**PRAKTIKUM SISTEM KEAMANAN DATA**

Sebuah gambar berisi teks

Deskripsi dibuat secara otomatis

Madu Zaneta Abadi / V3920036

Nindya Vinalia M / V3920043

Pandu Dwi Saputra / V3920048

Viorella Sunghaiyon V / V3920059

**D3 TEKNIK INFORMATIKA - PSDKU**

**SEKOLAH VOKASI**

**UNIVERSITAS SEBELAS MARET**

**TAHUN 2021**

Jurnal 1

1. **Judul :** IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES 256 DAN METODE STEGANOGRAFI LSB PADA GAMBAR BITMAP

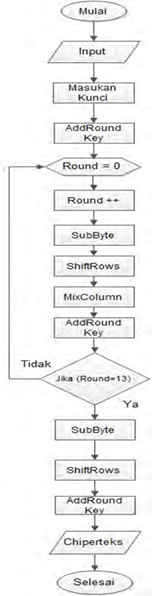
**Latar Belakang :** Seiring perkembangan zaman, saat ini manusia sedang memasuki era internet. Pertukaran informasi saat ini berlangsung tidak hanya dalam kehidupan sehari-hari tetapi juga di dunia maya.  
Kini pesan yang sering dikirim dan diterima melalui e-mail, jejaring sosial seperti Facebook, Twitter, dan lain sebagainya banyak berupa gambar. Gambar juga mengandung informasi yang penting pada sebagian orang untuk saling bertukar data. Keamanan file gambar tentu menjadi sangat penting agar tidak adanya pihak-pihak yang tidak berwenang meretas atau memanipulasi informasi dari gambar tersebut. Ada cara untuk mengamankan suatu informasi agar informasi itu tidak bocor kepada pihak yang tidak berwenang, yaitu dengan menggunakan kriptografi dan steganografi. Keamanan tersebut diperlukan untuk menghindari adanya penyadapan atau pembajakan terhadap gambar yang mengandung informasi penting bagi penggunanya.  
Keamanan diperlukan untuk menjaga integritas gambar tersebut agar tetap aman.

1. **Tujuan Penelitian :**

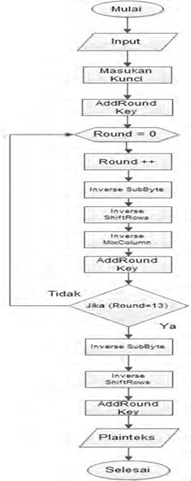
* untuk mengetahui informasi berupa pesan gambar yang terjadi di dunia maya semakin berkembang seiring dengan kebutuhan informasi manusia.
* Untuk informasi yang tak terbatas berdampak terhadap adanya tindak kejahatan dunia maya berupa penyadapan dan pembajakan.
* Dan untuk mengetahui pentingya sebuah keamanan terhadap informasi yang dikirim maupun diterima dengan cara kriptografi dan steganografi.

1. **Algoritma yang dipakai serta alur :**

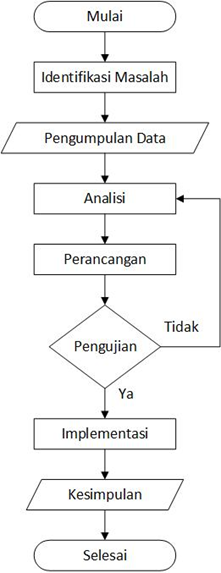
Enkripsi Algoritma AES 256



Deksripsi Algoritma AES 256



Alur Penelitian



1. **Hasil dan Kesimpulan :**

Berdasarkan dari hasil dan pembahasan yang telah didapatkan maka dapat ditarik kesimpulan bahwa algoritma kriptografi AES 256 dan metode steganografi LSB baik untuk diimplementasikan dalam mengamankan file gambar yang kerahasiaannya sangat dijaga. Dari hasil proses enkripsi didapatkan gambar *chiper* yang tidak dapat dimengerti. Dengan semakin bertambahnya ukuran file semakin besar waktu eksekusi dari proses enkripsi. Seperti yang terlihat pada tabel percobaan yang mendapatkan hasil dari waktu eksekusi yang bertambah seiring dengan bertambahnya ukuran file gambar. Dari hasil proses dekripsi didapatkan file gambar pesan asli. Begitu pula seperti proses enkripsi, pada proses dekripsi semakin besar ukuran file maka semakin besar pula waktu eksekusi proses dekripsi. Ini diperkuat dengan hasil uji SHA-1 yang menyatakan nilai hash file gambar hasil dekripsi sama dengan nilai hash file gambar asli. Ini berarti proses dari enkripsi maupun dekripsi telah berhasil. Selanjutnya dilihat dari hasil proses penyisipan dan ekstraksi. Gambar penampung sebelum disisipkan pesan (gambar cover) dan gambar penampung setelah disisipkan pesan (gambar stego) tidak ada perbedaan jika dilihat secara kasat mata. Pada saat dilakukan pengujian terhadap kualitas gambar stego, hasil nilai PSNR rata-rata memiliki nilai 44,14086 dB dengan nilai error rata-rata 2,830403 dB dan itu menyatakan kualitas hasil penyisipan yang baik. Jadi, aplikasi ini dapat diimplementasikan untuk mengamankan dan menjaga kerahasiaan file gambar.

