Methotika : Jurnal Ilmiah Teknik Informatika
ISSN : 2776 – 5792
Vol. 3, No. 2, Oktober 2023, pp. 21-30
https://ejurnal.methodist.ac.id/index.php/methotika

Implementasi Algoritma AES Rijndael Pada *QR Code* Untuk Validasi dan Keamanan Data Penerima Bantuan Sosial di Kelurahan Padang Bulan Selayang II

Yosua Situmeang[1], Alfonsus Situmorang[2], Posma Lumbanraja[3]
[1,2,3]Fakultas Ilmu Komputer, Universitas Methodist Indonesia

Info Artikel

Histori Artikel:
Received, Mei 24, 2023
Revised, June 26, 2023
Accepted, July 12, 2023

Keywords:
Validasi
Algoritma AES Rijndael
QR Code
Keamanan Data

ABSTRAK

Perkembangan teknologi yang sangat pesat memberikan dampak yang signifikan terhadap kehidupan sosial. Salah satu produk teknologi yang banyak digunakan saat ini adalah *QR Code*, karena dapat memberikan informasi dengan cepat. Pada penelitian ini dibahas tentang penggunaan *QR Code* untuk mempermudah proses validasi penerima bantuan sosial di Kelurahan Padang Bulan Selayang II. Saat ini proses pengelolaan data penerima bantuan sosial masih manual menggunakan Ms. Excel serta validasi data yang cukup lama dikarenakan prosesnya harus mencocokkan data pribadi pada kartu keluarga dan ktp dengan daftar penerima bantuan sosial, hal ini dianggap kurang efisien. Tujuan dari penelitian ini adalah merancang aplikasi validasi dengan menggunakan *QR Code* yang dicetak dalam bentuk surat undangan, kemudian pegawai akan melakukan scan *QR Code* yang diberikan oleh penerima bantuan sosial. *QR Code* yang ditampilkan yaitu berisi nomor kartu keluarga yang sudah dienkripsi. Untuk mengenkripsi data pada *QR Code* peneliti menggunakan Algoritma AES Rijndael. AES Rijndael merupakan algoritma kriptografi simetris, yaitu menggunakan kunci yang sama pada proses enkripsi dan dekripsi, algoritma ini menggunakan substitusi, permutasi dan sejumlah putaran berulang. Dari hasil beberapa percobaan, aplikasi dapat melakukan enkripsi dan dekripsi data yang terdapat pada *QR Code*. Dengan adanya aplikasi ini dapat mempermudah pegawai untuk melakukan pengelolaan dan validasi data penerima bantuan sosial serta menghindari terjadinya manipulasi dan kebocoran data.

Penulis Koresponden:

Yosua Situmeang,
Fakultas Ilmu Komputer,
Universitas Methodist Indonesia, Medan,
Jl. Hang Tuah No.8, Medan - Sumatera Utara.
Email: yosuasitumeang9@gmail.com

1. PENDAHULUAN

Perkembangan teknologi yang sangat pesat memberikan dampak yang signifikan terhadap kehidupan sosial manusia saat ini. Munculnya berbagai aplikasi menawarkan peluang untuk meningkatkan kinerja dan efektivitas suatu pekerjaan. Salah satu teknologi yang banyak digunakan saat ini adalah *QR Code*, karena dapat memberikan informasi dengan cepat. Meningkatnya penggunaan *QR Code* harus diiringi juga dengan tingkat keamanan dalam proteksi data. Salah satu metode yang dapat digunakan untuk menjaga keamanan dan kerahasiaan data adalah dengan menggunakan teknik kriptografi. Algoritma AES Rijndael merupakan salah satu algoritma kriptografi simetris, yaitu kunci yang digunakan sama pada saat proses enkripsi dan dekripsi. Proses

enkripsi dan dekripsi untuk algoritma Rijndael beroperasi pada panjang blok 128-bit dengan kunci 128-bit, total putaran (Nr) yang dilakukan hingga diperoleh ciphertext adalah 10 kali putaran [1]. Algoritma AES Rijndael secara komputasi aman terhadap serangan Brute-Force, Man-in-the-Middle [2].

Kelurahan Padang Bulan Selayang II merupakan salah satu kelurahan yang berada di kecamatan Medan Selayang yang memiliki jumlah penduduk 25.008 kk. Salah satu tugas dari kelurahan adalah melaksanakan pengelolaan dan pendistribusian bantuan sosial kepada masyarakat yang terdaftar dikelurahan tersebut. Namun dalam pelaksanaanya, proses pendataan dan rekapitulasi data masih manual menggunakan Ms.Excel serta validasi data yang cukup lama dikarenakan prosesnya harus mencocokkan data pribadi pada kk dan ktp dengan daftar penerima bantuan sosial, hal ini dianggap kurang efisien.

