

# Implementasi AES untuk Pengamanan Pesan Dalam Citra Grayscale

Nurul Utami Amaliah W - 13517132  
Program Studi Teknik Informatika  
Sekolah Teknik Elektro dan Informatika  
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung  
13517132@std.stei.itb.ac.id

**Abstract**—Kriptografi adalah ilmu menjaga atau mengamankan suatu informasi dengan cara mengacak atau menyembunyikan informasi sehingga sulit untuk dianalisis. Algoritma yang digunakan pada penelitian ini adalah algoritma AES 128 yang telah diubah menggunakan citra *grayscale*. Algoritma AES merupakan algoritma modern pengganti algoritma DES, dan merupakan algoritma yang dipilih untuk mengamankan suatu data/pesan karena efisien dan mempunyai keamanan yang kuat. Dalam prosesnya, kunci gambar *grayscale* dibagi menjadi 16 blok piksel, piksel dioperasikan pada setiap blok dengan operasi XOR sehingga akan diperoleh satu karakter untuk setiap blok. Dari proses XOR piksel dalam 16 blok akan diperoleh panjang 16 karakter atau 128 bit. Data yang digunakan dalam penelitian ini adalah gambar biasa berupa gambar *grayscale* dan kunci berupa gambar *grayscale* juga. Gambar *grayscale* (gambar biasa) akan dienkripsi dengan kunci gambar yang juga merupakan gambar *grayscale*. Mula-mula kunci akan diambil dari citra *grayscale* dengan cara membagi 16 blok sehingga diperoleh kunci dengan panjang 128 bit, kemudian dilakukan pembangkitan kunci dengan *key generator* pada algoritma AES sehingga diperoleh 10 sub kunci. Kemudian dilakukan enkripsi dengan 10 subkunci yang diperoleh dengan menggunakan algoritma AES. Hasil dari proses enkripsi akan menghasilkan gambar tersandi atau cipher image yang tidak mengandung informasi dari gambar biasa. Hasil dari algoritma ini terbilang aman terhadap serangan karena memiliki kunci yang bervariasi dan sensitif.

**Keywords**—kriptografi; AES; Algoritma Rijndael; *Grayscale*

## I. PENDAHULUAN

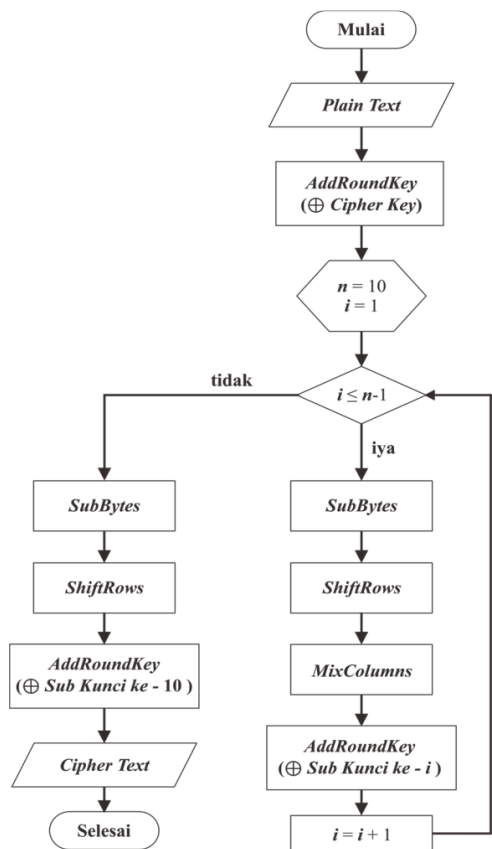
Perkembangan globalisasi tidak hanya memberikan dampak positif bagi lingkungan manusia, tetapi juga memberikan dampak negatif. Salah satunya yakni penyalahgunaan data privasi milik seseorang oleh pihak yang tidak berwenang. Kriptografi adalah ilmu untuk mengamankan suatu informasi/data. Rijmen dan Daemen mengajukan sebuah proposal standard algoritma kriptografi baru yang dinamakan sebagai Algoritma Rijndael, sebagai pengganti algoritma kriptografi lama (Data Encryption Standard / DES). Algoritma DES dianggap sudah tidak aman lagi karena dengan perangkat keras khusus kuncinya mampu ditemukan dalam beberapa hari. Algoritma Rijndael merupakan algoritma yang banyak dipilih

