KRIPTOGRAFI HILLCHIPHER DIGUNAKAN DALAM SISTEM KEAMANAN PADA TIKET DENGAN TEKNOLOGI *QR-CODE*

Akik Hidayat[1)], Buana Yogi M[2)] , Erick Paulus[3)]

[1,2,3]Prodi Teknik Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Padjadjaran, Bandung
E-mail: akik@unpad.ac.id[1], buana@gmail.com[2], erick.paulus@unpad.ac.id[3]

Abstrak

Tiket merupakan bukti seseorang telah membayar biaya untuk masuk ke dalam suatu tempat atau suatu acara. Karena mahalnya harga tiket, banyak oknum yang tidak bertanggung jawab dengan mudahnya memalsukan tiket ataupun mencatut tiket. Upaya pengamanan tiket dapat dilakukan dengan beberapa metode, salah satunya dengan menambahkan tanda pengaman pada cetakan tiket. Penelitian ini mengemukakan salah satu alternatif sistem pengamanan tiket menggunakan *QR-Code* dan kriptografi. Algoritma kriptografi yang digunakan pada penelitian ini adalah algoritma *Hill Cipher*. *QR-Code* dipilih karena dapat menampung lebih banyak karakter. Isi dari *QR-Code* yang tercetak pada tiket adalah hasil enkripsi dari kode yang ada pada tiket. Dalam penelitian ini *scanning QR-Code* menggunakan bantuan program *QuickMark v3.8.0 r5017*.Hasil penelitian yang telah dilakukan adalah aplikasi penjualan tiket dengan *QR-Code* dan kriptografi HillCipher yang telah dapat meminimalisir pemalsuan tiket dan pencatutan tiket.

Kata kunci: Tiket, *QR-Code*, kriptografi, *HillCipher*.

Abstract

The ticket is evidence someone has paid a fee to get into a place or an event. Due to the high price of tickets, many actors who aren't responsible falsifying tickets or profiteer ticket with ease. The effort to secure tickets can be done by several methods, one of them adding the security sign printed ticket. This research suggests an alternative ticket securing system using QR-Code and cryptography. Cryptographic algorithms used in this research are Hill Cipher algorithm. QR-Code was chosen because it can accommodate more characters. The contents of the QR-Code which is printed on the ticket is the HillCipher encryption result from the existing code on the ticket. In this research scanning the QR-Code using the help of QuickMark v3.8.0 r5017. The results of the research that has been done is the application of ticket sales using QR-Code and cryptography that has been able to minimize counterfeiting and profiteering ticket.

Keywords: *Ticket, QR-Code, Cryptography, Hill Cipher.*

I. PENDAHULUAN

Tiket adalah alat identifikasi yang paling sering digunakan dalam setiap *event* ataupun pada sebuah pelayanan jasa, seperti tiket pesawat dan tiket pertandingan sepakbola. Karena mahalnya harga tiket dan sistem keamanannya yang masih kurang optimal, banyak oknum yang tidak bertanggung jawab dengan mudahnya memalsukan tiket, seperti pemalsuan tiket sepak bola dan pemalsuan tiket konser musik yang akhir ini banyak terjadi.

Berkembangnya teknologi dan kebutuhan manusia yang semakin meningkat dapat dimanfaatkan untuk menciptakan suatu teknologi yang dapat menciptakan keamanan. Pembangunan sistem keamanan tiket yang baik dengan menggabungkan beberapa teknologi sangat diperlukan untuk mengoptimalkan keamanan. Salah satu contohnya dengan menggunakan metode kriptografi dan teknologi *QR-Code*.

Penggunaan *QR-Code* dapat memberikan keuntungan, seperti pembacaan *QR-Code* cukup hanya dengan menggunakan kamera, kapasitas yang *QR-Code* cukup besar, serta mudah menggunakannya, sehingga pengelolaan data akan lebih cepat. Sedangkan metode kriptografi berguna untuk mengkodekan suatu *input* baik berupa alphabet dan atau numerik menggunakan suatu algoritma enkripsi dan dekripsi sehingga kode tersebut tidak dapat diartikan atau diciptakan oleh orang lain.