Oleh karena itu dibutuhkan sebuah sistem yang dapat membantu pegawai kelurahan dalam melakukan pengelolaan dan proses validasi data yang lebih baik untuk meningkatkan pelayanan publik di kelurahan Padang Bulan Selayang II. Penelitian ini akan memanfaatkan teknologi *QR Code* yang dapat menyimpan informasi dan mempermudah dalam melakukan validasi data, dan megimplementasikan algoritma AES Rijndael pada *QR Code* untuk menghindari terjadinya manipulasi atau pencurian data yang dapat disalahgunakan oleh pihak yang tidak bertanggung jawab, sehingga keamanan dan kerahasiaan data pada *QR Code* dapat terjaga. Berdasarkan dari latar belakang yang ada, maka peneliti melakukan penelitian dengan judul "Implementasi Algoritma AES Rijndael Pada *QR Code* Untuk Validasi dan Keamanan Data Penerima Bantuan Sosial di Kelurahan Padang Bulan Selayang II".

2. METODE PENELITIAN

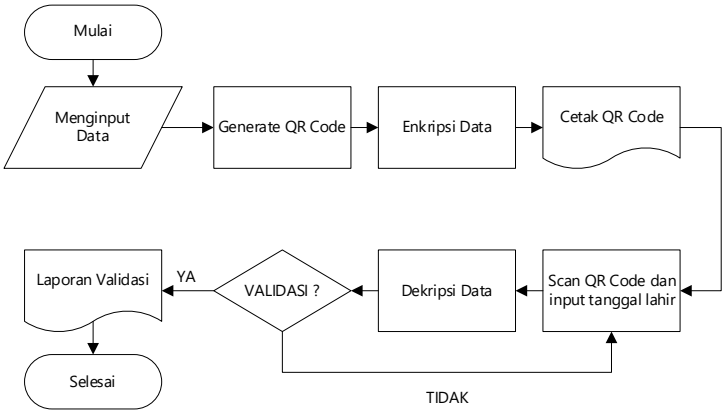
2.1. Validasi

Validasi berasal dari kata dalam bahasa Inggris yaitu validation, jika diterjemahkan ke dalam bahasa Indonesia maknanya adalah sejauh mana ketepatan atau kecermatan suatu alat ukur dalam melakukan pengujian. Secara umum arti validasi merupakan tindakan pengujian terhadap suatu data. Dalam KBBI, validasi diartikan sebagai pengesahan atau pengujian kebenaran atas sesuatu.

2.2. Perancangan Sistem

UML adalah sebuah standar pemodelan yang sangat membantu dalam pembangunan perangkat lunak yang dibangun dengan teknik pemograman model[3]. UML merupakan bahasa visual untuk pemodel dan komunikasi sebuah sistem dengan menggunakan diagram dan teks-teks pendukung [4].

Flowchart atau bagan alur adalah diagram yang menampilkan langkah-langkah dan keputusan untuk melakukan sebuah proses dari suatu program. Setiap langkah digambarkan dalam bentuk diagram dan dihubungkan dengan garis atau arah panah. Fungsi dari flowchart adalah memberi gambaran jalannya sebuah program dari satu proses ke proses lainnya dan menyederhanakan rangkaian prosedur agar mudah untuk memahami dari sebuah informasi. Flowchart untuk sistem yang akan dibangun dapat dilihat pada gambar 1.



Gambar 1. Perancangan Sistem

2.3. Kriptografi

Kriptografi (cryptography) berasal dari bahasa Yunani: “cryptos” artinya “secret” (rahasia), sedanghakn “graphein” artinya “writing” (tulisan). Jadi kriptografi berarti “secret writing” (tulisan rahasia). Menurut Menezes, kriptografi adalah suatu ilmu yang mempelajari tentang keamanan informasi menggunakan metode perhitungan matematika. Menurut Schneier, kriptografi adalah ilmu dan seni yang bertujuan untuk menjaga keamanan pesan (message)[5].

2.4. Algoritma AES Rijndael

Pada tahun 1999 algoritma Rijndael yang dibuat oleh Dr. Vincent Rijmen dan Dr. Joan Daenmen terpilih sebagai pemenang dan dijadikan sebagai standar algoritma kriptografi secara resmi pada 22 Mei 2002 oleh pemerintah Amerika Serikat dan algoritma Rijndael sekarang lebih dikenal sebagai AES (Advanced Encryption Standard) [1]. Algoritma AES Rijndael merupakan salah satu algoritma kriptografi simetris, yaitu kunci yang digunakan sama pada saat proses enkripsi dan dekripsi[6].

