Algoritma RSA Kombinasi dan Skema QR Code untuk Mengamankan Data Penjualan Tiket Online

Al Farissi
Teknik Informatika
Universitas Sriwijaya
Palembang, Indonesia
alfarissi@unsri.ac.id

Muhammad Fachrurrozi
Teknik Informatika
Universitas Sriwijaya
Palembang, Indonesia
mfachrz@unsri.ac.id

Kanda Januar Miraswan
Teknik Informatika
Universitas Sriwijaya
Palembang, Indonesia
kandajm@ilkom.unsri.ac.id

Anna Dwi Marjusalinah
Teknik Informatika
Universitas Sriwijaya
Palembang, Indonesia
annadm@ilkom.unsri.ac.id

Redo Jufarda
Teknik Informatika
Universitas Sriwijaya
Palembang, Indonesia
redojj@gmail.com

***Abstract*— Kriptografi adalah bidang ilmu komputer untuk menjaga keamanan data dan informasi. Salah satu penerapan kriptografi adalah mengamankan data penjualan tiket elektronik pada penjualan *online* tiket pertandingan sepak bola. Pada penelitian ini, penulis menerapkan skema pengamanan data penjualan dengan metode pengamanan menggabungkan algoritma RSA dan QR Code. Selanjutnya, algoritma RSA yang digunakan akan mengubah data tiket teks polos asli (*plaintext*) ke dalam bentuk lain yang tidak dapat dipahami (*ciphertext*). Data pembelian yang telah di enkripsi akan dikonversi menjadi QR *Code*. Kode ini digunakan oleh pembeli untuk memverifikasi data sebelum memasuki stadion. Dari hasil pengujian dengan perangkat lunak menunjukkan bahwa algoritma RSA dan QR Code dapat diterapkan pada keamanan data tiket**

Keyword—Tiket elektronik, kriptografi, algoritma RSA, QR *Code*.

Sepak bola adalah olahraga paling populer di Indonesia. Penjualan tiket manual dan jumlah counter terbatas bisa menyebabkan antrian panjang penonton. Tiket elektronik merupakan solusi untuk memecahkan masalah tersebut. Namun, penggunaan tiket elektronik membutuhkan teknik pengamanan untuk melindungi data transaksi. Internet sebagai salah satu media pertukaran informasi sangat tidak ama. Penyadapan, menguping, pemalsuan data, pencurian informasi dapat terjadi selama proses pertukaran di internet. Tiket elektronik memiliki potensi serangan data yang tinggi, tiket bisa dipalsukan. Maka dibutuhkan skema keamanan untuk memastikan transaksi berjalan dengan baik. Kriptografi dapat digunakan untuk memecahkan masalah keamanan.

Penelitian ini menggunakan Algoritma RSA pada proses enkripsi data pembelian. Algoritma RSA mengunakan pasangan kunci dari perkalian dua bilangan prima. Letak keamanan RSA teletak pada sulitnya untuk memfaktorkan bilangan besar menjadi faktor primanya[1]. Data hasil enkripsi kemudian disimpan pada *sebuah QR Code.* Penggunaan *QR Code* ditujukan sebagai media penyimpanan data tiket yang terenkripsi pada tiket yang dicetak. Kemudian QR Code ini akan digunakan pembeli untuk melakukan verifikasi tiket pada hari pertandingan.

II. CRYPTOGRAPHY

Algoritma kriptografi adalah fungsi matematis [illegible] dekripsi, bahwa kriptografi adalah seni dan sains untuk menjaga keamanan pesan [1].

Empat faktor penting yang perlu dipertimbangkan dalam kriptografi meliputi: [2]:

i. Kerahasiaan atau privasi adalah layanan untuk menyimpan semua informasi dari semua orang kecuali mereka yang memiliki hak untuk mengaksesnya. Ada banyak pendekatan untuk memberikan kerahasiaan, mulai dari perlindungan fisik hingga algoritma matematis

ii. Integritas data adalah layanan yang menyimpan data sehingga tidak ada perubahan pihak yang tidak memiliki hak. Untuk memastikan integritas data, harus memiliki kemampuan mendeteksi manipulasi data dari pihak yang tidak memiliki hak. Manipulasi data seputar penambahan (*insertion*), penghapusan (*deletion*), dan penggantian (*substitution*).

iii. Otentikasi adalah layanan yang berhubungan dengan identifikasi. Fungsi ini berlaku untuk entitas dan informasi itu sendiri. Kedua pihak harus saling berkomunikasi satu sama lain untuk saling mengenal. Informasi dikumpulkan dari saluran yang akan diidentifikasi asal, tanggal, isi data, waktu pengiriman, dan lain sebagainya. Untuk alasan ini, kriptografi biasanya dibagi menjadi dua kelas utama: otentikasi entitas dan otentikasi asal. Autentikasi asal data secara implisit memberikan integritas data.

iv. Non-penolakan adalah layanan yang mencegah entitas menolak komitmen atau tindakan sebelumnya. Ketika terjadi perselisihan sehubungan dengan entitas yang menolak tindakan tertentu telah dilakukan, sebuah cara untuk menyelesaikan situasi ini akan dibutuhkan.

