Enkripsi Pada QR Code Tiket Dengan RSA

Calvin Irwan 13507010
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If17010@students.if.itb.ac.id

Abstrak— **Tiket adalah alat identifikasi yang paling sering digunakan pada setiap event ataupun pada sebuah pelayanan jasa, seperti tiket musik, tiket seminar, tiket pesawa, tiket kereta api, dan tiket sepak bola. Karena mahalnya harga tiket, akhirnya banyak sekali oknum yang tergiur untuk mencari untung, seperti terjadi pemalsuan tiket sepak bola yang akhir ini marak terjadi dan pemalsuan tiket konser Justin Bieber yang kemarin baru melakukan konser. Seringkali tiket palsu tersebut juga tidak dapat teridentifikasi kepalsuannya oleh pihak penyelenggara dan akhirnya bisa menikmati pertunjukan. Oleh karena itu pada makalah ini akan dibuat sebuah mekanisme perlindungan tiket dengan cara enkripsi menggunakan RSA, karena RSA merupakan algoritma enkripsi reversible. Tiket ini nantinya akan dienkripsi dengan kunci yang dimiliki oleh pemilik itu sendiri seperti nomor KTP sebagai salah satu contohnya, kemudian dicetak dengan barcode yang merupakan hasil enkripsi tersebut. Pada saat tiket ditunjukan, QR code akan didekripsi menjadi sebuah data pribadi tersebut yang akan dicocokan dengan data pemilik tiket. Makalah ini akan menunjukan prototype program yang akan dibuat.**

***Kata Kunci*—Tiket, Enkripsi, RSA, QR code**

I. PENDAHULUAN

Konser musik, sepak bola, bola basket dan pertunjukan lainnya bila semua orang boleh menontonnya maka pasti akan terjadi kekacauan dan ketidak teraturan, apalagi bila pertunjukan tersebut dilakukan oleh seseorang atau grup yang terkenal. Sama halnya dengan pesawat, kereta, semua hal itu memerlukan sebuah mekanisme untuk mengatur itu semua.

Pada akhirnya ditemukanlah sebuah mekanisme identifikasi yaitu dengan menggunakan sebuah alat sederhana yaitu sebuah tiket, tiket sudah menjadi alat untuk transaksi yang sangat umum karena simplisitasnya. Namun karena sederhananya dan tergiurnya oknum-oknum yang tidak bertanggung jawab dengan tingginya harga tiket, tiket menjadi marak dipalsukan.

Banyak sekali berita tentang tiket palsu yang beredar seperti kutipan berita dibawah ini

"Antusias penggemar terhadap konser Bieber di Indonesia memang sangat tinggi. Banyak fans Tanah Air yang masih bingung untuk mendapatkan tiket konser idola mereka. Tak heran jika kemudian muncul pihak-pihak yang memanfaatkan.

Seperti yang dialami oleh Yadi yang ingin membeli tiket konser Bieber untuk anaknya. Mendapat info dari seorang teman, ia pun mengunjungi situs http://marygops.webs.com/ untuk melakukan pemesanan tiket secara online

Yadi kemudian menghubungi nomor yang tertera di situs tersebut untuk melakukan pembayaran atas tiket yang dipesan. Namun ia merasa ada keanehan usai mendapatkan jawaban dari nomor telepon tersebut. Yadi pun membatalkan rencananya untuk membeli tiket dari situs itu.

Situs tersebut mengaku sebagai promotor Marygops Studios yang melakukan penjualan tiket secara online. Padahal, sistem penjualan tiket secara online hanya dijual secara eksklusif di www.rajakarcis.com. Promotor akan menjual 6 ribu tiket pada 20 Maret 2011."

II. TEORI DASAR

2.1 Kriptografi

Kata cryptography berasal dari bahasa Yunani: krupto (hidden atau secret) dan grafh (writing) Artinya "secret writing"

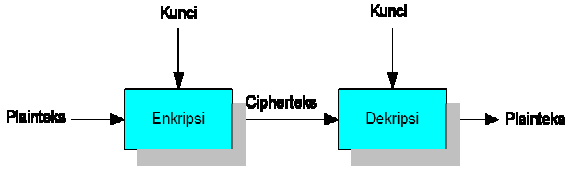
Definisi lama: Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.

Definisi baru: Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*message*) [Schneier, 1996].

