KELOMPOK 5 :

1. AGHA SYARILA M. (V3920002)
2. ALEXANDRO GABRIEL P.P (V3920004)
3. FEBY VALERINA A. (V3920023)
4. INEZ LAURENSYA (V3920027)
5. KHOIRUL DIANTORO (V3920031)

PRAKTIK SISTEM KEAMANAN DATA
PERTEMUAN 11

A. JURNAL 1

Judul : Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen

LATAR BELAKANG

Kerahasiaan dari data atau informasi merupakan suatu kelengkapan pelayanan yang dibuat untuk menjaga agar informasi yang tersimpan tidak dapat dibaca atau dibuka oleh pihak yang tidak berhak.
Upaya dalam menjaga kerahasiaan dari data informasi tersebut sudah tercetus sejak jaman dahulu tepatnya pada jaman romawi dengan metode pergeseran huruf atau karakter dengan dasar nilai tertentu.

Proses enkripsi di sini diartikan sebagai proses perubahan dari suatu pesan asli menjadi suatu pesan yang terlindungi dalam hal ini pesan yang tersandi , sedangkan untuk proses dekripsi adalah suatu proses pengembalian pesan tersandi yang terlindungi menjadi bentuk data asli pesan tersebut

Pada kedua proses tersebut dibutuhkan suatu pengaman yang menjamin bahwa pesan tersebut terlindungi pada prosesnya, pengaman tersebut dinamakan key. Penerapan algoritma ini akan dilakukan pada pengamanan jenis data berjenis dokumen dengan tipe pdf, doc, txt.

TUJUAN PENELITIAN

1. Dapat melakukan proses enkripsi file dokumen yang mempunyai ekstensi .pdf, .doc dan .txt dengan menggunakan symmetric key
2. Dapat melakukan proses dekripsi terhadap file dokumen yang telah di proses enkripsi sebelumnya.

ALGORITMA YANG DIPAKAI DAN ALUR PENELITIAN

Pada penelitian ini akan dibuat suatu aplikasi enkripsi dekripsi file dokumen dengan menggunakan algoritma AES-128 berbasiskan desktop application.

Pada perancangan sistem yang akan diterapkan pada penelitian ini akan dijelaskan melalui activity diagram. Proses pertama adalah proses enkripsi yang dimulai dengan memilih lokasi file yang akan di enkripsi, setelah itu dilanjutkan dengan memasukkan dan mengkonfirmasi kunci enkripsi untuk kemudian dilakukan proses enkripsi yang akan menghasilkan file hasil enkripsi dan informasi mengenai waktu beserta besar ukuran file hasil tersebut. Proses kedua adalah dekripsi, pada proses ini file yang sebelumnya sudah melalui proses enkripsi dimasukkan lagi sebagai file input-an yang kemudian ditambahkan dengan kunci yang sama. . Output dari proses ini adalah file dokumen yang telah terdekripsi beserta waktu dan besar ukuran file dekripsi.

HASIL PENELITIAN

Tampilan awal dan garis besar dari aplikasi ini. Terdapat menu file sumber yakni asal lokasi file yang akan di enkripsi, masukkan kata kunci yang akan dijadikan key, kata kunci ini gabungan dari huruf dan angka dan konfirmasi kata kunci untuk mengulang kata kunci yang sama (symmetric key).

Tampilan Input digunakan pengguna memilih file yang akan dienkripsi dan memasukkan encryption key. File dokumen yang akan dienkripsi disertai dengan memasukkan key dan konfirmasi key.

Tampilan File Enkripsi, Waktu yang dibutuhkan dan Ukuran File menampilkan ukuran file yang telah di enkripsi, waktu lama enkripsi dan file yang telah dienkripsi.

Pada proses dekripsi dimulai dengan memasukkan file hasil enkripsi dan decryption key yang sesuai dengan proses enkripsi awal. Hasil dekripsi terdapat proses dekripsi yang memproses file awal yang sama sebelum diproses. Di samping hasil file, juga tercantum informasi ukuran file hasil dekripsi dan waktu yang dibutuhkan untuk dekripsi.

