TUGAS PRAKTIKUM SISTEM KEAMANAN DATA

JURNAL ALGORITMA AES

Disusun Oleh:

(Clarissa Putri Aurellia) (V3920015)

(Farhanang Wahyu Aprian) (V3920021)

(Augesvina Seiyusanda L) (V3920011)

(Alfida Shofiya Mufti) (V3920005)

(Hildanniar Fauzi) (V3920026)

TI-D

PROGRAM STUDI INFORMATIKA

FAKULTAS SEKOLAH VOKASI

UNIVERSITAS SEBELAS MARET

SURAKARTA

2021

JURNAL I
PENGAMANAN FILE VIDEO DENGAN ALGORITMA *ADVANCED ENCRYPTION STANDARD(AES)*

I. Latar Belakang Masalah

Keamanan data merupakan hal yang sangat penting yang harus diperhatikan oleh setiap individu dan setiap organisasi. Data sangat penting karena beberapa data yang merupakan data pribadi dijaga kerahasiaannya oleh pihak yang tidak terkait atau tidak berkepentingan. Risiko serangan dari pihak yang tidak berhak untuk bisa mendapatkan dan melihat data pribadi individu atau organisasi selalu dapat terjadi kapan saja, dimana saja, terutama dalam situasi lalu lintas jaringan yang semakin luas dan tidak mengenal ruang, waktu di era kemajuan teknologi saat ini.

Salah satu metode yang dapat digunakan untuk melindungi data adalah menggunakan konsep enkripsi. Enkripsi adalah suatu metode untuk mengubah data text asli menjadi data text baru yang tidak dapat dibaca seperti text aslinya. Enkripsi dan dekripsi masuk dalam konsep utama kriptografi. Salah satu alat kriptografi yang terkenal adalah cryptool. kriptografi memiliki banyak algoritma berbeda yang dapat digunakan untuk mengamankan data, termasuk algoritma Advance Encryption Standard (AES). AES merupakan algoritma kriptografi modern yang dianggap memiliki tingkat keamanan yang tinggi. AES merupakan evolusi dari algoritma DES (Data Encryption Standard). AES memiliki blok cipher simetris yang menggantikan algoritma DES (Data Encryption Standard). Algoritma AES memiliki ukuran blok konstan 128 bit tetapi panjang kunci yang berbeda.

II. Tujuan Penelitian

Penelitian ini bertujuan untuk melakukan pengamanan data video berformat mp4 dengan menerapkan algoritma AES serta menggunakan salah satu software kriptografi yaitu cryptool untuk melakukan proses enkripsi dan dekripsi.

III. Algoritma Yang Dipakai Beserta Alur Penelitiannya

- Algoritma yang dipakai pada penelitian ini adalah Algoritma AES (*Advanced Encryption Standard*). AES merupakan kriptografi modern yang dianggap memiliki tingkat keamanan yang tinggi. Algoritma ini memiliki blok kode simetris yang menggantikan DES serta pengembangan dari algoritma DES.
- Terdapat dua proses utama pada penelitian ini, yaitu proses enkripsi dan proses dekripsi :
    1. Proses enkripsi data video .mp4
       Data video .mp4 akan dikonversi menjadi data video ke format hex dump. Lalu data tersebut dienkripsi menjadi AES. Setelah di enkripsi maka keluar hasil data video terenkripsi .mp4
    2. Proses dekripsi data video .mp4

data video yang sudah terenkripsi akan dikonversi menjadi data video ke format hex dump. Lalu video akan di deskripsi AES. Selanjutnya hasil data video sudah di deskripsi menjadi data video .mp4

IV. Hasil dan Kesimpulan

Berdasarkan tabel yang ditunjukan oleh jurnal ini memiliki hasil, file yang dienkripsi tidak menampilkan informasi pada video selain itu file video tidak dapat diputar ketika dienkripsi, namun file tersebut walaupun dienkripsi size pada file yang dienkripsi sama seperti sebelum dienkripsi. Jadi berdasarkan dari penelitian ini dapat disimpulkan bahwa enkripsi AES bagus untuk mengenkripsi file pada sebuah file video karena menggunakan kunci 128 bit selain itu keistimewaan dari pengenkripsian ini ukuran pada file memiliki ukuran yang sama dengan file asli sehingga hal ini cukup bagus untuk penyimpanan..