untuk mengamankan suatu data/pesan karena efisien dan pengamanannya yang kuat. Pada tahun 2001, algoritma yang diajukan oleh Rijmen dan Daemen ini kemudian dipilih oleh National Institute of Standards and Technologi (NIST) dengan sebutan Advanced Encryption Standart (AES) sebagai pengganti algoritma lama (DES). Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128, 192, dan 256. Fadhillah melakukan penelitian tentang algoritma AES dalam pengamanan citra digital. Penelitian tersebut menggunakan gambar sebagai plain image dan mencoba beberapa model kunci seperti huruf, angka dan symbol. Hasil dari penelitian tersebut yaitu keamanan pengamanan citra dengan algoritma AES bisa lebih optimal jika menggunakan jenis kombinasi dari angka, huruf dan symbol. Tujuan dari penelitian ini adalah memanfaatkan berbagai teknik pengamanan suatu informasi yang sudah dipaparkan. Penulis akan meneliti dan membuat suatu aplikasi untuk mengamankan suatu data berupa citra grayscale, dengan kunci citra grayscale menggunakan algoritma AES dengan panjang kunci 128 bit. Citra tersebut akan dibagi menjadi 16 blok dan di XOR-kan pikselnya pada tiap blok tersebut, sehingga menghasilkan 16 karakter untuk dijadikan kunci pada algoritma AES 128.

## II. LANDASAN TEORI

### A. Algoritma AES

Algoritma AES merupakan algoritma modern yang bersifat simetri, cipher block, dan menggunakan sistem basis hexadesimal dalam proses komputasinya. Ukuran kunci pada algoritma ini sebesar 128 bit, 192 bit, dan 256 bit. Pada Umumnya ukuran kunci yang digunakan yaitu 128 bit atau AES-128. Proses enkripsi dan dekripsi pada algoritma ini dilakukan dengan dua tahapan yaitu proses pembangkitan sub-kunci dari kunci awal, kemudian proses enkripsi/dekripsi. Jumlah sub-kunci pada AES-128 adalah 10 sub-kunci, masing-masing berukuran 128 bit.



Gambar 1. Flowchart Enkripsi Algoritma AES

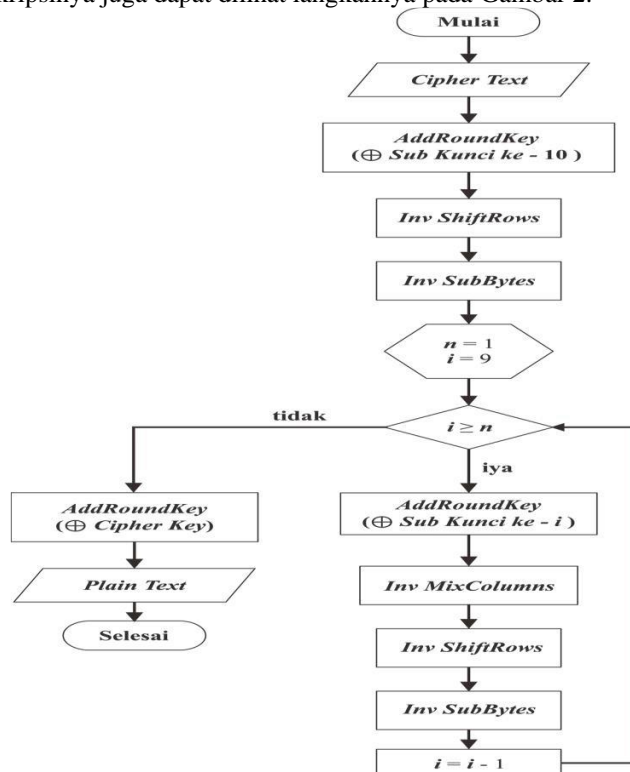
Proses pembangkitan sub-kunci dilakukan dengan mempartisi kunci awal menjadi 4 kolom/words, dilanjutkan dengan melakukan empat langkah/operasi berurutan, yaitu operasi RotWord, SubWord, Operasi XOR dengan R-Con, kemudian operasi XOR dengan kolom sebelumnya. Lakukan empat langkah yang sama untuk mendapatkan sub-kunci yang lain. Proses enkripsi dan dekripsi membutuhkan 10 subkunci yang sudah dibangkitkan dan plaintext atau ciphertext yang sudah dipartisi menjadi block-block 128 bit. Gambar 1 merupakan flowchart enkripsi pada algoritma AES 128 bit (AES-128). Sedangkan Gambar 2 merupakan flowchart dekripsi pada algoritma AES 128 bit (AES-128).