II. BAHAN DAN METODE

Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani *cryptos* yang artinya rahasia dan *graphein* yang artinya tulisan. Jadi kriptografi itu berarti tulisan rahasia. Ada beberapa definisi kriptografi yang digunakan sebelum tahun 1980 yang menyatakan bahwa kriptografi adalah ilmu untuk menjaga kerahasiaan pesan dengan cara menyandikan ke bentuk yang tidak dimengerti. Namun definisi tersebut berkembang pada masa sekarang ini, karena kriptografi tidak sekedar kerahasiaan pesan saja, tapi juga bertujuan untuk menjaga keabsahan data, integritas data, serta autentikasi data[1]. Kriptografi dapat diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain.

Enkripsi (*encryption*) atau *enciphering* merupakan proses penyandian yang melakukan perubahan sebuah pesan yang dimengerti (*plainteks*) menjadi pesan yang tidak dimengerti (*cipherteks*). Sedangkan dekripsi (*decryption*) atau *deciphering* merupakan proses mengembalikan pesan yang tidak dimengerti (*cipherteks*) menjadi pesan yang dimengerti (*plainteks*). Proses enkripsi dan dekripsi memerlukan suatu mekanisme dan kunci tertentu[2].

Hill Cipher

Hill cipher merupakan salah satu algoritma kriptografi *symmetric-key*. Algoritma *Hill Cipher* menggunakan matriks berukuran *m x m* sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam *Hill Cipher* antara lain adalah perkalian antar matriks dan melakukan invers pada matriks. *Hill Cipher* menggunakan matriks persegi sebagai kuncinya [3].

Hill Cipher mengambil matriks $k \in K$ berukuran $m \times m$ yang invertible sebagai kunci, dengan K adalah himpunan matriks-matriks persegi.

$$\begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix} = \begin{bmatrix} k_{1,1} & k_{1,2} & k_{1,3} & \cdots & k_{1,m} \\ k_{2,1} & k_{2,2} & k_{2,3} & \cdots & k_{2,m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{m,1} & k_{m,2} & k_{m,3} & \cdots & k_{m,m} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix}$$

Dengan kata lain fungsi enkripsinya adalah $y = kx$. Fungsi dekripsinya diturunkan dari formula diatas, karena $y = kx$, jika k^{-1} ada, maka dengan mengalikan kedua ruas dengan k^{-1} didapatkan

$$\begin{aligned} k^{-1}y &= k^{-1}(kx) \\ &= (k^{-1}k)x \text{ (sifat assosiatif)} \\ &= x \end{aligned}$$

Dalam Penelitian ini matriks yang akan digunakan sebagai kunci adalah matriks 3x3, sedangkan karakter yang akan digunakan adalah Z_{36}. Berikut adalah tabel korespondensi antara huruf dan bilangan dalam Z_{36}.

Tabel 1. Korespondensi antara huruf dan bilangan dalam Z_{36}

Karakter	A	B	C	.	.	F
Penomoran	0	1	2	.	.	5
Karakter	M	N	O	.	.	R
Penomoran	12	13	14	.	.	17
Karakter	Y	Z	1	.	.	4
Penomoran	24	25	26	.	.	29

QR-Code

QR Code (*Quick Response Code*) merupakan *barcode* matriks atau *barcode* dua dimensi yang dikembangkan oleh perusahaan Jepang, Denso-Wave, pada tahun 1994 dengan tujuan awal sebagai simbol yang mudah dibaca oleh peralatan pemindai. *QR Code* Berisi data baik dalam dua arah yaitu vertikal dan horisontal. Sedangkan *barcode* hanya berisi data dalam satu arah. *QR Code* memiliki kapasitas yang jauh lebih besar dibandingkan dengan *bar code*[4][5].

