# PEMANFAATAN QR CODE TERENKRIPSI MENGGUNAKAN ALGORITMA RSA UNTUK PEMBAGIAN SEMBAKO

**Rachmat Wiradi Surya, Deddy Rudhistiar, Fransiscus Xavier Ariwibisono**
Teknik Informatika, Institut Teknologi Nasional Malang
Jalan Raya Karanglo km 2 Malang, Indonesia
*rahmatwiradisurya@gmail.com*

**ABSTRAK**

Data kependudukan diIndonesia memiliki banyak sekali kegunaan dalam berbagai hal. Salah-satunya adalah Kantor Desa Pendem yang menggunakan data kependudukan dalam berbagai urusan khususnya pembagian sembako sehingga penduduk dapat dengan mudah menerima sembako sesuai dengan persyaratan. Namun, banyaknya penyalahgunaan identitas dan kebocoran data penduduk yang dilakukan oleh pihak yang tidak diinginkan. Oleh karena itu diperlukan sebuah solusi yang mampu mengamankan data penduduk menggunakan QR Code terenkripsi dengan metode RSA untuk menjaga data penduduk dengan aman. Algoritma RSA digunakan untuk mengenkripsi data penduduk dengan kunci public dan mendekripsi data dengan kunci private yang ditetapkan. Setelah data penduduk terenkripsi, data terenkripsi ditampung dalam bentuk gambar yang disebut dengan QR Code, kemudian gambar tersebut dipindai dengan suatu program atau perangkat lunak tertentu yang akan menghasilkan informasi yang tersimpan pada gambar tersebut kemudian didekripsi sehingga menghasilkan data sesungguhnya. Dengan menggunakan sistem ini, diharapkan data penduduk terlindungi dengan aman sehingga mengurangi terjadinya kebocoran dan penyalahgunaan data.

***Kata kunci:*** *Kriptografi, Asimetris, Simetris, Enkripsi dan Dekripsi, Algoritma RSA, QR Code*

## 1. PENDAHULUAN

Dalam era digital saat ini, sembako merupakan sesuatu yang penting untuk semua orang karena sembako merupakan kebutuhan pokok. Oleh karena itu, pembagian sembako kepada masyarakat sering sekali mengalami kendala seperti masyarakat belum mendapatkan sembako atau proses pembagian sembako terlalu lama karena pembagi harus mendata secara manual untuk masyarakat yang ingin mendapatkan sembako dan data masyarakat mudah sekali dipalsukan. Dalam penelitian ini, penulis merancang sebuah sistem informasi dengan pengamanan untuk pembagian sembako menggunakan algoritma RSA sehingga memungkinkan memiliki keamanan dengan tingkat yang baik dan terjamin yang disertai dengan QR Code sehingga memiliki kesan keamanan yang berlapis sampai informasi tersebut sampai pada masyarakat yang menerima sembako sehingga tidak mudah dipalsukan. Pengamanan informasi menjadi sangat penting dalam rangka menjaga privasi dan keamanan informasi tersebut. Salah satu cara untuk melindungi informasi adalah dengan menggunakan teknik kriptografi. Kriptografi adalah ilmu yang berkaitan dengan teknik penyandian informasi sehingga hanya orang yang memiliki hak akses yang dapat membaca informasi tersebut. Dalam konteks enkripsi, aplikasi pembagian sembako menjadi sangat penting dalam kemudahan dalam pembagian sembako dan menjaga keamanan data penduduk yang akan menerima sembako. Aplikasi pembagian sembako memungkinkan memberikan kemudahan dalam pengambilan sembako dan informasi pendudukan yang menerima sembako dilindungi dengan mudah, cepat, dan efektif, agar terlindungi dari ancaman pencurian data. Untuk mengatasi ancaman tersebut, diperlukan teknik pengamanan informasi yang tepat dan efektif. Salah satu teknik pengamanan informasi yang dapat digunakan adalah kriptografi. Dengan menggunakan teknik kriptografi, informasi kependudukan dapat dienkripsi sehingga hanya orang yang memiliki kunci enkripsi yang tepat yang dapat membaca

informasi tersebut. Dengan demikian, penggunaan teknik kriptografi dalam pengamanan data masyarakat untuk pembagian sembako menjadi sangat penting dalam menjaga kerahasiaan dan keamanan informasi tersebut. Hal ini akan memberikan kepercayaan dan jaminan bagi masyarakat dan pihak-pihak terkait bahwa informasi dalam data kependudukan aman dan terlindungi dari akses yang tidak sah.