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the A4 paper size. If you are using US letter-sized paper, please close this file and download the file “MSW\_USltr\_format”.

### B. Enkripsi AES dengan Kunci Citra Grayscale

Enkripsi-Pembangkit Kunci Bergeser adalah metode yang bertujuan untuk memodifikasi kunci yang diambil dari sebuah citra grayscale. Proses pembangkitan kunci dari metode ini yaitu dengan membagi piksel-piksel pada gambar menjadi 16 blok, kemudian di operasikan dengan operasi XOR semua piksel tersebut pada setiap bloknya. Sehingga akan didapatkan nilai 16 karakter atau kunci dengan panjang 128 bit. Proses enkripsi pada algoritma ini yaitu seperti pada proses enkripsi AES yang sudah dijelaskan sebelumnya dengan kunci yang didapat hasil dari pembangkitan kunci. Prosesnya dapat

dilakukan dengan beberapa metode yakni AddRoundKey, SubByte, ShiftRow dan MixColumns, atau lebih jelasnya semua langkah dapat dilihat pada gambar 1. Proses dekripsinya juga dapat dilihat langkahnya pada Gambar 2.



Gambar 2. Flowchart Dekripsi Algoritma AES

### C. Analisa Keamanan

Beberapa analisis keamanan dari penelitian ini adalah sebagai berikut:

#### a. Analisis Diferensial

Analisis diferensial digunakan untuk menentukan perbedaan dari dua citra yaitu dengan menghitung nilai dari number of pixels change rate (NPCR). NPCR dengan nilai lebih besar dari 90% akan menyulitkan kriptanalisis dalam mencari hubungan statistik antara citra asli dengan citra tersandi.

$$NPCR = \frac{\sum_i \sum_j D(i,j)}{W \times H} \times 100\%$$

dimana W dan H merepresentasikan lebar citra dan tinggi citra, dan bentuk dari  $D(i, j)$  dapat ditentukan seperti berikut:

$$D(i, j) = \begin{cases} 0, & C(i, j) = C'(i, j) \\ 1, & C(i, j) \neq C'(i, j) \end{cases}$$

dengan  $(i, j)$  dan  $C'(i, j)$  merepresentasikan nilai derajat keabuan dari baris  $i$ , dan kolom  $j$  dari citra  $C$  dan  $C'$ .

#### b. Analisis Sensitivitas Kunci

Analisis sensitivitas kunci digunakan untuk mengetahui kesensitifan kunci dari suatu algoritma. Dua hal yang menjadi tolak ukur yaitu, (i) ketika kunci yang digunakan untuk mengenkripsi citra tersebut sedikit berbeda maka akan

menghasilkan cipher image yang sangat berbeda, (ii) jika ada perbedaan kunci antara proses enkripsi dan dekripsi maka tidak akan memperoleh plain image yang diinginkan. Tolak ukur tersebut didapatkan dengan menggunakan Number of pixels change rate (NPCR).

c. Analisis Brute Force Attack

Proses Analisis keamanan suatu metode atau algoritma sangat penting untuk dilakukan untuk mengetahui seberapa aman ketika algoritma itu digunakan. Brute force attack adalah metode untuk menemukan skema kriptografi dengan mencoba semua kemungkinan password atau kunci. Brute force attack adalah metode untuk menemukan skema kriptografi dengan jumlah besar kemungkinan kunci. Brute force attack memungkinkan dapat menyerang kunci privat di hampir semua skema kriptografi, tipe serangan ini bergantung pada ukuran kunci dan mekanisme pada enkripsi yang digunakan. Dalam bidang kriptografi, brute force attack merupakan teknik yang digunakan penyerang untuk menemukan kunci enkripsi dengan cara mencoba semua kemungkinan kunci.

