BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Sebagai bahan acuan dalam mengerjakan skripsi ini akan dipaparkan hasil penelitian terdahulu yang digunakan sebagai bahan referensi oleh penulis, diantaranya :

a. (Patrisia, Wikusna, & Aji, 2019). APLIKASI PENJUALAN TIKET BUS SECARA ONLINE BERBASIS WEB DI CV HARUM PRIMA BANDUNG. CV Harum Prima Bandung adalah salah satu perusahaan yang bergerak dalam bidang sarana transportasi, yang melakukan penjualan tiket melibatkan po/loket di kantor pusat dan di agen yang bertempat di Jl. Soekarno Hatta No. 480. Penjualan dilakukan secara langsung yaitu setiap calon penumpang datang langsung ke tempat penjualan tiket. CV PO Harum Prima Bandung juga mengalami kewalahan dalam dokumentasi laporan dan penjualan tiket, Hal tersebut pastinya belum mendukung kegiatan proses bisnis yang ada dengan maksimal. Berdasarkan permasalah di atas dibangunlah aplikasi berbasis web yang dapat menjadi alternatif bagi penumpang untuk melakukan pemesanan tiket dan membantu pihak CV PO Harum Prima Bandung dalam membuat laporan. Aplikasi ini dibuat menggunakan bahasa pemrograman PHP dan MySQL sebagai basis datanya. Metode pengembangannya menggunakan SDLC (System Development Life Cycle) dengan model waterfall. Diharapkan aplikasi ini dapat meningkatkan kualitas pelayanan CV PO Harum Prima Bandung dalam melayani calon penumpang.

b. (Paramarta, Kusyanti, & Data, 2018). IMPLEMENTASI ALGORITMA ADVANCED ENCRYPTION STANDART PADA ENKRIPSI DAN DEKRIPSI QR CODE. Keamanan data merupakan masalah yang sangat penting dalam perkembangan teknologi saat ini. Oleh sebab itu dibutuhkan sebuah cara yang dapat menjaga keamanan merujuk pada perlindungan informasi dari penyingkapan pihak yang tidak sah. Salah satu mekanisme untuk meningkatkan keamanan data adalah dengan menggunakan teknik kriptografi. Ada berbagai macam algoritme dalam kriptografi salah satunya adalah Algoritme Advance Encryption Standard. Skripsi ini menggunakan Algoritme AES dengam ukuran ekspansi key 128 bit yang akan beroperasi dalam sebuah array 4x4. Pada proses state enkripsi akan melalui beberapa tahapan yakni Addroaundkey, Subbyte, Shiftrows, dan Mixcolumns sebanyak 10 kali putaran. Namun pada putaran terakhir tidak dilakukan lagi proses Mixcolumns langsung ke proses Addraoundkey, dan untuk proses dekripsi merupakan proses kebalikan dari proses enkripsi yakni InvAddrows, InvShiftrows, InvSubbyte, dan InvMixcolumns menggunakan kunci round yang sama dengan proses enkripsi. AES diimplementasikan dalam bahasa pemrograman PHP dan diterapkan pada QR Code karena merupakan sebuah teknologi labelling yang dapat menyimpan data dalam bentuk pola yang dapat diisi dengan informasi. Dari hasil implementasi algoritme AES dapat disimpulkan bahwa aplikasi ini dapat mengekripsi semua jenis karakter berupa string, huruf, angka, dan simbol. Pada saat mendekripsi QR Code aplikasi akan mengaktifkan fungsi kamera dan melakukan scanning QR Code yang akan menjadi plaintext kembali. Waktu eksekusi enkripsi dan dekripsi AES adalah 0.0034 detik untuk proses enkripsi dan untuk proses dekripsi membutuhkan waktu 0.0029 detik.