2.5. Algoritma Enkripsi AES Rijndael

Enkripsi adalah sebuah proses untuk menjadikan data yang bisa dibaca menjadi bentuk yang tidak bisa dibaca atau dimengerti melalui proses perhitungan yang rumit [7].
Urutan proses enkripsi AES Rijndael dalam mengamankan plaintext yaitu:

1. Pada tahap ini dilakukan ekspansi (perluasan) kunci sesuai dengan panjang kunci dan panjang ukuran blok yang akan digunakan, hasil ekspansi ini disebut dengan Roundkey.
2. Add round key, yaitu melakukan XOR antara state awal (plaintext) dengan cipher key. Tahap ini disebut juga initial round.
3. Putaran (Nr) sebanyak Nr-1

Pada proses ini akan dilakukan beberapa putaran, jumlah putaran telah ditentukan, pada tahap ini dilakukan 9 kali putaran, yaitu:

   a. SubByte : substitusi byte dengan menggunakan tabel substitusi s-box.
   b. ShiftRows : proses pergeseran baris array state dengan menggeser baris ke-r dalam array state ke kiri sebanyak r byte.
   c. MixColumns : mengalikan tiap elemen dari blok chiper dengan matriks yang sudah ditentukan.
   d. AddRoundKey : melakukan XOR antara state sekarang round key.

4. Final round, adalah proses untuk putaran terakhir yang meliputi Sub Bytes, Shift Rows, dan Add Round Key.

2.6. Algoritma Dekripsi AES Rijndael

Dekripsi adalah proses yang diperlukan untuk dapat membaca kembali data atau mengembalikan data kembali ke bentuk semula [7]. Proses dekripsi algoritma hampir sama dengan proses enkripsi, namun berbeda pada urutan prosesnya saja. Urutan proses dekripsi dalam mengembalikan ke plaintext yaitu:

1. Key Expansion

Pada proses dekripsi juga dilakukan ekspansi kunci. Kunci pada proses enkripsi kemudian diekspansi terlebih dahulu untuk menghasilkan RoundKey yang akan digunakan pada setiap putaran.

2. AddRoundKey

Dilakukan proses XOR antara state awal (ciphertext) dengan key terakhir hasil ekspansi. Tahap ini disebut juga initial round.

3. Putaran sebanyak Nr-1 kali Proses yang dilakukan pada setiap putaran adalah:
   a. InvShiftRow : Pergeseran baris-baris array state ke kanan dengan aturan pergesaran sama seperti pada tahap enkripsi.
   b. InvSubByte : Dilakukan substitusi byte dengan menggunakan tabel substitusi kebalikan (invers S-box).
   c. AddRoundKey : Pada proses ini dilakukan XOR antara state sekarang dengan round key.

d. InvMixColumn : mengalikan tiap elemen dari blok chiper dengan matriks yang sudah ditentukan.

4. Final round

Proses untuk putaran terakhir hanya dilakukan tiga tahap saja, proses dari ketiga tahap tersebut sama seperti proses pada tahap sebelumnya, yaitu InvShiftRow, InvSubByte, AddRoundKey.

2.7. *QR Code*

Menurut Law dkk [7] " *QR Code* adalah suatu kode matriks yang berbentuk dua dimensi yang dikembangkan oleh Denso Wave, sebuah divisi Denso coporation, sebuah perusahaan di Jepang, yang dipublikasikan pada tahun 1994". *QR Code* merupakan singkatan dari quick respond (respon cepat), yang bertujuan untuk menyampaikan dan mendapatkan informasi dengan cepat. *QR Code* dapat meyimpan informasi secara vertical dan horizontal dan dapat menyimpan informasi yang lebih banyak dibandingkan kode batang (barcode), dan bentuk dari *QR Code* diperoleh dengan acak[7]. *QR Code* bisa dilihat pada gambar 2.

Gambar 2. *QR Code*

Menurut Denso [8] *QR Code* memliki beberapa manfaat yaitu, dapat menyimpan data dalam jumlah banyak, ukurannya kecil, dapat membaca *QR Code* dengan benar walaupun rusak atau kotor dan dipermukaan tidak rata.

Pembentukan algoritma *QR Code* Generator yaitu [9]:

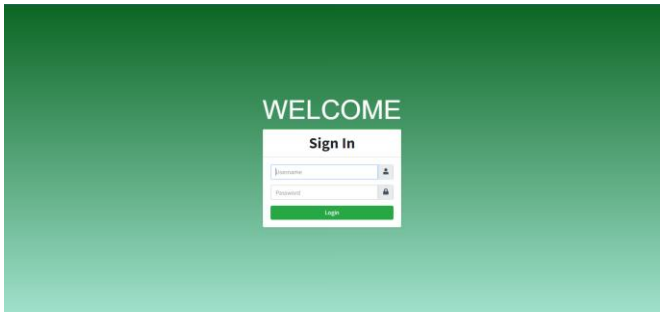
1. Menentukan kapasitas *QR Code*.
2. Encode data

- Membaca tipe data dari data inputan dan merepresentasikanya kedalam bilangan biner 4 bit.
- Konversi biner ke dalam bentuk desimal.
- Menghitung tingkat koreksi kesalahan.
- Alokasi data dalam bentuk gambar *QR Code*.
- Menentukan pola data.
- Format informasi data.