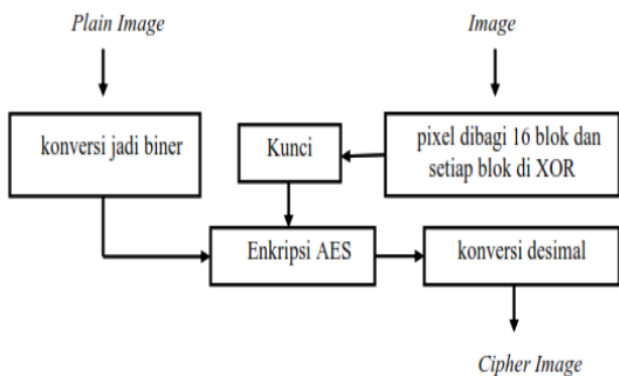
Contoh:

Kunci yang digunakan pada penulisan ini yaitu kunci dengan panjang 128 bit. Maka jumlah kunci yang harus dievaluasi oleh pihak lawan adalah sebanyak  $(2)(2)(2)(2)(2) = 2^{128} = 3,4028e + 38$ .

Artinya ada  $3,4028 \times 10^{38}$  kemungkinan kunci yang harus dicoba. Jika tahun ada 31.536.000 detik dan 1 komputer untuk menganalisis 1 kunci membutuhkan 1 detik, maka ada  $1,0790 \times 10^{31}$  tahun. Meskipun algoritma brute force tidak cocok karena membutuhkan waktu yang cukup lama, namun sebagaimana ciri algoritma brute force pada umumnya nilai plusnya terletak pada keberhasilannya yang selalu menemukan solusi (jika diberikan waktu yang cukup).

III. METODOLOGI

Metode penelitian yang dilakukan menggunakan algoritma AES dengan kunci sebuah citra grayscale. Pertama, membangkitkan kunci dari gambar dengan mengkonversinya menjadi 16 karakter. Kemudian dilakukan enkripsi AES dengan kunci yang sudah didapat dari sebuah citra. Gambar 3 adalah proses enkripsi AES dengan kunci citra grayscale. Proses Enkripsi AES dengan kunci citra grayscale pada Gambar 3 dijelaskan sebagai berikut,



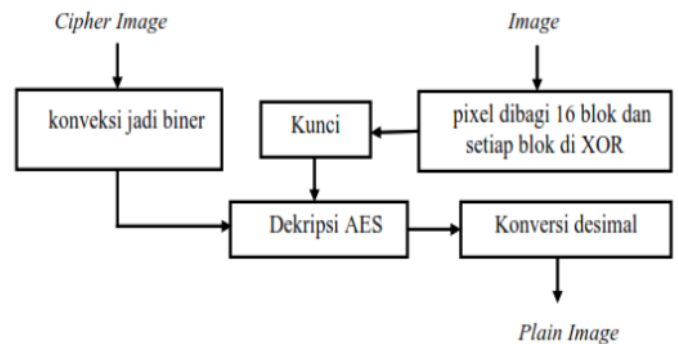
Gambar 3. Proses Enkripsi AES Kunci Citra Grayscale

- a. Konversi karakter plain image menjadi bilangan biner. Setiap karakter dalam plain image dikonversi menjadi bilangan desimal sesuai kode ASCII kemudian dikonversi menjadi bilangan biner.
- b. Membagi pixel menjadi 16 blok dan di XOR setiap pixelnya. Membagi 16 blok dari jumlah pixel yang ada dengan mengurutkan baris pertama sampai baris terakhir. Kemudian mengoperasikan setiap pixel yang ada pada setiap blok dengan operasi XOR sehingga didapatkan 16 karakter atau 128 bit untuk dijadikan kunci pada algoritma AES 128.
- c. Kunci yang didapat hasil dari proses pembagian gambar menjadi 16 blok yang nantinya akan mendapat 16 karakter atau 128 bit untuk digunakan dalam enkripsi algoritma AES.
- d. Enkripsi AES

Proses enkripsi dari plain image dan kunci yang sudah didapatkan dengan langkah sebagai berikut

- AddRoundKey
- SubByte
- Shiftrows
- MixColumns
- Konversi desimal

Setiap bilangan biner dari hasil enkripsi tersebut dikembalikan lagi dalam bentuk desimal dan dirangkai menjadi sebuah citra. Hasil konversi ini akan menjadi cipher image. Kedua, proses dekripsi cipher image menjadi plain image kembali dengan membalik dari proses enkripsi, diuraikan pada Gambar 4.



