

# Pemanfaatan QR Code dalam Kriptografi

Muhammad Treza Nolandra - 13515080

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

13515080@std.stei.itb.ac.id

**Abstrak**—Pada makalah ini dimuat rancangan kriptografi dengan menggunakan QR Code. QR Code adalah sekumpulan modul yang pada umumnya berupa kotak berwarna hitam atau putih. QR Code dapat menyimpan informasi yang dapat dilihat ketika dipindai. Peran QR Code dalam kriptografi adalah sebagai penyimpan cipherteks atau penyimpan kunci. Kriptografi dengan QR Code sebagai penyimpan cipherteks hanya dapat dilakukan dengan pesan yang berukuran terbatas. Kriptografi dengan QR Code sebagai penyimpan kunci dapat dilakukan dengan pesan yang relatif tak terbatas. Penggunaan QR Code dalam kriptografi dapat mengefisienkan proses dekripsi.

**Keywords**—QR Code, Enkripsi, Dekripsi, Algoritma Cipher

## I. PENDAHULUAN

Menurut (Scheiner, 1996), kriptografi adalah ilmu untuk menjaga keamanan pesan. Kata kriptografi berasal dari bahasa Yunani, “kryptós” yang berarti tersembunyi dan “gráphein” yang berarti tulisan [3]. Kriptografi melibatkan menyamarkan isi pesan sehingga tidak diketahui orang lain. Hasil samaran pesan tersebut dapat diubah kembali menjadi pesan semula. Hal ini bertujuan agar keamanan terjaga. Keamanan dilihat dari segi terjamin kerahasiannya dan keasliannya.

Kriptografi melibatkan algoritma kriptografi simetri dan nir-simetri. Saat ini sudah banyak berkembang berbagai algoritma cipher yang baik dan layak pakai. Pada makalah ini, dibahas mengenai metode lain memanfaatkan algoritma cipher untuk mengenkripsi dan mendekripsi pesan. QR Code dapat dipakai dalam mengenkripsi dan mendekripsi pesan agar kerahasiaan dan keaslian terjamin.

## II. DASAR TEORI

### A. Algoritma Cipher

Pesan agar terjamin kerahasiaannya perlu dilakukan enkripsi. Enkripsi adalah proses menyandikan plainteks menjadi cipherteks [3]. Plainteks adalah pesan semula, sedangkan cipherteks adalah pesan yang telah disandikan sehingga menjadi tidak bermakna [3]. Proses mengembalikan cipherteks menjadi plainteks disebut dengan dekripsi. Algoritma yang berperan mengenkripsi atau mendekripsi pesan adalah algoritma cipher.

Algoritma cipher terbagi menjadi 2, yaitu algoritma kunci publik dan algoritma kunci privat. Algoritma kunci publik disebut juga algoritma kriptografi nir-simetri. Pada algoritma ini, kunci enkripsi tidak sama dengan kunci dekripsi. Contohnya adalah RSA, ECC, El Gamal, dan lain-lain. Algoritma kunci privat disebut juga algoritma kriptografi simetri. Tidak seperti

kriptografi nir-simetri, kunci enkripsi dan dekripsi sama pada kriptografi simetri. Contoh algoritma kriptografi jenis ini adalah DES, 3-DES, AES, dan lain-lain.

### B. QR Code

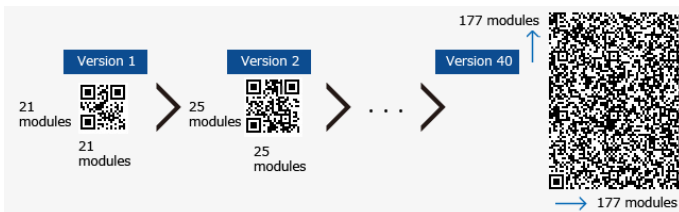
QR Code adalah sekumpulan titik berbentuk kotak yang pada umumnya berwarna hitam atau putih dan berdimensi dua dengan ukuran tertentu. Pada QR Code, tersimpan suatu informasi. QR merupakan kependekan dari *Quick Response*, yang berarti dapat dipindai dan dibaca oleh ponsel pintar dengan cepat. Ketika berhasil terpindai, informasi yang disisipkan pada QR Code dapat diekstraksi. Pada gambar 1 dapat dilihat QR Code yang berwarna hitam atau putih. Perlu diperhatikan bahwa QR Code tidak perlu berwarna hitam atau putih. [2] mendeskripsikan bermacam-macam QR Code yang dapat dibuat dengan warna dan bentuk yang beragam.