## 2. TINJAUAN PUSTAKA

Peneliti menemukan beberapa bahan bacaan yang bisa dijadikan referensi di antaranya skripsi dengan judul "IMPLEMENTASI PENGAMANAN BASIS DATA DENGAN TEKNIK ENKRIPSI" yang ditulis oleh Putra Rahmadi dan Hilda Dwi Yunita [1]. Skripsi dengan judul "Implementasi QR Code untuk Efisiensi Waktu Pemesanan Menu Makanan dan Minuman di Restoran maupun Kafe" yang ditulis oleh Suharianto, Lukman Bahar Agung Pambudi, Angga Rahagianto, Gandu Eko Julianto Suyoso [2]. Skripsi dengan judul "ALGORITMA KRIPTOGRAFI DAN STEGANOGRAFI UNTUK PENGAMANAN PESAN KE DALAM CITRA" yang ditulis oleh Khilmi Hani [3]. Skripsi dengan judul "IMPLEMENTATION OF THE RSA CRYPTOGRAPHIC ALGORITHM IN THE QR-CODE ANDROID-BASED BUILDING PERMIT CHECKING APPLICATION" yang ditulis oleh Darsanto, Rio Andriyat Krisdiawan, Dias Eka Prayuda [4]. Skripsi dengan judul "PENERAPAN KRIPTOGRAFI DENGAN MENGGUNAKAN ALGORITMA RSA UNTUK PENGAMANAN DATA BERBASIS DESKTOP PADA PT TRIAS MITRA JAYA MANUNGGAL" yang ditulis oleh Muhamad Rizki, Pipin Farida Ariyani [5]. Skripsi dengan judul "IMPLEMENTASI TEKNOLOGI QR-CODE SEBAGAI PENCARIAN DATA RUANGAN PADA IBI KOSGORO 1957 BERBASIS ANDROID" yang ditulis oleh Boy Firmansyah [6]. Skripsi dengan judul "Komparasi Waktu Algoritma RSA Dengan RSA-CRT Base On Computer" yang ditulis oleh Nur Cahyo Hendro Wibowo, Khotibul Umam, Afrikhatul Hikmah, Albradru Muh Izul Khaq, Favian Agung Rizki [7]. Skripsi dengan judul "Implementasi Sistem Pembayaran Quick Response Indonesia Standard Bagi Perkembangan UMKM di Medan" yang ditulis oleh Josef Evan Sihaloho, Atifah Ramadani, Suci Rahmayanti [8]. Skripsi dengan judul "Implementasi Algoritma Base64 Untuk Verifikasi Qr Code Login Jaringan Wifi Berbasis Android" yang ditulis oleh Abdul Hidayat, Pristiwanto [9]. Skripsi dengan judul "). Implementasi QR Code pada Sistem Informasi Presensi Lokakarya dan Seminar" yang ditulis oleh Rangga Sidik, Khamil Aryansyah [10].

### 2.1. Enkripsi

Enkripsi adalah suatu metode yang digunakan untuk mengkodekan data sedemikian rupa sehingga keamanan informasinya terjaga dan tidak dapat dibaca tanpa di dekripsi (kebalikan dari proses enkripsi) dahulu. Encryption berasal dari bahasa yunani kryptos yang artinya tersembunyi atau rahasia [1].

Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integritas dan autentikasi dari sebuah pesan. Contohnya, Message Authentication Code (MAC) atau digital signature. Penggunaan yang lain yaitu untuk melindungi dari analisis jaringan komputer (Saludin Muis, Dr., Ir., M. Kom,2013).

