Edusola : Journal Education, Sociology and Law
https://publisherqu.com/index.php/edusola
Vol. 1 No. 4 Desember 2025
https://issn.brin.go.id/terbit/detail/20250326110343005

IMPLEMENTASI KRIPTOGRAFI UNTUK KEAMANAN DATA MENGGUNAKAN ALGORITMA DES

Rozan Syaikh Ash Shiddieq Purnomo[1], Anindo Saka Fitri[2], Agung Brastama Putra[3]
Universitas Pembangunan Nasional "Veteran" Jawa Timur
Email : rozanpurnomo26@gmail.com[1], anindo.saka.si@upnjatim.ac.id[2], agungbp.si@upnjatim.ac.id[3]

Abstrak

Keamanan data merupakan aspek penting dalam sistem informasi seiring dengan meningkatnya penggunaan teknologi komputer dalam berbagai bidang. Data yang disimpan dan ditransmisikan melalui sistem digital memiliki risiko terhadap ancaman seperti pencurian, penyadapan, dan manipulasi informasi. Oleh karena itu, diperlukan mekanisme pengamanan data yang efektif, salah satunya melalui penerapan kriptografi. Penelitian ini bertujuan untuk mengimplementasikan algoritma Data Encryption Standard (DES) sebagai metode kriptografi untuk mengamankan data komputer. Metode penelitian yang digunakan adalah metode implementasi, yaitu dengan menerapkan algoritma DES pada proses enkripsi dan dekripsi data. Proses enkripsi dilakukan menggunakan struktur Feistel Network yang terdiri dari permutasi awal, 16 putaran enkripsi, dan permutasi akhir. Hasil penelitian menunjukkan bahwa data plaintext berhasil dienkripsi menjadi ciphertext yang tidak dapat dibaca secara langsung dan dapat dikembalikan ke bentuk semula melalui proses dekripsi dengan kunci yang sama. Pengujian efek avalanche menunjukkan bahwa perubahan kecil pada plaintext menghasilkan perubahan bit yang signifikan pada ciphertext, menandakan tingkat difusi yang baik. Selain itu, uji konsistensi dan validasi membuktikan bahwa algoritma DES menghasilkan output yang stabil dan akurat. Meskipun memiliki keterbatasan pada panjang kunci, algoritma DES tetap efektif sebagai media pembelajaran dan implementasi dasar dalam sistem keamanan data.
Kata Kunci : Kriptografi, Data Encryption Standard (DES), Keamanan Data, Enkripsi, Dekripsi.

Abstract

Data security is an important aspect in information systems along with the increasing use of computer technology in various fields. Data stored and transmitted through digital systems are at risk of threats such as theft, eavesdropping, and information manipulation. Therefore, an effective data security mechanism is needed, one of which is through the application of cryptography. This study aims to implement the Data Encryption Standard (DES) algorithm as a cryptographic method to secure computer data. The research method used is the implementation method, namely by applying the DES algorithm to the data encryption and decryption process. The encryption process is carried out using the Feistel Network structure consisting of an initial permutation, 16 rounds of encryption, and a final permutation. The results show that the plaintext data is successfully encrypted into ciphertext that cannot be read directly and can be restored to its original form through the decryption process with the same key. Avalanche effect testing shows that small changes in the plaintext result in significant bit changes in the ciphertext, indicating a good level of diffusion. In addition,

consistency and validation tests prove that the DES algorithm produces stable and accurate output. Despite its key length limitations, the DES algorithm remains effective as a learning tool and as a basic implementation in data security systems.
Keywords: Cryptography, Data Encryption Standard (DES), Data Security, Encryption, Decryption.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang semakin pesat telah mendorong peningkatan penggunaan sistem komputer dalam berbagai bidang, seperti pemerintahan, pendidikan, bisnis, dan industri. Penggunaan teknologi tersebut menghasilkan pertukaran dan penyimpanan data dalam jumlah besar yang memiliki nilai penting dan bersifat rahasia. Oleh karena itu, aspek keamanan data menjadi kebutuhan utama untuk melindungi informasi dari ancaman seperti pencurian data, penyadapan, maupun penyalahgunaan oleh pihak yang tidak berwenang.

