

Kriptografi Korelasi Quick Response Code (QR Code)

Nisa Dian Rachmadi (13512090)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13512090@std.itb.ac.id

Abstract—barcode merupakan sekumpulan data yang dicetak dalam bentuk visual tertentu berdasarkan teori kriptografi dengan bentuk yang dimimalisasi. Kini barcode telah dikembangkan menjadi 2 dimensi yang salah satu jenisnya adalah Quick Response Code (QR Code) yang dapat 4 jenis type standar yaitu angka, alphabet, biner/byte, dan kanji.

Index Terms—About four key words or phrases in alphabetical order, separated by commas. QR code, quick response code, Barcode, matrix barcode

I. PENDAHULUAN

Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan. Kriptografi sendiri sudah lama dipakai sejak 400 SM di Yunani untuk menjaga keamanan pesan.

Lambat laun, kriptografi tidak hanya dijadikan untuk mengamankan pesan saja, namun kriptografi juga digunakan untuk meminimalisasi data walaupun perlu melalui proses enkripsi.

Salah satu bentuk dari kriptografi yang diminimalisasi adalah barcode. Dewasa ini, barcode yang telah dienkripsi oleh pengguna sehingga pengguna mendapatkan informasi dari barcode tersebut.

Barcode sudah mengalami banyak perkembangan bahkan sudah mulai ada barcode 2D yang salah satu jenisnya adalah matrix barcode yang dikembangkan menjadi QR Code (Quick Response Code).

II. LANDASAN TEORI

2.1 Kriptografi

Kriptografi yang merupakan ilmu dan seni untuk menjaga kemana, yang merupakan salah satu aplikasi dari aritmatika modulo dan bilangan prima dalam ilmu computer.

Dalam merahasiakan pesan, pesan pertama-tama dibuat dulu, yang kali ini dinamakan plainteks. Plainteks akan dibuatkan sandinya, setelah itu plainteks berubah menjadi teks bersandi yang disebut cipherteks. Proses perubahan plainteks menjadi cipherteks dinamakan enkripsi. Cipteks nantinya akan diubah menjadi plainteks asal akan melalui proses yang dinamakan proses dekripsi.

Dewasa ini kriptografi digunakan untuk perdagangan elektronik, seperti penyediaan PIN dan lainnya.

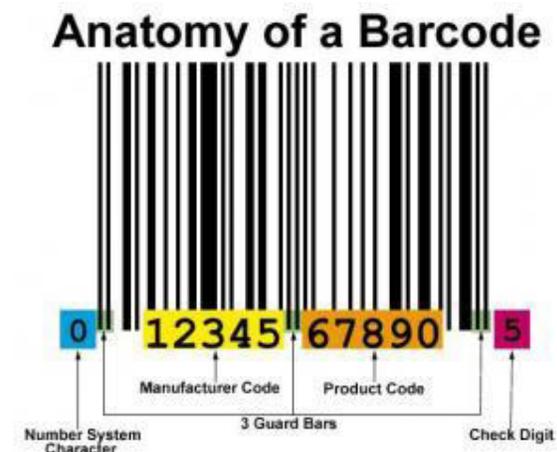
2.1.1 Sejarah Kriptografi

Kriptografi sudah digunakan sejak tahun 400 SM oleh tentara Sparta di Yunani. Mereka menggunakan alat yang dinamakan scytale. Scytale merupakan alat yang terbuat dari daun papyrus yang dibuat menjadi pita dan silinder. Cara kerjanya pesan disusun secara horizontal lalu dililitkan dengan pita. Sang penerima pesan akan membuka lilitan pita tersebut lalu huruf-huruf tersebut akan tersusun menjadi pesan aslinya.

2.2 Barcode

Barcode adalah kumpulan garis dalam dimensi tertentu yang dapat mewakili data atau informasi tertentu. Biasanya sering kita temukan pada barang-barang komersial untuk menyatakan jenis barang tersebut, sehingga kasih tidak perlu repot-repot untuk mengisi jenis barang apa, namun hanya menempelkan barcode pada barcode reader.

2.2.1 Anatomi barcode



Secara anatomi, barcode memiliki beberapa bagian.

