LAPORAN PRAKTIKUM

PRAKTIK SISTEM KEAMANAN DATA

**PRAKTIKUM TOPIK 11**

**ADVANCED ENCRYPTION STANDARD (AES)**



**Disusun oleh :**

1. Bagus Adam Farizi (V3921004)
2. Hasbi Yusuf Prasetyo (V39210012)
3. Meisy Anjarfika (V3921018)

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

**2022**

**JURNAL I**

1. **Judul dan Latar Belakang Masalah**
2. **Judul**

Pengembangan Aplikasi Chat Messenger dengan Metode Advanced Encryption Standard (AES) pada Smartphone

1. **Latar Belakang Masalah**

Chat Messenger adalah suatu sistem pengiriman pesan secara real time melalui jaringan internet dari satu perangkat ke perangkat yang lain. Menurut survei dari organisasi We Are Social pada Januari 2015, Indonesia memiliki populasi penduduk sebanyak 255,5 juta orang dengan pengguna paket data internet melalui mobile sejumlah 398,2 juta orang atau setara 121% populasi penduduk Indonesia. Pada survei perkembangan pengguna telepon genggam sejak januari 2014 sampai januari 2015 menunjukan adanya perkembangan sebanyak 9%. Dilihat dari data diatas maka dapat disimpulkan bahwa pengguna telepon genggam sangat banyak, dan menurut survei yang dilakukan oleh Nielsen menunjukan penggunaan telepon genggam lebih banyak digunakan untuk Chat yaitu dengan rata-rata sebanyak 72% sehari. Hal ini juga menyebabkan perlu kewaspadaan munculnya masalah kejahatan yang disebut dengan Cyber Crime atau kejahatan melalui jaringan informasi. Beberapa contoh dari kasus CyberCrime yang dapat menyerang pengguna chat messenger antara lain seperti penyadapan transmisi pesan dan pemanipulasian pesan.

1. **Tujuan Penelitian**

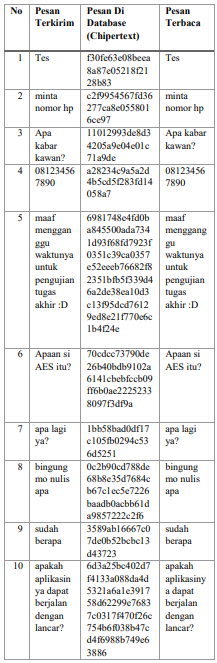
Penelitian ini membahas tentang proses AES dan keunggulan AES. Penelitian ini dapat menjelaskan keunggulan AES dibandingkan kriptografi lain. Berdasarkan referensi yang dijabarkan diatas akan dilakukan suatu penelitian untuk membuat aplikasi chat messenger yang terintegrasi dengan kriptografi AES. Penelitian ini diharapkan dapat digunakan untuk pertukaran pesan yang lebih aman.

1. **Algoritma yang dipakai dan alur penelitiannya**

Pada penelitian ini algoritma kriptografi yang digunakan adalah kriptografi Advanced Encryption Standard (AES) yang merupakan kriptografi dengan kunci simetri. Algoritma AES ini akan digunakan untuk mengenkripsi pesan yang akan dikirim menggunakan aplikasi chat messenger. Pesan yang diterima akan didekripsi kembali menggunakan algoritma AES pada saat pesan telah sampai pada penerima. Penelitian ini dimulai dari studi pustaka, yaitu mengumpulkan teori-teori serta kebutuhan yang diperlukan dalam pembuatan aplikasi. Langkah selanjutnya adalah perancangan antarmuka aplikasi yang akan dibuat yang kemudian dilanjutkan dengan pembuatan sistem aplikasi. Perancangan aplikasi sistem aplikasi sendiri akan dibagi menjadi dua tahap yaitu perancangan sistem chat messenger dan perancangan sistem enkripsi. Setelah perancangan sistem selesai dibuat akan dilanjutkan dengan tahap pengujian dan evaluasi sebelum kemudian diimplementasikan ke perangkat smartphone.

1. **Hasil penelitian pada jurnal tersebut dan kesimpulannya**

Hasil dari pengujian dengan mengirimkan pesan yang merupakan kombinasi dari berbagai jumlah kata, hasil yang keluar sesuai dengan yang diharapkan. Pesan yang dikirim dan dibaca berupa plaintext yang sama tetapi pesan yang masuk ke database berupa chipertext. Panjang chipertext yang dihasilkan akan sesuai dengan panjang pesan yang dikirimkan.



Berdasarkan hasil percobaan pengembangan aplikasi chat messenger dengan Metode Advanced Encryption Standard (AES) pada smartphone dapat diambil kesimpulan sebagai berikut :