3. HASIL DAN PEMBAHASAN

3.1. Tampilan Login

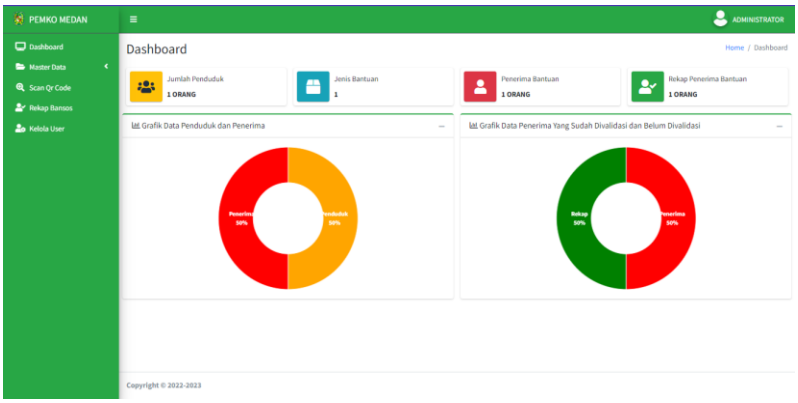
Tampilan login berfungsi bagi user untuk input username dan password sebelum masuk ke halaman dashboard. Tampilan login dapat dilihat pada gambar 3.



Gambar 3. Tampilan Login

3.2. Tampilan Menu Dashboard

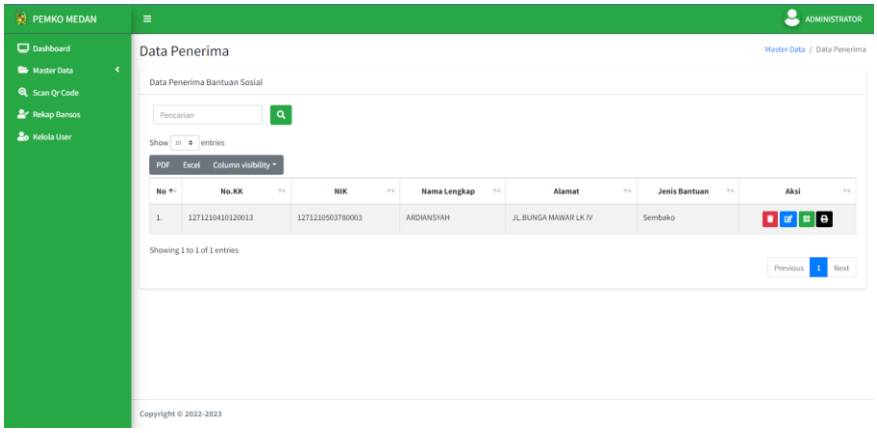
Menu dashboard akan tampil setelah user berhasil login, menu yang di tampilkan adalah seperti dibawah ini. Tampilan Menu user dapat dilihat pada gambar 4.



Gambar 4. Tampilan Menu Dashboard

3.3. Tampilan Menu Data Penerima

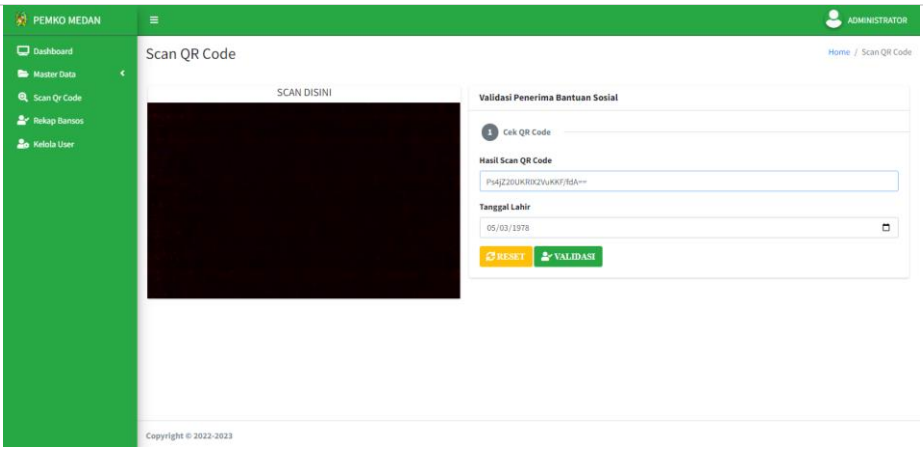
Menu data penerima berguna untuk mengelola data penduduk Kelurahan Padang Bulan Selayang II yang terdaftar menerima bantuan sosial. Tampilan menu data penerima dapat dilihat pada gambar 5.



