Implementasi *Advanced Encryption Standard* (AES) dalam Pengamanan *QR-Code* Berbasis *Mobile*

Implementation of Advanced Encryption Standard (AES) in Mobile Based QR-Code Security

Eka Sulastri[1], Kurniadin Abd. Latif [2], Muhammad Innuddin [3]
[1,2,3]Universitas Bumiogra, Kota Mataram, Indonesia

Article Info

Article history:

Diterima 28 01 2025
Direvisi 28 01 2025
Disetujui 28 01 2025

Kata Kunci:

Advanced Encryption Standard (AES)
QR-Code
Enkripsi
Dekripsi
Mobile

ABSTRAK

Tujuan penelitian ini adalah mengimplementasikan algoritma *Advanced Encryption Standard* yang berukuran blok data 128 bit dengan ukuran state 4x4. AES diimplementasikan menggunakan *Framework Flutter* dengan menerapkan *QR-Code* karena *QR-Code* adalah teknologi yang menyimpan informasi yang secara horizontal dan vertikal sehingga dapat menampung banyak informasi dalam bentuk angka, huruf, dan url. Dimana pada algoritma AES memiliki dua tahapan yaitu enkripsi adalah mengubah *plaintext* atau informasi asli yang bisa dibaca menjadi *chipertext* atau informasi ke dalam bentuk rahasia atau tidak dapat dibaca. Dan dekripsi kebalikan dari proses enkripsi yaitu mengubah *chipertext* menjadi *plaintext*. pada proses enkripsi akan melalui tahapan-tahapan yaitu *AddRoundkey*, *SubByte*, *ShitRows*, dan *MixColums* yang dilakukan sebanyak 10 kali putaran dan pada putaran terakhir hanya dilakukan tahapan *AddRoundkey*, *SubByte*, dan *ShiftRows* tanpa *MixColumns*, dan untuk tahap dekripsi yaitu kebalikan dari tahap enkripsi yaitu *InvAddrows*, *InvShiftrows*, *InvSubbyte*, dan *InvMixcolumns* dengan mengunakan privat key yang sama dengan tahap enkripsi. Hasil penerapan algoritma AES dapat memberikan aspek confidentiality. Algoritma AES menghasilkan output berupa chipertext berupa karakter yang sulit dipahami melalui proses enkripsi dan dekripsi. Aplikasi *QR-Code* AES128 telah berhasil dijalankan dan setiap komponon dan fungsi telah bekerja sesuai dengan hasil yang diharapkan dan dapat dijalankan pada versi android yang berbeda-beda.

ABSTRACT

The aim of this research is to implement the Advanced Encryption Standard algorithm with a data block size of 128 bits with a state size of 4x4. AES is implemented using the Flutter Framework by implementing QR-Code because QR-Code is a technology that stores information horizontally and vertically so that it can accommodate a lot in the form of numbers, letters and URLs. Where the AES algorithm has two stages of encryption, namely changing plaintext or original information that can be read into ciphertext or information in secret or unreadable form. And decryption is the opposite of the encryption process, namely changing ciphertext into plaintext. the encryption process will go through stages, namely AddRoundkey, SubByte, ShitRows, and MixColums which are carried out 10 times and in the last round only the AddRoundkey, SubByte, and ShiftRows stages are carried out without MixColumns, and for the decryption stage, it is the opposite of the encryption stage, namely InvAddrows , InvShiftrows, InvSubbyte, and InvMixcolumns using the same private key as the encryption stage. The results of applying the AES algorithm can provide confidentiality aspects. The AES algorithm produces output in the form of ciphertext in the form of characters that are difficult to understand through the encryption and decryption process. The AES128 QR-Code application has been successfully run and every component and function has worked according to the expected results and can be run on different Android versions.

Penulis Korespondensi:

Eka Sulastri
Program Studi Ilmu Komputer dan Fakultas Teknik,
Universitas Bumigora, Kota Mataram, Indonesia.
Email: ekasulastri228@gmail.com.

