ALGORITMA DES (DATA ENCRYPTION STANDARD) UNTUK KEAMANAN DIGITAL

Aditya Pratama[1], Mohd Nur Arif [2], Muhamad Nazir[3], Zainan Dannaun[4], Dara[5]
Institut Teknologi Batam
2021001@student.iteba.ac.id

Abstrak

Data security is an important issue in the current digital era. Data Encryption Standard (DES) Algorithm is one of the cryptographic algorithms widely used to protect the confidentiality and integrity of data in the advancing digital era. DES utilizes a symmetric encryption approach with a secret key to encode data and has been implemented in various contexts, such as encoding database records and securing text data. Although DES was once considered the de facto standard for data encryption, its security has been questioned due to technological advancements and more sophisticated cryptoanalytic attacks. This article also discusses the comparison between DES and the Advanced Encryption Standard (AES), a stronger and more efficient encryption algorithm that has replaced DES as the modern data security standard.

Key Words: Data security, DES Algorithm (Data Encryption Standard), Database record encryption, Text data protection, Cryptography

1. PENDAHULUAN

Dalam era digital yang semakin maju ini, keamanan data telah menjadi isu yang sangat penting. Dalam lingkungan yang terhubung secara digital, data yang disimpan dan ditransmisikan rentan terhadap ancaman dan serangan yang dapat mengakibatkan kerugian yang signifikan. Oleh karena itu, perlindungan data menjadi prioritas utama bagi dan algoritma yang handal. Salah satu algoritma kriptografi yang telah banyak digunakan organisasi dan individu. Untuk mencapai tingkat keamanan yang optimal, diperlukan penggunaan metode adalah Algoritma DES (Data Encryption Standard). Algoritma DES telah terbukti efektif dalam melindungi kerahasiaan dan integritas data dalam berbagai konteks, termasuk penyandian record database, pengamanan data teks, dan keamanan data secara umum.

Penyandian record database merupakan salah satu aspek penting dalam menjaga kerahasiaan data yang disimpan dalam basis data. Dengan menerapkan Algoritma DES, data sensitif dapat diubah menjadi format yang tidak dapat dimengerti oleh pihak yang tidak berwenang, sehingga meningkatkan tingkat keamanan dalam penyimpanan dan pertukaran informasi.

Selain itu, Algoritma DES juga berperan dalam pengamanan data teks. Dalam dunia yang didominasi oleh komunikasi melalui teks, perlindungan terhadap akses yang tidak sah dan perubahan data menjadi sangat penting. Dengan menggunakan Algoritma DES, data teks dapat dienkripsi dan didekripsi dengan menggunakan kunci rahasia yang hanya diketahui oleh pihak yang berwenang.

Penggunaan Algoritma DES dalam konteks keamanan data didasarkan pada prinsip-prinsip kriptografi. Kriptografi memainkan peran kunci dalam mengamankan data dengan menggunakan teknik matematika dan komputasi. Algoritma DES menggunakan enkripsi simetris dengan penggunaan kunci rahasia untuk melindungi kerahasiaan data, sementara teknik substitusi dan permutasi digunakan untuk meningkatkan keamanan proses enkripsi.

Dalam artikel ini, penulis akan membahas secara rinci tentang Algoritma DES, termasuk konsep dasar, implementasi, dan penggunaannya dalam keamanan data secara keseluruhan. Penulis juga akan melakukan evaluasi keamanan algoritma ini dan menyajikan beberapa studi kasus penggunaannya dalam lingkungan nyata.

2. METODELOGI PENELITIAN

Dalam artikel ini, penulis menggunakan pendekatan penelitian deskriptif-analitis untuk membahas Algoritma DES dan penggunaannya dalam keamanan data secara umum. Metode penelitian meliputi studi literatur untuk memahami konsep dasar Algoritma DES, analisis konsep keamanan data, dan penerapan Algoritma DES dalam berbagai skenario. Penulis juga akan melakukan evaluasi keamanan algoritma ini dan menyajikan beberapa studi kasus penggunaannya dalam lingkungan nyata. Tujuan penelitian ini adalah menyajikan informasi komprehensif tentang Algoritma DES dan relevansinya dalam menjaga keamanan data di era digital yang kompleks dan rawan.