Kriptografi dibagi menjadi dua bagian, kriptografi klasik dan kriptografi modern. Kriptografi modern bergantung pada kekuatan kriptografi kunci kerahasiaan. Ada dua strategi bagaimana enkripsi bekerja yaitu enkripsi simetris dan enkripsi asimetris. Keduanya menggunakan algoritma matematis yang dikenal sebagai kunci.

Kriptografi modern memiliki dua tipe kunci, yaitu:

i. Kunci Simetris (*Symetric Key*)

Untuk enkripsi simetris, menggunakan kunci yang sama untuk enkripsi dan dekripsi, sedangkan enkripsi asimetris mengharuskan setiap orang untuk memiliki satu kunci publik dan satu kunci pribadi. Enkripsi simetris berfungsi selama pengirim dan penerima memiliki kunci untuk mengenkripsi atau mendekripsi pesan. Algoritma kriptografi yang menggunakan kunci simetris adalah DES, IDEA, Blowfish, RC2, SEAL, TripleDES, Rijndael, dll.

ii. Kunci Asimetri (*Asymetric Key*)

Kunci asimetris menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Kunci yang digunakan untuk enkripsi disebut kunci publik dan kunci untuk dekripsi disebut kunci privat. Kunci publik bukan rahasia, artinya bisa diketahui siapa saja. Kegunaan kunci publik adalah mengenkripsi data yang akan dikirim ke pemilik kunci, sedangkan kunci privat adalah kunci rahasia yang hanya diketahui oleh pemiliknya. Kegunaan kunci privat adalah mendekripsi data yang diterima dalam keadaan terenkripsi. Contoh algoritma kriptografi simetris adalah RSA, McEliece, Pohlig-Helman, Knapsack, dan lain-lain.

Algoritma kriptografi simetris dapat dikelompokkan menjadi dua kategori [8]:

i. Stream Chiper

Stream cipher adalah algoritma kriptografi dimana teks cipher output dihasilkan sedikit demi sedikit atau byte per byte pada stream input plain text. Contoh untuk stream cipher: RC4, Seal, A5, Oryx, dll.

ii. Block Cipher

Block cipher adalah algoritma kriptografi dimana blok bit (biasanya 64 atau 128) secara keseluruhan mengubah teks biasa menjadi blok teks cipher dengan menggunakan panjang kunci yang sama. Contoh untuk block cipher: Blowfish, AES, DES, GOST, IDEA, RC5, XTEA, Square, Two fish, RC6, Loki97, RSA.

III. ALGORITMA RSA DAN QR *CODE*

1) PEMBANGKITAN KUNCI

Pembentukan pasangan kunci public dan privat pada algoritma rsa dibentuk dari perkalian dua bilangan prima[3]. Dengan tahapan sebagai berikut:

1. Pilih dua bilangan prima secara sembarang p dan q. contoh p=47 dan q=43.
2. Hitung n= p x q. n= 1591.
3. Hitung M=(p-1)(q-1). M=1512
4. Pilih e yang memenuhi FPB(m,e)=1. e = 47.
5. Hitung d dengan persamaan. ed=1(mod m). d=41.

Pasangan kunci (e,n) adalah kunci public dan (d,n) adalah kunci privat.

2) ENKRIPSI ALGORITMA RSA

Enkripsi akan mengubah plainteks (m) menjadi cipherteks (c). Proses enkripsi pada RSA dilakukan dengan menggunakan persamaan

$$c = m^e \bmod n$$

Contoh : untuk melakukan enkripsi huruf "r".

3) DEKRIPSI ALGORITMA RSA

Dekripsi proses pengubahan cipherteks menjadi plainteks. Proses dekripsi RSA dilakukan dengan menggunakan persamaan

$$m = c^d \bmod n$$

Contoh proses dekripsi.

$m = 435^{1319} \pmod{1591} = 114$, ubah menjadi karakter asalnya 'r'.

4) PEMBANGKITAN QR CODE

QR Code dapat menyimpan data berupa data bertipe numerik, alphanumerik, binary, dan kanji[4]. Untuk membuat *QR Code* pertama kita membuat string data bit. String ini berasal dari pesan yang akan disimpan dalam hal ini hasil enkripsi dan informasi tipe *QR Code* apa yang dipakai. Tahapan selanjutnya membuat koreksi kesalahan. QR Code menggunakan *Reed-Solomon Code Error Correction*[5].