1 PENDAHULUAN (10 PT)

Format Indonesia yang telah masuk era perkembangan ekmologi, dimana penyampaian informasi selalu terjadi sehingga membuat unsur keamana sangat penting. Teknologi juga memberikan banyak cara baru dalan melakukan aktifitas agar memudahkan aktifitas manusia dalam menyampaikan informasi(1). *QR-Code* adalah teknologi labeling yang saat ini sedang berkembang. *Densi wave* mengembangkan *QR-Code* yang evolusi dari kode batang yang satu dimensi menjadi dua dimensi (2). *QR* merupakan singkatan dari *Quick Response* dimana tujuannya adalah untuk menyampaikan informasi dengan cepat dan mendapatkan respon yang cepat pula. *QR-Code* mampu menyimpan informasi secara horizontal dan vertikal. Oleh kerena itu, *QR-Code* dapat menampung informasi yang lebih banyak, misalnya dalam bentuk URL, Text dan Angka (3).*QR-Code* sudah banyak diterapkan di berbagai macam industri seperti food dan beverages,Automotive, manufactur maupun sektor lainnya. Tentunya penerapan *QR-Code* pada setiap sektor industri memiliki fungsi dan karakteristiknya masing-masing. Selain itu tidak jarang pula dijumpai *QR-Code* pada kegiatan jual beli sebuah produk, seperti claim kupon harga ataupun hanya sekedar online payment(4).

pengamanan data adalah pada soal ujian atau hal-hal bersifat sensitif lainnya yang perlu diamankan dan pada pengirimin data yang dapat dilakukan melalui berbagai macam media yang ada, keamanan data yang dikirim membwa dampak yang besar pada proses pengirimannya yaitu dimana biasanya dilakukan secara polos atau tanpa pengaman, sehingga harus dilakukan proses pengamanan data yang akan dikirim . Kerahasiaan merajuk pada perlindungan informasi dari penyingkapan pihak yang tidak sah dengan cara memberi akses terbatas pada informasi atau dengan penyandian informasi sehingga tidak memiliki arti apapun bagi pihak yang tidak berhak tersebut. Jika kerahasiaan ini tidak terpenuhi akan mengakibatkan adanya penyalahgunaan wewenang oleh pihak yang tidak sah (3).

Kriptografi memiliki berbagai macam algoritma, salah satunya adalah *Advanced encryption standard.* AES menggunakan blok chiper simetris yang dimaksudkan untuk menganti algoritma DES. Ada dua tahapan dalam algoritma AES yaitu Enkripsi dan Dekripsi. Enkripsi adalah proses yang dilakukan untuk merubah suatu informasi ke dalam bentuk rahasia sehingga tidak dapat dibaca oleh orang yang tidak bertanggung jawab, sebaliknya proses dekripsi merupakan suatu proses mengembalikan informasi asli yang sudah di enkripsi menjadi bisa dibaca kembali (5).

Pada penelitian yang dilakukan oleh (3) yaitu Implementasi Algoritma Speck Untuk Enkripsi dan Dekripsi Pada *QR-Code* menggunakan algortma speck dengan pembahasan algoritma speck dapat diimplementasikan pada *QR-Code*, speck mengenkripsi plaintext dengan hasil chipertext yang dijadikan *QR-Code*. Penelitian selanjutnya yang dilakukan oleh (6) yaitu Implementasi *Advanced encryption standard* pada Enkripsi dan Dekripsi Dokumen Rahasia Di Tintelkam Poldda DIY) dengan pembahasan Aplikasi kriptografi dokumen berhasil mengimplementasikan metode kriptografi AES dalam proses enkripsi dan dekripsi dokumen dengan format docx, xls, xlsx, pdf dan txt. Pada lainnya dilakukan oleh (7) yaitu Implementasi Algoritma Base64 Untuk Verifikasi QR Code Login Jaringan Wifi Berbasis Android) dengan pembahasan mengiplementasikan algoritma base64 pada aplikasi login wifi dimana aplikasi dapat digunakan sebagai pengamanan jaringan wifi dari orang yang tidak berhak mengaksesnya dan aplikasi dibuat menggunakan bahasa pemrograman *mobile*.

Berdasarkan masalah dan literatur yang ada, maka peneliti akan melakukan penelitian tentang Implementasi *Advanced Encryption Standard (AES)* Dalam Pengamanan *QR-Code* Berbasis Mobile. Penerapan enkripsi AES tidak hanya mendukung perlindungan data tetapi juga mengarah pada peningkatan akurasi dan efisiensi dalam identifikasi keamanan Teknik (8). Pada penelitian ini diharapkan dengan menggunakan algoritma *Advanced Encryption Standard* (AES) dapat meningkatkan keamanan dan kerahasiaan yang mengimplementasikan *QR-Code* oleh pengguna.