2.2 Android

Menurut (Safaat H, 2011) : “Android adalah sebuah sistem operasi untuk perangkat mobile berbasis linux yang mencakup sistem operasi, middleware, dan aplikasi. Pengembangan android dimulai pada tahun 2003 dengan didirikannya perusahaan Android Inc. Oleh Andy Rubin, Rich Miner,Nick Sears, dan Chris White. Awalnya Android Inc. dioperasikan secara rahasia dan hanya dikenal sebagai pembuat aplikasi mobile. Pada tahun 2008, untuk pertama kalinya perangkat android tersedia secara komersil, yaitu HTC Dream. Sejak saat itu, Android terus berkembang dan perangkat yang memanfaatkannya juga semakin banyak (Tim Limbang Wahana Komputer, 2013). Menurut Wikipedia, Sistem operasi ini dirilis secara resmi pada tahun 2007, bersamaan dengan didirikannya Open Handset Alliance, konsorsium dari perusahaan-perusahaan perangkat keras, perangkat lunak, dan telekomunikasi yang bertujuan untuk memajukan standar terbuka perangkat seluler. Ponsel Android pertama mulai dijual pada bulan Oktober 2008. Android adalah sistem operasi dengan sumber terbuka, dan Google merilis kodenya di bawah Lisensi Apache. Kode dengan sumber terbuka dan lisensi perizinan pada Android memungkinkan perangkat lunak untuk dimodifikasi secara bebas dan didistribusikan oleh para pembuat perangkat, operator nirkabel, dan pengembang aplikasi. Selain itu, Android memiliki sejumlah besar komunitas pengembang aplikasi (apps) yang memperluas fungsionalitas perangkat, umumnya ditulis dalam versi kustomisasi bahasa pemrograman Java. Pada bulan Oktober 2013, ada lebih dari satu juta aplikasi yang tersedia untuk Android, dan sekitar 50 miliar aplikasi telah diunduh dari Google Play, toko aplikasi utama Android. Sebuah survei pada bulan April-Mei 2013

menemukan bahwa Android adalah platform paling populer bagi para pengembang, digunakan oleh 71% pengembang aplikasi bergerak. Di Google I/O 2014, Google melaporkan terdapat lebih dari satu miliar pengguna aktif bulanan Android, meningkat dari 583 juta pada bulan Juni 2013.

Versi-versi android yang sudah dirilis dari awal sampai saat ini menurut Irsyad H dalam (Birri, 2019) yaitu:

1. Versi 1.5 Cupcake dirilis pada tanggal 30 April 2009
2. Versi 1.6 Donate dirilis pada tanggal 15 September2009
3. Versi 2.0 - 2.1 Éclair dirilis pada tanggal 26 Oktober 2009
4. Versi 2.2 Froyo dirilis pada tanggal 20 Mei 2010
5. Versi 2.2.3 - 2.3.7 Gingerbread dirilis pada tanggal 9 Februari 2011
6. Versi 3.1 - 3.2 Honeycomb dirilis pada tanggal 10 mei 2011
7. Versi 4.0.3 - 4.0.4 Ice Cream Sandwich dirilis pada tanggal 16 Desember 2011
8. Versi 4.1 – 4.3 Jelly Bean dirilis pada tanggal 24 Juli 2013
9. Versi 4.4 Kitkat dirilis pada tanggal 31 Oktober 2013
10. Versi 5.0 Lollipop dirilis pada tanggal 15 Oktober 2014
11. Versi 6.0 Marshmallow dirilis pada tahun 2015
12. Versi 7.0 Nougat dirilis pada tahun 2016
13. Versi 8.1 Oreo dirilis pada tanggal 5 Desember 2017

2.3 Android Studio

Android Studio adalah Integrated Development Enviroment (IDE) untuk sistem operasi Android, yang dibangung diatas perangkat lunak JetBrains IntelliJ IDEA dan didesain khusus untuk pengembangan Android. IDE ini merupakan pengganti dari Eclipse Android Development Tools (ADT) yang sebelumnya merupakan IDE utama untuk pengembangan aplikasi android.

Android studio sendiri pertama kali diumumkan di Google I/O conference pada tanggal 16 Mei 2013. Ini merupakan tahap preview dari versi 0.1 pada Mei 2013, dan memasuki tahap beta sejak versi 0.8 dan mulai diliris pada Juni 2014. Versi liris stabil yang pertama diliris pada December 2014, dimulai sejak versi 1.0. Sedangkan versi stabil yang sekarang adalah versi 3.13 yang diliris pada Juni 2018. Fitur Fitur yang tersedia saat ini dalam stable version.