Setelah membuat string bit dan koreksi kesalahan tahapan selanjutnya adalah data masking. Proses ini akan menyusun modul hitam dan putih agar jumlahnya seimbang[6]. Tahapan selanjutnya akan membuat keterangan format dan versi QR Code yang dipakai. Format ini merupakan perpaduan dari tipe *error-correction* dan aturan masking yang dipakai, sedangkan version merupakan ukuran data yang disimpan.

Berikut contoh string data bit:

1. Input data berupa alphanumeric “1318 8”
2. Ubah menjadi grup dua nilai decimal

Jumlah	Binary (v1*45+v2)
(1,3)	48 00000110000
(1,8)	53 00000110101
(,8)	1628 11001011100

3. Ubah jumlah karakter menjadi biner
6. → 000000110
4. Tambah mode indikator, dalam contoh ini adalah 0010.
5. Kemudian susun secara sekuensial 0010 000000110 00000110000 00000110101 11001011100

Penelitian ini akan menggunakan Library ZXing pada proses pembuatan QR Code. ZXing merupakan *open source library* java yang mampu memproses berbagai format barcode[6].

IV. ANALISIS PERANGKAT LUNAK

Perangkat lunak ini mampu mengenkripsi dan mendekripsi data pembelian tiket. Sebelum data disimpan, data pertama kali dienkripsi untuk menyimpannya secara pribadi. Data sebagai cipher-state akan disimpan dalam basis data.

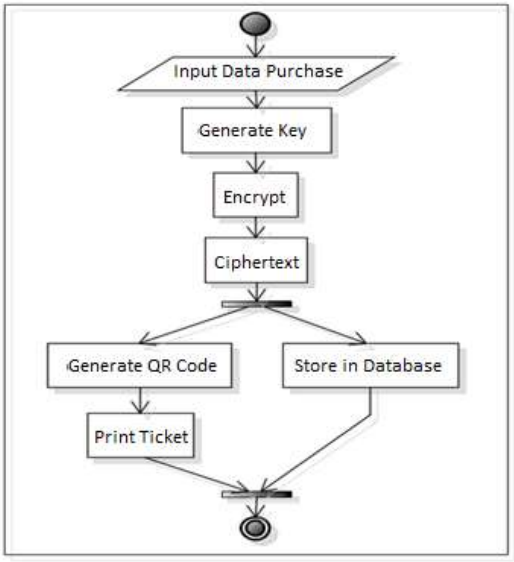

Figure I Skema Perangkat Lunak

Dari skema di atas, proses enkripsi data tiket, dilakukan sebelum data tiket dibangkitkan menjadi tiket berupa QR Code. Selanjutnya, QR Code diperoleh dari konversi ciphertext menjadi barcode dua dimensi. Algoritma kriptografi ini digunakan untuk mengamankan data pembelian tiket. Data yang aman adalah: nama, nomor identifikasi, alamat, nomor telepon, tanggal dan waktu pertandingan, jumlah tiket, dan posisi duduk. Data ini akan dikonversi bentuk string dengan karakter "-" sebagai pemisah antar variabel.

Contoh:"redojf-RedoJufarda-1771031006920001-Sriwijaya FC-Semen Padang-082374705389-1X25000---"

V. TEST RESULT

Tabel 1 menunjukkan hasil implementasi algoritma RSA dan kemudian hasil enkripsi diubah menjadi QR Code. Panjang kunci yang digunakan dalam pengujian adalah 128, 256, 512. Tabel berisi plaintext, kunci yang digunakan, ciphertext, dan QR Code.

Berdasarkan hasil eksperimen QR Code, penulis tidak mengalami masalah dalam proses enkripsi, membuat QR Code, dan proses membaca dan dekripsi. Dari segi keamanan dapat dilihat data yang tersimpan dalam QR Code berbeda dengan plaintext dan isinya tidak dapat dipahami. Semakin lama kunci yang digunakan, semakin sulit untuk memecahkan keamanannya.

QR Code memiliki fitur koreksi kesalahan dengan empat tingkat koreksi: L (7%), M (15%), Q (25%), H (30%). Koreksi kesalahan ini menggunakan algoritma reed-solomon untuk mengatasi kerusakan yang disebabkan oleh kotor atau rusak. Sedangkan daya tahan QR Code ditentukan pada kondisi QR Code yang dicetak. Tabel 2 menunjukkan kekokohan QR Code yang dicetak terhadap kerusakan.