Gambar 5. Tampilan Menu Data Penerima

3.4. Tampilan Menu Scan *QR Code*

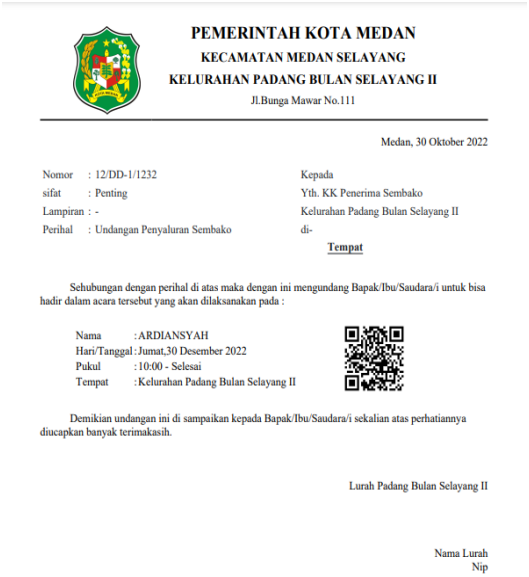
Menu scan *QR Code* berguna untuk memvalidasi *QR Code* dengan menggunakan kamera dan memasukkan tanggal lahir penerima bantuan sosial. Tampilan menu scan *QR Code* dapat dilihat pada gambar 6.



Gambar 6. Tampilan Menu Scan *QR Code*

3.5. Surat Undangan

Surat undangan berisi QR Code yang akan digunakan untuk validasi penerima bantuan sosial, QR Code tersebut berisi no.kk yang sudah terenkripsi. Surat undangan dapat dilihat pada gambar 7.



PEMERINTAH KOTA MEDAN
KECAMATAN MEDAN SELAYANG
KELURAHAN PADANG BULAN SELAYANG II
Jl.Bunga Mawar No.111

Medan, 30 Oktober 2022

Nomor : 12/DD-1/1232
sifat : Penting
Lampiran : -
Perihal : Undangan Penyaluran Sembako

Kepada
Yth. KK Penerima Sembako
Kelurahan Padang Bulan Selayang II
di-
Tempat

Sehubungan dengan perihal di atas maka dengan ini mengundang Bapak/Ibu/Saudara/i untuk bisa hadir dalam acara tersebut yang akan dilaksanakan pada :

Nama : ARDIANSYAH
Hari/Tanggal : Jumat,30 Desember 2022
Pukul : 10:00 - Selesai
Tempat : Kelurahan Padang Bulan Selayang II

Demikian undangan ini di sampaikan kepada Bapak/Ibu/Saudara/i sekalian atas perhatiannya diucapkan banyak terimakasih.

Lurah Padang Bulan Selayang II

Nama Lurah
Nip

Gambar 7. Gambar Surat Undangan

3.6. Proses Algoritma AES Rijndael

Untuk melakukan proses perhitungan dengan algoritma AES Rijndael dibutuhkan sebuah plaintext dan chiperkey dan telah diubah ke bentuk heksadesimal.
Plaintext : 1271210410120013 = 31323731323130343130313230303133
Chiperkey: 0617199101071590 = 30363137313939393130313037313539 30
Proses enkripsi Algoritma AES Rijndael putaran 1 sampai putaran 10 dapat dilihat pada tabel 1 dan proses dekripsi Algoritma AES Rijndael dapat dilihat pada tabel 2.

Tabel 1. Proses Enkripsi Algoritma AES Rijndael

	Initial Round	SubBytes	Shiftrows	MixColumn		Round Key
Input	31 32 31 30 32 31 30 30 37 30 31 31 31 34 32 33				⊕	30 31 30 31 36 39 31 35 31 39 30 39 37 31 37 30
Round 1	01 03 01 01 04 A1 5C 05 06 09 01 08 06 05 05 03	7C 7B 7C 7C F2 30 7C 6B 6F 01 7C 30 6F 6B 6B 7B	7C 7B 7C 7C 30 7C 6B F2 7C 30 6F 01 7B 6F 6B 6B	AF 2D 41 9F E3 BC 70 EB 39 D6 74 31 3E 1F 56 A1	⊕	A7 96 A6 97 24 1D 2C 19 35 0C 3C 05 F0 C1 F6 C6
Round 2	08 BB E7 08 C7 A1 5C F2 0C DA 48 34 CE DE A0 67	30 EA 94 30 C6 32 4A 89 FE 57 52 18 8B 1D E0 85	30 EA 94 30 32 4A 89 C6 52 18 FE 57 85 8B 1D E0	E1 82 50 86 27 DD 99 BE 32 16 DD 63 21 7A EA 1A	⊕	71 E7 41 D6 4F 52 7E 67 81 8D B1 B4 78 B9 4F 89
Round 3	90 65 11 50 68 8F E7 D9 B3 9B 6C D7 59 C3 A5 93	60 4D 82 53 45 73 94 35 6D 14 50 0E CB 2E 06 DC	60 4D 82 53 73 94 35 45 50 0E 6D 14 DC CB 2E 06	D9 F8 03 7B AA A7 71 E3 CC 83 1F 34 20 C0 99 A8	⊕	F0 17 56 80 C2 90 EE 89 26 AB 1A AE 8E 37 78 F1