Keamanan data dalam sistem komputer tidak hanya berkaitan dengan perlindungan fisik perangkat, tetapi juga mencakup pengamanan data secara logis. Salah satu teknik yang banyak digunakan untuk menjaga kerahasiaan data adalah kriptografi. Kriptografi merupakan ilmu dan seni untuk mengamankan informasi dengan cara mengubah data asli (plaintext) menjadi data tersandi (ciphertext) sehingga tidak dapat dibaca tanpa kunci tertentu. Dengan penerapan kriptografi, data yang dikirim maupun disimpan dapat terjaga kerahasiaan dan integritasnya.

Data Encryption Standard (DES) adalah algoritma kriptografi simetris yang pernah menjadi standar keamanan data dan banyak digunakan dalam berbagai sistem informasi. Algoritma ini menggunakan satu kunci rahasia yang sama pada proses enkripsi dan dekripsi data. DES bekerja dengan memproses data dalam blok berukuran 64 bit melalui serangkaian operasi permutasi dan substitusi yang dilakukan dalam 16 putaran. Mekanisme tersebut bertujuan untuk menghasilkan ciphertext yang sulit untuk dipecahkan tanpa mengetahui kunci yang digunakan.

Meskipun saat ini telah berkembang algoritma kriptografi yang lebih kuat, seperti Advanced Encryption Standard (AES), algoritma DES masih relevan untuk dipelajari sebagai dasar pemahaman kriptografi. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan algoritma DES dalam keamanan data komputer guna mengetahui cara kerja serta efektivitas penerapannya dalam menjaga kerahasiaan data. Hasil penelitian ini diharapkan dapat memberikan gambaran yang jelas mengenai penerapan kriptografi sebagai

solusi pengamanan data.

METODE PENELITIAN

Pada penelitian kali ini, penulis menggunakan metode implementasi kriptografi dengan menerapkan algoritma Data Encryption Standard (DES) dalam keamanan data komputer. Implementasi menurut Kamus Besar Bahasa Indonesia (KBBI) memiliki arti pelaksanaan atau penerapan. Oleh karena itu, penelitian ini berfokus pada penerapan algoritma DES secara langsung untuk mengamankan data.

HASIL DAN PEMBAHASAN

Struktur Sistem Sandi DES (Data Encryption Standard)

Algoritma Data Encryption Standard (DES) merupakan algoritma kriptografi simetris berbasis blok (block cipher) yang bekerja dengan ukuran blok data sebesar 64 bit dan panjang kunci efektif sebesar 56 bit. Delapan bit tambahan pada kunci 64 bit digunakan sebagai bit paritas sehingga tidak berperan langsung dalam proses enkripsi. DES dirancang untuk menyediakan mekanisme pengamanan data dengan tingkat kerahasiaan yang tinggi melalui proses transformasi bit yang kompleks dan berlapis. Struktur algoritma DES dibangun menggunakan konsep Feistel Network, yaitu suatu struktur kriptografi yang membagi data menjadi dua bagian yang diproses secara berulang dalam beberapa putaran (round). Keunggulan utama dari struktur Feistel adalah penggunaan mekanisme yang sama untuk proses enkripsi dan dekripsi, di mana perbedaannya hanya terletak pada urutan penggunaan sub-kunci. Hal ini membuat implementasi algoritma menjadi lebih efisien dan sistematis.