Jenis-jenis enkripsi :

1. ECC (Elliptic Curve C
2. Enkripsi Elgamal
3. Diffie-Hellman Key Exchange
4. RSA
5. Twofish
6. AES (Advanced Encryption Standard)
7. Blowfish
8. Triple DES

### 2.2. QR Code

Kode QR (Quick Response) adalah jenis kode batang matriks atau kode dua dimensi yang dapat menyimpan informasi data dan dirancang untuk dibaca oleh telepon pintar yang menunjukkan bahwa isi kode harus diterjemahkan dengan sangat cepat dengan kecepatan tinggi. Kode terdiri dari modul hitam yang disusun dalam pola persegi pada latar belakang putih (Lihat gambar 1). Informasi yang disandikan mungkin berupa teks, URL, atau data lainnya [4]. QR Code dibuat oleh anak perusahaan Toyota, Denso Wave pada tahun 1994, dan pada awalnya digunakan untuk melacak inventaris dalam pembuatan suku cadang kendaraan. Gagasan di balik pengembangan kode QR adalah keterbatasan kapasitas informasi barcode (hanya dapat menampung 20 karakter alfanumerik) [2].

Perbedaan karakteristik utama dari kode QR dibandingkan dengan barcode tradisional adalah bahwa kode QR berisi informasi vertikal dan horizontal dan tidak dibatasi oleh satu dimensi. Mengenai kapasitas penyimpanan informasi, kode QR dapat menyimpan sekitar 7.089 digit, sekitar 1.800 karakter Cina (kode 5 Besar), dan kode batang khas menampung maksimum 20 digit.

### 2.3. Kriptografi

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan (message). Algoritma kriptografi adalah Aturan untuk enkripsi (enciphering) dan dekripsi (deciphering). Fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Algoritma

kriptografi berkembang terus dan terbagi atas dua bagian yaitu algoritma kriptografi klasik dan modern. Pada kriptografi klasik, kriptografer menggunakan algoritma sederhana, yang memungkinkan cipherteks dapat dipecahkan dengan mudah (melalui penggunaan statistik, terkaan, intuisi, dan sebagainya). Algoritma kriptografi modern dibuat sedemikian kompleks sehingga kriptanalis sangat sulit untuk memecahkan cipherteks tanpa mengetahui kunci. Algoritma kriptografi modern umumnya beroperasi dalam mode bit. Algoritma ini dapat dikelompokkan menjadi dua kategori yaitu cipher aliran (stream cipher ± beroperasi dalam bentuk bit tunggal) dan cipher blok (block cipher ± beroperasi dalam bentuk blok bit). Pengelompokan algoritma juga dilakukan berdasarkan kunci enkripsi ± dekripsi yang digunakan, yaitu simetris (menggunakan kunci yang sama untuk proses enkripsi ± dekripsi) dan asimetris atau kunci ± publik menggunakan kunci yang berbeda untuk proses enkripsi ± dekripsi (Yulianingsih, 2014) [3].

### 2.4. Steganografi

Kata steganografi berasal dari bahasa yunani yaitu "Steganos" yang berarti tersembunyi dan "Graphein" yang berarti tulisan (Ibrahim,2017). Secara estimologi, steganografi dapat diartikan tulisan tersembunyi. Secara terminologi steganografi adalah ilmu dan seni menyembunyikan pesan rahasia sedemikian sehingga keberadaan pesan tidak terdeteksi oleh indera manusia (Munir,2004). Steganografi bisa disebut sebagai kelanjutan dari kriptografi, dimana pesan dari kriptografi disandikan menjadi ciphertext, sedangkan steganografi menyembunyikan ke dalam media lain, sehingga pesan rahasia tersebut tersamarkan [3].

Dalam steganografi terdapat dua proses yang harus dilewati, seperti proses encode yaitu proses penyisipan kode pesan ke dalam citra, hasil dari penyisipan disebut stego image dan proses decode yaitu proses pemisahan kode pesan dengan cover image.

### 2.5. Istilah Dalam Kriptografi

Kriptografi mempunyai beberapa istilah seperti berikut [4]:

1. Plaintext adalah pesan asli atau pesan yang maknanya masih jelas.
2. Ciphertext adalah hasil dari enkripsi, bisa disebut dengan teks tersandi.
3. Enkripsi adalah algoritma untuk mentransformasikan plaintext menjadi ciphertext.
4. Dekripsi adalah algoritma untuk memulihkan kembali ciphertext menjadi plaintext (Sadikin,2012).
5. Kunci (Key) adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Kunci biasanya berupa string atau deretan bilangan.
6. Sistem kriptografi (Cryptosystem) adalah kumpulan yang terdiri dari algoritma kriptografi, semua plaintext, ciphertext dan kunci.
7. Kriptanalisis yaitu bidang yang berlawanan dengan kriptografi. Kriptanalisis adalahseni dan ilmu untuk memecahkan ciphertext menjadi plaintext tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Jika seorang kriptografer mentranformasikan plaintext menjadi ciphertext dengan suatu algoritma dan kunci, maka sebaliknya seorang kriptanalis berusaha untuk memecahkan ciphertext untuk menemukan plaintext atau kunci. (Munir,2019).
8. Kriptologi (Cryptology) adalah studi mengenai kriptografi dan kriptanalis, baik kriptografi dan kriptanalis keduanya saling berkaitan.

### 2.6. Kriptografi Asimetris

Algoritma ini sering disebut dengan algoritma kunci publik, dengan arti kunci yang digunakan untuk enkripsi dan dekripsi berbeda, dalam algoritma asimetri kunci dibagi menjadi dua bagian yaitu :

1. Kunci umum (public key): kunci yang di publik atau semua orang boleh mengetahuinya.
2. Kunci Privat (Privat Key): kunci yang dirahasiakan yang hanya diketahui oleh pembuat kunci itu sendiri.

Algoritma yang memakai kunci asimetri diantaranya: DSA (digital signatur algorithm), RSA (Rivest, Shamir, Adleman), DH (DiffieHellman) (Ariyus,2008).

Algoritma kunci asimetri juga mempunyai kelebihan dan kekurangan antara lain [3]:

1. Kelebihan:
   a. Keamanan dalam pendistribusian kunci dapat diatasi karena tidak ada jalur khusus dalam pendistribusiannya.
   b. Manajemen kunci dapat diatasi, karena hanya kunci privat saja yang perlu dijaga kerahasiaannya.
   c. Dapat digunakan untuk mengamankan kunci simetri.
2. Kekurangan:
   a. Proses enkripsi dan dekripsi lebih lambat dibandingkan dengan sistem simetri, karena enkripsi dan dekripsi menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar.
   b. Untuk tingkat keamanan, algoritma ini menggunakan kunci yang relatif besar.

### 2.7. Kriptografi Simetris

Algoritma Simetri bisa disebut dengan algoritma klasik, karena memakai kunci yang sama antara enkripsi dan dekripsi. Keamanan dari algoritma ini tergantung kerumitan dari kuncinya, jika kunci dari algoritma ini mudah ditebak maka kerahasiaan pesan terancam diketahui oleh orang lain. Algoritma yang

memakai kunci simetri diantaranya: DES, AES, RC2, RC4, RC5, RC6, dan lain sebagainya (Ariyus,2006).
Algoritma kunci simetri memiliki kelebihan dan kekurangan yaitu [4]:

1. Kelebihan :
   a. Waktu yang dibutuhkan dalam proses enkripsi dan dekripsi relatif cepat, karena efisiensi yang terjadi dalam proses pembangkitan kunci.
   b. Ukuran kunci simetri relatif pendek.
   c. Kunci simetri digunakan pada sistem secara real time seperti saluran telepon digital, karena cepatnya proses enkripsi dan dekripsi.
2. Kekurangan:
   a. Terdapat banyak kunci yang digunakan dalam penggunaanya. Karena setiap pasang pengguna membutuhkan kunci yang berbeda, sehinga sulit dalam hal manajemen kunci, karena banyak kunci yang harus diingat.
   b. Adanya kesepakatan jalur untuk pendistribusian khusus untuk kunci, karena tidak mudah dalam menentukan jalur yang aman, seperti pengiriman melalui jalur tertentu yang telah disepakati ataupun bisa bertemu secara langsung. Kunci harus sering diubah, mungkin disetiap sesi komunikasi.

### 2.8. Kriptografi RSA

Dari banyaknya algoritma kriptografi asimetris yang ada, algotirma yang sering dipakai adalah RSA. Algortima RSA dibuat oleh tiga orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976. Nama RSA merupakan singkatan dari nama tiga orang pembuatnya, yaitu Rivest, Shamir, dan Adleman. Algoritma RSA menggunakan pemfaktoran bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk menemukan kunci privat [4].