Gambar 4. Proses Dekripsi

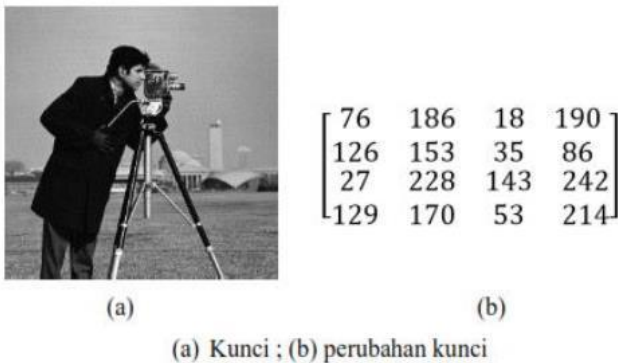
IV. HASIL DAN PEMBAHASAN

Data penelitian yang digunakan sebagai plain image yaitu citra grayscale berukuran 128x128 (lena.jpg), dan kunci citra grayscale berukuran 256x256 (cameraman.tif), ditunjukkan pada Gambar 5(a) dan 5(b). Proses enkripsi menggunakan satu buah kunci awal yaitu berupa citra grayscale (cameraman.tif). Kunci tersebut dimodifikasi dengan membagi seluruh pixel menjadi 16 blok kemudian setiap blok tersebut dioperasikan dengan operasi XOR, sehingga akan memperoleh 16 nilai derajat keabuan dan di konversi kedalam bentuk

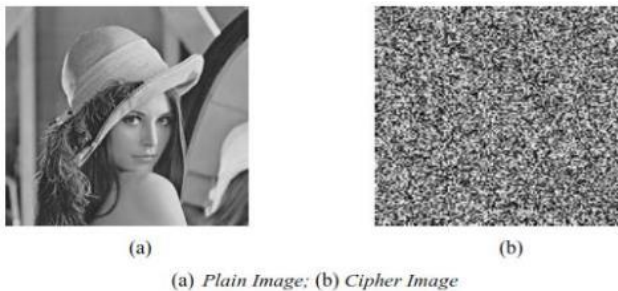
desimal. Gambar 6 menunjukkan gambar awal kunci dan hasil konversi menjadi 16 derajat keabuan yang akan digunakan dalam tahap enkripsi. Proses selanjutnya yaitu proses enkripsi algoritma AES dengan kunci yang sudah dibangkitkan dari citra grayscale. Proses enkripsi bias dilihat langkah langkahnya seperti pada Gambar 1. Enkripsi dilakukan mulai dengan 16 data awal yang ada pada plain image hingga pada data akhir. Hasilnya dapat dilihat pada Gambar 7.



Gambar 5. Data Penelitian



Gambar 6. Kunci dan Hasil Konversi

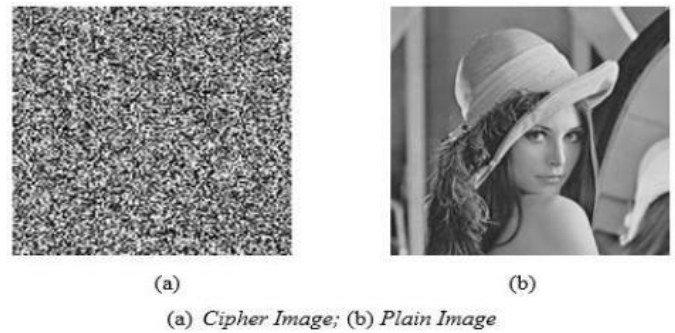


Gambar 7. Hasil Proses Enkripsi

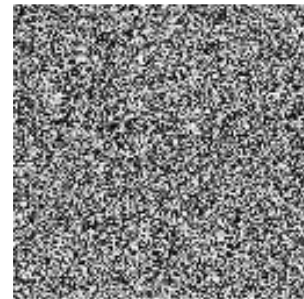
Nilai NPCR lebih besar dari 90% menunjukkan algoritma tersebut baik digunakan untuk enkripsi data. Nilai NPCR yang didapatkan antara cipher image akhir dengan plain image adalah 99,6582%. Sehingga metode ini aman untuk digunakan.