	Initial Round	SubBytes	Shiftrows	MixColumn		Round Key
Round 4	29 EF 55 FB 68 37 9F 6A EA 28 05 9A AE F7 E1 59	A5 DF FC 0F 45 9A DB 02 87 34 6B B8 E4 68 F8 CB	A5 DF FC 0F 9A DB 02 45 6B B8 87 34 CB E4 68 F8	44 8F 0A 1D FC 45 02 21 AF 58 53 31 88 CA 4A 8B	⊕	5F 48 1E 9E 26 B6 58 D1 87 2C 36 98 43 74 0C FD
Round 5	1B C7 14 83 DA F3 5A F0 28 74 65 A9 CB BE 46 76	AF C6 FA EC 57 0D BE 8C 34 92 4D D3 1F AE 5A 38	AF C6 FA EC 0D BE 8C 57 4D D3 34 92 38 1F AE 5A	27 82 FA F2 5A D0 0B B5 70 E4 F7 6A DA 02 EA 5E	⊕	71 39 27 B9 60 D6 8E 5F D3 FF C9 51 48 3C 30 CD
Round 6	56 BB DD 4B 3A 06 85 EA A3 1B 3E 3B 92 3E DA 93	B1 EA C1 B3 80 6F 97 87 0A AF B2 E2 4F B2 57 DC	B1 EA C1 B3 6F 97 87 80 B2 E2 0A AF DC 4F B2 57	A6 C0 B3 1E 7E AD 78 15 DE 73 9F 8F B6 CE AA 4F	⊕	9E A7 80 39 B1 67 E9 B6 6E 91 58 09 1E 22 12 DF
Round 7	38 67 33 27 CF CA 91 A3 B0 E2 C7 86 A8 EC B8 90	07 85 C3 CC 8A 74 81 0A E7 98 C6 44 C2 CE 6C 60	07 85 C3 CC 74 81 0A 8A C6 44 E7 98 60 C2 CE 6C	34 0F AA F2 DE 92 2B 1C 44 D1 55 D9 7B CE 34 85	⊕	90 37 B7 8E B0 D7 3E 88 F0 61 39 30 0C 2E 3C E3
Round 7	38 67 33 27 CF CA 91 A3 B0 E2 C7 86 A8 EC B8 90	07 85 C3 CC 8A 74 81 0A E7 98 C6 44 C2 CE 6C 60	07 85 C3 CC 74 81 0A 8A C6 44 E7 98 60 C2 CE 6C	34 0F AA F2 DE 92 2B 1C 44 D1 55 D9 7B CE 34 85	⊕	90 37 B7 8E B0 D7 3E 88 F0 61 39 30 0C 2E 3C E3
Round 8	A4 38 1D 7C 6E 45 15 94 B4 B0 6C E9 77 E0 08 66	49 07 A4 10 9F 6E 59 22 8D E7 50 1E F5 E1 30 33	49 07 A4 10 6E 59 22 9F 50 1E 8D E7 33 F5 E1 30	43 0E 59 4D 56 62 8D 37 D2 66 BF 0A 83 BF 81 28	⊕	D4 E3 54 DA B4 63 5D D5 E1 80 B9 89 15 3B 07 E4
Round 9	97 ED 0D 97 E2 01 D0 E2 33 E6 06 83 96 84 86 CC	88 55 D7 88 98 7C 70 98 C3 8E 6F EC 90 5F 44 4B	88 55 D7 88 7C 70 98 98 6F EC C3 8E 4B 90 5F 44	AB 46 9A 72 8A 0A FD 6E F7 4D 33 DB 06 58 87 1D	⊕	CC 2F 7B A1 13 70 2D F8 88 08 B1 38 42 79 7E 9A
Round 10	67 69 E1 D3 99 7A D0 96 7F 45 82 E3 44 21 F9 87	85 F9 F8 66 EE DA 70 90 D2 6E 13 11 1B FD 99 17	85 F9 F8 66 DA 70 90 EE 13 11 D2 6E 17 1B FD 99		⊕	BB 94 EF 4E 14 64 49 B1 30 38 89 B1 70 09 77 ED
Output	3E 6D 17 28 CE 14 D9 5F 23 29 5B DF 67 12 8A 74	CIPHERTEXT				

Hasil akhir proses enkripsi yang berisi nilai heksadesimal diubah menjadi karakter menggunakan kode ASCII, maka akan menghasilkan ciphertext sebagai berikut.