Algoritma kriptografi (*cipher*)
- aturan untuk enchipering dan dechipering, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi pesan. "art and science to keep message secure"
Kunci: parameter yang digunakan untuk transformasi enciphering dan dechipering. Jika kekuatan kriptografi

ditentukan dengan menjaga kerahasiaan algoritmanya, maka algoritma kriptografinya dinamakan algoritma restricted.

Algoritma resricted tidak cocok lagi saat ini. Kriptografi modern mengatasi masalah ini dengan menggunakan kunci. Kunci bersifat rahasia (secret), sedangkan algoritma kriptografi tidak rahasia (public).



Gambar 2.1 Skema Kriptografi

2.1.1 Algoritma RSA

Di bidang kriptografi adalah sebuah algoritma pada enkripsi public key. RSA merupakan algoritma pertama yang cocok untuk digital signature seperti halnya ekripsi, dan salah satu yang paling maju dalam bidang kriptografi public key. RSA masih digunakan secara luas dalam protokol electronic commerce, dan dipercaya dalam mengamnkan dengan menggunakan kunci yang cukup panjang.

2.1.2 Sejarah RSA

Algortima RSA dijabarkan pada tahun 1977 oleh tiga orang : Ron Rivest, Adi Shamir dan Len Adleman dari Massachusetts Institute of Technology. Huruf RSA itu sendiri berasal dari inisial nama mereka (Rivest—Shamir—Adleman).

Clifford Cocks, seorang matematikawan Inggris yang bekerja untuk GCHQ, menjabarkan tentang sistem equivalen pada dokumen internal di tahun 1973. Penemuan Clifford Cocks tidak terungkap hingga tahun 1997 karena alasan top-secret classification.

Algoritma tersebut dipatenkan oleh Massachusetts Institute of Technology pada tahun 1983 di Amerika Serikat sebagai U.S. Patent 4405829. Paten tersebut berlaku hingga 21 September 2000. Semenjak Algoritma RSA dipublikasikan sebagai aplikasi paten, regulasi di sebagian besar negara-negara lain tidak memungkinkan penggunaan paten. Hal ini menyebabkan hasil temuan Clifford Cocks di kenal secara umum, paten di Amerika Serikat tidak dapat mematenkannya.

Gambar 2.2 RonRivest

Gambar 2.3 Adi Shamir

Gambar 2.2 Len Adlemen

2.1.3 Cara Kerja RSA

Semisal Alice berkeinginan untuk mengizinkan Bob untuk mengirimkan kepadanya sebuah pesan pribadi (private message) melalui media transmisi yang tidak aman (insecure). Alice melakukan langkah-langkah berikut untuk membuat pasangan kunci public key dan private key:

Pilih dua bilangan prima p ≠ q secara acak dan terpisah untuk tiap-tiap p dan q. Hitung N = p q. N hasil perkalian dari p dikalikan dengan q.

Hitung φ = (p-1)(q-1).

Pilih bilangan bulat (integer) antara satu dan φ (1 < e < φ) yang juga merupakan coprime dari φ.

Hitung d hingga d e = 1 (mod φ).

bilangan prima dapat diuji probabilitasnya menggunakan Fermat's little theorem- a^(n-1) mod n = 1 jika n adalah bilangan prima, diuji dengan beberapa nilai a menghasilkan kemungkinan yang tinggi bahwa n ialah bilangan prima. Carmichael numbers (angka-angka Carmichael) dapat melalui pengujian dari seluruh a, tetapi hal ini sangatlah langka.

langkah 3 dan 4 dapat dihasilkan dengan algoritma extended Euclidean; lihat juga aritmetika modular.

langkah 4 dapat dihasilkan dengan menemukan integer x sehingga d = (x(p-1)(q-1) + 1)/e menghasilkan bilangan bulat, kemudian menggunakan nilai dari d (mod (p-1)(q-1));

langkah 2 PKCS#1 v2.1 menggunakan &lamda; = lcm(p-1, q-1) selain daripada φ = (p-1)(q-1)).

Pada public key terdiri atas:

N, modulus yang digunakan.
e, eksponen publik (sering juga disebut eksponen enkripsi).

Pada private key terdiri atas:

N, modulus yang digunakan, digunakan pula pada public key.
d, eksponen pribadi (sering juga disebut eksponen dekripsi), yang harus dijaga kerahasiaannya.

Biasanya, berbeda dari bentuk private key (termasuk parameter CRT):

p dan q, bilangan prima dari pembangkitan kunci.
d mod (p-1) dan d mod (q-1) (dikenal sebagai dmp1 dan dmq1).
(1/q) mod p (dikenal sebagai iqmp).