1. **Kekurangan dan kelebihan jurnal :**

**Kelebihan**

Kelebihan dari Jurnal ini adalah berdasarkan ide dan gagasannya penulismenggunakan dasar teori yang beragam dan relevan sesuai dengan permasalahan yang ditelitidalam penelitian ini. Selain itu penulis menggunakan sumber-sumber dan literatur yang banyak sekali, tersusun secara sistematis, dan bahasa yang digunakan mudah dipahami.

**Kekurangan**

Dokumentasi dari jurnal ini sangat kecil sehingga gambar juga nampak kurang jelas.

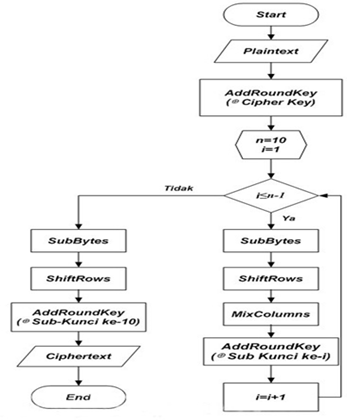
**Jurnal 2**

1. **Judul :** Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar

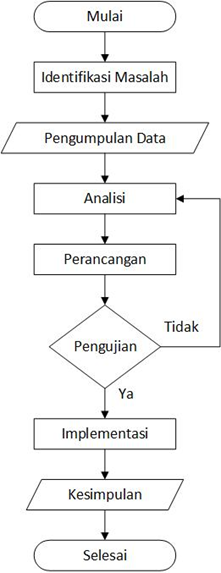
**Latar Belakang :** Advanced Encryption Standard yang merupakan metode kriptografi yang bisa dimanfaatkan untuk menyelamatkan data dalam berbagai aplikasi . AES adalah blok chipertext simetrik yang digunakan untuk mengenkripsi dan mendekripsi informasi. Sementara rasio hasil kompresi pada Kompresi yang mengimplementasikan metode Kriptografi AES menjadi sistem terpadu adalah sebesar 41,80% untuk file uji \*. Selanjutnya melakukan penelitian dalam pengamanan data untuk pesan teks yang berupa isi data dokumen atau file dan data dokumen menggunakan algoritma AES. AES adalah algoritma kriptografi untuk mengamakan data dimana algoritmanya adalah blokchipertext simetrik yang dapat mengenkripsi dan mendekripsi informasi. Pengamanan dan penyandian yang berlapis-lapis dilakukan agar keamanan data informasi dapat terjaga.

1. **Tujuan Penelitian :** untuk mencegah terjadinya kasus manipulasi data yang akan menyebabkan kerugian bagi si pemilik data.
2. **Algoritma yang dipakai serta alur**

Algoritma yang dipakai



Alur Penelitian



1. **Hasil dan Kesimpulan:**

Setelah selesai dilakukan analisis, perancangan serta implementasi menggunakan algoritma Advance Encryption Standard (AES) dapat ditarik kesimpulan sebagai berikut:

1. Dengan adanya sistem keamanan data penduduk di DISDUKCAPIL Kota Pematangsiantar dapat terbantu

dalam mengamankan data-data yang bersifat rahasia di instansi DISDUKCAPIL.

2. Hasil enkripsi merupakan sekumpulan kombinasi karakter yang tidak dapat dimengerti oleh manusia.

3. Untuk hasil enkripsi akan selalu sama dengan hasil dekripsi dengan menggunakan kunci yang sama.

4. Dari implementasi Algoritma kriptografi AES dapat mengamankan file penduduk dengan jenis ekstensi

seperti : .doc, .xls, .ppt, .pdf, .jpg dan .png.

1. **Kekurangan dan kelebihan jurnal :**

**Kelebihan**

Jurnal ini memiliki kelebihan pada hasilnya banyak diberikan gambaran gambaran seperti

table dan diagram membuat pembaca lebih mudah memahami hasil dari penelitian jurnal

tersebut.

**Kekurangan**

Tidak menyediakan ruang bagi masyarakat untuk memberikan respon.