**LAPORAN PRAKTIKUM**

**PRAKTIK SISTEM KEAMANAN DATA**

**“RESUME JURNAL ALGORITMA ADVANCED ENCRYPTION STANDARD(AES) ”**

Dosen Pengampu : Yusuf Fadlila Rachman, S.Kom., M. Kom.



Disusun oleh :

Muhammad Hanif Arafi V3920038

Narutama Phinda Baskara V3920042

Oktarinia Rossa Atanaswati V3920046

Wibiati Sekar Kinasih V3920061

**PROGRAM STUDI DIII TEKNIK INFORMATIKA PSDKU**

**SEKOLAH VOKASI**

**UNIVERSITAS SEBELAS MARET**

**2021**

**RESUME JURNAL 1 (Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen)**

a. Judul dan Latar Belakang Masalah

Judul yang dipakai dalam jurnal ini adalah Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen, Latar Belakang masalah yang diangkat dari jurnal ini adalah seiring berkembangnya sebuah teknologi saat ini tentunya keterbukaan data pribadi akan semakin rentan terjadi, khususnya jika kita sering mengirimkan file dokumen yang rahasia, ini menjadi incaran oleh para cracker. Oleh karenanya, Ilmu kriptografi hadir untuk mempelajari teknik -teknik matematika yang berhubungan dengan aspek keamanan data dan informasi seperti integritas data, autentikasi data, dan keabsahan data. Lalu, ilmu kriptografi melahirkan teknologi yang bernama AES, yang dapat digunakan untuk pengamanan penyandian dengan cara melakukan enkripsi per blok (128 bit) atau 16 karakter yang dapat digunakan juga untuk enkripsi teks.

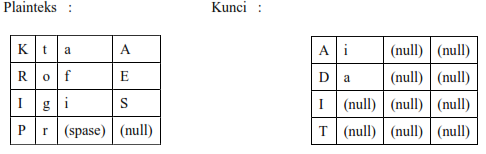
b. Tujuan Penelitian

Dari latar belakang yang telah diuraikan di atas, tujuan dari penelitian ini adalah untuk mengetahui bagaimana proses penyandian dengan Advanced Encryption Standard (AES) dan akan diuraikan menjadi beberapa pokok seperti dibawah ini :

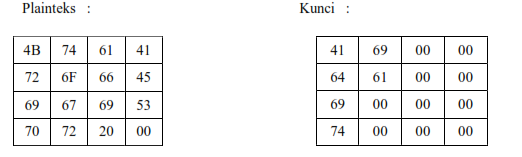
1. Memahami proses penyandian dengan Advanced Encryption Standard (AES).
2. Mengetahui penerapan Algoritma kriptografi AES pada file teks.
3. Dapat merancang dan menggunakan program pengamanan data teks metode Kriptografi AES dengan menggunakan Graphical User Interface (GUI) MATLAB.

c. Algoritma yang dipakai beserta alur penelitiannya

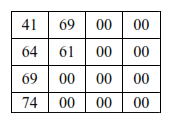
- Mengubah plaintext menjadi sebuah state



- Konversi text menjadi bilangan heksadesimal dengan melihat tabel kode ASCII



Proses Ekspansi Kunci



Atau dapat ditulis

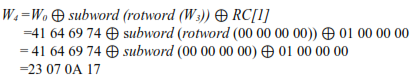
W0= 41 64 69 74

W1= 69 61 00 00

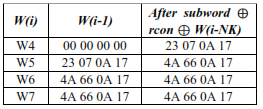
W2= 00 00 00 00

W3= 00 00 00 00

Jadi, untuk mencari *W4* adalah seperti berikut :

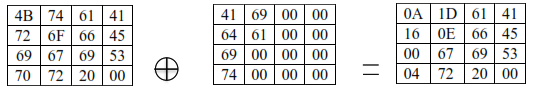


Hasil perhitungan untuk ekspansi untuk 1



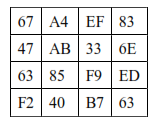
Proses Enkripsi

* Melakukan xor antara plaintext dan kunci

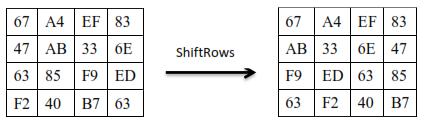


* Ronde 1

Hasil Proses Subbyte ( menggunakan table s- box)

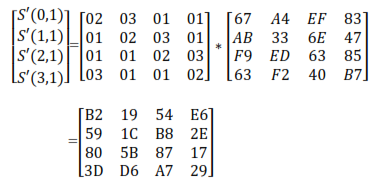


Transformasi ShiftRows



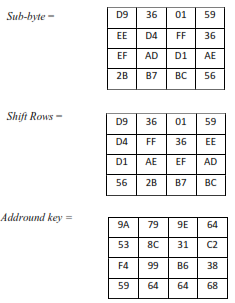
Proses MixColumns, akan proses ini menjadi 4 bagian untuk kesebuah matriks atau state