Bentuk ini membuat proses dekripsi lebih cepat dan signing menggunakan Chinese Remainder Theorem (CRT). Dalam bentuk ini, seluruh bagian dari private key harus dijaga kerahasiaannya.

Alice mengirimkan public key kepada Bob, dan tetap merahasiakan private key yang digunakan. p dan q sangat sensitif dikarenakan merupakan faktorial dari N, dan membuat perhitungan dari d menghasilkan e. Jika p dan q tidak disimpan dalam bentuk CRT dari private key, maka p dan q telah terhapus bersama nilai-nilai lain dari proses pembangkitan kunci.

2.1.4 Proses Enkripsi RSA

Misalkan Bob ingin mengirim pesan m ke Alice. Bob mengubah m menjadi angka n < N, menggunakan protokol yang sebelumnya telah disepakati dan dikenal sebagai padding scheme.

Maka Bob memiliki n dan mengetahui N dan e, yang telah diumumkan oleh Alice. Bob kemudian menghitung ciphertext c yang terkait pada n:

$$c = n^e \mod N$$

Perhitungan tersebut dapat diselesaikan dengan cepat menggunakan metode exponentiation by squaring. Bob kemudian mengirimkan c kepada Alice.

2.1.5 Proses Dekripsi RSA

Alice menerima *c* dari Bob, dan mengetahui *private key* yang digunakan oleh Alice sendiri. Alice kemudian memulihkan *n* dari *c* dengan langkah-langkah berikut:

$$n = c^d \mod N$$

Perhitungan diatas akan menghasilkan *n*, dengan begitu Alice dapat mengembalikan pesan semula *m*. Prosedur dekripsi bekerja karena

$$c^d \equiv (n^e)^d \equiv n^{ed} \pmod N.$$

Kemudian, dikarenakan $ed \equiv 1 \pmod{p-1}$ dan $ed \equiv 1 \pmod{q-1}$, hasil dari *Fermat's little theorem*.

$$n^{ed} \equiv n \pmod p$$

dan

$$n^{ed} \equiv n \pmod q$$

Dikarenakan *p* dan *q* merupakan bilangan prima yang berbeda, mengaplikasikan *Chinese remainder theorem* akan menghasilkan dua macam kongruen

$$n^{ed} \equiv n \pmod{pq}.$$

serta

$$c^d \equiv n \pmod N$$

III. IMPLEMENTASI

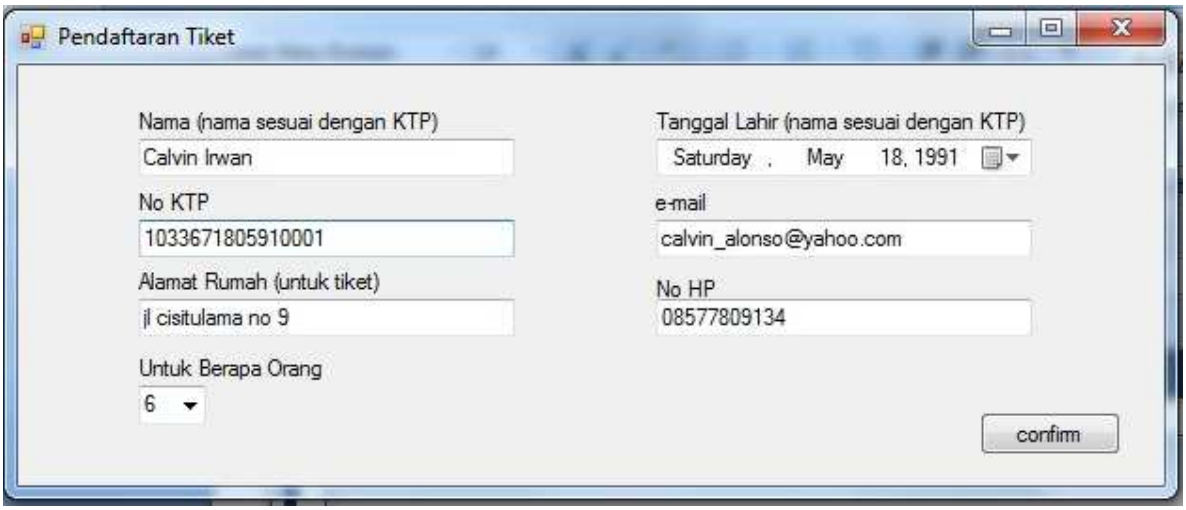
Saat ini diperlukan sebuah mekanisme perlindungan untuk tiket agar tidak dapat dipalsukan yaitu dengan cara memperbarui cara untuk membeli tiket, yaitu secara online dan juga memberi mekanisme enkripsi pada tiket dengan cara membuat sebuah QR code pada tiket. Dimana nantinya tiket tersebut akan di scan oleh pihak panitia untuk menjamin keaslian tiket tersebut.