QR Code memiliki versi-versi simbol yang berkisar dari versi 1 sampai versi 40. Setiap versi memiliki konfigurasi modul atau jumlah modul yang berbeda. Modul merupakan titik-titik berwarna hitam dan putih yang membentuk *QR Code*. Konfigurasi modul merupakan jumlah modul yang berada pada satu simbol, dimulai dari versi 1 dengan 21 x 21 modul sampai versi 40 dengan 177 x 177 modul.

QR Code menggunakan algoritma Reed-Solomon untuk mengoreksi error apabila kode QR tersebut rusak atau kotor. Kemampuan koreksi *error QR Code* memiliki empat tingkat seperti yang dijelaskan pada tabel berikut ini,

Tabel 2 Kemampuan koreksi *error QR Code*

Tingkat	Perkiraan Kemampuan Koreksi *Error*	Penggunaan
L (*Low*)	7%	Lingkungan pabrik bersih dengan jumlah data yang besar.
M (*Medium*)	15%	Semua lingkungan pabrik (paling banyak digunakan)
Q (*Quality*)	25%	Lingkungan pabrik dimana *QR Code* menjadi kotor.
H (*High*)	30%	

Metode Sistem

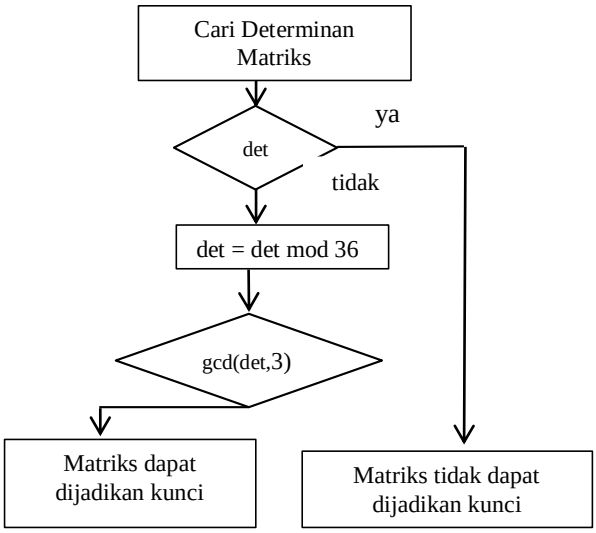
Secara Garis besar metode yang digunakan adalah membuat *QR-Code* dari hasil enkripsi kode tiket. *QR-Code* yang telah dibuat tersebut nantinya akan dicetak pada tiket. Sistem ini menggunakan bantuan program *QuickMark* dalam proses pembacaan isi *QR-Code* . Setelah isi dari *QR-Code* didapat, akan dilakukan proses dekripsi terhadap isi dari *QR-Code* tersebut sehingga didapatkan kembali kode tiket. kode tiket yang didapat dari hasil dekripsi akan di cocokan dengan *database* yang ada.

Perancangan Sistem

Sistem pengamanan tiket ini terdiri dari beberapa bagian, yaitu: proses penentuan kunci, proses *input* data, proses enkripsi, proses *generate QR-Code*, proses pencetakan tiket, proses pembacaan isi *QR-Code* dan proses dekripsi.

Proses Penentuan Kunci

Berikut ini adalah algoritma pemilihan matriks untuk dijadikan kunci dalam metode *Hill Cipher*.



Gambar 5. Algoritma pemilihan kunci

Proses Pembuatan Kode Tiket

Proses Pembuatan kode tiket dapat dilihat

Gambar 7. Keterangan kode tiket

Proses Enkripsi

Proses enkripsi pada penelitian ini menggunakan metode *Hill Cipher* dengan Z_{36} dan kunci matriks berukuran 3*x*3. Z_{36} dapat dilihat pada Tabel 1.