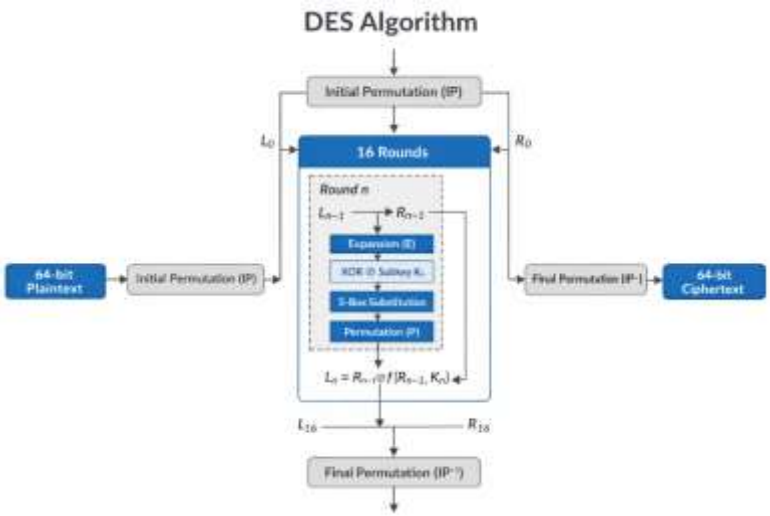
Secara umum, struktur sistem sandi DES terdiri dari tiga komponen utama, yaitu Initial Permutation (IP), proses 16 putaran enkripsi, dan Final Permutation (IP^{-1}). Proses enkripsi diawali dengan melakukan Initial Permutation terhadap plaintext berukuran 64 bit. Permutasi ini berfungsi untuk mengacak posisi bit-bit data berdasarkan tabel permutasi tertentu, sehingga distribusi bit menjadi lebih merata sebelum memasuki tahap inti enkripsi. Setelah proses IP, data hasil permutasi dibagi menjadi dua bagian yang sama besar, yaitu bagian kiri (L_0) dan bagian kanan (R_0), masing-masing berukuran 32 bit. Kedua bagian ini kemudian diproses melalui 16 putaran (round) enkripsi. Pada setiap putaran, bagian kanan data diproses menggunakan fungsi kompleks yang disebut fungsi f, kemudian hasilnya dioperasikan dengan bagian kiri menggunakan operasi XOR. Setelah itu, posisi bagian kiri dan kanan ditukar untuk diproses pada putaran berikutnya.

Setiap putaran menggunakan sub-kunci yang berbeda yang dihasilkan dari kunci utama melalui proses pembangkitan kunci (key schedule). Sub-kunci ini berukuran 48 bit dan berperan penting dalam meningkatkan kompleksitas algoritma. Penggunaan sub-kunci yang berbeda pada setiap putaran bertujuan untuk memperkuat keamanan sandi, sehingga ciphertext yang dihasilkan menjadi sulit untuk dianalisis atau dipecahkan tanpa mengetahui kunci rahasia yang benar. Setelah seluruh 16 putaran selesai, bagian kiri dan kanan digabung kembali dengan urutan terbalik, kemudian diproses melalui Final Permutation (IP^{-1}). Permutasi akhir ini merupakan kebalikan dari permutasi awal dan menghasilkan ciphertext 64 bit sebagai output akhir dari proses enkripsi DES. Struktur berlapis inilah yang menjadikan algoritma DES mampu memberikan perlindungan terhadap data meskipun memiliki keterbatasan pada panjang kunci.

Skema Global Algoritma DES

Skema global algoritma DES menggambarkan alur proses enkripsi secara keseluruhan, mulai dari input plaintext hingga menghasilkan ciphertext. Proses tersebut dapat dijelaskan sebagai berikut:

1. Plaintext 64 bit → Initial Permutation (IP)
2. Pembagian data menjadi L_0 dan R_0
3. Proses 16 round Feistel
4. Penggabungan R_{16} dan L_{16}
5. Final Permutation (IP^{-1}) → Ciphertext



Gambar 1. Skema Global Algoritma DES

Setiap round melakukan operasi fungsi f(R, K) yang terdiri dari ekspansi bit, XOR

dengan kunci, substitusi melalui S-Box, dan permutasi.

Proses Round DES dan Fungsi f

Pada algoritma Data Encryption Standard (DES), proses inti enkripsi terletak pada mekanisme 16 putaran (round) yang menggunakan struktur Feistel Network. Pada setiap putaran, bagian kanan data (R) diproses menggunakan fungsi f, yang berperan sebagai komponen utama dalam menciptakan kompleksitas dan keamanan algoritma DES. Fungsi ini dirancang untuk menghasilkan perubahan bit yang signifikan meskipun hanya terjadi perubahan kecil pada plaintext atau kunci. Fungsi f terdiri dari empat tahap utama, yaitu Expansion (E-Box), XOR dengan Subkey, Substitution (S-Box), dan Permutation (P-Box). Setiap tahap memiliki peran penting dalam meningkatkan keamanan data.