Urutan langkah-langkah yang terjadi pada sistem ini adalah pertama pelanggan membuka website kemudian melakukan register pada website tersebut. Setelah itu bila pelanggan memilih layanan pesan tiket, maka akan muncul sebuah formulir tiket yang berisikan nama, no KTP, tanggla lahir, alamat, no HP dan alamat e-mail, yang baru dari form ini adalah adanya pertanyaan "untuk berapa orang" karena enkripsi yang dilakukan memanfaatkan nomor KTP sehingga fitur ini memberi kesempatan agar orang yang belum memiliki KTP untuk bisa diwakilkan oleh orang yang sudah memiliki KTP dan fitur ini juga bisa mempersingkat pengecekan pada saat pelanggan ingin menikmati pertunjukan agar pengecekan tiket tidak berlangsung satu persatu.

Pada tampilan pengecek QR code, ditampilkan P yang berupa 3 digit pertama dari No KTP dan Q yang berupa 3 digit kedua dari No KTP, kemudian barcode hasil scan yang berisikan cipher text dan nilai e. Dari seluruh data yang didapat dari atas, didekripsilah cipher text melalui nilai n dan d yang kemudian didapat.

Hasil dekripsi pada sistem ini berupa data pribadi yang dimasukkan pada form pendaftaran, pada makalah ini yang digunakan adalah nama dengan tanggal lahir.

3.1 Tampilan Antarmuka



Gambar 3.1 tampilan form pendaftaran

Gambar 3.2 tampilan form deteksi QR code

Gambar 3.3 tampilan Tiket yang dihasilkan

3.2 Penjelasan Cara Kerja Sistem

Berikut ini merupakan contoh dari enkripsi RSA dan dekripsinya. Parameter yang digunakan disini berupa bilangan kecil.

Kita membuat

p = 103 — bilangan prima pertama (harus dijaga kerahasiannya atau dihapus secara hati-hati)

q = 367 — bilangan prima kedua (harus dijaga kerahasiannya atau dihapus secara hati-hati)

N = pq = 37801— modulus (diberikan kepada publik)

e = 149 — eksponen publik (diberikan kepada publik)

d = 32321 — eksponen pribadi (dijaga kerahasiannya)

Public key yang digunakan adalah (e,N). Private key yang digunakan adalah d. Fungsi pada enkripsi ialah:

encrypt(n) = n^e mod N = n^149 mod 37801

dimana n adalah plaintext Fungsi dekripsi ialah:

decrypt(c) = c^d mod N = c^32321 mod 37801

dimana c adalah ciphertext

Untuk melakukan enkripsi plaintext bernilai "Calvin Irwan 18 05 91" kemudian bentuk string ini diubah dulu menjadi angka

“98476800601547620457925099526714292946749003675953”

encrypt(98476800601547620457925099526714292946749003675953) = 98476800601547620457925099526714292946749003675953 ^ 149 mod 37801 = 35176784360941950252482476531911521482580240710709756634 57

Untuk melakukan dekripsi ciphertext bernilai "a" perhitungan yang dilakukan

decrypt(35176784360941950252482476531911521482580240710709756634 57) = 35176784360941950252482476531911521482580240710709756634 57^32321 mod 37801 = 98476800601547620457925099526714292946749003675953 . Kemudian diubah menjadi text “Calvin Irwan 18 05 91”

Kedua perhitungan diatas diselesaikan secara effisien menggunakan square-and-multiply algorithm pada modular exponentiation.

Hal yang perlu diperhatikan pada sistem RSA ini adalah, belum tentu 3 digit pertama dan kedua dari seseorang tersebut bernilai prima oleh karena itu dibutuhkan bantuan oleh algoritma sederhana yaitu *primafinder* dimana algoritma ini akan menambah terus bilangan tersebut satu persatu hingga bilangan tersebut menjadi bilangan prima terdekat. Alasan pemilihan penggunaan 6 digit pertama dari nomor KTP menjadi nilai p dan q adalah hal angka tersebut nilainya berbeda di setiap kecamatan, dan di Indonesia ada sangat banyak kecamatan sehingga dinilai lebih unik dari nomor yang lain. Nilai dari N atau p x q tidak dicantumkan dimanapun pada tampilan karena cukup dengan menghitung nilai dari p dan q yang di input kedalam sistem.