1. Dari hasil pembuatan sistem enkripsi dan dekripsi pesan diperlukan sebuah beberapa modul pendukung seperti base64 yang digunakan untuk menstandarisasi pesan yang masuk sehingga bisa diubah menjadi nilai hexadesimal termasuk nilai spasi. Sehingga pesan yang dienkripsi pada saat dikirimkan dan didekripsi pada saat diterima bisa sama.
2. Perangkat telepon genggam dapat berkomunikasi secara realtime menggunakan nodeJS. Perangkat akan terhubung satu sama lain dengan menggunakan ID sementara yang disebut SocketID. SocketID akan menjadi identitas pada server pada saat login pada aplikasi sehingga pesan yang dikirimkan bisa tertuju pada penerima yang dituju dengan alamat SocketID yang ada pada server.
3. Pada saat pengimplementasian sistem AES diperlukan beberapa penyesuaian sehingga pesan yang dikirimkan bisa memiliki nilai byte yang diperlukan untuk melakukan proses enkripsi. Pesan yang memiliki nilai byte yang kurang dari 128 byte perlu ditambahkan dengan spasi untuk mengisi nilai yang kurang. Pesan yang memiliki nilai lebih dari 128 byte perlu dibuatkan sistem untuk membagi pesan menjadi beberapa bagian dengan nilai 128 byte untuk proses enkripsi dan dekripsi kemudian digabungkan kembali saat selesai dienkripsi atau didekripsi. Proses enkripsi dan dekripsi pesan akan dilakukan pada aplikasi sehingga selama proses transmisi pesan, pesan yang yang dikirimkan merupakan chipertext yang walaupun disadap tidak bisa dibaca oleh orang yang menyadap tersebut.
4. **Kelebihan dan kekurangan jurnal**
   * + 1. Pengembangan fitur baru untuk melengkapi aplikasi chat messenger seperti fitur kirim file, foto, penghapusan pesan, dan voice call.
       2. Penerapan kriptografi AES ini juga bisa dikembangkan ke media pertukaran data lain seperti untuk enkripsi pengiriman file atau foto.
       3. Membuat fitur untuk pengembalian password jika sewaktu-waktu user lupa password.
       4. Pembuatan fitur untuk mengajak teman untuk menggunakan aplikasi chat messenger dengan pesan singkat, email, dan media sosial lainnya.
       5. Membuat autentifikasi melalui email untuk mengecek email pengguna yang dimasukan.

**JURNAL II**

1. **Judul dan Latar Belakang Masalah**
2. **Judul**

Kriptografi Advanced Encryption Standard (AES) untuk Penyandian File Dokumen

1. **Latar Belakang Masalah**

Advanced Encryption Standard (AES) secara garis besar beroperasi pada blok 128-bit atau 16 karakter, yang berarti dapat digunakan untuk enkripsi teks. File dokumen terdiri dari barisan teks yang tentu saja berukuran lebih dari 16 karakter, akan tetapi AES dapat digunakan untuk penyandian yaitu dengan melakukan enkripsi perblok (128 bit) secara paralel untuk memudahkan proses enkripsi maupun dekripsi digunakan software aplikasi MATLAB.

1. **Tujuan Penelitian** 
   1. Memahami proses penyandian dengan Advanced Encryption Standard (AES).
   2. Mengetahui penerapan Algoritma kriptografi AES pada file teks.
   3. Dapat merancang dan menggunakan program pengamanan data teks metode Kriptografi AES dengan menggunakan Graphical User Interface (GUI) MATLAB.
2. **Algoritma yang dipakai dan alur penelitiannya**

Pada Proses enkripsi awalnya teks asli dibentuk sebagai sebuah state. Kemudian sebelum ronde 1 dimulai blok teks asli dicampur dengan kunci ronde ke-0 (transformasi ini disebut AddRoundKey). Setelah itu, ronde ke-1 sampai dengan ronde ke-(Nr-1) dengan Nr adalah jumlah ronde. AES menggunakan 4 jenis transformasi yaitu:

1. SubBytes, sebagai transformasi substitusi.

2. ShiftRows, sebagai transformasi permutasi.

3. MixColumns, sebagai transformasi pengacakan.

4. AddRoundKey, sebagai transformasi penambahan kunci.

Pada ronde terakhir, yaitu ronde ke-Nr dilakukan transformasi serupa dengan ronde lain namun tanpa transformasi serupa dengan ronde lain namun tanpa transformasi MixColumns.

1. **Hasil penelitian pada jurnal tersebut dan kesimpulannya**

Pada data teks, proses enkripsi dalam algoritma kriptografi AES 128, 128 bit (1 blok) plainteks terlebih dahulu dikonversi menjadi kode ASCII dalam bilangan heksadesimal dan dibentuk sebagai matriks byte berukuran 4x4 yang disebut state. Proses enkripsi pada AES 128 merupakan transformasi terhadap state secara berulang dalam 10 ronde. Data yang diproses pada setiap ronde berupa data biner. Setiap ronde AES membutuhkan satu kunci hasil generasi kunci dan menggunakan 4 transformasi dasar yaitu subbytes, shiftrows, mixcolumns, dan addroundkey. Sedangkan pada proses dekripsi mempunyai transformasi-transformasi dengan urutan invshiftrows, invsubbytes, addroundkey, dan invmixcolumns. Pada file dokumen yang sudah dipastikan memiliki jumlah karakter lebih dari 16 karakter akan dilakukan proses enkripsi dan dekripsi setiap 128 bit atau 16 karakter. Sehingga proses enkripsi dan dekripsi AES dilakukan secara paralel. Sedangkan untuk file teks yang jumlah karakternya kurang dari 16 karakter maka akan dilakukan padding. Padding adalah penggunaan karakter ASCII null untuk mengisi jumlah karakter yang kurang agar dapat diproses dan tidak akan mempengaruhi hasil enkripsi maupun dekripsi. Dengan bantuan MATLAB proses enkripsi dan dekripsi dapat dilaksanakan dengan cepat tepat dan efisien. Yang dibutuhkan hanya menginputkan plainteks dan kunci maka proses enkripsi dan dekripsi dapat menghasilkan output dengan cepat.

1. **Kelebihan dan kekurangan jurnal**

Pada file dokumen yang sudah dipastikan memiliki jumlah karakter lebih dari 16 karakter akan dilakukan proses enkripsi dan dekripsi setiap 128 bit atau 16 karakter. Sehingga proses enkripsi dan dekripsi AES dilakukan secara paralel. Implementasi program dapat dilakukan dengan menggunakan software selain dari MATLAB yang dapat mengakomodasi kebutuhan sistem.