Expansion (E-Box)

Tahap pertama adalah **ekspansi**, di mana data bagian kanan (**R**) yang berukuran 32 bit diperluas menjadi 48 bit menggunakan tabel ekspansi (*Expansion Box*). Tujuan dari proses ini adalah untuk menyesuaikan ukuran data dengan panjang sub-kunci serta menciptakan duplikasi bit tertentu sehingga meningkatkan efek difusi.

Tabel 1. Perubahan Ukuran Bit pada Tahap Expansion

Tahap	Ukuran Bit
Input R	32 bit
Output E(R)	48 bit

XOR dengan Subkey

Hasil ekspansi 48 bit kemudian dioperasikan menggunakan operasi XOR dengan sub-kunci KnK_nKn yang juga berukuran 48 bit. Proses ini menggabungkan kunci rahasia ke dalam data, sehingga tanpa kunci yang benar, ciphertext tidak dapat didekripsi.

Tabel 2. Operasi XOR pada Fungsi f

Komponen	Ukuran
Data hasil ekspansi	48 bit
Sub-kunci (Kn)	48 bit
Hasil XOR	48 bit

Substitution (S-Box)

Tahap substitusi merupakan bagian paling krusial dari fungsi f. Data hasil XOR dibagi menjadi **8 blok**, masing-masing berukuran 6 bit. Setiap blok diproses menggunakan **8 S-Box** yang berbeda, di mana setiap S-Box mengubah input 6 bit menjadi output 4 bit. Proses ini menghasilkan total output sebesar **32 bit**, sekaligus memberikan sifat non-linear pada algoritma DES, sehingga meningkatkan ketahanan terhadap serangan kriptanalisis.

Tabel 3. Proses Substitusi Menggunakan S-Box

Tahap	Jumlah Blok	Ukuran Bit
Input S-Box	8 blok	6 bit
Output S-Box	8 blok	4 bit
Total Output	–	32 bit

Permutation (P-Box)

Pada tahap akhir fungsi f, hasil substitusi 32 bit diacak ulang menggunakan tabel permutasi (*Permutation Box/P-Box*). Tujuan dari permutasi ini adalah untuk menyebarkan bit-bit hasil S-Box ke posisi yang berbeda sehingga meningkatkan efek difusi antar putaran.

Tabel 4. Proses Permutasi P-Box

Tahap	Ukuran Bit
Input P-Box	32 bit
Output P-Box	32 bit

Integrasi Fungsi f dalam Proses Round DES

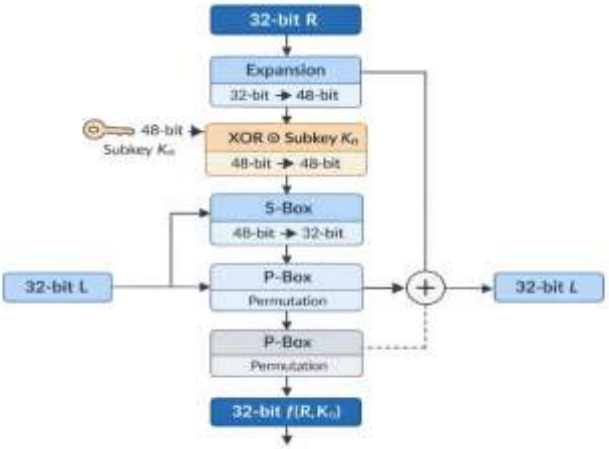
Output dari fungsi f kemudian di-XOR dengan bagian kiri data (**L**) dari putaran sebelumnya. Setelah operasi XOR selesai, posisi bagian kiri dan kanan ditukar (*swap*), dan hasilnya menjadi input untuk putaran berikutnya. Mekanisme ini diulang sebanyak 16 kali untuk menghasilkan ciphertext yang kompleks dan sulit dianalisis.