Dalam proses pembangkitan kunci hal pertama yang dilakukan adalah membangkitan dua bilangan prima besar. Algoritma RSA mempunyai pasangan nilai yang disebut dengan kunci public yang dapat dipublikasikan untuk enkripsi dan pasangan nilai yang lain disebut dengan kunci private yang bersifat rahasia untuk dekripsi. Untuk melakukan enkripsi dan dekrispi, algoritma ini menggunakan operasi eksponen dan modular. Algoritma RSA memiliki tingkat keamanan yang berfokus pada sulitnya faktorisasi bilangan besar pada nilai N menjadi 2 bilangan prima (p dan q).

### 2.9. Tujuan Kriptografi

Ilmu kriptografi mempunyai empat tujuan mendasar dan merupakan aspek keamanan informasi yaitu [4]:
Kerahasiaan: sebuah layanan untuk melindungi isi informasi dari siapapun yang tidak memiliki kunci rahasia untuk membuka informasi.

1. Integrity: keaslian pesan yang dikirim melalui media sosial dapat dipastikan bahwa pesan tidak di modifikasi oleh orang yang tidak berhak.
2. Authentication: berhubungan dengan identifikasi atau pengenalan agar penerima dapat memastikan keaslian dan isi pesan, dan pesan tersebut datang dari orang yang dimintai informasi.
3. Non-repudiation: usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman informasi oleh orang yang mengirimkan.

## 3. METODE PENELITIAN

### 3.1. Algoritma Kriptografi RSA

Algoritma yang digunakan untuk mengenkripsi dan mendekripsi data adalah algoritma kriptografi RSA. Algoritma RSA itu sendiri merupakan algoritma asimetris, sehingga memiliki kunci public dan kunci private [4].

RSA memiliki dasar proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmatika modulo. Kunci dekripsi dan enkripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diketahui oleh umum sehingga kunci enkripsi biasa disebut juga dengan kunci publik, namun kunci untuk dekripsi bersifat rahasia. Kunci deskripsi dibangkitkan dari beberapa buah bilangan prima bersama-sama dengan kunci enkripsi. Semakin besar bilangan non primanya maka semakin sulit pemfaktorannya. Semakin sulit pemfaktorannya, maka semakin kuat algoritma RSA-nya.

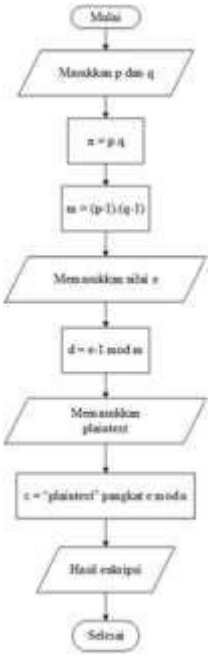
Algoritma pembangkitan kunci dalam algoritma RSA dapat dijelaskan sebagai berikut:

1. Dipilih dua bilangan prima $p \neq q$ secara acak dan terpisah untuk tiap-tiap p dan q.
2. Hitung N dengan persamaan: $N = p\ q$.
3. Hitung $\varphi$ dengan persamaan: $\varphi = (p-1)(q-1)$.
4. Dipilih bilangan bulat (integer) antara satu dan $\varphi$ $(1 < e < \varphi)$ yang juga merupakan coprime dari $\varphi$.
5. Hitung d dengan persamaan : $de \equiv 1 \pmod{\varphi}$.

Hasil dari algoritma ini:

1. Kunci public : pasangan (N,e)
2. Kunci privat : pasangan (N,d)

Flowchart algoritma RSA:




Gambar 3. Flowchart Algoritma RSA

Contoh penggunaan algoritma RSA misalkan:

1. Pembangkitan Kunci
   a. Tentukan sembarang nilai p = 47 dan q = 71 (keduanya prima)
   b. Hitung nilai n = p.q = 47.71 = 3337
   c. Hitung m = (p-1).(q-1) = (47-1).(71-1) = 32220
   d. Pilih kunci public yaitu e = 79, pastikan 79 relatif prima dengan 3220, syarat FPB(e,m)=1
   e. Hitung d = e-1 mod m atau e.d (mod m) = 1. Dengan perolehan 79.d mod 3220 = 1 dengan membuktikan diperoleh nilai kunci pribadi yang bulat dengan 1019.
2. Enkripsi
   a. M = TEGUH merupakan pesan (plaintext)
   b. Ubah ke kode ASCII decimal dengan hasil 8469718572.
   c. Pecah menjadi beberapa blok m1 = 84, m2 = 69, m3 = 71, m4 = 85, m5 = 72.
   d. Enkripsikan pecahan-pecahan blok tadi yang berasal dari variable m yang merupakan variable yang berisi pesan, yakni: C1 = 84 ^ 79 mod 3337, C2 = 69 ^ 79 mod 3337, C3 = 71 ^ 79 mod 3337, C4 = 85 ^ 79 mod 3337, C5 = 72 ^ 79 mod 3337.
   e. Ciphertext:1995 1988 3048 285
3. Dekripsi
   a. C = 1995 1689 1988 3048 285 merupakan pesan terenkripsi (ciphertext)
   b. Pecah menjadi beberapa blok c seperti c1 = 1995, c2 = 1685 c3 = 1988, c4 = 3048, c5 = 285.
   c. Dekripsikan blok ciphertext yakni c1 = 1995 ^ 1019 mod 3337, c2 = 1685 ^ 1019 mod 3337, c3 = 1988 ^ 1019 mod 3337, c4 = 3048 ^ 1019 mod 3337, c5 = 285 ^ 1019 mod 3337.
   d. Diperoleh kode ASCII dari C = 8469718572.
   e. Jika diubah menjadi karakter maka M = TEGUH.

## 4. HASIL DAN PEMBAHASAN

### 4.1 Halaman Login


Gambar 4. Hasil Tampilan Login

Pada halaman login pengguna melakukan autentikasi terlebih dahulu dengan memasukkan nama pengguna dan kata sandi yang telah terdaftar pada basis data.

### 4.2. Halaman Dashboard


Gambar 4. Halaman Dashboard

Pada halaman dashboard, pengguna telah berhasil melakukukan autentikasi sehingga pengguna diarahkan sistem menuju halaman ini, namun jika gagal maka sistem tidak akan berlanjut.

### 4.3. Halaman Tampilan Data


Gambar 4. Halaman Tampilan Data

Pada halaman tampilan data terdapat tampilan data yang telah tersimpan dibasis data. Data tersebut ditampilkan jika data benar-benar tersimpan, jika tidak maka tampilan akan kosong.

### 4.4. Halaman Tambah Data

Gambar 4. Hasil Halaman Tambah Data Pada halaman tambah data, pengguna dapat menambahkan data dengan mengisikan beberapa form, jika form telah diisi maka pengguna dapat menekan tombol submit untuk menyimpan data pada basis data dan menampilkan pada halaman tampilan data.

### 4.5. Halaman Ubah Data

Gambar 4. Hasil Halaman Ubah Data

Pada halaman ubah data, pengguna dapat mengubah data yang telah tersimpan sebelumnya dengan menganti form yang telah terisi data dengan data yang baru. Setelah itu pengguna dapat menekan tombol submit untuk menyimpan data yang telah diubah ke basis data dan menampilkannya pada halaman tampilan data.

### 4.6. Halaman Tampilan Hasil Enkripsi

Gambar 4. Hasil Halaman Hasil Enkripsi Pada halaman tampilan hasil enkripsi, pengguna dapat melihat hasil data terenkripsi dari data yang tersimpan dibasis data. Data dienkripsi menggunakan algoritma RSA.

### 4.7. Halaman Tampilan QR Code

Gambar 4. Hasil Halaman Tampilan QR Code

Pada Halaman tampilan QR Code. Pengguna dapat melihat hasil dari data terenkripsi diubah menjadi QR Code. Proses tersebut dapat dilakukan dengan menekan fitur tombol yang terletak pada halaman tampilan data enkripsi. Pengguna dapat melakukan scanning pada gambar QR Code dengan menekan fitur tombol yang terletak dibawah hasil tampilan QR Code pada halaman tampilan QR Code.

### 4.8. Halaman Tampilan Hasil Scan QR Code

Gambar 4. Tampilan Hasil Scan QR Code

Pada halaman tampilan hasil scan QR Code, pengguna dapat melihat data yang tersimpan dan didekripsi dari gambar QR Code yang ditampilkan pada halaman sebelumnya.