1. Dukungan Gradle-based build
2. Android-specific refactoring dan perbaikan cepat
3. Lint tools untuk menangkap kinerja, kegunaan, kompatibilitas versi, dan masalah lainnya
4. Integrasi Proguard dan kemampuan penananda tanganan aplikasi
5. Template-based wizards untuk membuat template design umum seperti drawer atau empty activity
6. Mendukung untuk pengembangan aplikasi Android Wear.

7. Editor tata letak yang memungkinkan pengguna untuk menyeret dan menjatuhkan (drag-and-drop) komponen UI, opsi untuk melihat tata letak pada beberapa konfigurasi layar
8. Dukungan bawaan untuk Google Cloud Platform, memungkinkan integrasi dengan Firebase Cloud Messaging ('Perpesanan Google Cloud' Sebelumnya) dan Google App Engine
9. Android Virtual Device (Emulator) untuk menjalankan dan men-debug aplikasi di studio Android.

2.4 Android SDK

Android Software Development Kit (SDK) merupakan *kit* yang bisa digunakan oleh para *developer* untuk mengembangkan aplikasi berbasis Android. Di dalamnya, terdapat beberapa *tools* seperti *debugger*, *software libraries*, *emulator*, dokumentasi, *sample code* dan tutorial. Java SE Development kit adalah salah satu contoh Android SDK dan menjadi bahasa pemrograman yang paling sering digunakan untuk mengembangkan aplikasi Android. Di samping itu ada beberapa bahasa lainnya seperti C++, Go, dan Kotlin bahasa yang ditetapkan Google pada tahun 2017 lalu.

2.5 Java

Java adalah bahasa pemrograman yang dapat dijalankan di berbagai komputer termasuk telepon genggam. Bahasa ini awalnya dibuat oleh James Gosling saat masih bergabung di Sun Microsystems saat ini merupakan bagian dari Oracle dan dirilis tahun 1995. Bahasa ini banyak mengadopsi sintaksis yang terdapat pada C dan C++ namun dengan sintaksis model objek yang lebih

sederhana serta dukungan rutin-rutin aras bawah yang minimal. Aplikasi-aplikasi berbasis java umumnya dikompilasi ke dalam p-code (*bytecode*) dan dapat dijalankan pada berbagai Mesin Virtual Java (JVM). Java merupakan bahasa pemrograman yang bersifat umum/non-spesifik (*general purpose*), dan secara khusus didisain untuk memanfaatkan dependensi implementasi seminimal mungkin. Karena fungsionalitasnya yang memungkinkan aplikasi java mampu berjalan di beberapa platform sistem operasi yang berbeda, java dikenal pula dengan slogannya, "*Tulis sekali, jalankan di mana pun*". Saat ini java merupakan bahasa pemrograman yang paling populer digunakan, dan secara luas dimanfaatkan dalam pengembangan berbagai jenis perangkat lunak aplikasi ataupun aplikasi.

Menurut (Sukamto & Shalahuddin, 2013) “Java adalah nama untuk sekumpulan teknologi untuk membuat dan menjalankan perangkat lunak pada komputer standalone ataupun pada lingkungan jaringan”.

Menurut (Kurniawan dkk, 2011)“Java adalah bahasa pemrograman yang dapat dijalankan diberbagai perangkat komputer, termasuk pada ponsel. Dikembangkan oleh Sun Microsystem dan dirilis pada 1995”.

Versi awal Java pada tahun 1996 sudah merupakan versi release sehingga dinamakan Java Versi 1.0. Java versi ini menyertakan banyak paket standar awal yang terus dikembangkan pada versi selanjutnya:

a. java.lang : Peruntukan kelas elemen-elemen dasar.
b. java.io : Peruntukan kelas *input* dan *output*, termasuk penggunaan berkas.

c. java.util : Peruntukan kelas pelengkap seperti kelas struktur data dan kelas kelas penanggalan.

d. java.net : Peruntukan kelas TCP/IP, yang memungkinkan berkomunikasi dengan komputer lain menggunakan jaringan TCP/IP.

e. java.awt : Kelas dasar untuk aplikasi antarmuka dengan pengguna (GUI)

f. java.applet : Kelas dasar aplikasi antar muka untuk diterapkan pada penjelajah web.

