**TUGAS PRAKTIKUM**

**SISTEM KEAMANAN DATA**

**Resume**



**Disusun Oleh:**

(Andrean L N A) (V3920007)

(Andriyan Tatak W) (V3920008)

(Arin Dwi Padmasari) (V3920010)

( Dandy Dicky T ) (V3920016)

Kelas : TID

**PROGRAM STUDI D3 TEKNIK INFORMATIKA MADIUN**

**FAKULTAS SEKOLAH VOKASI**

**UNIVERSITAS SEBELAS MARET**

**2021**

# Resume 1

1. **Judul dan Latar Belakang Masalah**

Judul :

Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen

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 pararel 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.

**C. Algoritma yang dipakai beserta alur penelitiannya**

AES merupakan sistem penyandian blok yang bersifat non-Feistel karena AES menggunakan komponen yang selalu memiliki invers dengan panjang blok 128 bit. Kunci AES menggunakan proses yang berulang yang disebut dengan ronde. Proses di dalam AES merupakan transformasi terhadap state. Sebuah teks asli dalam blok (128 bit) terlebih dahulu diorganisir sebagai state. Enkripsi AES adalah transformasi terhadap state secara berulang dalam beberapa ronde. State yang menjadi keluara ronde k menjadi masukan untuk ronde ke-k +1. 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.

Algotirma dekripsi AES secara ringkasnya algoritma deskripsi merupakan kebalikan algoritma enkripsi AES. Algoritma dekripsi AES menggunakan Tansformasi invers semua transformasi dasar yang digunakan pada algoritma enkripsi AES. Setiap tranformasi dasar dari algoritma kriptografi AES memiliki transformasi invers, yaitu: InvSubBytes, InvShiftRows dan InvMixColumns. AddroundKey merupakan transformasi yang bersifat self-invers dengan syarat mengunakan kunci yang sama .

**D. Hasil penelitian dan Kesimpulannya**

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 pararel. 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 di proses dan tidak akan mempengaruhui 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.

**E. Kelebihan dan Kekurangan masing-masing jurnal**

Kelebihan : Dengan bantuan MATLAB proses enkripsi dan deskripsi bisa dilakukan dengan tepat dan efisien**.**

Kekurangan : terjadi kesulitan dalam manajemen kunci. Hal ini terjadi karena untuk setiap pengiriman dan penerimaandata dengan pengguna yang berbeda dibutuhkan kunci yang berbeda pula. Masih dari segi jenis kunci yang simetris dimana pengirim dan penerima datamemiliki kunci yang sama untuk setiap proses pengiriman-penerimaan data, hal ini akan menyebabkan kunci mudah bocor meskipun dalam waktu yang lama.

# Resume 2

**A. Judul dan Latar Belakang Masalah**

**>**Judul

APLIKASI SMS KRIPTOGRAFI MENGGUNAKAN METODE AES BERBASIS ANDROID

>Latar Belakang

Algoritma AES (Advanced encryption standar) merupakan algoritma kriptografi simetrik yang beroperasi dalam mode penyandi blok (block cipher) yang memproses blok data 128-bit dengan panjang kunci 128-bit (AES- 128), 192-bit (AES-192), atau 256-bit (AES-256). AES juga merupakan algoritma yang sangat terkenal di Amerika dan pernah menjadi keamanan dasar yang digunakan di seluruh dunia dalam kriptografi kunci simetrik. Selain keunggulan yang telah disebutkan, Algoritma AES juga dirancang untuk memiliki properti ketahanan terhadap semua jenis serangan yang telah diketahui, kesederhanaan rancangan dan kekompokan kode serta kecepatan koputasi pada berbagai platform.

Berdasarkan uraian diatas, maka penulis tertarik untuk melakukan sebuah penelitian dengan judul Aplikasi SMS Kriptografi Menggunakan Metode AES Berbasis Android.