* Proses mixcolum kolom pertama



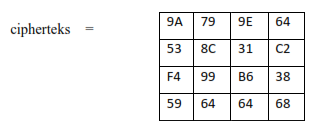
Pada ronde pertama akan didapatkan sebuah ciphertext, yang nantinya akan menjadi input untuk ronde 2, begitu juga ronde 2 akan digunakan untuk input ronde 3, proses berlangsung sampai ronde 10, seperti hasilnya berikut ini

Ronde 10 :



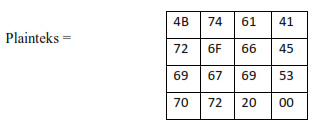
Pada ronde 10 ini dilakukan 3 transformasi yaitu, Subbyte, ShiftRows,

Addroundkey, sehingga didapatkan ciphertext yang sesungguhnya



jika di dalam bentuk ASCII maka didapat cipherteks: š S ô Y y Œ ™ d ž 1¶ d d Â 8 h

Dari proses dekripsi yang dilaksanakan 10 ronde didapat:



Hasil plaintext yang dikonversi ke bentuk ASCII = “Kriptografi AES”, pada algoritma AES plaintextnya = “Kriptografi AES”, dan kuncinya = “Aditia”, maka didapat ciphertext “š S ô Y y Œ ™ d ž 1¶ d d Â 8 h”.

d. Ceritakan hasil penelitian pada jurnal tersebut dan kesimpulannya

Dalam penelitian tersebut akan meneliti tentang proses penyandian kriptografi AES pada file. Pada kesimpulannya, proses enkripsi dalam algoritma kriptografi AES 128, 128 bit (1 bit) plainteks terlebih dahulu akan dikonversi menjadi kode ASCII dan dibentuk dalam matriks byte berukuran 4x4 (state). Pada file dokumen yang sudah dipastikan memiliki jumlah karakter lebih dari 16 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 maka dilakukan padding. Dengan bantuan MATLAB proses enkripsi dan dekripsi dapat dilakukan dengan cepat dan efisien yang dibutuhkan hanya menginputkan plainteks dan kuncinya saja maka proses enkripsi dan dekripsi akan menghasilkan output dengan cepat

e. Kelebihan dan kekurangan jurnal

1. Kelebihan

* Topik yang dibahas sering digunakan oleh sebagian orang untuk penerapan penyandian pada file dokumen yang penting
* Penjelasan di Pendahuluan lumayan jelas dan detail sehingga pembaca mengetahui isi dengan baik
* Konsep Pada Pembuatan Enkripsi lumayan jelas

1. Kekurangan

* Struktur yang membingungkan
* tidak dijelaskan cara untuk menggunakan heksadesimal dari huruf menjadi angka
* Proses Mixcolumn yang tidak dijelaskan pengenalan awal dulu.

**RESUME JURNAL 2 (Implementasi Algoritma Advance Encryption Standard (AES) pada Enkripsi dan Dekripsi QR-Code )**

a. Judul dan Latar Belakang Masalah

Jurnal yang digunakan berjudul Implementasi Algoritma *Advance Encryption Standard* (AES) pada Enkripsi dan Dekripsi QR-Code. Latar belakang masalah pada jurnal tersebut adalah pentingnya permasalahan keamanan data pada perkembangan teknologi saat ini membutuhkan suatu cara untuk menjaga kerahasiaan dan keamanan informasi. Salah satu cara untuk meningkatkan keamanan tersebut adalah dengan menggunakan teknik kriptografi. Ada berbagai macam algoritma yang digunakan dalam kriptografi, salah satunya adalah *Advance Encryption Standard*. Kriptografi dengan algoritma *Advance Encryption Standard* dapat diterapkan pada QR-*Code,* di mana QR-*Code* ini merupakan suatu teknologi labelling yang menyimpan data dalam bentuk pola yang dapat diisi dengan informasi. Pengenalan pola dilakukan dengan mendeteksi informasi yang dibutuhkan. Tujuannya adalah untuk menyampaikan informasi dengan cepat dan mendapatkan respon yang cepat pula. Berdasarkan penelitian-penelitian yang telah ada dan disertakan dalam jurnal tersebut, dapat diambil kesimpulan bahwa algoritma AES memiliki tingkat keamanan yang lebih baik daripada algoritma yang lainnya, sehingga jurnal ini membahas mengenai implementasi algoritma AES 128 bit dengan key dan plaintext 128 bit untuk enkripsi dan dekripsi pada QR-*Code.*

b. Tujuan Penelitian

Tujuan Penelitian (Implementasi Algoritma Advance Encryption Standard (AES) pada Enkripsi dan Dekripsi QR-Code Untuk mengetahui pentingnya permasalahan keamanan data pada perkembangan teknologi saat ini untuk menjaga kerahasiaan dan keamanan informasi, dengan menggunakan teknik kriptografi atau menggunakan penerapan pada Qr Code untuk menyimpan data dalam bentuk pola tertentu, pengguna hanya perlu scan saja saja dan pada algoritma AES untuk mengetahui keamanan apa yang baik dari algoritma yang lain.