2.5.1 Fungsi Java

a. Bahasa yang digunakan sedehana
b. Pengamanan yang cukup ketat
c. Dapat digunakan pada sistem operasi apapun
d. Mendukung native method
e. Daftar perpustakaan yang lengkap

2.5.2 Kelebihan Java

1. Mudah untuk dikembangkan
2. Sifatnya multiplatform
3. Memiliki kemudahan dalam menyusun suatu script
4. Dinamis
5. Bahasa pemrograman berorientasi objek

2.5.3 Kekurangan Java

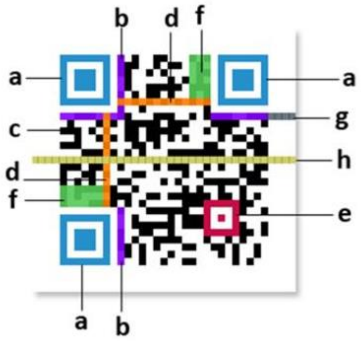
a) Penggunaan memori yang cukup besar

b) Mudah didekompilasi

2.6 QR Code

Quick Response Code sering di sebut QR Code atau Kode QR adalah semacam simbol dua dimensi yang dikembangkan oleh Denso Wave yang merupakan anak perusahaan dari Toyota sebuah perusahaan Jepang pada tahun 1994. Tujuan dari QR Code ini adalah untuk menyampaikan informasi secara cepat dan juga mendapat tanggapan secara cepat. QR Code adalah perkembangan dari barcode atau kode batang yang hanya mampu menyimpan informasi secara horizontal sedangkan QR Code mampu menyimpan informasi lebih banyak, baik secara horizontal maupun vertikal.

Pada dasarnya bahwa QR Code dikembangkan sebagai suatu kode yang memungkinkan isinya untuk dapat diterjemahkan dengan kecepatan tinggi (Rouillard, 2008). Keunggulan dari QR Code adalah mampu menyimpan informasi secara horizontal dan vertikal. Oleh karena itu, QR Code dapat menampung informasi yang lebih banyak dibandingkan dengan barcode satu dimensi (David, 2007). Saat ini, untuk penggunaan QR Code telah banyak diimplementasikan dalam bentuk aplikasi QR Code Reader dan QR Code Generator, sehingga seseorang akan sangat mudah untuk membuat informasi dalam bentuk QR Code dan mendapatkan informasi yang ingin diketahuinya, hanya dengan melakukan proses scanning dan pemindaian data melalui media dari kamera handphone (Anastasia, Istiadi, dan Hidayat, 2010).



Gambar 2. 1 Anatomi QR Code

Beberapa penjelasan anatomi QR Code Menurut (Ariadi, 2011) antara lain

a. Finder Pattern berfungsi untuk identifikasi letak QR Code.
b. Format Information berfungsi untuk informasi tentang error correction level dan mask pattern.
c. Data berfungsi untuk menyimpan data yang dikodekan.
d. Timing Pattern merupakan pola yang berfungsi untuk identifikasi koordinat pusat QR Code, berbentuk modul hitam putih.
e. Alignment Pattern merupakan pola yang berfungsi memperbaiki penyimpangan QR Code terutama distorsi non linier.]
f. Version Information adalah versi dari sebuah QR Code.
g. Quiet Zone merupakan daerah kosong di bagian terluar QR Code yang mempermudah mengenali pengenalan QR oleh sensor CCD.
h. QR Code version adalah versi dari QR Code yang digunakan.

2.6.1 Karakteristik QR Code

Karakteristik dari QR Code yaitu dapat menampung jumlah data yang besar. Secara teori sebanyak 7089 karakter numerik maksimum data dapat tersimpan di

dalamnya, kerapatan tinggi (100 kali lebih tinggi dari kode simbol linier) dan pembacaan kode dengan cepat. QR Code juga memiliki kelebihan lain baik dalam hal unjuk kerja dan fungsi (Ariadi, 2011). Berikut ini merupakan kelebihan unjuk kerja dan fungsi yang dimiliki oleh QR Code.