Heksadesimal : 3E CE 23 67 6D 14 29 12 17 D9 5B 8A 28 5F DF 74

Ciphertext : Ps4jZ20UKRIX2VuKKF/fdA==

Tabel 2. Proses Dekripsi Algoritma AES Rijndael

	Initial Round	InvShiftRows	InvSubBytes		Round Key	AddRoundKey
Input	3E 6D 17 28 CE 14 D9 5F 23 29 5B DF 67 12 8A 74			⊕	BB 94 EF 4E 14 64 49 B1 30 38 89 B1 70 09 77 ED	
InvRound 1	85 F9 F8 66 DA 70 90 EE 13 11 D2 6E 17 1B FD 99	85 F9 F8 66 EE DA 70 90 D2 6E 13 11 1B FD 99 17	67 69 E1 D3 99 7A D0 96 7F 45 82 E3 44 21 F9 87	⊕	CC 2F 7B A1 13 70 2D F8 88 08 B1 38 42 79 7E 9A	AB 46 9A 72 8A 0A FD 6E F7 4D 33 DB 06 58 87 1D
InvRound 2	88 55 D7 88 7C 70 98 98 6F EC C3 8E 4B 90 5F 44	88 55 D7 88 98 7C 70 98 C3 8E 6F EC 90 5F 44 4B	97 ED 0D 97 E2 01 D0 E2 33 E6 06 83 96 84 86 CC	⊕	D4 E3 54 DA B4 63 5D D5 E1 80 B9 89 15 3B 07 E4	43 0E 59 4D 56 62 8D 37 D2 66 BF 0A 83 BF 81 28
InvRound 3	49 07 A4 10 6E 59 22 9F 50 1E 8D E7 33 F5 E1 30	49 07 A4 10 9F 6E 59 22 8D E7 50 1E F5 E1 30 33	A4 38 1D 7C 6E 45 15 94 B4 B0 6C E9 77 E0 08 66	⊕	90 37 B7 8E B0 D7 3E 88 F0 61 39 30 0C 2E 3C E3	34 0F AA F2 DE 92 2B 1C 44 D1 55 D9 7B CE 34 85
InvRound 4	07 85 C3 CC 74 81 0A 8A C6 44 E7 98 60 C2 CE 6C	07 85 C3 CC 8A 74 81 0A E7 98 C6 44 C2 CE 6C 60	38 67 33 27 CF CA 91 A3 B0 E2 C7 86 A8 EC B8 90	⊕	9E A7 80 39 B1 67 E9 B6 6E 91 58 09 1E 22 12 DF	A6 C0 B3 1E 7E AD 78 15 DE 73 9F 8F B6 CE AA 4F
InvRound 5	B1 EA C1 B3 6F 97 87 80 B2 E2 0A AF DC 4F B2 57	B1 EA C1 B3 80 6F 97 87 0A AF B2 E2 4F B2 57 DC	56 BB DD 4B 3A 06 85 EA A3 1B 3E 3B 92 3E DA 93	⊕	71 39 27 B9 60 D6 8E 5F D3 FF C9 51 48 3C 30 CD	27 82 FA F2 5A D0 0B B5 70 E4 F7 6A DA 02 EA 5E
InvRound 6	AF C6 FA EC 0D BE 8C 57 4D D3 34 92 38 1F AE 5A	AF C6 FA EC 57 0D BE 8C 34 92 4D D3 1F AE 5A 38	1B C7 14 83 DA F3 5A F0 28 74 65 A9 CB BE 46 76	⊕	5F 48 1E 9E 26 B6 58 D1 87 2C 36 98 43 74 0C FD	44 8F 0A 1D FC 45 02 21 AF 58 53 31 88 CA 4A 8B
InvRound 7	A5 DF FC 0F 9A DB 02 45 6B B8 87 34 CB E4 68 F8	A5 DF FC 0F 45 9A DB 02 87 34 6B B8 E4 68 F8 CB	29 EF 55 FB 68 37 9F 6A EA 28 05 9A AE F7 E1 59	⊕	F0 17 56 80 C2 90 EE 89 26 AB 1A AE 8E 37 78 F1	D9 F8 03 7B AA A7 71 E3 CC 83 1F 34 20 C0 99 A8
InvRound 8	60 4D 82 53 73 94 35 45 50 0E 6D 14 DC CB 2E 06	60 4D 82 53 45 73 94 35 6D 14 50 0E CB 2E 06 DC	90 65 11 50 68 8F E7 D9 B3 9B 6C D7 59 C3 A5 93	⊕	71 E7 41 D6 4F 52 7E 67 81 8D B1 B4 78 B9 4F 89	E1 82 50 86 27 DD 99 BE 32 16 DD 63 21 7A EA 1A
InvRound 9	30 EA 94 30 32 4A 89 C6 52 18 FE 57 85 8B 1D E0	30 EA 94 30 C6 32 4A 89 FE 57 52 18 8B 1D E0 85	08 BB E7 08 C7 A1 5C F2 0C DA 48 34 CE DE A0 67	⊕	A7 96 A6 97 24 1D 2C 19 35 0C 3C 05 F0 C1 F6 C6	AF 2D 41 9F E3 BC 70 EB 39 D6 74 31 3E 1F 56 A1
InvRound 10	7C 7B 7C 7C 30 7C 6B F2 7C 30 6F 01 7B 6F 6B 6B	7C 7B 7C 7C F2 30 7C 6B 6F 01 7C 30 6F 6B 6B 7B	01 03 01 01 04 08 01 05 06 09 01 08 06 05 05 03	⊕	30 31 30 31 36 39 31 35 31 39 30 39 37 31 37 30	
Output	31 32 31 30 32 31 30 30 37 30 31 31 31 34 32 33					