2 METODE PENELITIAN

Menjelaskan metode yang digunakan pada penelitian ini yaitu metode pengembangan perangkat lunak. metode pengembangan perangkat lunak atau disebut juga dengan *Systems Development Life Cycle* (SDLC), merupakan proses yang digunakan untuk mengembangkan sistem informasi, metode pemgembangan perangkat lunak merupakan alur pengembangan baku software aplikasi (9):

Gambar 1. Alur Metode SDLC

2.1 Analisa

Pada tahap analisa kebutuhan sistem dilakukan pengumpulan data dan informasi terkait perancangan system ini. Seperti kebutuhan pengguna seperti framework flutter, tex editor, library *QR-Code*

2.1.2 Kebutuhan Pengguna

Kebutuhan pengguna dilakukan untuk menganalisis kebutuhan- kebutuhan apa saja yang akan dibutuhkan oleh pengguna dalam implementasi penelitian.

2.2 Development/Kontruksi

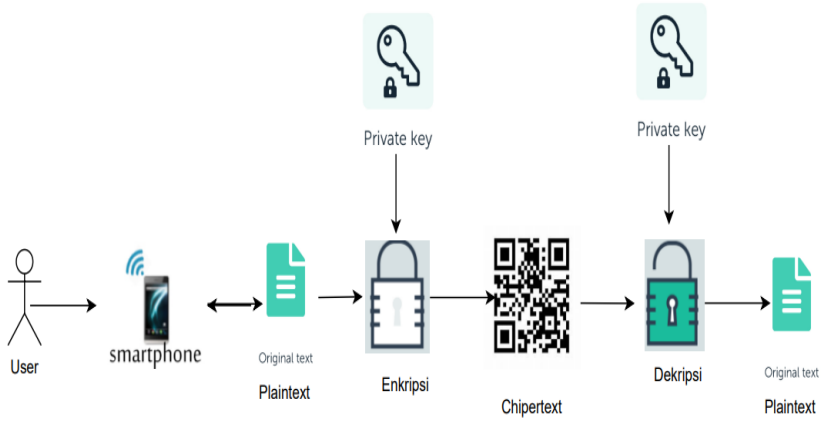
Tahap ini melakukan coding sistem yaitu menyusun bahasa pemrograman yang dipilih, membuat form sistem. Disamping itu juga mendesain *grapichal User Interface* (GUI), menampilkan objek yang bisa menyampaikan informasi dan mempresentasikan aksi dan pengguna.

2.2.1 Framework Flutter

flutter adalah sebuah framework aplikasi *mobile* yang bersifat terbuka (*Open Source)* yang dibuat oleh Google. Flutter berfungsi untuk mengembangan apliksai untuk sistem operasi android dan iOS. “sky” merupakan versi pertama flutter yang berjalan pada sistem operasi Android. Pada tahun 2015 Diresmikan perhelatan Dart Developer Summit, dengan tujuan untuk mampu merender grafis secara konsisten pada 120 bingkai per detik (10). Dart adalah bahasa berorientasi objek (objek oriented) dengan sintaksis C-style yang dapat diubah secara opsional menjadi javaScript (11). Mendukung berbagai macam alat bentuk pemrograman seperti interface, class, collection, generics, dan opsional typing. Dart bisa digunakan untuk membuat aplikasi Web, Android,iOS dan menjalankan sebuah server.

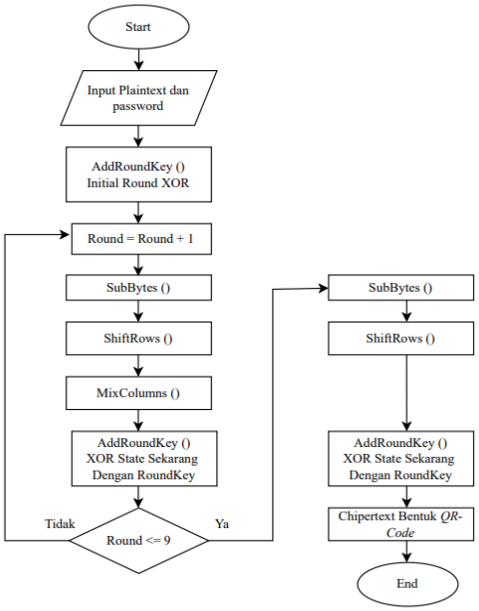
2.3 Design

Pada tahap ini membuat rancangan yang meliputi rancangan jaringan uji coba, rancangan sistem dan kebutuhan perangkat lunak maupun perangkat keras.