1. Pembacaan data dari segala arah
2. Ketahanan terhadap penyimpangan simbol
3. Fungsi Pemulihan Data (ketahanan terhadap kotor maupun kerusakan)
4. Kemampuan enkode karakter kanji dan kana jepang
5. Fungsi Linking pada simbol
6. Proses masking

2.6.2 Mode Input Data

Mode input data yang dikenali oleh QR Code ada beberapa macam, diantaranya adalah sebagai berikut (Ariadi, 2011) :

1) Mode ECI (Extended Channel Interpretation)

2) Mode Numerik

3) Mode Alfanumerik

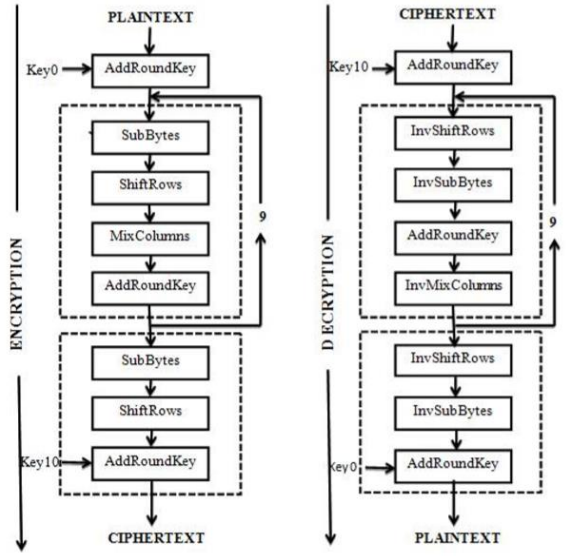
4) Mode 8 bit

5) Mode Huruf Kanji

2.7 Advanced Encryption Standart (AES)

Advanced Encryption Standard (AES) adalah Federal Information Processing Standard (FIPS) yang dipublikasikan oleh National Institute of Standards and Technology (NIST) pada tahun 2001. AES adalah salah satu teknik

enkripsi yang paling banyak dipakai kerana tingkat efisiensi yang tinggi dan sederhana. AES juga merupakan algoritma yang aman. AES, Advanced Encryption Standart, adalah symmetric encryption. Symetric berarti AES mengunakan key yang sama untuk proses enkripsi dan dekripsi. AES adalah block-cipher yang mengenkripsi 128-bit blok (plaintext) menjadi 128-bit blok (ciphertext), atau mendekripsi 128-bit blok (ciphertext) menjadi 128-bit blok (plaintext). AES menggunakan kunci (cipher key) berukuran 128, 192, atau 256 bit. Masing-masing ukuran kunci menggunakan jumlah round yang berbeda. 10 round untuk 128 bit, 12 round untuk 192 bit, dan 14 round untuk 256 bit.

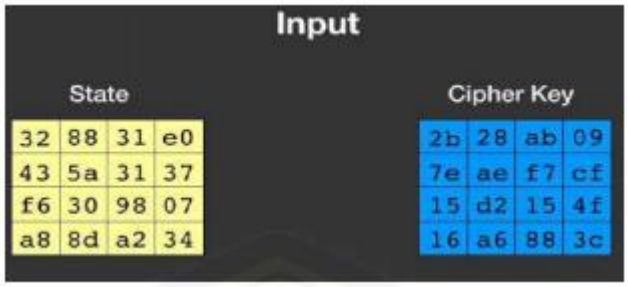


Gambar 2. 2 Proses Enkripsi dan Dekripsi pada AES

Sumber : (Armirara, 2017)

Setiap langkah tersebut dapat dijabarkan sebagai berikut :