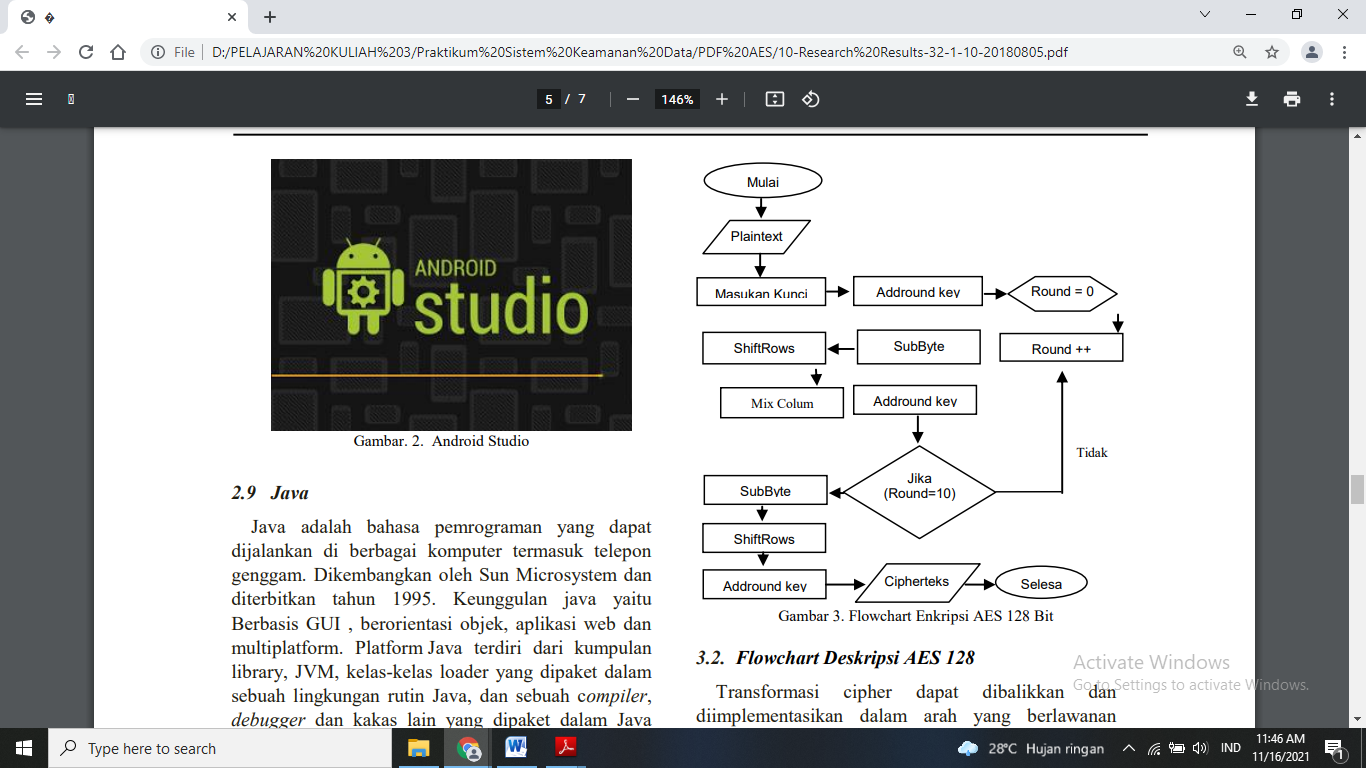
**B. Tujuan Penelitian**

Yang menjadi tujuan penelitian ini adalah menghasilkan suatu aplikasi pada telepon seluler berbasis android yang dapat mengenkripsi pesan SMS dengan menggunakan metode AES agar pesan tersebut tidak dapat diketahui oleh orang lain

**C. Algoritma yang dipakai beserta alur penelitiannya**

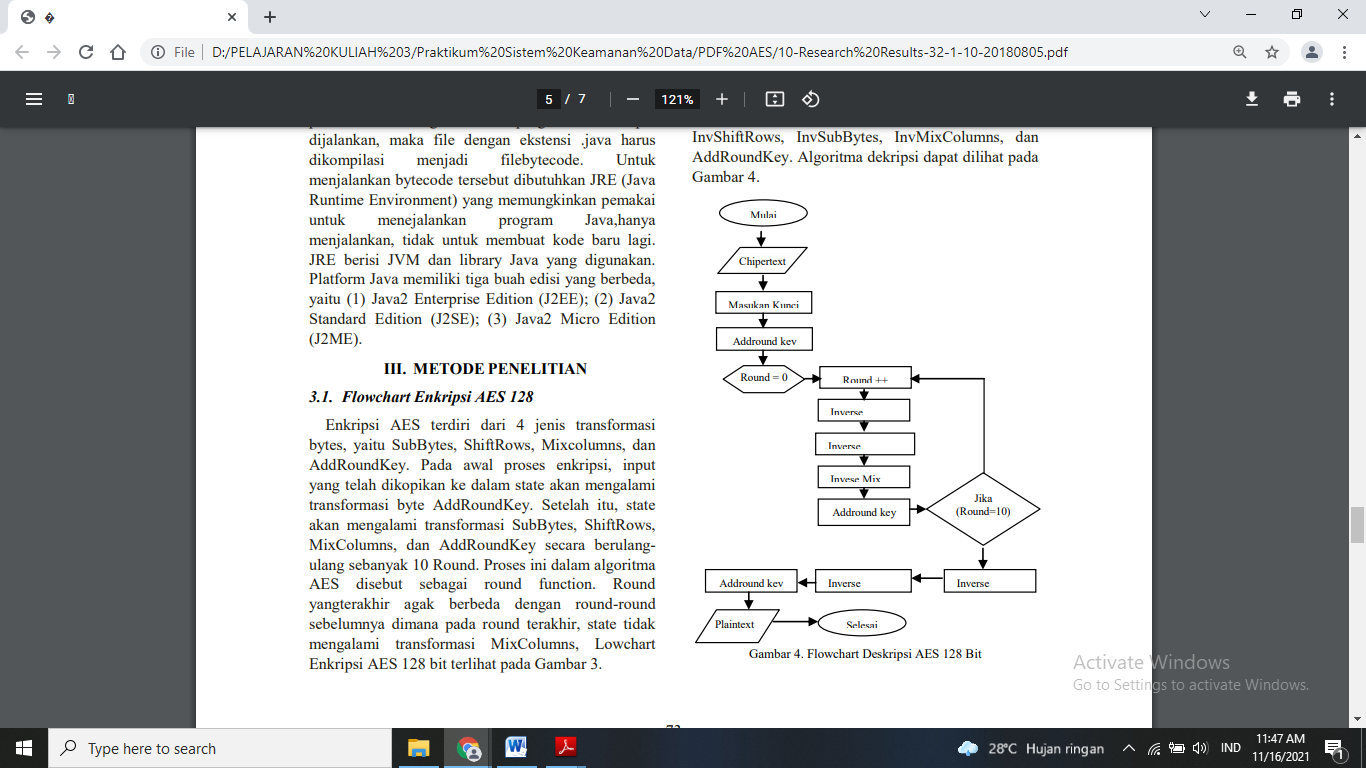
>Algoritma yang di gunakan adalah AES 128

