PERBANDINGAN ALGORITMA DES DAN ALGORITMA AES PADA TEKNOLOGI *QR-CODE*

Aji Damura Depayusa[1], Diana[2], RM Nasrul Halim[3]

Universitas Bina Darma[1],
Jalan Jendral Ahmad Yani No.03 Palembang
ajidappa@gmail.com[1]

Universitas Bina Darma[2]
Jalan Jendral Ahmad Yani No.03 Palembang
diana@binadarma.ac.id[2]

Universitas Bina Darma[3]
Jalan Jendral Ahmad Yani No.03 Palembang
nasrul.halim@binadarma.ac.id[3]

ABSTRAK

Teknologi Quick Response Code (QR-Code) adalah suatu jenis kode matriks yang dikembangkan oleh Denso Corporation, dengan tujuan menjadi suatu kode penerjemah dengan kecepatan tinggi. Dalam penerapannya QR-Code dapat menggunakan standard algoritma enkripsi kunci-simetri Algoritma DES (Data Encryption Standard) dan Algoritma AES(Advanced Encryption Standard). Tolak ukur pada pembahasan ini apakah terdapat perbedaan antara Algoritma DES dan algoritma AES pada Teknologi QR-Code dengan mengukur ukuran dan keakuratan file setelah proses enkode dan dekode data dan informasi. Metode yang digunakan adalah metode penelitian deskriptif kualitatif. Berdasakan hasil penelitian dapat dilihat perbandingan catatan waktu Algoritma DES memiliki waktu Proses yang lebih Singkat daripada algoritma AES, ukuran file yang menggunakan Algoritma DES memiliki ukuran file yang lebih kecil dibandingkan Algoritma AES, Dari perbandingan ukuran file menggunakan algoritma DES dan AES kedua Algoritma memiliki tingkat Akurat yang hampir sama yaitu pada saat pembacaan QR-Code hasiilnya sama dengan plainteks.

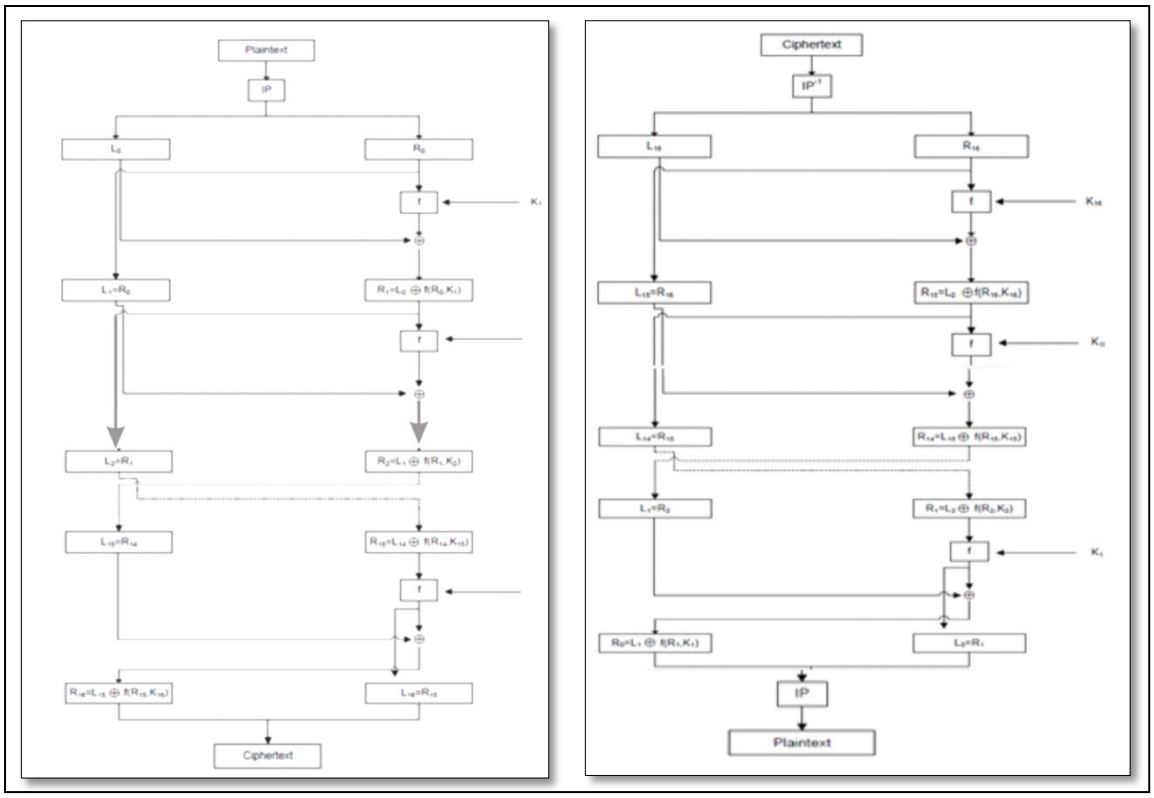
***Kata Kunci** : AES, DES, Kriptografi, QR-Code*