A. Proses Enkripsi

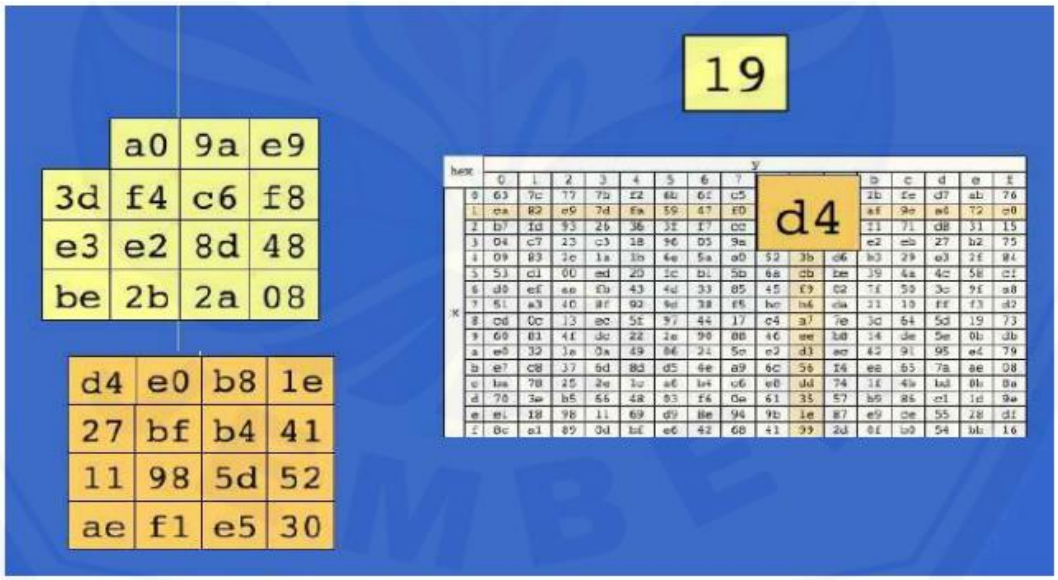


Gambar 2. 3 Matriks 4 x 4

Sumber : (Pariddudin & Syauqi, 2020)

Setelah Didapatkan *Round Key 1* di atas, selanjutnya state yang telah dikonversi ke dalam kode ASCII akan di *SubBytes* menggunakan *S-Box.*

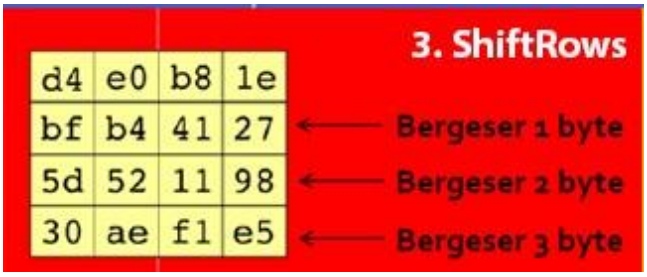
1. *SubBytes* adalah permutasi non-linier pada S-Box. Setiap *byte* input digantikan oleh byte lain berdasarkan table lookup. Cara penggunaan *SubBytes* yaitu dengan cara mensubstitusikan 1 sel pada state dengan 1 sel yang bersesuaian pada S-Box. Elemen-elemen pada S-Box itu sendiri telah ditentukan sebelumnya.



Gambar 2. 4 SubBytes State

Sumber : (Pariddudin & Syauqi, 2020)

2. ShiftRows adalah proses yang melakukan shift atau penggeseran pada setiap elemen blok atau table yang dilakukan per baris.



Gambar 2. 5 ShiftRows

Sumber : (Pariddudin & Syauqi, 2020)

Setelah melalui tahap *SubBytes*, tahap selanjutnya yaitu *ShiftRows*. Transformasi *ShiftRows* dilakukan dengan cara menggeser baris secara *wrapping* (siklik) pada 3 baris terakhir dari *array state*. Jumlah pergeseran bergantung pada nilai baris (r). Baris *r* = 1 digeser sejauh 1 *byte*, baris r = 2 digeser sejauh 2 *byte*, dan baris *r* = 3 digeser sejauh 3 *byte*. Baris *r* = 0 tidak digeser

3. MixColumns adalah mengalikan setiap elemen dari blok cipher dengan matriks biasa yaitu menggunakan dot product. Setiap byte akan digantikan oleh hasil operasinya. Menurut (Surian, 2006) Proses *MixColumns* akan beroperasi pada tiap kolom dari tabel state. Operasi ini menggabungkan 4 *bytes* dari setiap kolom tabel state dan menggunakan transformasi linier.