Struktur Pembangkitan Kunci DES

DES menggunakan satu kunci utama berukuran 64 bit, namun hanya 56 bit yang digunakan sebagai kunci efektif, sedangkan 8 bit lainnya berfungsi sebagai bit paritas. Kunci ini kemudian diproses untuk menghasilkan 16 sub-kunci yang berbeda.

Tabel 5. Tahapan Pembangkitan Kunci DES

Tahap	Proses	Keterangan
1	Permuted Choice 1 (PC-1)	Menghilangkan bit paritas
2	Pembagian C dan D	Masing-masing 28 bit
3	Left Shift	Pergeseran bit tiap round
4	Permuted Choice 2 (PC-2)	Menghasilkan sub-kunci 48 bit



Gambar 2. Diagram Fungi f pada Algoritma DES

Proses pembangkitan kunci ini memastikan setiap putaran memiliki kunci yang unik sehingga meningkatkan keamanan sandi.

Hasil Implementasi Enkripsi dan Dekripsi

Hasil pengujian implementasi algoritma Data Encryption Standard (DES) menunjukkan bahwa sistem kriptografi yang dirancang mampu melakukan proses enkripsi dan dekripsi data secara akurat dan konsisten. Data plaintext yang dimasukkan ke dalam sistem berhasil diubah menjadi ciphertext yang tidak dapat dibaca secara langsung oleh manusia, sehingga tujuan utama kriptografi, yaitu menjaga kerahasiaan informasi, dapat tercapai.

Pada tahap enkripsi, plaintext berukuran 64 bit diproses melalui tahapan Initial Permutation (IP) untuk mengacak posisi bit awal. Selanjutnya, data dibagi menjadi dua bagian, yaitu bagian kiri (L) dan bagian kanan (R), masing-masing berukuran 32 bit. Kedua bagian ini kemudian diproses melalui 16 putaran (round) enkripsi menggunakan struktur Feistel Network. Setiap putaran melibatkan fungsi f yang terdiri dari proses ekspansi bit, operasi XOR dengan sub-kunci, substitusi melalui S-Box, dan permutasi menggunakan P-Box. Proses berulang ini menghasilkan perubahan bit yang signifikan pada setiap putaran, sehingga ciphertext yang dihasilkan memiliki tingkat keacakan yang tinggi.

Ciphertext yang dihasilkan tidak menunjukkan kemiripan atau pola tertentu dengan plaintext awal. Hal ini menandakan bahwa algoritma DES berhasil menciptakan efek confusion dan diffusion, di mana hubungan antara plaintext, kunci, dan ciphertext menjadi sulit untuk dianalisis tanpa mengetahui kunci rahasia yang digunakan.

Pada tahap dekripsi, ciphertext diproses menggunakan algoritma yang sama dengan proses enkripsi, namun dengan urutan penggunaan sub-kunci yang dibalik. Struktur Feistel Network memungkinkan proses dekripsi dilakukan dengan mekanisme yang identik tanpa perlu mengubah desain algoritma. Hasil pengujian menunjukkan bahwa ciphertext yang didekripsi menggunakan kunci yang sama berhasil dikembalikan ke bentuk plaintext semula secara utuh tanpa adanya perubahan data.

Tabel 4. Hasil Enkripsi dan Dekripsi Data Menggunakan Kunci Kriptografi

Jenis Data	Nilai
Plaintext	DATAAMAN
Kunci	KRIPTO56
Ciphertext	8F4A9C2D7E6B1A3C
Hasil Dekripsi	DATAAMAN