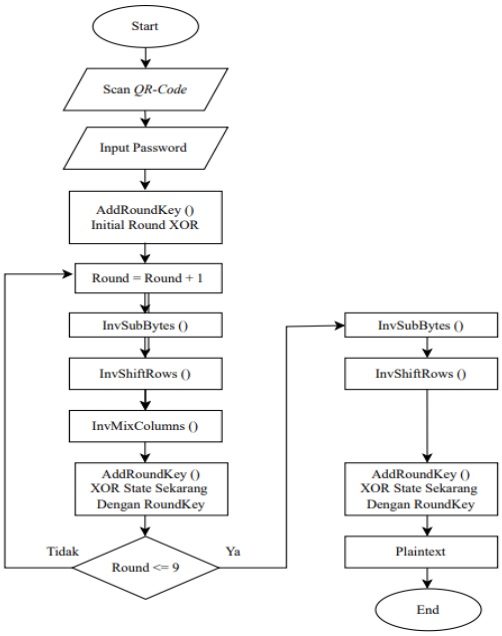
Gambar 2. Rancangan Penggunaan Sistem

Gambar di atas menunjukkan rancangan penggunaan sistem atau aplikasi yang dikembangkan. Proses Enkripsi dan Dekripsi hanya bisa dilakukan pada aplikasi yang sama. Hasil generate *QR-Code* oleh aplikasi yang dikembangkan ini akan sulit dieksatrak menjadi informasi asli oleh aplikasi scan *QR-Code* lainnnya. Cara ini memebrikan lapisan perlindungan informasi dari sebuah *QR-Code*. Selanjutnay dalam penelitian ini *flowchart* digunakan untuk menampilkan langkah-langkah dan keputusan untuk melakukan sebuah proses dari pembuatan *system.*



Gambar 3. Flowchart Enkripsi

Pada gambar diatas dijelaskan alur proses enkripsi dari algoritma *Advanced encryption standard* (AES) hingga penyisipan informasi yang telah terenkripsi ke dalam *QR-Code*. Pada proses penyisipan informasi, proses pertama yaitu masuk pada menu enkripsi kemudian memasukkan informasi atau plain text dan password yang akan di enkripsi dengan menggunakan algoritma AES kemudia data yang sudah terenkripsi akan menghasilkan sebuah chipertext yang berbentuk *QR-Code*. sehingan informasi yang dihasilkan berbentuk *QR-Code*.



Gambar 4. Flowchart Dekripsi

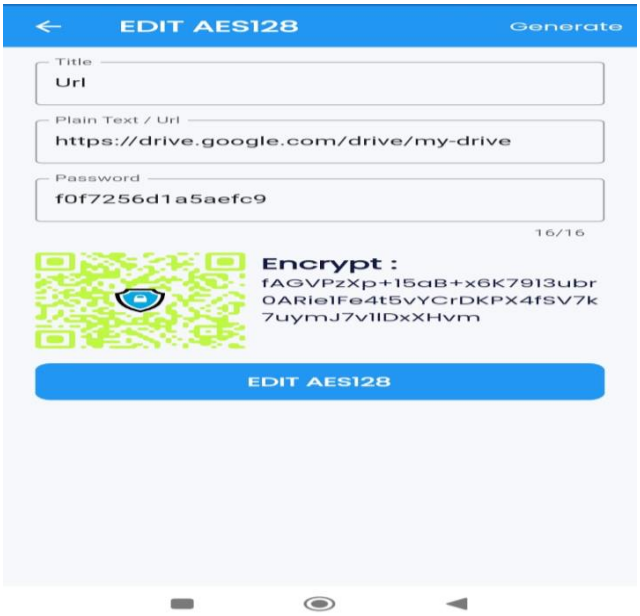
Pada gambar diatas dijelaskan flowchart alur dari proses dekripsi dari informasi yang telah di enkripsi sebelumnya yang berbentuk *QR-Code* dengan menggunakan algoritma *Advanced encryption standard (AES)* dengan melakukan scan informasi yang berbentuk *QR-Code* pada menu dekripsi, kemudian memasukkan privat key atau password sehingga informasi informasi yang berbentuk cipher text dapat dikembalikan ke dalam bentuk plaintext.