- Number system character, dimana mengkarakteristikkan jenis-jenis khusus barcode, biasanya direpresentasikan dengan angka 0 dimana angka 0 merupakan sebuah system bilangan barcode yang universal.
- Manufactured code biasanya terdiri dari 5 buah

angka. Manufactured code merupakan bilangan khusus yang dilindungi dan diciptakan oleh Uniform Code Council (UCC).

- Product code biasanya terdiri dari 5 buah angka. Biasanya ditetapkan oleh perusahaan masing-masing
- Check digit merupakan satu angka terakhir yang digunakan untuk melakukan validasi terhadap kode manufaktur (manufactured code) dan kode produk (product code). Cara mendapatkan angka Check digit adalah
 - Jumlahkan semua digit-digit yang ganjil ($0+2+4+6+8+0=20$).
 - Kalikan hasil penjumlahan pada langkah sebelumnya dengan 3 ($20 \times 3=60$).
 - Jumlahkan dengan semua bilangan genap ($1+3+5+7+9+60$ (hasil sebelumnya) = 85), tidak termasuk check digit karena itu akan dicari.
 - Lalu $check\ digit = 85 \bmod 10 = 5$.

Diantara keempat tipe angka diatas, terdapat pemisah yang dinamakan guard bar. Antara number system character dengan manufacture code terdapat batang pembatas pertama yang bila dienkripsi menjadi "bar-space-bar" atau "101". Setelah itu, ditengah-tengah terdapat pembatas juga terdapat batang pembatas yang bila dienkripsi menjadi "space-bar-space-bar-space" atau "01010"

2.2.2 Sejarah Barcode

Tahun 1932, Wallace Flint membuat system pemeriksaan barang perusahaan retail. Lalu munculah teknologi barcode, yang dikenalkan oleh perusahaan retail yang diikuti oleh perusahaan industry. Lalu, pada tahun 1948 pemilik toko makanan local meminta Drexel Institute of Technology di Philadelphia untuk membuat system pembacaan otomatis untuk informasi produk selama checkout.

Beberapa lulusan Drexel bergabung untuk mencari solusi, dimana lulusan-lulusannya itu bernama Bernard Silver dan Norman Joseph Woodland. Woodland member saran untuk menggunakan tinta yang sensitive terhadap ultraviolet namun ditolak karena mahal. Akhirnya pada tanggal 7 oktober 1952 mereka mendapatkan hak paten dari hasil penelitian mereka. Lalu pada tahun 1966 barcode pertamakali dipakai secara komersial.

2.3 Bentuk Barcode

Bentuk barcode terdiri dari dua macam yaitu 1D (Linier barcode) dan 2D.

- Barcode satu dimensi (Linier barcode) biasanya digunakan pada produk-produk

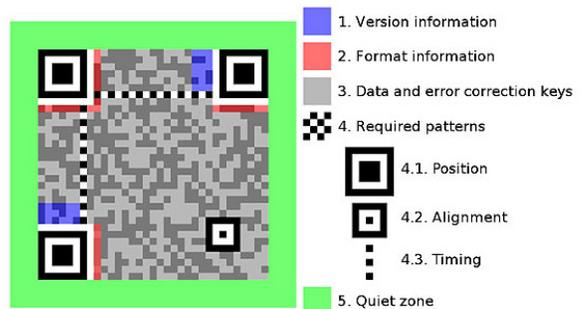
yang biasanya memuat jenis apa barang tersebut.

- Barcode dua dimensi (2D) merupakan barcode yang dikembangkan dari barcode satu dimensi yang memiliki beberapa keuntungan yaitu:
 - Informasi yang disimpan lebih banyak
 - Dapat disimpan pada ruang yang lebih kecil daripada barcode 1D

2.4 QR Code

QR code merupakan salah satu tipe barcode 2D dimana merupakan pengembangan dari matrix barcode yang memiliki kelebihan lebih banyak menampung informasi dan memiliki kecepatan yang besar dalam pembacaan informasinya (enkripsi).