Gambar 1  
QR Code Versi 1  
(Sumber:

<https://upload.wikimedia.org/wikipedia/commons/5/5b/QR-1.png>)

QR Code pada gambar 1 merupakan QR Code versi 1. QR Code memiliki versi di antara 1 hingga 40. Masing-masing versi memiliki ukuran modul yang berbeda-beda. QR Code versi 1 berukuran 21x21 modul. Setiap modul pada umumnya berupa titik berwarna hitam atau putih. QR Code versi tertinggi memiliki 177x177 modul. Setiap kenaikan versi QR Code, jumlah modul bertambah 4 pada tiap sisi. Sebagai contohnya, QR Code versi 1 berukuran 21x21 modul. QR Code versi 2 berukuran 24x24 modul. Pada gambar 2 ditunjukkan bagaimana kenaikan 4 modul pada tiap sisi terjadi.



Gambar 2

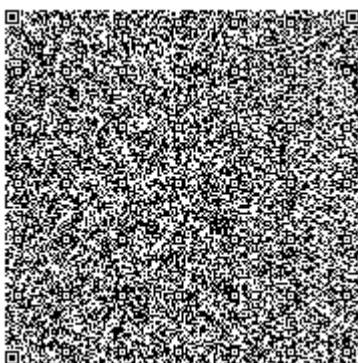
Seiring dengan Meningkatnya Versi, Modul juga Meningkat  
(Sumber: <https://www.qrcode.com/en/about/version.html>)

Pada QR Code, tersimpan berbagai informasi, seperti mode encoding, tingkat koreksi *error*, panjang pesan, dan lain-lain. Tingkat koreksi *error* memungkinkan pesan dapat terbaca walaupun beberapa simbol kotor atau rusak. Terdapat 4 tingkat koreksi kesalahan, yaitu ‘L’, ‘M’, ‘Q’, dan ‘H’. Menurut [1], Level ‘L’ memiliki persentase ECC (*Error Correction Capability*) sekitar 7%. Level ‘M’, ‘Q’, dan ‘H’ masing-masing memiliki persentase koreksi kesalahan sekitar 15%, 25%, dan 30%.

Tingkat koreksi *error* dapat dihitung dari persentase jumlah kode yang dapat diperbaiki dibandingkan dengan keseluruhan kode. Misalkan terdapat 100 *codeword* pada QR Code, 50 *codeword*, yaitu separuh total, adalah jumlah yang harus dapat diperbaiki. Diperlukan 2n Reed-Solomon *code* agar n jumlah *codeword* dapat diperbaiki. Disebabkan oleh jumlah yang harus diperbaiki adalah 50 *codeword*, diperlukan 100 tambahan *codeword* yang merupakan Reed-Solomon. Jumlah keseluruhan *codeword* menjadi 200. Tingkat koreksi *error* QR Code tersebut adalah 25% karena jumlah yang harus dapat diperbaiki adalah 50 dari 200 *codeword*.

QR Code juga memuat pola-pola deteksi posisi, Dengan adanya *position detection patterns*, QR Code dapat dipindai dari arah manapun. Kotak bertepi hitam tebal dengan memiliki ruang putih antara inti dengan tepian merupakan *pattern* yang dimaksud. QR Code juga memuat informasi, seperti panjang pesan dan mode encoding.

Perlu diperhatikan bahwa kapasitas informasi yang dapat dimuat pada QR Code terbatas. Kapasitas terbesar dicapai pada QR Code versi 40 dengan tingkat koreksi ‘L’. QR Code versi ini dapat menampung maksimal 23.648 *data bits*, 7089 numerik, 4.296 alfanumerik, 2.953 biner, dan 1.817 kanji [1]. Gambar 3 adalah QR Code versi 40.



Gambar 3  
QR Code Versi 40

(Sumber: [https://en.wikipedia.org/wiki/QR\\_code#/media/File:Qr-code-ver-40.png](https://en.wikipedia.org/wiki/QR_code#/media/File:Qr-code-ver-40.png))

### III. RANCANGAN KRIPTOGRAFI DENGAN QR CODE

QR Code dapat digunakan untuk keperluan kriptografi. Pada makalah ini, akan dijelaskan bagaimana proses enkripsi dan dekripsi dengan bantuan QR Code dapat dilakukan. Enkripsi dan dekripsi yang dimaksud adalah yang memanfaatkan algoritma kriptografi simetri atau nir-simetri. QR Code dapat memiliki 2 peran, yaitu sebagai penyimpan *cipherteks* atau sebagai penyimpan kunci.