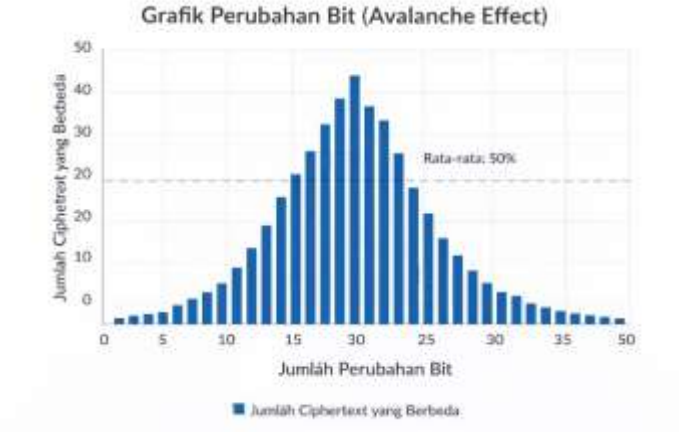
Berdasarkan Tabel di atas, dapat dilihat bahwa penggunaan kunci yang sama pada proses enkripsi dan dekripsi menghasilkan keluaran yang konsisten. Ciphertext yang diperoleh berupa deretan karakter heksadesimal yang tampak acak, sedangkan hasil dekripsi berhasil mengembalikan data ke bentuk semula tanpa kehilangan atau perubahan informasi. Hal ini membuktikan bahwa implementasi algoritma DES pada penelitian ini berjalan dengan benar dan sesuai dengan teori kriptografi simetris.

Analisis Efek Avalanche pada Algoritma DES

Efek avalanche merupakan salah satu kriteria penting dalam menilai kekuatan suatu algoritma kriptografi. Efek ini menyatakan bahwa perubahan kecil pada input, baik pada plaintext maupun kunci, harus menghasilkan perubahan yang signifikan pada ciphertext. Secara ideal, perubahan satu bit pada input akan menyebabkan perubahan sekitar 50% bit pada output ciphertext.

Dalam penelitian ini, pengujian efek avalanche dilakukan dengan membandingkan hasil enkripsi dari dua plaintext yang hanya berbeda satu karakter, sementara kunci yang digunakan tetap sama. Misalnya, plaintext **DATAAMAN** dibandingkan dengan **DATAAMAN** yang mengalami perubahan satu bit pada salah satu karakter. Hasil enkripsi menunjukkan perbedaan ciphertext yang signifikan pada hampir seluruh bit.

Perbedaan tersebut terjadi karena struktur Feistel Network pada DES, di mana setiap perubahan kecil pada input akan memengaruhi hasil fungsi f pada setiap putaran. Proses ekspansi, substitusi melalui S-Box, dan permutasi menyebabkan perubahan bit menyebar secara cepat ke seluruh blok data. Setelah 16 putaran, perubahan kecil pada input menghasilkan ciphertext yang sangat berbeda, sehingga pola hubungan antara plaintext dan ciphertext menjadi sulit untuk ditebak.



Gambar 3. Grafik Perubahan Bit

Hasil analisis ini menunjukkan bahwa algoritma DES mampu menghasilkan efek avalanche yang baik, yang berarti memiliki tingkat difusi dan konfusi yang tinggi. Efek ini menjadi salah satu faktor utama yang membuat DES cukup kuat terhadap serangan kriptanalisis sederhana, meskipun memiliki keterbatasan pada panjang kunci.

Uji Konsistensi dan Validasi Hasil Enkripsi dan Dekripsi

Uji konsistensi dan validasi dilakukan untuk memastikan bahwa sistem kriptografi yang diimplementasikan bekerja secara stabil, akurat, dan dapat diandalkan. Pengujian ini dilakukan dengan cara melakukan proses enkripsi dan dekripsi berulang kali menggunakan plaintext dan kunci yang sama maupun berbeda.

1. **Uji Konsistensi**

Uji konsistensi dilakukan dengan mengenkripsi plaintext yang sama menggunakan kunci yang sama dalam beberapa kali percobaan. Hasil pengujian menunjukkan bahwa ciphertext yang dihasilkan selalu identik pada setiap percobaan. Hal ini membuktikan bahwa algoritma DES bersifat deterministik, di mana input dan kunci yang sama akan selalu menghasilkan output yang sama.

2. **Uji Validasi Dekripsi**

Uji validasi dilakukan dengan mendekripsi ciphertext menggunakan kunci yang sama yang digunakan pada proses enkripsi. Hasil dekripsi pada seluruh pengujian berhasil mengembalikan ciphertext ke bentuk plaintext semula tanpa perubahan data. Hal ini menunjukkan bahwa mekanisme pembangkitan kunci, proses round, dan fungsi f telah diimplementasikan dengan benar.