Gambar 2. 6 MixColumns

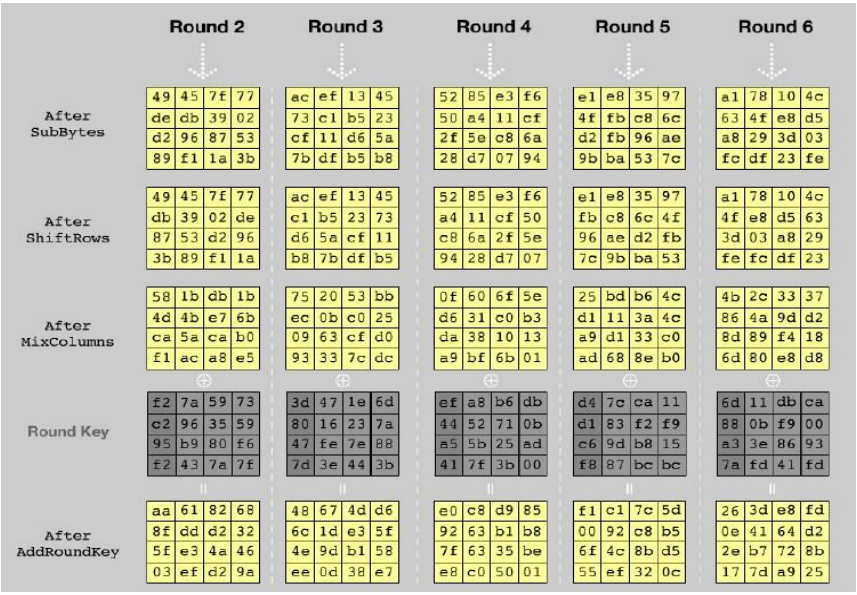
Sumber : (Pariddudin & Syauqi, 2020)

4. AddRoundKey adalah menggabungkan cipher text dengan cipher key mengunakan operasi XOR.

Gambar 2. 7 Add Round Key

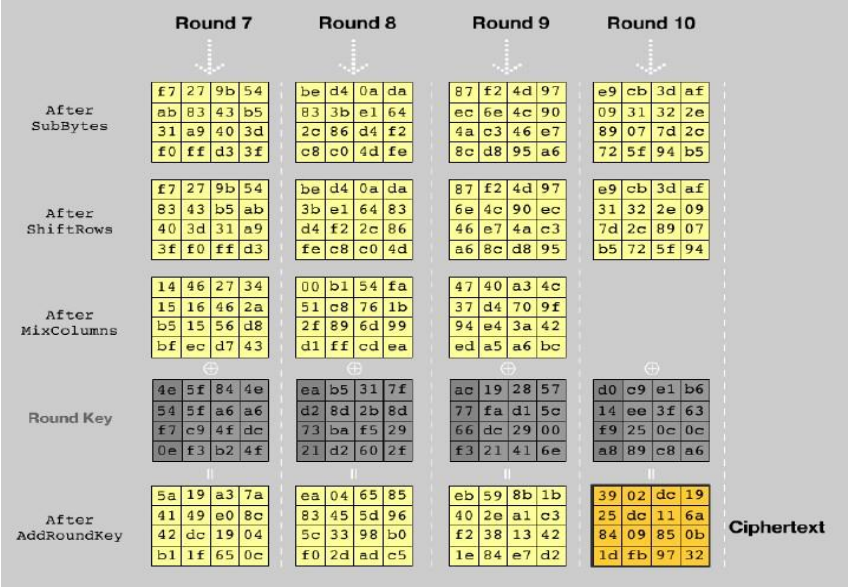
Sumber : (Pariddudin & Syauqi, 2020)

Hasil Enkripsi Algoritma AES mendefinisikan proses enskripsi dari tahap awalsampai akhir yang menggunakan byte sebagai gambaran ilustrasi.