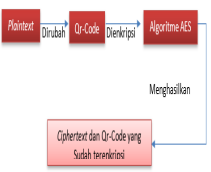
c. Algoritma yang dipakai beserta alur penelitiannya

Algoritma yang digunakan pada jurnal ini adalah algoritma *Advance Encryption Standard* (AES). Sementara itu, untuk alur penelitian dalam jurnal tersebut adalah sebagai berikut:

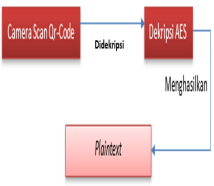
1. Perancangan

1. 1 Perancangan Umum Sistem

Perancangan umum sistem merupakan tahap awal dari perancangan perangkat lunak. Perancangan ini merepresentasikan arsitektur sistem secara umum. Berikut ini merupakan gambar dari rancangan untuk proses enkripsi yang berfungsi untuk mengubah plaintext menjadi QR-*Code* dan dienkripsi dengan AES, setelah itu menghasilkan ciphertext dan QR-*Code* yang dienkripsi.



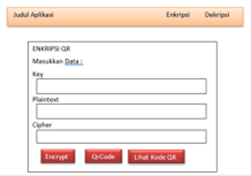
Untuk rancangan pada proses dekripsi yang berfungsi untuk mengembalikan ciphertext menjadi plaintext adalah sebagai berikut:



1. 2 Perancangan Antarmuka

Perancangan antarmuka merupakan tahap setelah perancangan arsitektur system. Berikut ini adalah tampilan menu dekripsi dan tampilan menu enkripsi.

a. Menu dekripsi b. Menu enkripsi

1. Implementasi

2.1. Implementasi antarmuka

Implementasi antarmuka pada sistem ada dua, yaitu halaman enkripsi dan halaman dekripsi.

2.2. Implementasi AES

Implementasi AES untuk enkripsi dan dekripsi pada QR-*Code* adalah dengan cara menginputkan key dan plaintext yang akan diubah menjadi QR-*Code.*

a. Enkripsi

* System menjalankan proses enkripsi sebanyak 10 kali putaran yaitu *AddRoundKey, ShiftRows, SubBytes*, dan *MixColumns* namun pada putaran terakhir tidak dilakukan *MixColumns* dan menghasilkan sebuah ciphertext QR-*Code*.
* QR-*Code* menampung data a-z, 0-1 dan simbol sehingga memperbanyak variasi key dan data yang dienkripsi serta meningkatkan keamanan data.

b. Dekripsi

* Melakukan scanning pada ciphertext QR-*Code* dan memasukkan key lalu system menjalankan proses dekripsi sebanyak 10 kali putaran yaitu *AddRoundKey, InvShiftRows, InvSubBytes*, dan *InvMixColumns* namun pada putaran terakhir tidak dilakukan *InvMixColumns* dan menghasilkan isi pesan asli atau plaintext.

Penjelasan mengenai bagaimana alur enkripsi dan dekripsi dengan menggunakan algoritma AES pada jurnal tersebut tidak dijelaskan secara rinci.

d. Ceritakan hasil penelitian pada jurnal tersebut dan kesimpulannya

Hasil Penelitian diatas yang berjudul **Implementasi Algoritma Advance Encryption Standard (AES) pada Enkripsi dan Dekripsi QR-Code** yaitu kita dapat mengetahui bahwa AES atau Advanced Encryption Standard adalah teknik untuk penyandian pesan yang menggunakan penyandian pesan yang menggunakan blok simetris yang terdapat penjelasan Enkripsi, Deskripsi. dan terdapat penjelasan Qr Code atau Quick Response dan dapat ditarik kesimpulan dari penjelasan pada jurnal diatas bahwa Algoritma AES dapat diterapkan pada QRCode. Algoritma AES akan memberikan aspek confidentiality, hal ini dapat dibuktikan dengan pengujian keamanan. dan pengujian validasi ditunjukan hasil yang valid dan hasil pengujian kinerja dari algoritma AES pada QR Code tersebut hanya membutuhkan waktu yang singkat yaitu 0,0034 detik pada enkripsi dan 0,0029 detik pada deskripsi

e. Kelebihan dan kekurangan jurnal

e.1. Kelebihan

- Struktur bagian jurnal yang jelas

- Topik yang dibahas unik, bahkan mungkin jarang ditemui yang membahas penerapan pada QR-Code

- Konsep perancangan dengan tujuan dan manfaat yang bagus dan jelas

- Perancangan sudah berbasis GUI

e.2. Kekurangan

- Penjelasan metode alur enkripsi dan dekripsi yang kurang penjelasannya

- Belum bisa menentukan suatu objek apakah algoritma yang dipakai lebih baik atau tidak

- Alur perancangan sistem yang kurang detail

- Kurangnya sample penerapan akan uji dan analisis