2.4.1 anatomi QR code



- Finder pattern
Pola yang mendeteksi posisi dari QR code. Dengan penyusunan pola ini pada ketiga sudut kotak sehingga dapat dideteksi dari 360°
- Alignment pattern
Suatu pola untuk mengoreksi distorsi pada QR Code. Hal ini efektif dapat mengatasi distorsi non linier. Koordinat pada alignment pattern dapat diidentifikasi untuk membentuk suatu simbol.
- Timing pattern
Suatu pola untuk mengidentifikasi pusat yang tersusun atas pola hitam putih yang tersusun secara berurutan.
- Quiet zone
Suatu ruang batas dalam pembacaan QR Code. quiet zone dapat mempermudah

terdeteksinya suatu simbol.

- o Area data
Data disimpan di area data (Abu-abu). Data akan dikodekan menjadi bilangan biner '1' dan '0' ke dalam sel hitam dan putih.

2.4.2 sejarah QR code

Pada tahun 1960, dimana Jepang memasuki masa pertumbuhan ekonomi yang tinggi, cashier pada supermarket-supermarket di Jepang mengalami keluhan. Mereka mengalami mati rasa pada pergelangan tangan mereka dan berharap seandainya beban mereka lebih ringan.

Setelah itu, dibentuklah sebuah tim yang hanya terdiri dari dua orang saja dimana salah satunya Masahiro Hara untuk mengembangkan QR Code.

Melihat kebelakang, pembuatan barcode 2D bertujuan agar barcode tersebut dapat menampung informasi lebih banyak. Maka dari itu, tantangan terbesar mereka adalah membuat kode yang dapat dibaca dengan mudah dan cepat.

III. PEMBAHASAN

3.1 QR Code

Quick Response Code adalah salah satu tipe 2D code yang merupakan pengembangan dari Matrix Barcode. QR Code sendiri sudah banyak dikembangkan bahkan sekarang sudah banyak generator-generator yang gratis di internet juga QR Code scannernya yang gratis pula. Di beberapa tempat bahkan sebuah iklan hanya memvisualisasikan QR Codenya yang bila dienkripsi akan menghasilkan informasi yang berisi dengan iklan tersebut.



3.2 Enkripsi data pada Quick Response Code

Pengenkripsian QR Code, sangat tidak umum karena pengekripsian memiliki beberapa algoritma.

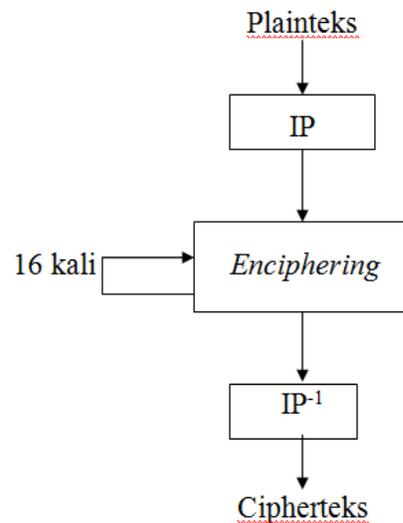
Pada sebuah aplikasi android pengekripsian dan pengdeskripsian QR Code menggunakan algoritma DES (56 bit).

Konvensional kode matrik 2-D yang dibutuhkan cukup banyak waktu untuk mencari kode simbol juga menentukan posisinya.

Untuk mengatasi masalah tersebut, QR Code dirancang dengan pola khusus dimana meletak 3 buah simbol di tiga sudutnya. Pola tersebut memiliki rasio scan garis simetri 1:1:3:1:1, sehingga memungkinkan scan dari segala arah.

Skema Global DES:

