PRAKTIK SISTEM KEAMANAN DATA

Introducing AES 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 Advanced Encryption Standard (AES). Jurnal tiap kelompok tidak boleh sama.

2. Buatlah resume berdasarkan jurnal-jurnal tersebut dengan bahasamu 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

   e. Kelebihan dan kekurangan masing-masing jurnal tersebut

JAWABAN

1. Jurnal Pertama, link jurnal : https://www.eksplora.stikom-bali.ac.id/index.php/eksplora/article/view/139/115

   Resume Jurnal: "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File"

   a. Judul dan Latar Belakang Masalah:

   Jurnal ini berjudul "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File" dan memberikan penekanan pada keamanan data informasi dalam pertukaran file dokumen. Dalam latar belakangnya, penelitian ini menggarisbawahi pentingnya keamanan data dalam konteks pertukaran informasi melalui internet, khususnya terkait dengan kekhawatiran terhadap penyadapan pesan atau informasi.

   b. Tujuan Penelitian:

   Penelitian ini bertujuan untuk mengimplementasikan algoritma kriptografi AES-128 pada proses enkripsi dan dekripsi file dokumen, seperti PDF, DOC, dan TXT. Fokus utama penelitian adalah meningkatkan keamanan pertukaran informasi dengan memanfaatkan tingkat keamanan yang tinggi yang dimiliki oleh AES.

c. Algoritma yang Dipakai Beserta Alur Penelitiannya:

Algoritma yang diimplementasikan dalam penelitian ini adalah Advanced Encryption Standard (AES) dengan panjang kunci 128 bit. Proses enkripsi dan dekripsi melibatkan beberapa langkah, seperti SubBytes, ShiftRows, MixColumns, dan AddRoundKey. Implementasi dilakukan menggunakan Microsoft Visual Studio 2012 sebagai bahasa pemrograman.

d. Hasil Penelitian dan Kesimpulan:

Penelitian ini menghasilkan aplikasi enkripsi dan dekripsi file dokumen menggunakan AES-128. Uji coba dilakukan pada berbagai jenis file dan ukuran. Hasil uji coba menunjukkan bahwa algoritma AES-128 berhasil mengenkripsi file dengan baik, menghasilkan file terenkripsi yang lebih kecil, dan mempertahankan keamanan selama kunci simetri tidak bocor. Waktu yang dibutuhkan untuk proses enkripsi dan dekripsi bervariasi tergantung pada ukuran file.

e. Kelebihan dan Kekurangan Masing-Masing Jurnal:

Kelebihan:

- Algoritma AES-128 dipilih karena tingkat keamanannya yang tinggi.
- Implementasi melibatkan uji coba pada berbagai jenis file dan ukuran.
- Aplikasi enkripsi dan dekripsi dapat digunakan untuk meningkatkan keamanan data informasi.

Kekurangan:

- Tidak disebutkan secara rinci mengenai metode evaluasi keamanan yang digunakan.
- Penelitian tidak membahas potensi kerentanannya terhadap serangan tertentu.
- Tidak ada analisis performa yang mendalam terkait dengan waktu yang dibutuhkan untuk proses enkripsi dan dekripsi.

2. Jurnal Kedua, link jurnal : https://ejournal.sisfokomtek.org/index.php/jikom/article/view/181/170

Resume Jurnal: "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan"

a. Judul dan Latar Belakang Masalah:

Judul: "Implementasi Metode Advanced Encryption Standard (AES 128 Bit) Untuk Mengamankan Data Keuangan"

Latar Belakang Masalah: Dengan kemajuan teknologi komputer dan telekomunikasi, perlindungan data keuangan menjadi krusial. Pencurian data, terutama data keuangan yang sensitif, dapat menyebabkan kerugian signifikan. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan metode Advanced Encryption Standard (AES) 128 Bit sebagai solusi untuk mengamankan data keuangan.

b. Tujuan Penelitian:

- Menilai efektivitas metode AES 128 Bit dalam mengamankan data keuangan, khususnya pada kasus data uang SPP di SMK Harapan Bangsa.
- Menerapkan algoritma AES pada berbagai jenis dokumen keuangan seperti PDF, DOC, dan TXT.
- Meningkatkan tingkat keamanan data keuangan di lingkungan sekolah.

c. Algoritma yang Dipakai Beserta Alur Penelitiannya:

Algoritma: Advanced Encryption Standard (AES) 128 Bit.

Alur Penelitian:

- Ekspansi Kunci: Pembangkitan kunci rahasia untuk proses enkripsi dan dekripsi.
- Enkripsi: Proses pengamanan data uang SPP menggunakan algoritma AES.
- Dekripsi: Proses mengembalikan data keuangan yang telah dienkripsi.
- Analisis Data: Evaluasi hasil enkripsi dan dekripsi untuk menilai keamanan dan efektivitas algoritma.

d. Hasil Penelitian dan Kesimpulan:

- Hasil penelitian menunjukkan bahwa metode AES 128 Bit efektif mengamankan data keuangan, khususnya pada data uang SPP di SMK Harapan Bangsa.
- Proses enkripsi dan dekripsi berhasil dilakukan pada berbagai jenis dokumen keuangan.
- Kesimpulan: Implementasi AES 128 Bit dapat menjadi solusi yang efektif untuk meningkatkan keamanan data keuangan di lingkungan pendidikan.

e. Kelebihan dan Kekurangan:

Kelebihan:

- Meningkatkan tingkat keamanan data keuangan.
- Dapat diaplikasikan pada berbagai jenis dokumen keuangan.
- Efektif dalam melindungi data sensitif.

Kekurangan:

- Memerlukan pemahaman teknis yang baik untuk implementasi.
- Proses enkripsi dan dekripsi mungkin memerlukan sumber daya komputasi yang signifikan.