Proses *Generate QR-Code*

Setelah proses enkripsi didapatlah *cipher* teks. Dari *cipher* teks tersebut akan dibuat sebuah *QR-Code.* Proses *generate QR-Code* dilakukan dengan menggunakan sebuah *library*. *Library* yang digunakan adalah *Messaging Toolkit.QRCode*.

Proses Pencetakan Tiket

Setelah data tentang pembeli telah didapatkan dan kode tiket telah dienkripsi lalu dimasukan kedalam *QR-Code*, kemudian tiket tersebut dicetak. Sebelum dicetak, sebagian data dari pembeli tiket serta *QR-Code* yang telah dibuat akan ditaruh didalam tiket. Tampilan dari tiket seperti gambar 8.

Gambar 8. Tampilan tiket

Proses Pembacaan Isi *QR-Code*

Dalam makalah ini isi dari *QR-Code* dibaca melalui *webcam* dengan menggunakan sebuah *software* yaitu *QuickMark v3.8.0 r5017*. Setelah isi dari *QR-Code* didapat, isi dari *QR-Code* ini akan disalin secara manual kedalam aplikasi sistem keamanan tiket ini.

Proses Dekripsi

Sama halnya dengan proses enkripsi, proses dekripsi pada makalah ini juga menggunakan metode *Hill Cipher* dengan Z_{36} dan kunci matriks berukuran 3*x*3 yang sebelumnya digunakan dalam proses enkripsi. Proses dekripsi ini bertujuan untuk mengubah *cipher* teks yang didapatkan dari proses pembacaan *QR-Code* menjadi *plain* teks.

Setelah didapatkan *plain* teks yang sebenarnya adalah kode tiket, akan dicari pada *database* yang ada berdasarkan kode tiket yang telah terdekripsi. jika data ditemukan dan setiap datanya cocok maka tiket itu adalah tiket asli. Jika data tidak ditemukan maka kemungkinan besar tiket itu adalah tiket palsu.

III. HASIL DAN PEMBAHASAN

Pada saat menjalankan aplikasi sistem keamanan pada tiket menggunakan teknologi *QR-Code* dan kriptografi akan ditampilkan *form* utama. Tampilan form utama dapat dilihat dalam gambar 9. Dalam *form* utama *user* dapat melihat status tiket dan juga kunci yang sedang digunakan. Pada *form* utama *user* juga dapat langsung melakukan proses pendaftaran tiket atau memilih untuk melakukan proses pemilihan kunci, proses *database*, dan proses pengecekan tiket hanya dengan menekan judul yang ada pada bagian atas *form* utama. Semua proses tersebut akan dijelaskan pada sub bab berikut.

Gambar 9. Tampilan *form* utama

Pilih Kunci

Saat program pertama kali dijalankan, yang harus di lakukan adalah pemilihan kunci. Kunci yang telah dipilih nantinya akan digunakan dalam proses kriptografi.

Gambar 10. Tampilan *form* pemilihan kunci.

Berdasarkan gambar 10 kita dapat melihat terdapat dua pilihan yaitu kunci baru dan kunci terkahir yang digunakan. Dalam proses ini *user* hanya dapat memilih satu. Jika memilih kunci baru maka *user* diharuskan mengisi angota - angota matriks pada kotak yang telah disediakan. Jika matriks yang diisi tadi bisa dijadikan kunci maka kunci dalam program ini akan berubah. Namun apabila *user* memilih pilihan yang lainnya, maka kunci yang digunakan adalah kunci yang sedang digunakan atau dengan kata lain *user* tidak merubah kunci.