KESIMPULAN

1. Algoritma AES-128 dapat dijadikan salah satu alternatif untuk proses keamanan data dalam hal ini enkripsi dan dekripsi file dokumen.
2. Ukuran file merupakan salah satu variabel yang cukup penting karena berpengaruh terhadap waktu proses enkripsi dan dekripsi. Pada variabel hasil, waktu merupakan tolak ukur dari proses, apakah terhitung cepat atau lambat dari ukuran file yang harus diproses.

3. Hasil dari enkripsi ini bisa dijamin keamanannya selama symmetry key encryption tidak bocor ke pihak yang tidak bertanggung jawab.
4. Dari hasil penelitian telah dibuktikan bahwa isi file awal yang mengalami proses enkripsi, kemudian mengalami proses dekripsi, maka akan kembali seperti file awal semula.

B. JURNAL 2

Judul : Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard)

LATAR BELAKANG

Seiring dengan kemajuan teknologi informasi maka sangat di perlukan sebuah keamanan data terhadap kerahasiaan informasi yang saling dipertukarkan melalui jaringan internet, apa lagi jika data tersebut dalam suatu jaringan komputer yang terhubung atau terkoneksi dengan jaringan lain. Hal tersebut tentu saja menimbulkan resiko bila informasi yang sensitif dan berharga tersebut di akses oleh orang yang tidak bertangung jawab. Yang mana jika hal tersebut sampai terjadi, kemungkinan besar akan merugikan bahkan membahayakan orang yang akan mengirim pesan, maupun organisasinya.

Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima pesan.
Selain itu data yang dibajak kemungkinan rusak atau hilang yang menimbulkan kerugian material yang besar. Oleh karena itu untuk menghindari agar hal tersebut tidak terjadi, menggunakan algoritma kriptografi AES untuk proses enkripsi dan deskripsi data.

TUJUAN PENELITIAN

1. Mengenalkan konsep keamanan data pada kriptografi AES serta penerapannya.
2. Dapat melakukan proses Enkripsi dan Deskripsi file ataupun teks pada algoritma AES.
3. Dapat membuat program aplikasi komputer yang dapat melakukan proses Enkripsi dan Deskripsi sesuai dengan algoritma AES: Rijndael.

ALGORITMA YANG DIPAKAI DAN ALUR PENELITIAN (KHOIRUL)

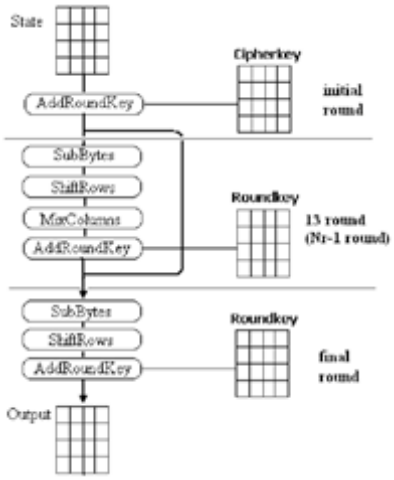
Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis. Kata logis merupakan kata kunci dalam algoritma. Langka-langka dalam algoritma harus logis dan harus dapat ditentukan bernilai salah atau benar.

Algoritma yang digunakan berupa kriptografi Advanced Encryption Standard (AES). Advanced Encryption Standard (AES) merupakan algoritma cryptographic yang dapat digunkan untuk mengamankan data. Algoritma AES adalah blok chipertext simetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) informasi. Enkripsi merubah data yang tidak dapat lagi dibaca disebut ciphertext, sebaliknya dekripsi adalah merubah ciphertext data menjadi bentuk semula yang kita kenal sebagai plaintext. Algoritma AES menggunakan kunci kriptografi 128, 192, dan 256 bits untuk mengenkrip dan dekripsi data.