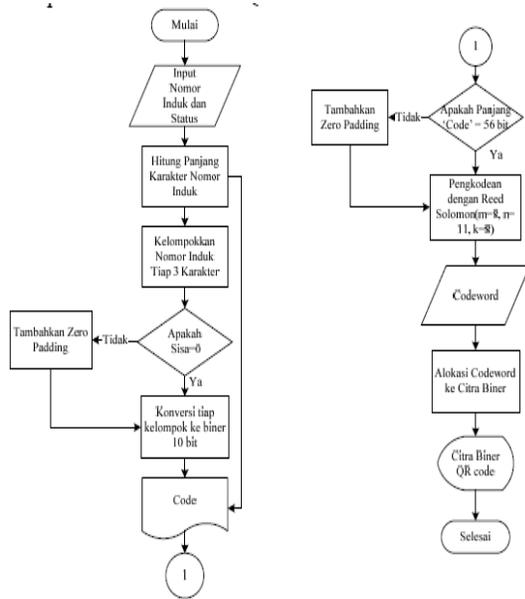
1. Blok plainteks dipermutasi dengan matriks permutasi awal (*initial permutation* atau IP).
2. Hasil permutasi awal kemudian di-*enciphering*- sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.
3. Hasil *enciphering* kemudian dipermutasi dengan matriks permutasi balikan (*invers initial permutation* atau IP^{-1}) menjadi blok cipherteks



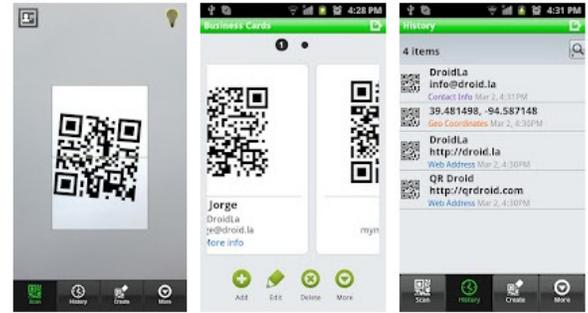
Pada pembuatan QR Code yang diimplementasikan di IT Telkom menggunakan langkah-langkah sebagai berikut:

1. Perhitungan jumlah karakter, serta pemberian indicator status dan jumlah karakter.
2. Encoding data dalam representasi biner
3. Pemenuhan jumlah bit dan simbol sesuai jumlah yang ditentukan.

Diagram alur system encodernya:



dapat mengdecoder sehingga dapat dibaca pesan rahasia tersebut.



- **Pemuatan informasi**
Di beberapa Negara pemuatan informasi berupa penyimpanan alamat dan URL, nomor telpon, teks, dan sms menggunakan QR Code. misalnya pada suatu tempat yang mana tidak bisa memberikan informasi yang banyak namun tak muat, maka dibuatkan QR Code sehingga pengunjung dapat meng-scan sehingga mendapatkan informasi yang lengkap.

3.2.1 Error Correction pada QR Code
Pada QR Code, sangat besar error yang ada pada QR Code. Bila Error correction lebih besar, maka akan semakin banyak variasi dari tampilan QR Code.

Kelebihan lainnya bila QR Code kotor atau rusak, maka QR Code masih bisa dibaca. Hal ini membuat QR Code lebih mudah diterima di bidang industry.



Kelebihan lainnya pada error yg dihasilkan QR Code adalah variasi visual QR Code yang dapat menarik perhatian (eye catching) sehingga untuk iklan dapat ditampilkan QR Code sekaligus terdapat design yang dapat menarik perhatian.

- **Reservasi Tiket Pesawat**
Pada beberapa tiket, salah satunya tiket pesawat, diterapkan QR Code. QR Code tersebut didapatkan saat pembelian tiket online, sehingga pada saat check-in di bandara, petugas tinggal memindai dengan cepat lalu dapat dicetak boarding pass.

Beda lagi dengan salah satu perusahaan penerbangan dari jepang. Sehabis check-in penumpangnya diberikan sebuah QR Code yang memuat berbagai informasi. Informasi tersebut antara lain adalah mengakses masuk area keberangkatan, sampai masuk pesawat, juga nomor tempat duduk penumpang.

3.3 Penggunaan QR Code

- **Pengkodean pesan rahasia**
Pada aplikasi QR Droid, pesan rahasia dapat dibentuk melalui QR Code. Aplikasi QR Droid

- **Identitas**
Di beberapa rumah sakit di jepang, identitas seorang pasien (hingga catatan dokter) disimpan dalam sebuah QR Code sehingga seorang dokter dapat lebih cepat mendapatkan informasi pasien

lebih cepat dengan memindai QR Code yang dimiliki pasiennya. Sehingga sang dokter lebih cepat bertindak.