ISBN : 979-587-705-4
Vol. 3 No. 1

TABEL I

PENGUJIAN

Plaintext	Key	Ciphertext	QR Code
redojf-Redo Jufarda- 177103100692 0001- Sriwijaya FC VS Semen Padang-Jalan Sarjana no.99 Timbangan, Indralaya-	128 bit N : 7524953653580073034564243722093402667094442479 19513180318097032494989 99939261 E: 23846374679448581074917047921306239 1077	5306535605599114416738013492750830176203402564967473830800318672411841835313974819331366599923976332927488168665394569323703450139556343737466544046129565 35342058123573200264606655861387876732283382664938043002632757864154671223353722289302670869781292739982461338019072434927780509446653232220910408739219538410607785541839218379210265930939683821026529267951307664185107005389833790	
redojf-Redo Jufarda- 177103100692 0001- Sriwijaya FC VS Semen Padang-Jalan Sarjana no.99 Timbangan, Indralaya- 082374705389 - 2X25000---	256 bit N: 374098322984062827232800828849226842723262956118686030199290662914115623838007459350019727365883793202099306672577191434862686111801639578 7767488498952283 E: 94057512243870547158123966962810541422012769510223578780161191155857242241623	30489949459478860921390823389208399407968596246815005569048509001709821169129630462811668561045752205893176454626886918113616307467856472965925651783514192169743323888594012164433278036155778221666145780978959748152417758707709551233392078902744527700744999056362162142117233742500938249654042272072904163382 22690446912786374482748309924844161806849975552423610619187190925524877140775712913290827578936430654425810076540741010005445781893479186300276301030679 87	
redojf-Redo Jufarda- 177103100692 0001- Sriwijaya FC VS Semen Padang-Jalan Sarjana no.99 Timbangan, Indralaya- 082374705389 - 3X25000---	512 bit N : 73945170712749846949993 18920956154327956914989 86508367672397157787478 48494016260120526488512 64939304964485175484828 25102554281968031150629 44360094126061620684050 28714177387909963283864 87834312984519518252115 33559617345898993444203 84116128823311565605624 29141741875969714127464 82831060725889316612915 626795619 E: 86277011552808990411781 4 830012762271775406196672 308012838873373471373906 304615727494562147810917 876677316067726065508820 621852076599610058080849 5143772541	63313970801503996959186696369762134994387458092622464395273758442429555659502569178951598560009600057379223408350713220932138386610114938833459654096338137147952712464225037369298992566373341342585351398853452003327820657542378632064104015992312582172802546799041851990286079654005550570061389454736260014622 10111623609738098573599772584308216780175137567371661524195567155177570255280509788881201054328322301400269934718780433538173342093865214943520591073702955485607822775666333502464767650324740660514567671439174918254495373090714665958612792273345699743732948648633228161818816556022303652105574866634769911421	

TABEL II

QR CODE *Robustness*

QR Code	Testing Result
	Terbaca
	Terbaca

	Tidak Terbaca
	Tidak Terbaca
	Tidak Terbaca

Dari hasil pengujian terhadap ketahanan didapat *QR Code* mampu bertahan pada setiap kerusakan kecuali kerusakan yang terjadi pada *finder pattern* / pola pengenal yang telatak pada sudut sudutnya. *QR Code* tidak mampu untuk dibaca dikarenakan pola untuk mengenali *QR Code* tidak ditemukan.

IV.KESIMPULAN

Dari hasil penelitian yang dilakukan dapat disimpulkan:

1. Aplikasi algoritma RSA memberikan keamanan data tiket sehingga tidak mudah dibaca.
2. Kode QR mampu menyimpan data yang dienkripsi menggunakan kunci 128, 256, dan 512 bit.
3. Hasil uji bacaan QR Code menunjukkan tidak ada data yang mengandung kesalahan yang ditemukan pada proses dekripsi.
4. Kode QR dapat bertahan dalam menangani kerusakan selain kerusakan pola pola penemu / identifikasi di sudutnya.

DAFTAR PUSTAKA

[1] Scheiner, Bruce. 1996. *Applied Cryptography, Second Edition: Protocols, Algorithm, and Source Code in C.* John Wiley & Sons, Inc.

[2] Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A. (1997). Handbook of Applied Cryptography. CRC Press. pp. 107–109. ISBN 0-8493-8523-7.

[3] Zhang, Mu., Yao, D., and Zhou, Q. 2012. *The Application and Design of QR Code in Scenic Spot's eTicketing System –A Case Study of Shenzhen Happy Valey. International Journal of Science and Tehnology,* Volume 2 No.12 December 2012.

[4] ISO/IEC 18004. 2000. *Information Technology – Automatic Identification and Data Capture Techniques – Bar Code Symbology – QR Code*. Switzerland : International Standard

[5] Dey. S, Nath. B.J, and Nath.C.A. A New Technique to Hide Encrypted Data in QR Code.

[6] Ariadi. 2011. Analisis Dan Perancangan Kode Matriks Dua Dimensi Quick Response (QR) Code. Universitas Sumatera Utara.

[7] Zxing *Zebra Crossing* (Zxing), https://github.com/zxing/zxing , *accessed on* December 5th 2014

[8] Stallings, W. (2005). Cryptography and Network Security (4th Edition). :Prentice Hall