#### A. Skema Kriptografi dengan QR Code sebagai Penyimpan Cipherteks

Pada skema ini, informasi yang disisipkan ke QR Code berupa *cipherteks* hasil enkripsi dengan algoritma *cipher*. Ketika pengguna ingin melihat informasi yang tersimpan, pengguna perlu menginput kunci yang diperlukan lalu memindai QR Code untuk mendapatkan *cipherteks*. Sistem kemudian mendekripsi *cipherteks* yang diperoleh baru kemudian menampilkan informasi yang tersimpan. Informasi akan tertampil dengan benar jika kunci yang dimasukkan benar.

#### B. Skema Kriptografi dengan QR Code sebagai Penyimpan Kunci

Pada skema ini, informasi yang disisipkan pada QR Code berupa kunci yang diperlukan untuk dekripsi. Pemindai sebelumnya memiliki *cipherteks*. Untuk mendekripsi *cipherteks* tersebut, pengguna memasukkan kunci dengan cara memindai QR Code. Ketika kunci berhasil terbaca, dekripsi dilakukan agar *cipherteks* diubah kembali menjadi *plaintexts* yang dapat dibaca.

### IV. EKSPERIMEN

Pengujian dilakukan untuk mengimplementasi skema yang telah dirancang. Pengujian dilakukan dengan bahasa pemrograman Python. *Library* yang digunakan adalah *pyqrcode* dan *library* *qrcode*. *Pyqrcode* digunakan untuk membuat QR Code, sedangkan *qrcode* digunakan untuk membaca QR Code. Pesan dapat dienkripsi atau didekripsi dengan bantuan *library* *pycrypto*. Algoritma *cipher* yang digunakan adalah algoritma AES. Pada eksperimen ini, pesan sebelumnya di-*padding* terlebih dahulu agar berukuran kelipatan 16 *byte* jika diperlukan.

Skema pertama yang diimplementasi (skema dengan QR Code sebagai penyimpan *cipherteks*) menyimpan *cipherteks* ke QR Code dalam bentuk numerik. Hal ini disebabkan oleh numerik adalah mode encoding dengan kapasitas terbesar yang didukung oleh *library*. Misalkan pesan adalah “Kriptografi itu menyenangkan!”. Hasil enkripsi dengan kunci “Kriptografi cool” dalam heksadesimal menghasilkan *cipherteks* berupa “\x74\x86\x8e\xb3\x18\xd5\xcf\xc3\x19\x3d\x54\x8a\x63\x22\x3\x71\x39\x2b\x8e\x7d\xbf\x9b\xaf\xe6\xf7\xe\x89\x85\xe3\x55\x81\xbc”. Ketika diubah ke dalam bentuk desimal, bilangan-bilangan yang diperoleh adalah “116134142179024213207195025061084138099034195113057043142125191155175230247030137133227085129188.”

Perlu diperhatikan bahwa desimal berupa satuan atau puluhan akan ditambah satu '0' atau dua '0'. Hal ini bertujuan agar mudah mengetahui antar nilai desimal. Pada gambar 4 ditunjukkan QR Code yang menyimpan cipherteks tersebut. Tabel 1 menunjukkan waktu eksekusi enkripsi dan dekripsi dengan dan tanpa QR Code.



Gambar 4  
QR Code Penyimpan Cipherteks dari Plainteks “Kriptografi itu Menyenangkan!”

Tabel 1  
Waktu Eksekusi Enkripsi dan Dekripsi Dengan dan Tanpa QR Code yang berperan sebagai Penyimpan Cipherteks

|                         | Waktu Eksekusi           |
|-------------------------|--------------------------|
| Enkripsi Tanpa QR Code  | 0,0001328 s              |
| Enkripsi Dengan QR Code | 0,02818 s                |
| Dekripsi Tanpa QR Code  | $2,289 \times 10^{-5}$ s |
| Dekripsi Dengan QR Code | 0,01158 s                |

Skema kedua yang diimplementasi menyimpan kunci ke QR Code dalam bentuk alfanumerik. Kunci tersebut dipakai untuk mengenkripsi dan mendekripsi pesan. Kunci yang digunakan untuk pengujian adalah “Kriptografi cool”. Pesan yang diproses sama seperti sebelumnya, yaitu pesan teks berupa “Kriptografi itu menyenangkan!”. Pesan teks yang digunakan adalah “Kriptografi itu menyenangkan!”. Gambar 5 menunjukkan QR Code dari kunci yang digunakan. Tabel 2 menunjukkan waktu eksekusi enkripsi dan dekripsi dengan dan tanpa QR Code.