Hasil akhir proses dekripsi yang berisi nilai heksadesimal diubah menjadi karakter menggunakan kode ASCII, maka akan menghasilkan plaintext sebagai berikut.
Heksadesimal : 31 32 37 31 32 31 30 34 31 30 31 32 30 30 31 33
Plaintext : 1271210410120013

3.7. PENGUJIAN SISTEM

Pengujian aplikasi dilakukan untuk menguji algoritma AES Rijndael pada sistem. Pengujian algoritma AES Rijndael dilakukan pada *QR Code* dengan mengenkripsi no.kk. Dengan algoritma tersebut data yang ada pada *QR Code* menjadi aman karena tidak dapat dibaca, pengujian algoritma AES Rijndael pada *QR Code* dapat dilihat pada tabel 3.

Tabel 3. Implementasi Algoritma AES Rijndael Pada *QR Code*

NO	Plaintext	Ciphertext	*QR Code*
1	1271216802120002	Xh5a72/xvizwcYP3P3S30A==	
2	1271214404070001	ZdAZehTnz4yf0UEMKSQRxg==	
3	1272102404100001	XrBpBIkTY/YpLTP8m2MD8A==	
4	1271210410120013	Ps4jZ20UKRIX2VuKKF/fdA==	
5	1271214805130003	rzoMJ2LMyXVL2WKVZXOJyg==	

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah diuraikan, maka kesimpulan yaitu:

1. Dengan menerapkan Algoritma AES Rijndael pada *Quick Response Code (QR Code)*, sistem dapat menghindari terjadinya kebocoran dan manipulasi data pada *QR Code* dari pihak yang tidak berwenang.
2. Perancangan aplikasi mempermudah pegawai untuk melakukan pengelolaan data penerima bantuan sosial dan proses validasi berjalan dengan baik tanpa melakukan kesalahan *scan QR Code* dalam beberapa percobaan.

REFERENSI

[1] R. Siringoringo, "Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File," *KAKIFIKOM (Kumpulan Artik. Karya Ilm. Fak. Ilmu Komputer)*, vol. 02, no. 01, pp. 31–42, 2020, doi: 10.54367/kakifikom.v2i1.666.

[2] F. Syafaat and A. Finandhita, "Implementasi Kriptografi Aes-128 Pada Unmanned Aerial Vechile Dan Ground Control System," 2019.

[3] A. P. Silalahi and H. G. Simanullang, "Dashboard management penjualan dan pembelian pada tangkahan ikan," *INFORMATIKA*, vol. 13, no. 1, p. 46, 2021, doi: 10.36723/juri.v13i1.260.

[4] H. N. Putra, "Implementasi Diagram UML (Unified Modelling Language) dalam Perancangan Aplikasi Data Pasien Rawat Inap pada Puskesmas Lubuk Buaya," *Sink. J. dan Penelit. Tek. Inform.*, vol. 2, no. 2, pp. 67–77, 2018.

[5] M. Y. Simargolang, "Implementasi Kriptografi Rsa Dengan Php," *J. Teknol. Inf.*, vol. 1, no. 1, p. 1, 2017, doi: 10.36294/jurti.v1i1.1.

[6] A. Tumanggor, H. Rumapea, and A. Silalahi, "Implementasi Algoritma Advance Encryption Standard (AES) Pada Keamanan Dokumen Keuangan (Studi Kasus : CV . Multikreasi Bersama)," vol. 3, no. 1, pp. 83–90, 2023.

[7] H. Hidayatulloh, "Implementasi Algoritma Aes-128 Dan Qr Code Untuk Validasi Tiket Pada Perusahaan Travel Pt. Bumindo Jaya Cemerlang Skripsi," *Repository.Unej.Ac.Id*, no. September 2019, pp. 2019–2022, 2017.

[8] J. K. Azhar and S. Yuliany, "Implementasi Algoritma RSA (Rivest , Shamir dan," no. December, 2019.

[9] R. Prathivi, "Analisa Sistem Qr Code Untuk Identifikasi Buku Perpustakaan," *J. Pengemb. Rekayasa dan Teknol.*, vol. 14, no. 2, p. 37, 2019, doi: 10.26623/jprt.v14i2.1225.