I. PENDAHULUAN

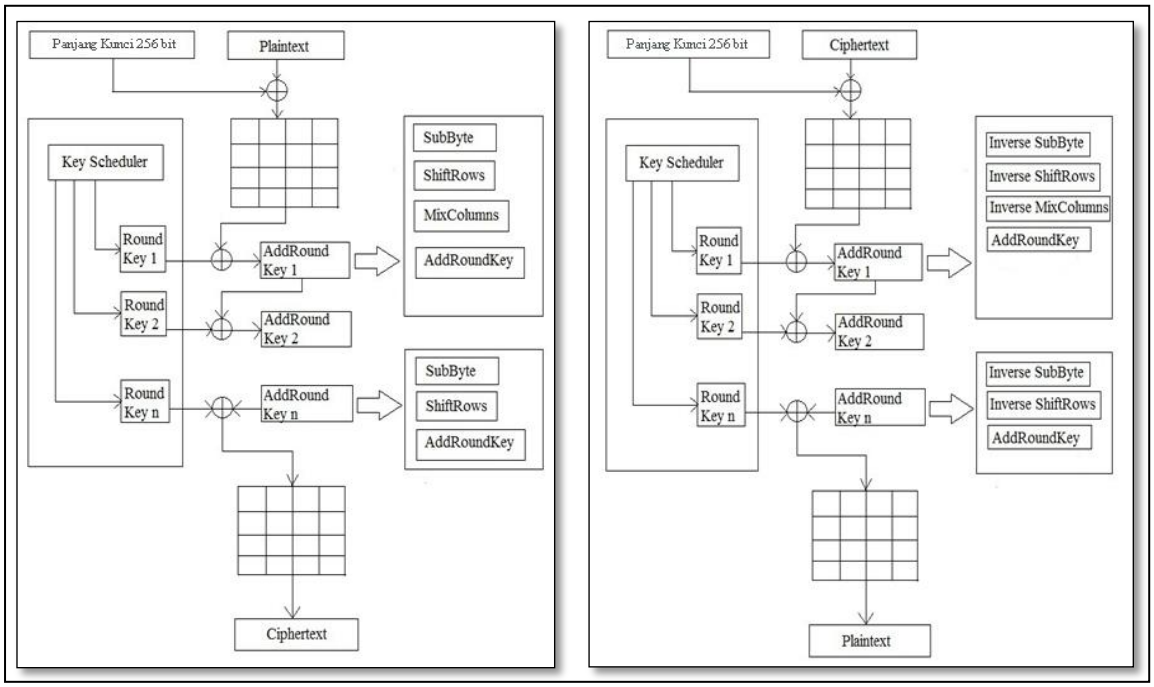
Teknologi QR-Code merupakan jenis kode matriks yang dikembangkan oleh *Denso Corporation* sebuah perusahaan besar di negara Jepang dan dipublikasikan pada tahun 1994, dengan tujuan sebagai salah satu teknologi kode penerjemah yang mempunyai kecepatan tinggi. QR-Code sebenarnya menyimpan informasi berupa alamat dan URL media, sehingga dapat menghubungkan konten-konten *online* melalui konten yang *offline*. Teknologi QR-Code juga dapat digunakan untuk mengamankan data dengan cara mengenkripsi data menggunakan beberapa algoritma enkripsi data. Dalam penerapannya QR-Code dapat menggunakan standar algoritma enkripsi kunci-simetri Algoritma DES dan Algoritma AES.

Standar algoritma enkripsi kunci-simetri *DES (Data Encryption Standard)* merupakan algoritma *cipher* blok yang populer karena dipakai menjadi standard algoritma enkripsi kunci-simetri, meskipun saat ini DES telah digantikan dengan algoritma yang baru yaitu *AES*, karena algoritma tersebut sudah dianggap tidak aman lagi. DES beroperasi pada ukuran blok 64-bit. DES mengenkripsikan 64-bit plainteks menjadi 64-bit cipherteks dengan menggunakan 56-bit kunci internal yang dibangkitkan dari kunci eksternal yang panjangnya 64-bit. Pada proses pembangkitan Kunci-kunci Internal DES, Kunci eksternal yang diinputkan akan diproses untuk mendapatkan 16 kunci internal (Satria, 2009) . Dan algoritma AES (*Advanced Encrytion Standard*) adalah Algoritma *cryptographic* yang dapat digunakan untuk mengamankan data atau informasi. Algoritma AES juga merupakan algoritma *Chiper* blok yang dapat meng-enkripsi dan dekripsi informasi. Dalam konsep algoritma ini input dan output terdiri dari urutan data sebesar 256bit (Bagus, 2013).