Gambar 4  
QR Code Penyimpan Kunci “Kriptografi cool”

Tabel 2  
Waktu Eksekusi Enkripsi dan Dekripsi Dengan dan Tanpa QR Code yang berperan sebagai Penyimpan Kunci

|                         | Waktu Eksekusi           |
|-------------------------|--------------------------|
| Enkripsi Tanpa QR Code  | 0,0001328 s              |
| Enkripsi Dengan QR Code | 0,02775 s                |
| Dekripsi Tanpa QR Code  | $2,289 \times 10^{-5}$ s |
| Dekripsi Dengan QR Code | 0,3438 s                 |

## V. ANALISIS SKEMA DAN HASIL EKSPERIMEN

Skema kriptografi dengan QR Code sebagai penyimpan cipherteks hanya dapat mengenkripsi pesan dengan ukuran yang sangat terbatas. Hal ini mengakibatkan skema yang memanfaatkan QR Code sebagai penyimpan kunci lebih fleksibel. Hal ini disebabkan ukuran pesan dapat berukuran sangat besar sehingga gambar ataupun video dapat dienkripsi dengan skema ini. Kunci pun tidak perlu butuh terlalu banyak bit atau karakter sehingga dapat dipastikan muat dalam QR Code. Oleh karena itu, skema ini lebih disarankan.

Pemanfaatan QR Code dalam proses kriptografi juga layak digunakan karena waktu eksekusi yang dihasilkan tidak terlalu lambat. Skema QR Code sebagai penyimpan kunci dapat pula mengefisienkan proses dekripsi. Misalkan kunci yang digunakan ingin sangat panjang. Dengan menggunakan QR Code, pendekripsi tidak perlu menghafal dan menginput kunci yang panjang melainkan hanya perlu memindai QR Code.

## VI. KESIMPULAN DAN SARAN

Penggunaan QR Code dalam proses enkripsi dan dekripsi pesan merupakan metode yang tidak biasa dalam kriptografi. Namun, metode tersebut layak dan aman digunakan. Meskipun waktu eksekusi kriptografi dengan dan tanpa QR Code agak berbeda jauh, perbedaan tersebut tidaklah terlalu besar sehingga waktu proses masih terbilang cepat dan responsif. Pada makalah ini, dibahas peran QR Code sebagai penyimpan cipherteks dan penyimpan kunci. Skema QR Code sebagai penyimpan kunci jauh lebih efektif dan efisien disebabkan oleh enkripsi dan dekripsi dapat dilakukan untuk pesan dengan ukuran yang relatif tidak terbatas. Penggunaan QR Code juga dapat mengefisienkan proses dekripsi jika menggunakan kunci yang sangat panjang. Dibandingkan menghafal dan menginput kunci yang sangat panjang, pengguna hanya perlu memindai melalui QR Code. Untuk ke depannya, studi kasus mengenai penggunaan QR Code untuk berbagai versi, berbagai ukuran plainteks, berbagai jenis pesan, dan berbagai kunci perlu dilakukan agar dapat melihat lebih baik kinerja yang dihasilkan.

## REFERENSI

- [1] “Answers to Your Questions About the QR Code”. Internet: <https://www.qrcode.com/> [10 Mei 2019]
- [2] “Shannon’s Idea of Confusion and Diffusion”. Internet: <https://www.cse.ust.hk/faculty/cding/CSIT571/SLIDES/confdiffu.pdf> [12 Maret 2019]
- [3] Rinaldi Munir. *Pengantar Kriptografi*. Slide Kuliah IF4020 Kriptografi, 2018.

## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 10 Mei 2019

A handwritten signature in black ink, appearing to read 'Muhammad Treza N', with a long horizontal stroke extending to the right.

Muhammad Treza N  
(13515080)