A. Analisis Sensitivitas Kunci

Kunci yang digunakan untuk enkripsi plain image pada tahap ini yaitu cameraman.tif berdimensi 256x256, cameraman.jpg berdimensi 256x256 piksel dan cameraman.png berdimensi 255x255 piksel.



Gambar 8. Hasil Proses Dekripsi



Gambar 9. Hasil Dekripsi

Seperti yang ditunjukkan pada tabel 3, no 1 adalah nilai NPCR dengan kunci AES yang digunakan dalam tahap enkripsi pada penulisan ini. No 2 yaitu perbedaan hasil enkripsi dengan nilai NPCR 99,5483% yang dibandingkan dengan hasil enkripsi no 1. Sedangkan pada no 3, nilai NPCR 99,6643% yang dibandingkan hasil enkripsinya dengan no 1. Gambar 9 merupakan gambar hasil dekripsi yang kunci aslinya cameraman.tif akan tetapi diinput dengan kunci cameraman.jpg, sehingga tidak mampu mengembalikan gambar menjadi plain image.

V. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan pada penelitian ini, maka didapatkan beberapa kesimpulan sebagai berikut:

- a. Proses pembangkitan kunci algoritma AES dari citra grayscale dengan mengkonversi menjadi 16 blok dan mengoperasikan setiap pikselnya pada setiap blok menggunakan operasi XOR. Hasil operasi tersebut akan mendapatkan 16 karakter atau bilangan biner sepanjang 128 bit dan akan digunakan pada tahapan enkripsi maupun dekripsi terhadap algoritma AES.
- b. Proses enkripsi dengan kunci citra grayscale yaitu dengan membangkitkan sebuah kunci dari citra grayscale tersebut menjadi 128 bit. Kemudian dilakukan tahapan-tahapan pada algoritma AES yakni pembangkitan 10 sub kunci, AddRoundKey, SubBytes, ShiftRows, MixColumns. Sedangkan pada proses dekripsi yaitu caranya sama dengan mengkonversi kunci grayscale dan membangkitkan menjadi 10 sub kunci, kemudian melakukan tahapan algoritma AES dengan kunci kunci ke-10 sampai ke-1. Tahapan tersebut meliputi AddRoundKey, InvShiftRows, InvSubBytes dan

InvMixColumns. Proses enkripsi maupun dekripsi memiliki putaran tahapan yang sama, yakni 10 putaran.

c. Analisis keamanan pada penelitian ini menunjukkan bahwa metode yang diajukan oleh penulis dengan menerapkan kunci citra grayscale untuk enkripsi algoritma AES 128 merupakan metode yang aman dalam penyandian informasi. Dibuktikan dengan cipher image yang memiliki nilai NPCR = 90% dari semua data penelitian. Dilakukan juga percobaan enkripsi dengan kunci yang mirip dan semuanya mendapatkan nilai NPCR > 90% yang dapat diartikan bahwa algoritma ini memiliki kunci yang sensitif.

#### REFERENCES

- [1] Atani, R. E., Rad, R. M. dan Attar, A. (2013). A new fast and simple image encryption algorithm using scan patterns and xor. *International Journal of Signal Processing, Image Processing and Pattern Recognition*. Vol.6(5): 275-290.
- [2] Rijmen, V. dan Daemen, J. (1999). AES Proposal: Rijndael. <http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf>.
- [3] Patel, A. dan Padate, R. (2015). Image encryption and decryption using aes algorithm. *International Journal of Electronics and Communication Engineering & Technology (IJECE)*. Vol. 6(1). 23-29.

#### PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 12 Juni 2024



Nurul Utami Amaliah W 13517132