Pada algoritma ini ada proses enkripsi dan dekripsi, dapat digambarkan sebagai berikut: (Sumber: Stallings, 2011)



Gambar 1. Proses Enkripsi dan dekripsi algoritma DES



Gambar 2. Proses Enkripsi dan dekripsi algoritma AES

Agar permasalahan dalam pembahasan ini tidak terlalu luas ruang lingkup pembahasannya, maka dalam penelitian ini membatasi permasalahan pada kinerja yang meliputi:

1. Waktu encode teks ke qr code menggunakan algoritma DES dan Algoritma AES yang berbentuk teks;
2. Ukuran file sebelum dan sesudah di-enkode ataupun di-dekode menggunakan algoritma DES dan Algoritma AES yang berbentuk teks;
3. Seberapa akurat file data antara data asli dengan data hasil dekode menggunakan algoritma DES dan Algoritma AES yang berbentuk teks.

II. METODOLOGI PENELITIAN

Penelitian ini mempergunakan pendekatan dari metode analisis komparatif. Metode analisis komparatif adalah metode untuk membandingkan hasil analisis terhadap dua atau lebih fenomena sehingga didapatkan hasil berupa kesamaan dan perbedaan fenomena tersebut.

Menurut Sugiyono (2013, dalam Ochid) penelitian komparatif merupakan sejenis penelitian deskriptif yang ingin mencari jawaban secara mendasar tentang sebab-akibat, dengan menganalisis faktor-faktor penyebab terjadinya ataupun munculnya suatu fenomena tertentu. Pada penelitian ini variabelnya masih mandiri tetapi untuk sampel yang lebih dari satu atau dalam waktu yang berbeda. Pada penelitian ini yang dibandingkan adalah kinerja dari algoritma DES dan algoritma AES. Pada penelitian peneliti membangun dua buah aplikasi yang masing-masing menerapkan algoritma DES dan algoritma AES.

Metode pengembangan sistem yang digunakan adalah *Waterfall*. Menurut Pressman (2012), model waterfall adalah model klasik yang bersifat sistematis, berurutan dalam membangun software. Model ini melakukan pendekatan secara sistematis dan berurutan. Disebut dengan *waterfall* karena tahap demi tahap yang dilalui harus menunggu selesainya tahap sebelumnya dan berjalan berurutan.

III. HASIL

Penelitian ini menghasilkan aplikasi QR-Code DES dan AES. Adapun tampilan aplikasi yang telah dibuat sebagai berikut :

Gambar 3. Menu utama

Gambar 4. Menu generator DES

Gambar 5. Menu generator AES

Gambar 6. Menu reader

Peneliti akan membahas perbandingan ukuran file ,waktu encode dan Seberapa akurat file data asli dengan data dekode menggunakan algoritma DES dan AES yang berbentuk teks. Pada penelitian ini menggunakan 5 *plaintext* sebagai objek kajian, yaitu pada tabel 1.

Tabel 1. Tabel Data Plainteks

NO.	Plaintext	Ukuran data (byte)
1.	Nama saya Aji Damura Depayusa	31 byte
2.	Saya tinggal di kota Palembang	27 byte
3.	Saya sedang melakukan penelitian	25 byte
4.	Judul penelitianku Anallisis perbandingan algoritma DES dan AES Pada teknologi QR-Code	83 byte
5.	Mudah-mudahan segera selesai	29 byte

1) Perbandingan Waktu Encode

Hasil pengujian Perbandingan waktu encode yang dihasikan oleh aplikasi QR-Code DES dan AES pada tahap sebelumnya, didapatkan hasil perbandingan seperti pada tabel 2.

