PRAKTIK SISTEM KEAMANAN DATA

RESUME JURNAL DES

Disusun Oleh :

Diana Lathifa

V3922016/ TI D

Dosen

Yusuf Fadlila Rachman S.Kom.,M.Kom

PS D-III TEKNIK INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS SEBELAS MARET

2023

RESUME JURNAL

Jurnal 1

https://media.neliti.com/media/publications/130596-ID-penerapan-enkripsi-dan-dekripsi-file-men.pdf

“Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)”

Jurnal ini ditulis oleh Rifkie Primartha dari Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Sriwijaya. Latar belakang masalah dari jurnal ini adalah perkembangan teknologi internet yang membuat data menjadi sangat berharga dan rentan terhadap serangan oleh para cracker. Karenanya, diperlukan suatu metode untuk mengamankan data, salah satunya adalah dengan menggunakan kriptografi.

A. Tujuan Penelitian

Tujuan penelitian dari jurnal ini adalah untuk mengimplementasikan algoritma DES untuk mengamankan file digital dengan menggunakan bahasa pemrograman Java. Jurnal ini juga bertujuan untuk menampilkan hasil pengujian dan analisis dari aplikasi yang dibuat.

B. Algoritma yang dipakai beserta alur penelitiannya: Algoritma yang dipakai dalam jurnal ini adalah algoritma DES, yang sama dengan algoritma yang digunakan dalam jurnal pertama. Alur penelitian dari jurnal ini adalah sebagai berikut:
   a. Menjelaskan konsep dasar dari kriptografi, termasuk jenis-jenis kriptografi, plainteks, cipherteks, enkripsi, dekripsi, dan kunci.
   b. Menjelaskan tinjauan pustaka dari algoritma DES, termasuk sejarah, skema global, permutasi awal, pembangkitan kunci, fungsi transformasi, dan dekripsi.
   c. Menjelaskan rancangan aplikasi yang dibuat, termasuk diagram use case, diagram class, diagram sequence, dan diagram activity.
   d. Menjelaskan implementasi aplikasi yang dibuat, termasuk kode program, tampilan antarmuka, dan proses enkripsi dan dekripsi file.
   e. Menjelaskan hasil pengujian dan analisis dari aplikasi yang dibuat, termasuk pengujian fungsional, pengujian keamanan, dan analisis performa.

C. Hasil penelitian

Hasil penelitian pada jurnal ini adalah aplikasi yang dapat mengamankan file digital dengan menggunakan algoritma DES dan bahasa pemrograman Java. Aplikasi ini dapat melakukan enkripsi dan dekripsi file dengan mudah dan cepat, serta memiliki tingkat keamanan yang cukup tinggi. Kesimpulan dari jurnal ini adalah algoritma DES dapat diimplementasikan untuk mengamankan file digital dengan menggunakan bahasa pemrograman Java, meskipun masih memiliki beberapa kekurangan seperti ukuran kunci yang kecil dan adanya serangan kriptoanalisis yang dapat memecahkan kunci.

Jurnal 2

https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/Data%20Encryption%20Standard%20%28DES%29.pdf

"Data Encryption Standard (DES)"

Jurnal ini ditulis oleh Ir. Rinaldi Munir, M.T. dari Departemen Teknik Informatika Institut Teknologi Bandung. Latar belakang masalah dari jurnal ini adalah perlunya suatu algoritma kriptografi yang dapat mengamankan data dari ancaman penyadapan, pengubahan, atau penghapusan oleh pihak yang tidak berhak.

A. Tujuan Penelitian

Tujuan penelitian dari jurnal ini adalah untuk menjelaskan secara rinci bagaimana algoritma DES bekerja, mulai dari permutasi awal, pembangkitan kunci, fungsi transformasi, hingga dekripsi. Jurnal ini juga bertujuan untuk memberikan contoh perhitungan DES dengan menggunakan plainteks dan kunci tertentu.

B. Algoritma yang dipakai beserta alur penelitiannya

Algoritma yang dipakai dalam jurnal ini adalah algoritma DES, yang termasuk ke dalam sistem kriptografi simetri dan tergolong jenis cipher blok. Algoritma DES beroperasi pada ukuran blok 64 bit dan menggunakan 56 bit kunci internal yang dibangkitkan dari 64 bit kunci eksternal. Alur penelitian dari jurnal ini adalah sebagai berikut:

a. Menjelaskan sejarah dan tinjauan umum dari algoritma DES, termasuk skema global, jaringan Feistel, dan pra-cipherteks.

b. Menjelaskan permutasi awal yang dilakukan terhadap blok plainteks sebelum masuk ke dalam 16 putaran DES, termasuk matriks permutasi awal yang digunakan.

c. Menjelaskan pembangkitan kunci yang dilakukan untuk menghasilkan 16 kunci internal yang berbeda dari kunci eksternal, termasuk permutasi pilihan, pergeseran kiri, dan kompresi.

d. Menjelaskan fungsi transformasi yang dilakukan pada setiap putaran DES, termasuk ekspansi, XOR, substitusi, dan permutasi lurus.

e. Menjelaskan dekripsi yang dilakukan untuk mengembalikan blok cipherteks menjadi blok plainteks, termasuk permutasi awal balikan dan urutan kunci internal yang terbalik.

f. Memberikan contoh perhitungan DES dengan menggunakan plainteks dan kunci tertentu, termasuk tabel dan diagram yang menunjukkan proses permutasi, pembangkitan kunci, fungsi transformasi, dan dekripsi.

C. Hasil penelitian

Hasil penelitian pada jurnal ini adalah penjelasan yang rinci dan lengkap tentang algoritma DES, yang dapat membantu pembaca untuk memahami cara kerja dan prinsip-prinsip dari algoritma tersebut. Kesimpulan dari jurnal ini adalah algoritma DES merupakan algoritma kriptografi yang cukup kuat dan efisien untuk mengamankan data, meskipun memiliki beberapa kelemahan seperti ukuran kunci yang relatif kecil, struktur yang terlalu teratur, dan adanya kriptoanalisis diferensial dan linear yang dapat menyerang algoritma tersebut.