### 4.9. Halaman Tampilan Hasil Dekripsi

Gambar 4. 9 Halaman Tampilan Hasil Dekripsi

Pada halaman tampilan hasil dekripsi, pengguna dapat melihat data yang telah terdekripsi dari data yang terenkripsi. Data tersebut terdekripsi dengan menekan fitur tombol yang terletak pada halaman hasil tampilan data terenkripsi.

### 4.10. Pengujian Fungsionalitas

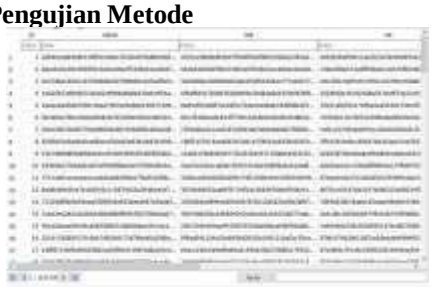
Tabel 4. Hasil Pengujian Fungsionalitas

| No | Menu | Fitur | Browser | | |
|---|---|---|---|---|---|
| | | | Chrome | Edge | Mozilla |
| 1 | Register | Pendaftaran Nama Pengguna | √ | √ | √ |
| 2 | Login | Masuk Akses | √ | √ | √ |
| 3 | Beranda | Tampilan Kalimat Berheading | √ | √ | √ |
| 4 | Logout | Keluar Akses | √ | √ | √ |

| | | | | | |
|---|---|---|---|---|---|
| 5 | Tampilan Data | Tabel Data | √ | √ | √ |
| 6 | Hasil Enkripsi | Tabel Data Terenkripsi | √ | √ | √ |
| 7 | Hasil Dekripsi | Tabel Data Terdekripsi | √ | √ | √ |
| 8 | Tambah | Form Tambah Data | √ | √ | √ |
| 9 | Ubah | Form Ubah Data | √ | √ | √ |
| 10 | Hapus | Menghapus Data | √ | √ | √ |
| 11 | Enkripsi | Mengenkripsi Data | √ | √ | √ |
| 12 | Dekripsi | Mendekripsi Data | √ | √ | √ |
| 13 | QR Code | Gambar QR Code | √ | √ | √ |

Dari tabel diatas dapat dijelaskan bahwa 14 menu dan fitur yang tersedia pada aplikasi dapat diakses oleh berbagai platform browser yang berbeda yaitu google chrome dengan versi 125.0.6422.142 (Official Build) (64-bit), microsoft edge dengan versi 125.0.2535.92 (Official build) (64-bit), dan mozilla firefox dengan versi versi 125.0.7015.130 (Official Build) (64-bit) sehingga aplikasi dapat berjalan semestinya.

### 4.11. Pengujian Metode



Gambar 4. Hasil Pengujian Metode (Enkripsi)

Pada gambar diatas menunjukkan hasil tampilan data terenkripsi. Data tersebut dienkripsi menggunakan algoritma RSA dengan hasil ciphertext yang diubah ke dalam bentuk hexadecimal agar tidak terlalu panjang.

Proses enkripsi data diatas dengan menerapkan ukuran kunci yang besar dan kunci yang acak. Pada dasarnya kunci RSA yang lebih aman memerlukan bilangan prima dengan banyak digit sehingga menghasilkan ukuran kunci yang sangat besar karena keamanannya terletak pada kesulitan faktorisasi bilangan besar menjadi faktor- faktor primanya.

Bilangan prima dengan digit yang banyak dihasilkan dengan melakukan operasi matematika yang komplek, hal ini cenderung menyebabkan kinerjanya menjadi lambat untuk data dalam ukuran tertentu sehingga menjdi kekurangan dari algoritma tersebut.

Gambar 4. Hasil Pengujian Metode (Dekripsi)

Pada gambar diatas menunjukkan hasil tampilan data terdekripsi. Data tersebut terdekripsi dengan menggunakan kunci private. Kunci ini berbeda dengan kunci publik untuk enkripsi, karena algoritma RSA merupakan algoritma kriptografi asimetris yang artinya menerapkan kunci yang berbeda untuk melakukan enkripsi dan dekripsi. Hal ini menyebabkan algoritma kriptografi asimetris memiliki tingkat keamanan yang cukup baik.