3. ANALISA DAN PERANCANGAN

Algoritma DES (Data Encryption Standard) adalah sebuah algoritma kriptografi yang telah menjadi standar de facto dalam penyandian data selama beberapa dekade. Algoritma ini

pertama kali diperkenalkan oleh NIST (National Institute of Standards and Technology) pada tahun 1977 dan dirancang oleh tim IBM yang dipimpin oleh Horst Feistel dengan bantuan dari NSA (National Security Agency). Algoritma DES menggunakan pendekatan enkripsi kunci-simetris, di mana kunci yang sama digunakan untuk mengamankan data (proses enkripsi) dan untuk mengembalikan data ke bentuk aslinya (proses dekripsi). Panjang kunci yang digunakan dalam DES adalah 56 bit, meskipun panjang kunci efektifnya hanya 48 bit karena 8 bit dari kunci digunakan sebagai bit paritas. Proses enkripsi dalam DES melibatkan beberapa tahapan utama, termasuk penggandaan kunci (key expansion), pengulangan putaran (rounds), serta substitusi dan permutasi (S-Box dan P-Box). Total ada 16 putaran enkripsi yang dilakukan pada blok data sebelum menghasilkan blok data terenkripsi.

Proses kerja enkripsi dan dekripsi Algoritma DES (Data Encryption Standard) mengikuti langkah-langkah berikut:

a. Proses Enkripsi:
    - Penggandaan Kunci (Key Expansion): Kunci rahasia yang awalnya berukuran 56 bit akan diubah menjadi bentuk yang sesuai untuk digunakan dalam algoritma DES. Proses ini melibatkan penggandaan kunci untuk membentuk kunci dengan panjang 64 bit, dengan 8 bit tambahan berfungsi dibagi menjadi blok-blok data dengan ukuran tetap, biasanya 64 bit. Setiap blok data ini akan diubah urutannya menggunakan initial permutation (IP).
b. Proses Dekripsi:
    - Penggandaan Kunci (Key Expansion): Langkah pertama dalam proses dekripsi adalah melakukan penggandaan kunci untuk membentuk subkunci yang akan digunakan dalam putaran dekripsi.
    - Pemisahan Data dan Initial Permutation: Data terenkripsi yang akan didekripsi akan dibagi menjadi blok-blok data dengan ukuran 64 bit. Blok data ini akan diubah urutannya menggunakan initial permutation (IP) yang akan disusun ulang berdasarkan tabel permutasi.
    - Putaran Dekripsi (Rounds): Proses dekripsi melibatkan 16 putaran dekripsi yang mirip dengan putaran enkripsi, tetapi dengan menggunakan subkunci dalam urutan terbalik.
    - Penukaran dan Penyatuan Blok: Setelah melalui 16 putaran dekripsi, blok data

akhir akan mengalami penukaran posisi antara bagian kiri (L) dan bagian kanan (R). Kedua bagian blok kemudian disatukan menjadi satu blok 64 bit.

- Final Permutation: Blok data 64 bit yang telah disatukan akan melalui final permutation (FP) untuk menyusun ulang bit-bit data sesuai dengan tabel

4. KESIMPULAN

Algoritma Data Encryption Standard (DES) telah berperan penting dalam keamanan data selama beberapa dekade. Dengan menggunakan pendekatan enkripsi simetris dan teknik substitusi dan permutasi, DES berhasil menyandikan data dalam alasan mengapa DES tidak lagi dianggap aman untuk pengamanan data modern.

Sebagai pengganti DES, Advanced Encryption Standard (AES) telah diadopsi sebagai standar enkripsi yang lebih kuat dan efisien. Dengan panjang kunci yang lebih besar dan menggunakan prinsip keamanan Substitution-Permutation Network (SPN),

REFERENSI

National Institute of Standards and Technology. (1977). Data Encryption Standard (DES). FIPS Publication 46.

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.

Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.

Lunt, T. F. (Ed.). (1997). A Guide to Understanding Data Remanence in Automated Information Systems. National Institute of Standards and Technology.

Singh, S. (2019). Mastering Linux Security and Hardening. Packt Publishing.Huda, N., & Sihotang, H. (2018). Implementasi Algoritma DES dalam Pengamanan Data Transaksi Perbankan. Jurnal Teknologi dan Sistem Komputer, 6(2), 94-99.

Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography: Principles and Protocols. CRC Press.

Syahputra, H. (2019). Analisis Keamanan Data Perbankan dengan Algoritma DES. Jurnal Ilmiah Infotel, 11(1), 54-59.