Di sebuah sekolah pun, kartu pelajar siswa-siswinya menggunakan QR Code. QR Code memberikan URL, siswa, guru, dan orang tua dapat dengan lebih mudah untuk mengetahui semua informasi-informasi proses belajar mengajar misalnya informasi nilai, biodata, iuran sekolah, pelajaran apa saja yang diambil siswa, program sekolah apa saja yang mereka ikut, pengumuman sekolah dan juga persentasi keaktifan siswa disetiap pelajaran.

IV. KESIMPULAN

Quick Response Code (QR Code) merupakan teknologi barcode yang dapat meng dekripsi dengan cepat. Penggunaan barcode yang selama ini sebatas pada barang-barang saja, kini bisa lebih dimaksimalkan terlebih lagi kemampuan QR Code yang dapat memuat lebih banyak informasi.

REFERENCES

- [1] <http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2011-2012/Makalah2011/Makalah-IF2091-2011-013.pdf>
Diakses pukul 23.15 tanggal 14 desember 2013
- [2] Munir,Rinaldi.2012.Matematika Diskrit. Revisi Kelima.Penerbit Informatika.Bandung.
- [3] <http://pusatbarcode.wordpress.com/2008/10/27/definisi-dan-sejarah-barcode/>
diakses tanggal 15 desember 2013 jam 00:50
- [4] <http://mirfagah.com/2008/10/20/76/>
Diakses tanggal 16 desember 2013 pukul19:49
- [5] <http://www.colourlovers.com/business/blog/2011/09/20/are-they-here-to-stay-history-anatomy-and-the-many-uses-of-qr-codes>
diakses tanggal 15 desember 2013 pukul 00:59
- [6] <http://www.qrcode.com/en/history/>
diakses 15 desember 2013
- [7] www.qrcode.com/en/about/
diakses tanggal 15 desember 2013 pukul 11:45
- [8] https://www.google.com/search?q=QR+Code&client=firefox-beta&hs=Sbk&rls=org.mozilla:en-US:official&source=lnms&tbm=isch&sa=X&ei=GjWtUpWGGcGHrAeS7YCQDA&ved=0CAkQ_AUoAQ&biw=669&bih=608
diakses tanggal 15 desember 2013 jam 11:55
- [9] <http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fkur2003.if.itb.ac.id%2Ffile%2FDES.doc&ei=L0OtUpWIAcrtrQfy54GgDA&usq=AFQjCNHVJqGAUByv0xO0iHTx9Fc7c6Pm7Q&sig2=HzLXTfNQdaF3jLtrybRLkg&bvm=bv.57967247.d.bmk>
diakses tanggal 15 desember 2013 jam 12:59
- [10] <http://www.nacs.org/LinkClick.aspx?fileticket=DIFpVAvvJuo%3D&tabid=1426&mid=4802>
Diakses tanggal 16 desember 2013 jam 10:35
- [11] https://www.google.com/search?q=visual+unique+qr+code&client=firefox-beta&hs=Rx5&rls=org.mozilla:en-US:official&source=lnms&tbm=isch&sa=X&ei=wHWuUuq0K4exrgfinoHIDA&ved=0CAcQ_AUoAQ&biw=669&bih=581
diakses tanggal 16 desember 2013 jam 10 43
- [11] http://kru.blog.ittelkom.ac.id/blog/files/downloads/2012/12/JURNAL_S EPTI_KRU_LDN_U_SNAKOM2012.pdf
Diakses tanggal 16 desember jam 14:47

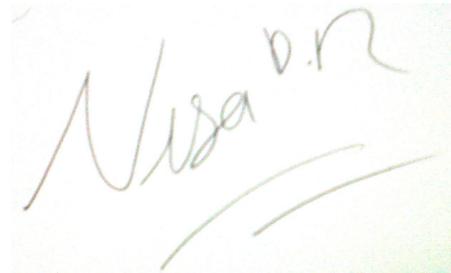
[12] <http://dhietaangraini.blogspot.com/2011/09/implementasi-qr-code.html>

Diakses tanggal 16 desember jam 15:16

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,7 Desember 2013



Nisa Dian Rachmadi (13512090)