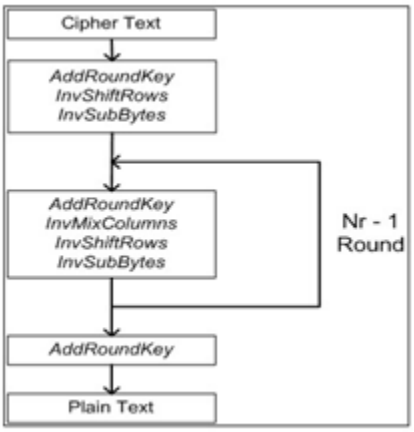
HASIL PENELITIAN (AGHA)

Kemajuan teknologi informasi memudahkan orang dalam berkomunikasi, mengirim dan menerima informasi. Dengan kemudahan tersebut banyak informasi yang bersifat sensitif dan berharga tersebut diakses oleh orang yang tidak bertangung jawab, kemungkinan besar akan merugikan bahkan membahayakan orang yang akan mengirim pesan maupun penerimanya, oleh karena itu sangat diperlukan sebuah keamanan data terhadap kerahasiaan informasi. Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima pesan. Selain itu data yang dibajak kemungkinan rusak atau hilang yang menimbulkan kerugian material yang besar. Oleh karena itu untuk menghindari agar hal tersebut tidak terjadi, kami menggunakan algoritma kriptografi AES (Advanced Encryption Standard) untuk proses enkripsi dan deskripsi data**.**

Dalam kriptografi dikenal algoritma block chiper yang didalamnya terdapat AES (Anvanced Encyption Standard) merupakan bagian dari Modern Symmetric Key Cipher, algoritma ini menggunakan kunci yang sama pada saat proses enkripsi dan deskripsi sehingga data yang kita miliki akan sulit dimengerti maknanya. Teknik algoritma tersebut digunakan untuk mengkonversi data dalam bentuk kode-kode tertentu, untuk tujuan agar informasi yang tersimpan tidak bisa di baca siapa pun kecuali orang-orang yang berhak. Oleh karena itu, sistem keamanan data sangat di perlukan untuk menjaga kerahasian informasi agar tetap terjaga. Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey.



Sedangkan proses Dekripsi Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey.



KESIMPULAN (ALEX)

Berdasarkan pemaparan diatas dapat disimpulkan bahwa penerapan algoritma advanced encryption standard untuk pengamanan file dokumen menjadi lebih aman, waktu yang dibutuhkan dalam proses enkripsi juga lebih cepat dan pengguna juga bisa menggunakan sistem ini dimanapun.

Aplikasi sistem keamanan data ini berhasil mengimplementasikan proses enkripsi dan dekripsi untuk mengamankan file dokumen . Hal ini

dibuktikan bahwa semua file yang di enkripsi dengan sistem keamanan data dapat dikembalikan ke file semula dalam proses dekripsi dan file tidak mengalami perubahan.

C. KELEBIHAN DAN KEKURANGAN

1) JURNAL 1

Judul : Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen

- Kelebihan
  - ➔ Memaparkan secara jelas dan lengkap mulai dari pendahuluan atau latar belakang dari permasalahan
  - ➔ Disertai dengan gambar skema
  - ➔ Isi dari jurnal sangat jelas
  - ➔ Space penulisan teratur
  - ➔ Tahapan implementasi disertai dengan screenshot hasil
- Kekurangan
  - ➔ Kesimpulan yang diberikan masih kurang
  - ➔ Hasil dan pembahasan tidak dijelaskan dengan lengkap

2) JURNAL 2

Judul : Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard)

- Kelebihan
  - ➔ Memaparkan secara jelas dan lengkap mulai dari pendahuluan atau latar belakang dari permasalahan
  - ➔ Disertai dengan gambar skema
- Kekurangan
  - ➔ Pada penjelasan materi tulisan menggunakan bold
  - ➔ Penulisan kurang rapi
  - ➔ Space penulisan Tidak teratur
  - ➔ Pembahasan yang disampaikan kurang jelas