V. Kelebihan dan Kekurangan dari jurnal

Kelebihan dari jurnal tersebut adalah penggunaan bahasa yang digunakan sangat simple sehingga mudah dimengerti oleh orang awam sekalipun, selain itu isi jurnal yang ringkas memudahkan pengguna memahami informasi lebih cepat

Untuk kekurangan dari jurnal tersebut adalah pembahasan kurang spesifik dari sini pengguna tidak mengetahui bagaimana enkripsi bekerja karena hanya menampilkan sebuah proses perubahan pada file saja

JURNAL II
PENERAPAN ALGORITMA AES DAN KONVERSI SMS KE DALAM BAHASA KHEK PADA APLIKASI ENKRIPSI BERBASIS MOBILE APPLICATION

I. Latar Belakang Masalah

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan atau informasi yang dapat dibaca. Pesan sering disebut sebagai teks biasa. Algoritma AES adalah permutasi substitusi tipikal dari Primitive Network Cipher (SPN) berdasarkan pada struktur cipher blok simetris. Jumlah operasi iteratif pada AES adalah 10, 12, 14 untuk AES-128, AES-192 dan AES-26 secara terpisah dengan bit kunci 128, 129 dan 256. Algoritma Advanced Encryption Standard (AES) adalah algoritma kriptografi simetris modern. Pada algoritma AES kunci yang dipakai memiliki panjang bervariasi yaitu 128, 192, 256 dengan memiliki jumlah ronde yang berbeda pula tergantung panjang kuncinya, sehingga algoritma ini sangat baik untuk pengaman teks maupun data.

Pertama, pengirim mengetik pesan, kemudian pesan diubah menjadi dialek Lufang dalam bahasa Khek, kemudian pesan konversi dikirim, dienkripsi dengan kunci 16 dan ciphertext dihasilkan. ketika mendeskripsi pesan recipient menggunakan kode ketika enkripsi, dan pesan diubah dalam bahasa Indonesia.

II. Tujuan penelitian

Penelitian ini dilakukan untuk mengetahui bagaimana mengimplementasikan algoritma AES yang dikombinasikan dengan bahasa khek untuk meningkatkan keamanan sebuah informasi pada perangkat lunak mobile android,sehingga data hanya dapat dibaca oleh orang yang memiliki hak akses.

III. Algoritma Yang Dipakai Beserta Alur Penelitiannya

- ★ Algoritma AES merupakan standar pemrosesan informasi Federal Pemerintah Amerika Serikat yang digunakan untuk enkripsi simetris. Algoritma AES merupakan kombinasi suatu algoritma yang kuat dan kunci aman. algoritma ini memiliki panjang kunci variabel 128,192, dan 256 bit yang menghasilkan tingkat kecepatan dan keamanan. AES merupakan cipher blok simetris dengan 10 putaran untuk kunci 128-bit,12 putaran dengan kunci 192-bit, dan 14 putaran untuk kunci 256-bit.
- ★ Alur penelitian ada beberapa tahap yaitu Enkripsi,Deskripsi dan Konversi.
    1. proses enkripsi AES

       proses pengacakan pesan dengan menunjukan state sebagai objek utama yang akan disimulasikan secara per-blok untuk kunci panjang 128-bit ke dalam bentuk hexadecimal.

       Langkah pertamanya yaitu dengan mengcopy plaintext sebagai St1 dan kunci sebagai St2. St3 didapat dari proses AddRoundKey antara St1

dan St2 yang dikonversikan kedalam bentuk hexadecimal. Yang kedua SubBytes() yang mensubstitusikan St3 dalam bentuk hexadecimal ke dalam tabel S-box sehingga menghasilkan St4. kemudian untuk St5 ini hasil dari prosess shiftrows() dengan menggeser secara cyclic. yang terakhir ada MixColumns() yang mengkonversi nilai shiftrows() ke dalam biner.

2. Proses dekripsi AES
   Dekripsi merupakan penerjemah ciphertext menjadi ke bentuk semula atau plaintext. Langkah pertamanya InvShiftRows() dengan menggeser St1 menjadi St2. Kemudian InvSubBytes() yang akan mensubstitusikan St3 ke dalam bentuk hexadecimal ke dalam tabe; S-box1(invers S-box). Selanjutnya ada langkah terakhir yaitu AddRoundKey dengan mengoperasikan XOR antara InvSubByte dengan KeySchedule, sehingga menghasilkan AddRoundKey ke 10 sebagai plaintext.

IV. Hasil dan Kesimpulan

Penerapan algoritma AES berhasil diterapkan ke dalam aplikasi SMS enkripsi berbasis android dengan baik, sehingga pesan tidak bisa dibaca oleh pihak yang tidak berkepentingan. Konversi bahasa dari bahasa indonesia ke dalam bahasa Khek juga berhasil diterapkan ke dalam aplikasi SMS enkripsi sehingga tingkat keamanan informasi yang disampaikan menjadi lebih aman.

V. Kelebihan dan Kekurangan dari Jurnal

Kelebihan dari jurnal ini yaitu di dalam jurnalnya menjelaskan secara detail alur penelitian mengenai Algoritma AES. Kekurangan dari jurnal ini menurut kami yaitu banyak menggunakan perulangan kata dan kerapian penulisannya kurang,sehingga sulit memahami jurnal ini.