Pendaftaran

Setelah pemilihan kunci selesai *user* akan langsung terhubung dengan *form* utama. Tampilan *form* utama dapat dilihat pada gambar 9. *User* dapat melakukan pendaftaran tiket dengan cara mengklik tombol DAFTAR BARU lalu mengisikan data pembeli sesuai dengan data yang dibutuhkan. Setelah mengisi data pembeli, *user* harus mengeklik tombol GENERATE KODE TIKET untuk mendapatkan kode tiket. Jika sudah selesai *user* harus mengeklik tombol SELESAI. Setelah itu akan muncul tampilan tiket yang berisikan data dari pembeli dan juga *QR-Code* yang berisi hasil enkripsi kode tiket dari pembeli serta tanggal tiket tersebut dicetak. Tampilan tiket dapat dilihat pada gambar 11. Selanjutnya untuk mencetak tiket, *user* harus mengeklik tombol yang bergambar *printer* yang ada di pojok kanan bawah dari tampilan tiket yang muncul tadi. Setelah tiket tercetak *user* akan terhubung kembali dengan *form* utama.

Gambar 11. Tampilan tiket

Cek Tiket

Saat *user* mengeklik tombol CEK TIKET yang berada dibagian atas dari *form* utama maka akan langsung terhubung dalam *form* cek. Tampilan *form* cek dapat dilihat pada gambar 12.

Form cek ini digunakan untuk mengecek tiket apa tiket tersebut terdaftar atau tidak. Jika tidak terdaftar, ada kemungkinan tiket tersebut tiket palsu.

Gambar 12. Tampilan *form* cek

Dalam proses pengecekan tiket hal yang dilakukan adalah membaca *QR-Code* yang ada pada tiket menggunakan *webcam* dengan bantuan program *QuickMark. User* harus mengeklik tombol BACA QR-CODE yang ada dalam *form* cek untuk melakukan pembacaan *QR-Code.* Setelah muncul program *QuickMark user* harus menempatkan *QR-Code* yang ada di tiket pada webcam sampai *QR-Code* tersebut terbaca oleh *QuickMark.* setelah itu *user* harus menyalin isi dari *QR-Code* yang telah berhasil dibaca program *QuickMark* tadi kedalam *textbox* yang tersedia pada *form* cek. Kemudian untuk memeriksa apakah tiket tersebut terdaftar atau tidak, *user* harus mengeklik tombol PERIKSA yang ada dalam *form* cek. Jika tiket tersebut terdaftar maka akan muncul data diri dari pembeli tiket.

Gambar 13. Proses pembacaan *QR-Code* dengan bantuan program *QuickMark*

Database

Dalam program ini *user* bisa melihat dan menghapus data pembeli yang telah terdaftar dalam *database* dengan cara mengeklik tombol DATABASE yang berada dibagian atas *form* utama atau *form* cek.

IV. KESIMPULAN

1. Dengan menggabungkan metode kriptografi dengan *QR-Code* dapat dibuat suatu aplikasi penjualan tiket yang telah dapat meminimalisir pemalsuan tiket dan pencatutan tiket. Metode yang dilakukan adalah dengan mengenkripsi kode yang ada pada tiket lalu memasukannya kedalam *QR-Code*. Cara mengecek tiket adalah dengan membaca isi dari *QR-Code* menggunakan *webcam* lalu mendekripsikan kode yang didapat kemudian mencocokannya dengan data yang ada.
2. Metode *Hill Cipher* dengan kunci matriks berukuran 3x3 ini dapat meningkatkan keamanan pada tiket.

DAFTAR PUSTAKA

[1]. Menezes, A., Oorschot, P., dan Vanstone, A. 1996. *Handbook of Applied Cryptography.* New York: CRC Press, Inc.

[2]. Munir, R. 2006. *Kriptografi*. Bandung: Penerbit Informatika.

[3]. Anton, H. 2000. *Dasar – Dasar Aljabar Linear Jilid 1*, Edisi ke 7. Jakarta: Penerbit Interaksara.

[4]. Rahmawati, A. dan Rahman, A. 2014. *Sistem Pengamanan Keaslian Ijasah Menggunakan QR-Code dan Algoritma Base64.* http://is.uad.ac.id/jusi/files/10-JUSI-Vol-1-No-2-Sistem-Pengamanan-Keaslian-Ijasah.pdf (diakses tanggal 16 April 2015)

[5]. http://www.qrcode.com/en (diakses tanggal 28 Juni 2015)