Gambar 2. 8 Proses Enkripsi AES Round 2 – Round 6

Sumber : (Pariddudin & Syauqi, 2020)



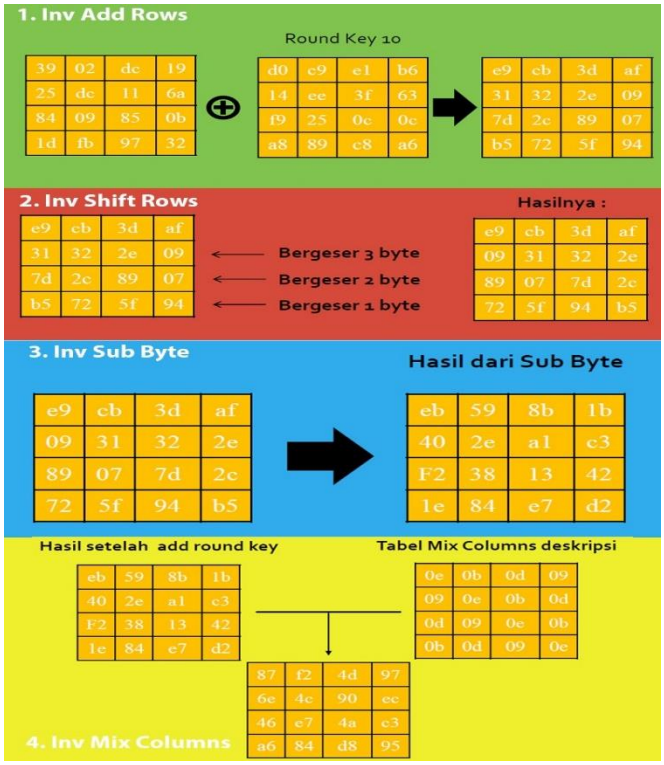
Gambar 2.9 Proses Enkripsi Round 7 - Round 10

Sumber : (Pariddudin & Syauqi, 2020)

Pada system 32-bit atau lebih, memungkinkan untuk mempercepat eksekusi dengan menggabungkan SubByte dan ShiftRow dengan MixColloum, dan mengubahnya menjadi sequence table lookup. Performa algoritma AES yang cepat cocok untuk enkripsi text yang panjang. Namun memiliki kekurangan yaitu manajemen key sangat komplek dan tidak aman.

B. Proses Dekripsi

Proses Dekripsi Algoritma AES mendefinisikan proses dekripsi algoritma AES di mulai dengan melakukan XOR chipertext dengan Add Rows setelah itu lakukan Inv ShiftRows dan Inv SubByte kemudian Tranformasi InvMixColumns sama dengan MixColumns, dimana perbedaannya adalah a(x) yang digunakan adalah inversnya (a-1).



Gambar 2. 10 Proses Dekripsi Algoritma AES

Sumber : (Pariddudin & Syauqi, 2020)

2.7.1 Kelebihan AES

a. AES terbukti kebal menghadapi serangan konvensional (linear dan diferensial attack) yang menggunakan statistik untuk memecahkan sandi.

b. Kesederhanaan AES memberikan keuntungan berupa kepercayaan bahwa AES tidak ditanami trapdoor.
c. AES didesain dengan sangat hati-hati dan baik sehingga setiap komponennya memiliki tugas yang jelas.
d. AES memiliki sifat cipher yang diharapkan yaitu, tahan menghadapi analisis sandi yang diketahui, fleksibel digunakan dalam berbagai perangkat keras dan lunak, baik digunakan untuk fungsi hash karena tidak memiliki weak (semi weak) key, cocok untuk perangkat yang membutuhkan key agility yang cepat, dan cocok untuk stream cipher.

2.8 Kriptografi

Kriptografi Menurut (Klein, 2014) "Kriptografi merupakan suatu teknik guna mengamankan suatu data maupun informasi dengan menyembunyikan isi pesan atau dokumen. Sebuah cryptosystem adalah sistem untuk melakukannya yang terdiri dari dua bagian metode enkripsi dan metode dekripsi dengan mengubah bentuk dari pesan atau dokumen yang dapat dibaca disebut plaintext atau teks-jelas menjadi bentuk yang tidak terbaca disebut cyphertext". (Ko´scielny, Kurkowski, & Srebrny, 2013) mengemukakan bahwa "kriptografi adalah ilmu mengubah, atau encoding, informasi menjadi bentuk yang tidak dipahami bagi siapa saja yang tidak mengetahui kunci yang tepat dalam bentuk seperti informasi dapat dengan aman dikirimkan melalui setiap saluran komunikasi ataupun disimpan dalam arsip data dengan akses terbatas atau bahkan dilarang untuk diakses (dengan alasan tertentu)".