PRAKTIK SISTEM KEAMANAN DATA

Introducing DES Algorithm

Disusun oleh :
Afif Khalid Fadhillah
V3922001

Dosen
Yusuf Fadlila Rachman S. Kom., M. Kom.

PS D-III TEKNIK INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS SEBELAS MARET
2023

SOAL

1. Mencari dua jurnal yang berkaitan dengan algoritma Data Encrytion Standard (DES). Jurnal tiap kelompok tidak boleh sama.

2. Buatlah resume berdasarkan jurnal-jurnal tersebut dengan bahasa mu sendiri. Resume jurnal harus memuat poin-poin berikut :

a. Judul dan Latar Belakang Masalah
b. Tujuan Penelitian
c. Algoritma yang dipakai beserta alur penelitiannya
d. Ceritakan hasil penelitian pada jurnal tersebut dan kesimpulannya

JAWABAN

1. Jurnal Pertama, link jurnal : https://download.garuda.kemdikbud.go.id/article.php?article=151352&val=5840&title=Penerapan%20Enkripsi%20Dan%20Dekripsi%20File%20Menggunakan%20Algoritma%20Data%20Encryption%20Standard%20DES

   Judul dan Latar Belakang Masalah:

   Jurnal ini berjudul "Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)" oleh Rifkie Primartha. Latar belakang masalahnya adalah kemajuan teknologi internet sebagai media penghantar informasi yang telah diadopsi oleh hampir semua orang dewasa ini. Informasi menjadi sangat berharga, dan keamanan informasi menjadi krusial karena sering menjadi target serangan oleh para cracker.

   Tujuan Penelitian:

   Tujuan penelitian ini adalah mendesain dan membuat aplikasi yang dapat melakukan penyandian (enkripsi dan dekripsi) menggunakan algoritma simetri DES (Data Encryption Standard) dengan bahasa pemrograman Java. Aplikasi ini diharapkan dapat membantu mengamankan informasi yang bernilai.

Algoritma yang Dipakai Beserta Alur Penelitiannya:

Penelitian ini menggunakan algoritma Data Encryption Standard (DES), sebuah algoritma enkripsi simetris yang diadopsi sebagai standar pengolah informasi Federal AS. Alur penelitian melibatkan pembangkitan kunci internal dari kunci eksternal, proses enkripsi, dan proses dekripsi. Pembangkitan kunci melibatkan matriks permutasi dan pergeseran bit, sementara proses enkripsi dan dekripsi melibatkan putaran enkripsi dengan kunci yang berbeda.

Hasil Penelitian dan Kesimpulan:

Hasil penelitian ini adalah pengembangan aplikasi kriptografi berbasis algoritma DES menggunakan bahasa pemrograman Java. Aplikasi ini mampu melakukan enkripsi dan dekripsi pada teks maupun file. Dengan adanya aplikasi ini, data-data penting dapat diamankan ketika dikirim melalui media internet. Kesimpulan dari penelitian ini adalah aplikasi kriptografi DES berhasil dikembangkan dan dapat digunakan untuk meningkatkan keamanan informasi.

Kelebihan dan Kekurangan:

Kelebihan dari jurnal ini adalah implementasi aplikasi yang menggunakan algoritma DES untuk meningkatkan keamanan informasi. Aplikasi ini dapat digunakan untuk enkripsi dan dekripsi file atau teks dengan menggunakan kunci tertentu. Namun, kekurangan dari jurnal ini tidak dijelaskan secara rinci. Penelitian lebih lanjut dapat mencakup evaluasi keamanan aplikasi, analisis kinerja, atau perbandingan dengan metode kriptografi lainnya.

2. Jurnal Kedua, link jurnal : https://jurnal-backup.kaputama.ac.id/index.php/JTIK/article/view/185/202

Judul dan Latar Belakang Masalah:

Jurnal ini berjudul "IMPLEMENTASI ALGORITMA DES (DATA ENCRYPTION STANDARD) PADA ENKRIPSI DAN DEKRIPSI SMS BERBASIS ANDROID." Latar belakang masalahnya melibatkan perkembangan teknologi, terutama dalam konteks pengiriman pesan SMS yang membutuhkan perlindungan terhadap privasi dan keamanan data.

Tujuan Penelitian:

Tujuan penelitian ini adalah mengimplementasikan algoritma DES untuk mengamankan pesan SMS pada platform Android. Dalam konteks ini, penelitian bertujuan untuk menciptakan metode enkripsi dan dekripsi yang dapat menjaga kerahasiaan informasi yang sangat rahasia dari akses yang tidak sah.

Algoritma yang Dipakai Beserta Alur Penelitiannya:

Penelitian menggunakan algoritma DES (Data Encryption Standard), yang merupakan algoritma enkripsi simetris. Alur penelitian dimulai dengan memasukkan pesan teks dan kunci enkripsi, mengonversi teks dan kunci ke dalam format biner, melakukan Initial Permutation (IP) dan PC-1, serta melakukan proses enkripsi sebanyak 16 putaran dengan subkunci yang dihasilkan dari proses PC-1 dan shifting. Proses dekripsi dilakukan dengan langkah-langkah yang serupa, tetapi dengan menggunakan subkunci dalam urutan terbalik.

Hasil Penelitian dan Kesimpulan:

Hasil penelitian menunjukkan bahwa implementasi algoritma DES pada enkripsi dan dekripsi SMS berbasis Android berhasil. Dengan memasukkan nomor tujuan, isi pesan, dan kunci, pengguna dapat mengamankan pesan SMS mereka. Proses dekripsi juga memerlukan kunci yang benar untuk mengembalikan pesan ke bentuk aslinya. Kesimpulan dari penelitian ini adalah bahwa algoritma DES efektif dalam melindungi pesan SMS dari akses yang tidak sah.

Kelebihan dan Kekurangan:

Kelebihan dari penelitian ini adalah implementasi algoritma DES yang berhasil untuk melindungi privasi pesan SMS. Namun, beberapa kekurangan mungkin termasuk kurangnya pembahasan tentang performa dan efisiensi algoritma, serta ketidakjelasan mengenai skenario pengujian yang digunakan. Selain itu, penggunaan DES yang sudah tua mungkin kurang sesuai untuk keamanan tingkat tinggi saat ini.