3 HASIL DAN ANALISIS (10 PT)

3.1 Implementasi

Tahap ini mengimplementasikan semua perancangan pada sistem yang telah dibuat sebelumnya, sehingga sistem dapat dijalankan dan diuji kelayakannya. Berikut merupakan implementasi algoritma Advanced encryption standarddalam pengamanan *QR-Code*. Pada proses implementasi interfacee untuk sistem ini dibagi menjadi dua yaitu: interface dekripsi dan interface enkripsi.

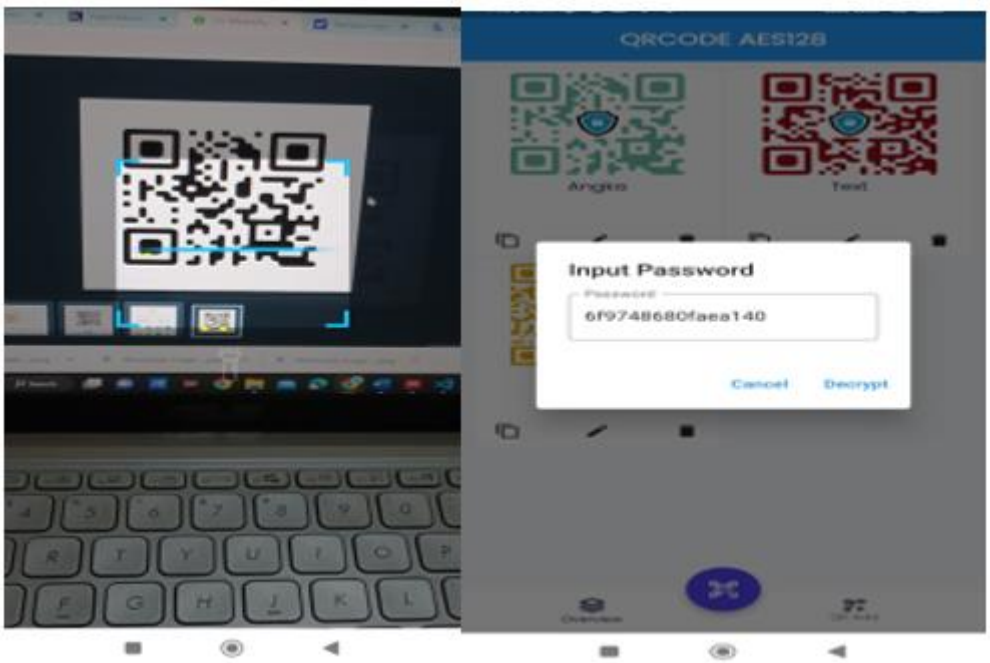
a. Menu enkripsi untuk mengubah informasi asli menjadi kode acak yang tidak bermakan dan tersimpan di dalam *QR-Code*. Adapun hasil implementasi dari menu enkripsi dapat dilihat pada gambar dibwah ini.



Gambar 5. Menu Enkripsi dan Generate QR-Code

Halaman enkripsi merupakan interface untuk melakukan proses enkripsi pada plaintext atau informasi menjadi *QR-Code* dalam sistem QRCode AES128 oleh pengguna. Yaitu dengan cara memberikan title atau judul pada informasi yang akan dilakukan enkripsi, kemudian memasukkan plaintext yang dapat berupa angka, text dan URL, selanjutkan dapat menentukan password atau privat key yang bersifat privasi bagi pengguna dan pihak yang berhak, password/privat key dapat diinputkan secara manual dan dapat juga mengenerate. Button save digunakan untuk menyimpan chiper text atau informasi yang telah terenkripsi sebelumnya yang berbentuk *QR-Code*.

b. Menu dekripsi untuk mengembalikan informasi ke bentuk asli yang berbentuk kamera scan untuk *QR-Code* yang telah terenkripsi pada tahap sebelumnya.



