.php/janapati/article/view/9827

Kromodimoeljo, S. (2009). Teori dan Aplikasi Kriptografi. SPK IT Consulting.

Primartha, R. (2011). Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES). Jurnal Sistem Informasi (JSI), 3(2), 371–387. http://ejournal.unsri.ac.id/index.php/jsi/index

Tampubolon, A. (2021). Implementasi Kombinasi Algoritma RSA dan Algoritma DES Pada Aplikasi Pengaman Pesan Teks. Jurnal Sains Manajemen Informatika Dan Komputer, 20(1), 38–43. https://ojs.trigunadharma.ac.id/