Tabel 2. Tabel Perbandingan Waktu Encode

Plaintext	QR-Code	Waktu encode DES	Waktu encode AES	Selisih waktu
1		0,000088s	0,000137s	0,000049s
2		0,000095s	0,000109s	0,000014s
3		0,000099s	0,000111s	0,000012s
4		0,000217s	0,000220s	0,000008s
5		0,000086s	0,000091s	0,000005s

Dari tabel 2 dapat disimpulkan bahwa terdapat rata- waktu encode atas 5 plainteks yang diuji memiliki rataan hitung sebagai berikut :

$$\overline{x} = \frac{x_1+x_2+x_3+x_4+x_5}{n}$$
$$= \frac{0{,}000049 + 0{,}000014 + 0{,}000012 + 0{,}000008 + 0{,}00005}{5}$$
$$= 0{,}0000176s$$

jadi, berdasarkan perhitungan diatas didapatkan rataan hitung dari jumlah rata-rata perbandingan waktu encode menggunakan algoritma DES dan AES sebesar 0,0000303s.

2) Perbandingan Ukuran File

Dari hasil uji perbandingan menggunakan aplikasi QR-Code DES dan AES yang telah dilakukan pada tahap sebelum nya, didapatkan hasil perbandingan seperti pada tabel 3.

3. Tabel Perbandingan ukuran file algoritma DES dengan AES

Plainteks	Ukuran file DES	Ukuran file AES	Selisih ukuran
1	266 byte	325 byte	59 byte
2	263 byte	331 byte	68 byte
3	261 byte	323 byte	62 byte
4	466 byte	511 byte	45 byte
5	274 byte	321 byte	47 byte

Dari tabel 3 dapat disimpulkan bahwa terdapat rata- rata ukuran file atas 5 plain teks yang diuji memiliki rataan hitung sebagai berikut :

$$\overline{x} = \frac{x_1+x_2+x_3+x_4+x_5}{n}$$

$$= \frac{59 + 68 + 62 + 45 + 47}{5}$$
$$= 56{,}2 \text{ byte}$$

Jadi, berdasarkan perhitungan diatas didapatkan rataan hitung dari jumlah rata-rata perbandingan ukuran file encode menggunakan algoritma DES dan AES sebesar 59,6 byte.

3) Perbandingan Keakuratan Encode

Hasil pengujian Perbandingan Keakuratan encode yang dihasikan oleh aplikasi QR-Code DES dan AES didapatkan hasil perbandingan seperti pada tabel 4.

Tabel 4. Tabel Perbandingan keakuratan Encode DES

Plaintext DES	QR-Code	Plaintext setelah di encode
Nama saya Aji Damura Depayusa		Nama saya Aji Damura Depayusa
Saya tinggal di kota Palembang		Saya tinggal di kota Palembang
Saya sedang melakukan penelitian		Saya sedang menyusun penelitian
Judul penelitianku Anallisis perbandingan algoritma DES dan AES Pada teknologi QR-Code		Judul penelitianku Anallisis perbandingan algoritma DES dan AES Pada teknologi QR-Code
Mudah-mudahan segera selesai		Mudah-mudahan segera selesai

IV. KESIMPULAN

Setelah melakukan studi literatur, Analisis, perancagan, Implementasi dan diakhiri dengan pengujian dari penelitian yang membandingkan algoritma DES dan AES pada teknologi QR-code, maka penulis mengambil kesimpulan sebagai berikut:

a. Algoritma DES memiliki waktu Proses yang lebih Singkat daripada Algoritma AES, karna pada proses Enkripsi dari plainteks ke chiperteksnya Algoritma DES hanya sedikit melakukan proses enkripsi dibandingkan Algoritma AES .
b. Ukuran file menggunakan Algoritma DES memiliki ukuran file yang lebih kecil dibandingkan Algoritma AES, karna pada proses Enkripsi dari plainteks ke chiperteksnya Algoritma DES hanya sedikit melakukan proses enkripsi dibandingkan AES.
c. Kedua Algoritma memiliki tingkat Akurat yang hampir sama yaitu pada saat pembacaan *QR-Code* hasiilnya sama dengan plainteks .

DAFTAR PUSTAKA

Bagus, Putu Wirajaya Kusuma, Ida, 2013. *Implementasi QR-Code dan Algoritma Kriptografi AES Pada Pengamanan Keaslian Dokumen.* Universitas Udayana.

Pressman, R.S. 2012. Rekayasa Perangkat Lunak. Yogyakarta: Andi.

Stallings, William. 2011. *Cryptography and Network Security: Principles and Practice*, Prentice Hall

Ochid. *Penelitian Komparatif*. 20 agustus 2016. http://pgsdberbagi.blogspot.co.id/2014/01/penelitian-komparatif.html

Satria, Eko. 2009. *Studi Algoritma Rijndael dalam Sistem Keamanan Data.* Universitas Sumatra Utara.