Gambar 6. Menu Dekripsi dan Ekxtrak QR-Code

Halaman dekripsi meruapakan halaman untuk melakukan proses dekripsi pada *QR-Code* yang ingin diubah menjadi plaintext atau informasi asli menggunakan sistem QRCODE AES128 oleh pengguna. dimana terdapat kamera yang digunkan oleh user mengscan *QR-Code* yang berisi plaintext yang sudah terenkripsi sebelumnya, selanjutnya diminta memasukkan password atau privat key, password yang diinput pada proses dekripsi harus sama dengan password yang diinput pada proses enkripsi, setelah memasukkan password denggan benar maka akan menampilkan plaintext atau informasi asli dari *QR-Code*.

3.2 Testing

Pada tahapan ini dilakukan pengujian fungsi dari masing-masing fitur aplikasi yang dikembangkan. Pada tahap ini dilakukan pengujian dengan menggunakan Black-Box Testing.

3.2.1 Pengujian Black Box

NO	PENGUJIAN	AKSI	HASIL YANG DIHARAPKAN	HASIL	STATUS
1	Pengujian halaman enkripsi	User dapat masuk ke halaman enkripsi	Sistem mampu merespon dengan menampilkan halaman enkripsi	Sistem mampu merespon dengan menampilkan halaman enkripsi	**Berhasil**
2	Pengujian melakukan enkripsi aes	User dapat menekan button save	Sistem mampu merespon dengan menghasilkan sebuah QR Code yang sudah terenkripsi	Sistem mampu merespon dengan menghasilkan sebuah QR Code yang sudah terenkripsi	**Berhasil**
3	Pengujian generate key	User menekan button generate	Sistem mampu merespon dengan menghasilkan inputan key di halaman enkripsi, key berjumlah sebanyak 16 karakter	Sistem mampu merespon dengan menghasilkan inputan key di halaman enkripsi, key berjumlah sebanyak 16 karakter.	**Berhasil**
3	Pengujian edit enkripsi AES	User menekan button edit AES	Sistem mampu merespon dengan menyimpan perubahan menu enkripsi.	Sistem mampu merespon dengan menyimpan perubahan menu enkripsi.	**Berhasil**
4	Pengujian hasil enkripsi	User menekan QR Code	Sistem mampu menampilkan hasil enkripsi	Sistem mampu menampilkan hasil enkripsi	**Berhasil**

NO	PENGUJIAN	AKSI	HASIL YANG DIHARAPKAN	HASIL	STATUS
5	Pengujian pengiriman *QR-Code*	User menekan button share	Sistem mampu menampilkan media yang digunakan dan berhasil membagikan QR Code.	Sistem mampu menampilkan media yang digunakan dan berhasil membagikan QR Code.	**Berhasil**
6	Pengujian melakukan dekripsi	User dapat menekan button berlogo QR Code	Sistem mampu marespon dengan menghasilkan kamera scan QR Code	Sistem mampu marespon dengan menghasilkan kamera scan QR Code	**Berhasil**
7	Pengujian key dekripsi	User dapat memasukkan key	Sistem mampu mengenali kunci yang diinputkan pada proses dekripsi sama dengan kunci yang di inputkan pada proses enkripsi	Sistem mampu mengenali kunci yang diinputkan pada proses dekripsi sama dengan kunci yang di inputkan pada proses enkripsi	**Berhasil**
8	Pengujian hasil dekripsi	User menekan button decryp	Sistem mampu menampilkan informasi asli dari QR Code yang telah terenkripsi.	Sistem mampu menampilkan informasi asli dari QR Code yang telah terenkripsi.	**Berhasil**
9	Pengujian browser	User menekan button browser	Sistem mampu menampilkan alamat dari url.	Sistem mampu menampilkan alamat dari url.	**Berhasil**

3.2.2 Pengujian Keamanan

Pada tahapan ini dilakukan pengujian implementasi keamana AES terhadap aplikasi QR Code lainnya. Pada pengujian keamanan menggunakann aplikasi yang bernama "QR Scanner" untuk mengscan *QR-Code* yang sudah di enkripsi maupun belum dienkripsi. Adapun hasil perbandingan *QR-Code* yang belum dan yang sudah diterapkan AES dapat dilihat pada gambar .