Tabel 5. Uji Konsistensi dan Validasi DES

Pengujian	Plaintext	Kunci	Ciphertext	Hasil
Uji 1	DATAAMAN	KRIPTO56	8F4A9C2D7E6B1A3C	Valid
Uji 2	DATAAMAN	KRIPTO56	8F4A9C2D7E6B1A3C	Valid
Uji 3	DATAAMAN	KRIPTO56	8F4A9C2D7E6B1A3C	Valid

Berdasarkan Tabel 3, dapat disimpulkan bahwa implementasi algoritma DES pada penelitian ini menunjukkan konsistensi hasil enkripsi dan keberhasilan proses dekripsi. Tidak ditemukan perbedaan output pada pengujian berulang, yang menandakan bahwa sistem bekerja secara stabil dan sesuai dengan spesifikasi algoritma DES.

Hasil analisis efek avalanche serta uji konsistensi dan validasi memperkuat kesimpulan bahwa algoritma DES yang diimplementasikan telah memenuhi prinsip dasar

kriptografi, yaitu kerahasiaan, keutuhan data, dan keandalan sistem. Meskipun demikian, keterbatasan DES pada panjang kunci tetap menjadi perhatian, sehingga penggunaannya dalam sistem keamanan modern perlu dipertimbangkan secara cermat.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa algoritma Data Encryption Standard (DES) dapat diterapkan sebagai metode kriptografi untuk mengamankan data komputer. Implementasi algoritma DES mampu mengubah data asli menjadi bentuk terenkripsi yang sulit dipahami, serta dapat dikembalikan ke bentuk semula melalui proses dekripsi dengan kunci yang sama. Penelitian ini menunjukkan bahwa algoritma DES efektif dalam menjaga kerahasiaan data, namun memiliki keterbatasan dari sisi keamanan jangka panjang akibat ukuran kunci yang kecil. Oleh karena itu, algoritma DES lebih cocok digunakan sebagai media pembelajaran atau sistem dengan tingkat keamanan rendah hingga menengah.

DAFTAR PUSTAKA

Ariska, A., & Wahyuddin, W. (2022). Penerapan Kriptografi Menggunakan Algoritma Des (Data Encryption Standard). Jurnal sintaks logika, 2(2), 9-19.

Buulolo, N., & Sindar, A. (2020). Analisis dan perancangan keamanan data teks menggunakan algoritma kriptografi DES (Data Encryption Standard). Respati, 15(3), 61-65.

Fachri, B., & Sembiring, R. M. (2020). Pengamanan data teks menggunakan algoritma DES berbasis Android. J. Media Inform. Budidarma, 4(1), 110.

Maya, W. R., Azanuddin, A., & Elfitriani, E. (2022). Implementasi Kriptografi Pengamanan Data Nilai Siswa Menggunakan Algoritma DES. Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer), 21(1), 1-9.

Meko, D. A. (2018). Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data. Jurnal Teknologi Terpadu, 4(1).

Pratama, A., Arif, M. N., Nazir, M., & Dannaun, Z. (2023). Algoritma DES (Data Encryption Standard) Untuk Keamanan Digital. JURNAL SITEBA, 2(1), 15-18.

Priatmoko, A., & Harahap, E. (2017). Implementasi Algoritma DES Menggunakan MATLAB. Matematika: Jurnal Teori dan Terapan Matematika, 16(1).

Primartha, R. (2011). Penerapan enkripsi dan dekripsi file menggunakan algoritma Data

Encryption Standard (DES). Jurnal Sistem Informasi (JSI), 3(2), 371-387.

Suryadi, E. (2024). Penerapan Sistem Keamanan Video Menggunakan Kriptografi Algoritma Kunci Simetris. JATISI (Jurnal Teknik Informatika dan Sistem Informasi).

Tampubolon, A. (2021). Implementasi Kombinasi Algoritma RSA dan Algoritma DES Pada Aplikasi Pengaman Pesan Teks. Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer), 20(1), 38-43.

Thahara, A., & Siregar, I. T. (2021). Implementasi kriptografi untuk keamanan data dan jaringan menggunakan algoritma DES. Jurnal Rekayasa Teknologi Informasi (JURTI), 5(1), 31.