> Enkripsi AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dikopikan ke dalam state akan mengalami transformasi byte AddRoundKey. Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulangulang sebanyak 10 Round. Proses ini dalam algoritma AES disebut sebagai round function. Round yangterakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns, Lowchart Enkripsi AES 128 bit terlihat pada Gambar 3.



> Deskripsi

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. Algoritma dekripsi dapat dilihat pada Gambar 4.



**D. Ceritakan hasil penelitian pada jurnal tersebut dan kesimpulannya**

>HASIL DAN PEMBAHASAN

1 Transformasi Algoritma AES A

ES menggunakan 4 jenis transformasi byte untuk mengenkripsi pesan yaitu SubByte, ShiftRows, MixColumns dan AddRoundKey. Kecuali tahap MixColumns, ketiga tahap lainnya akan diulang sebanyak 10 Round kecuali tahap MixColumns tidak akan dilakukan pada tahap terakhir. 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 InvAddRoundKey.

2 Implementasi

Aplikasi ini diimplementasikan dari desain dan kode berdasarkan rancangan bab sebelumnya. Aplikasi ini dibuat dengan dasar coding java yang dikembangkan dalam software dari android.

3 Antar Muka Awal

Form ini merupakan tampilan awal ketika aplikasi ini di jalankan yang terdiri dari empat menu utama yaitu menu tulis pesan, menu kotak masuk menu kotak keluar dan menu keluar

4 Form Menulis Pesan Form ini berfungsi untuk membuat pesan terenkripsi sebelum pesan dikirim yang terdiri dari 4 EditText dan 3 Button

5 Form Kotak Masuk Menu ini berfungsi untuk menampilkan pesan terenkripsi untuk di dekripsi

6 Proses Enkripsi Uji coba sistem dibutuhkan untuk memeriksa apakah sistem yang dibua tsudah sesuai rancangannya. Tujuan uji coba sistem adalah untuk memastikan semua fitur berfungsi dengan baik sesuai yang diharapkan oleh pengguna

>KESIMPULAN DAN SARAN

> Kesimpulan Dalam pembuatan aplikasi sms kriptografi menggunakan metode AES, penulis dapat menarik kesimpulan sebagai berikut :

1) Algoritma AES dapat diimplementasikan pada telepon seluler berbasis Android, sebagai sistem keamanan pesan.

2) Cara mengamankan pesan dengan menggunakan algoritma AES mampu meningkatkan keamanan pengirim dan penerima SMS dengan cara enkripsi dan dekripsi untuk smartphone android. Dan ini membantu pengguna yang ingin menjaga keamanan dalam berkomunikasi khususnya lewat SMS dari pihak-pihak yang tidak diinginkan.

**E. Kelebihan dan kekurangan masing-masing jurnal**

Kelebihan dari jurnal ini adalah menghasilkan suatu aplikasi pada telepon seluler berbasis android yang dapat mengenkripsi pesan SMS dengan menggunakan metode AES agar pesan tersebut tidak dapat diketahui oleh orang lain

Kekurangannya adalah pembuatannya yang rumit yang memerlukan Android SDK, Android Studio, Android Virtual Device (AVD), Java.