## 5. KESIMPULAN DAN SARAN

Kesimpulan:

Sistem Informasi dapat diuji pada berbagai browser seperti microsoft edge, google chrome, dan mozilla firefox sehingga dengan hasil dapat diakses dan fitur-fitur didalamnya dapat berfungsi dengan baik.

Data terenkripsi menggunakan algoritma RSA dapat diubah menjadi QR Code dengan hasil berupa gambar yang dapat dipindai dan terdekripsi, sehingga dapat menghasilkan sebuah informasi data.

Algoritma RSA yang digunakan merupakan algoritma kriptografi yang paling mumpuni saat ini karena algoritma RSA menerapkan dua kunci yang berbeda (asimetris) dan proses enkripsi yang menganjurkan penggunaan angka bilangan prima yang besar untuk menghasilkan kunci dengan ukuran besar sehingga peretas ingin melakukan pembobolan mengalami kesulitan dalam melakukan pemfaktoran bilangan.

Saran:

Penulis mengharapkan adanya pengembangan aplikasi dari mahasiswa lainnya agar tercipta aplikasi yang lebih baik lagi dikemudian hari, Penulis mengharapkan pengembangan kedepannya dapat

menambahkan fitur seperti cetak pdf sehingga lebih memudahkan user, Penulis mengharapkan aplikasi ini dapat dibangun dengan sistem operasi android dan ios sehingga tidak hanya dapat berjalan diaplikasi web saja.

**DAFTAR PUSTAKA**

[1]. Rahmadi, P., & Yunita, H. D. (2020). Implementasi Pengamanan Basis Data Dengan Teknik Enkripsi. Jurnal Cendikia, 19(1), 413-418.

[2]. Pambudi, L. B. A., Rahagiyanto, A., & Suyoso, G. E. J. (2020). Implementasi QR code untuk efisiensi waktu pemesanan menu makanan dan minuman di restoran maupun kafe. BIOS: Jurnal Teknologi Informasi dan Rekayasa Komputer, 1(1), 35-39.

[3]. Hani, K. (2020). Algoritma kriptografi dan steganografi untuk pengamanan pesan ke dalam citra (Doctoral dissertation, Universitas Islam Negeri Maulana Malik Ibrahim).

[4]. Faiz, D., Krisdiawan, R. A., & Prayuda, D. E. (2021). IMPLEMENTATION OF THE RSA CRYPTOGRAPHIC ALGORITHM IN THE QR-CODE ANDROID-BASED BUILDING PERMIT CHECKING APPLICATION. NUANSA INFORMATIKA, 15(1), 74-80.

[5]. Rizki, M., & Ariyani, P. F. (2021). Penerapan Kriptografi Dengan Menggunakan Algoritma Rsa Untuk Pengamanan Data Berbasis Desktop Pada Pt Trias Mitra Jaya Manunggal. SKANIKA: Sistem Komputer dan Teknik Informatika, 4(2), 77-82.

[6]. Firmansyah, B. (2020). Implementasi Teknologi Qr-Code Sebagai Pencarian Data Ruangan Pada Ibi Kosgoro 1957 Berbasis Android. Jurnal Nasional Informatika (JUNIF), 1(1), 30-42.

[7]. Wibowo, N. C. H., Umam, K., Khaq, A. M. I., & Rizki, F. A. (2020). Komparasi Waktu Algoritma RSA dengan RSA-CRT Base On Computer. Walisongo Journal of Information Technology, 2(1), 13-26.

[8]. Sihaloho, J. E., Ramadani, A., & Rahmayanti, S. (2020). Implementasi Sistem Pembayaran Quick Response Indonesia Standard Bagi Perkembangan UMKM di Medan. Jurnal Manajemen Bisnis, 17(2), 287-297.

[9]. Hidayat, A., & Pristiwanto, P. (2020). Implementasi Algoritma Base64 Untuk Verifikasi Qr Code Login Jaringan Wifi Berbasis Android. Jurnal Sistem Komputer dan Informatika (JSON), 2(1), 25-30.

[10]. Sidik, R., & Aryansyah, K. (2021). Implementasi QR Code pada Pengembangan Sistem Informasi Presensi Lokakarya dan Seminar. Jurnal Manajemen Informatika (JAMIKA), 11(2), 88-101.