No KTP menjadi variabel yang dipilih untuk menjadi kunci karena hal tersebut merupakan sesuatu yang pasti dimiliki setiap orang dewasa di Indonesia dan mempermudah saat pengecekan berlangsung, setelah pelanggan memberikan KTP diambil 3 digit pertama dan keduanya, kemudian setelah dekripsi dilakukan pihak penyelenggara, nama dan tanggal lahir langsung bisa dicek dengan KTP yang digunakan. Oleh karena itu nama dan tanggal lahir yang dimasukkan kedalam form pendaftaran harus sama dengan yang tercantum pada KTP.

Alamat dicantumkan pada pendaftaran bertujuan untuk tempat tiket dikirimkan oleh karena itu akan ada mekanisme untuk penutupan pembelian tiket H-3 sebelum acara, agar tidak ada pembeli yang belum mendapat tiket pada hari H.

Satu tiket dapat mencakup beberapa orang fitur ini sebenarnya diterapkan untuk menanggulangi anak-anak yang belum punya KTP dan ingin melihat pertunjukan, tapi secara tidak langsung fitur ini juga mempermudah pengecekan tiket agar tidak setiap orang dicek tiketnya. Batas orang yang bisa dicakup pertiket adalah sampai 10 orang, tentu harga tiket berbeda tergantung jumlah orang yang dicakup didalam tiket tersebut. Fitur ini juga dapat mencegah percaloan secara tidak langsung dan mencegah bila ada orang yang ingin menimbun tiket untuk dijual nantinya.

Cara untuk melakukan scaning QR code belum dieksplorasi karena fokus makalah ini adalah pada pengolahan RSA nya dan untuk membuat QR code yang benar-benar dapat di scan nampak sulit.

IV. KESIMPULAN

Kesimpulan dari makalah ini adalah dengan adanya enkripsi pada tiket dengan teknik RSA, tiket palsu dapat dicegah untuk bisa melewati pengecekan yang dilakukan oleh penyelenggara. Namun semua sistem memiliki kelebihan dan kekurangan.

Kelebihan dari sistem enkripsi QR code ini selain keamanannya adalah simplisitas pada tiket untuk beberapa orang dan hal tesebut juga bisa mencegah percaloan. Pembelian tiket menjadi teratur dan semua disimpan didalam data base apabila terjadi suatu masalah.

Kelemahan dari sistem ini adalah apabila ada suatu acara dimana perbandingan anak-anak dan orang tuanya cukup jauh sehingga jumlah anak yang dicakup tidak cukup dengan 10 orang, dalam menghadapi hal ini

mungkin dari pihak penyelenggara akan membuat regulasi tersendiri. Juga kelemahan yang cukup berarti pada sistem ini adalah waktu yang cukup lama dalam pengecekan QR code, namun bisa diatasi dengan cara membuka beberapa lokasi pengecekan tiket bila acara benar-benar besar.

Teknik penerapan RSA pada tiket sejauh ini masih terlihat cukup aman selama masyarakat tidak tahu cara kerja sistem. Namun pada akhirnya teknik enkripsi tiket menjadi QR code ini hanya sebuah pilihan dari banyak pilihan lainnya.

REFERENCES

[1] Munir. Rinaldi. Kriptografi. Institut Teknologi Bandung. 2006.

[2] *http://www.wikimu.com/News/DisplayNews.aspx?id=6834* diakses pada tanggal 1 Mei 2011 pukul 16.00

[3] http://en.wikipedia.org/wiki/RSA. diakses pada tanggal 1 Mei 2011 pukul 16.00

[4] http://www.di-mgt.com.au/rsa_alg.html diakses pada tanggal 3 Mei 2011 pukul 20.00

[5] http://people.csail.mit.edu/rivest/ diakses pada tanggal 4 Mei 2011 pukul 13.00

[6] http://arenamusik.indosat.com/news-detail.php?id=2011/03/18/228/228_1595249_20110318_111317 diakses pada tanggal 4 Mei 2011 pukul 16.00

[7] http://203.148.253.29/mblog/category/qr-codes/ diakses pada tanggal 6 Mei 2011 pukul 13.00

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, 9 Mei 2010

ttd

Calvin Irwan 13507010