Gambar 7. Perbandingan QR-Code tanpa AES dan QR-Code dengan AES

Gambar di atas merupakan QR Code yang berisi pesan asli yang belum di enkripsi mengunakan sistem, dan pada gambar 4.36 adalah QR Code yang telah terenkripsi sehingga orang lain tidak mengetahui isi pesan aslinya. Dari penerapan AES tersebut mampu menyembunyikan atau mengaburkan informasi yang sebenarnya menjadi suatu text yang sulit dimengerti oleh

orang lain. Sehingga perlu aplikasi yang sama untuk mengekstrak *QR-Code* tersebut menjadi informasi yang mudah dipahami. Cara ini mampu meningkatkan keamanan informasi melalui *QR-Code*.

4 KESIMPULAN (10 PT)

Berdasarkan hasil analisis, implementasi, dan menggunakan algoritma AES untuk enkripsi dan dekripsi *QR-Code*. Algoritma AES dapat memberikan aspek confidentiality. Algoritma AES menghasilkan output berupa chipertext berupa karakter yang sulit dipahami melalui proses enkripsi dan dekripsi. Untuk tahapan enkripsi AES diterapkan sebelum dilakukan generate ke dalam bentuk *QR-Code* sedangkan untuk tahap dekripsi AES diterapkan sesudah *QR-Code* di extract.Aplikasi QRCODE AES128 telah berhasil dijalankan dan setiap komponon dan fungsi telah bekerja sesuai dengan hasil yang diharapkan. Berdasarkan hasil uji coba portabilitas perangkat aplikasi QRCODE AES128 dapat dijalankan pada perangkat smartphone dengan sistem operasi android dengan versi yang berbeda-beda baik pada perangkat android yang memiliki sistem operasi 9.0 (Pei) hingga 13, ukuran layar 6,4 inci hingga 6,5 inci.

REFERENSI (10 PT)

1. Ramadhan R, Soetanto H. Penerapan Kriptografi Menggunakan Advanced Encryption Standard 128 Untuk Pengamanan File Pada SMK Muhammadiyah 4. In: Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI). 2022. p. 29–38.
2. de Seta G. QR code: The global making of an infrastructural gateway. Glob Media China. 2023;8(3).
3. Fatmala YS, Kusyanti A, Data M. Implementasi Algoritme Speck untuk Enkripsi dan Dekripsi pada QR Code. J Pengemb Teknol Inf Dan Ilmu Komput. 2018;2(12):6253–60.
4. Martawireja ARH, Ridwan R, Hafidzin AP, Taufik M. Proteksi Keamanan Data pada Quick Response (QR) Code. JTRM (Jurnal Teknol dan Rekayasa Manufaktur). 2021;3(2):99–110.
5. Ferdian F, Id AIHA, Rakhmat Fruf. Penggunaan Qr Code Berbasis Kriptografi Algoritma Aes Advanced Encryption Standard Untuk Administrasi Rekam Medis: Using Qr Code Based On Aes Advanced Encryption Standard Cryptography Algorithm For Medical Record Administration. J Inf Technol. 2021;3(2):20–7.
6. Widodo BE, Purnomo AS. Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy. J Tek Inform. 2020;1(2):69–77.
7. Hidayat A, Pristiwanto P. Implementasi Algoritma Base64 Untuk Verifikasi Qr Code Login Jaringan Wifi Berbasis Android. J Sist Komput dan Inform. 2020;2(1):25–30.
8. Li B, Xu M, Zhou Y, Liu H, Zhang R. Optimization of Security Identification in Power Grid Data through Advanced Encryption Standard Algorithm. J Cyber Secur Mobil. 2024;13(2).
9. Afrian MD, Raharja PA. Implementasi Augmented Reality Media Pengenalan Hardware Dengan Metode Multimedia Development Life Cycle Dan Prototype. INOVTEK Polbeng-Seri Inform. 2022;7(2):229–42.
10. Tashildar A, Shah N, Gala R, Giri T, Chavhan P. APPLICATION DEVELOPMENT USING FLUTTER. International Research Journal of Modernization in Engineering Technology and Science @International Research Journal of Modernization in Engineering. 1262.
11. Swathiga UUA., Vinodhini P, Sasikala V. an Interpretation of Dart Programming Language. UGC Care Gr I J. 2022;11(03).