Algoritma Multivariate Quadratic untuk Keamanan *E-commerce*

Gressia Melissa – NIM : 13506017

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jalan Ganesha no.10 Bandung
E-mail : if16017@students.if.itb.ac.id

Abstrak :

Internet telah memberikan pengaruh radikal bagi kehidupan manusia. *E-commerce*, penyedia layanan transaksi via website merupakan salah peluang akibat kemunculan internet. Kartu kredit digunakan sebagai alat pembayaran, dengan begitu pembeli harus mengirimkan PIN kartu kredit dan informasi penting lainnya via internet. Pengiriman informasi penting tersebut melalui internet membutuhkan fitur keamanan untuk menjaganya agar tidak dimanfaatkan oleh orang yang tidak bertanggung jawab. Untuk itu, digunakan kriptografi asimetri untuk pengamanan informasi transaksi melalui internet tersebut. Algoritma RSA dinilai masih kurang aman untuk kebutuhan ini, maka skema *multivariate quadratic* dapat dimanfaatkan sebagai algoritma yang cukup aman untuk sekuritas transaksi di internet. Berbeda dengan RSA, *Multivariate quadratic* menggunakan enkripsi berlapis yang memungkinkannya untuk menjaga kerahasiaan data dan membuatnya lebih sulit ditembus.

Kata kunci : *e-commerce*, *multivariate quadratic*, enkripsi berlapis, internet.

1. Pendahuluan

E-commerce termasuk salah satu istilah yang berarti perdagangan elektronik, yaitu bentuk lain perdagangan yang berubah sejalan dengan waktu. Awalnya, perdagangan elektronik merupakan aktivitas perdagangan yang memanfaatkan transaksi komersial, misalnya mengirim dokumen komersial seperti pesanan pembelian secara elektronik. Kemudian berkembang menjadi suatu aktivitas yang mempunya istilah yang lebih tepat yaitu "perdagangan web" (pembelian barang dan jasa melalui *World Wide Web*). Pada awalnya ketika *web* mulai terkenal di masyarakat pada 1994, banyak jurnalis memperkirakan bahwa *e-commerce* akan menjadi sebuah sektor ekonomi baru. Sehingga pada era 1998 hingga 2000 banyak bisnis di AS dan Eropa yang mengembangkan situs *web* perdagangan ini.

E-com, atau *Electronic Commerce* merupakan salah satu teknologi yang berkembang pesat dalam dunia bisnis dan per-internet-an. Penggunaann sistem *E-commerce* sebenarnya dapat menguntungkan banyak pihak, baik pihak konsumen, maupun pihak produsen dan penjual (*retailer*). Misalnya bagi pihak konsumen, menggunakan *e-commerce* dapat membuat waktu berbelanja menjadi singkat. Selain itu, harga barang-barang yang dijual melalui *e-commerce* biasanya lebih murah dibandingkan dengan harga di toko, karena jalur distribusi dari produsen barang ke pihak penjual lebih singkat dibandingkan dengan toko konvensional.

Di Indonesia, sistem *e-commerce* ini kurang populer, karena banyak pengguna internet yang masih meragukan keamanan sistem ini, dan kurangnya pengetahuan mereka mengenai apa itu *e-commerce* yang sebenarnya. Sehingga sampai saat ini, web resmi yang telah menyelenggarakan *e-commerce* di Indonesia adalah RisTI Shop. Risti, yaitu Divisi Riset dan Teknologi Informasi milik PT. Telkom, menyediakan layanan *e-commerce* untuk penyediaan informasi produk peralatan telekomunikasi dan non-telekomunikasi. Web ini juga telah mendukung proses transaksi secara *online*.

Pembayaran barang dilakukan dengan menggunakan kartu kredit, yang berarti bahwa pembeli harus mengirimkan kode PIN kartu kredit dan informasi lainnya melalui internet. Karena alasan keamanan yang menyangkut

informasi kartu kredit maka transaksi barang lewat internet tidak terlalu populer.

Browsing web secara aman adalah fitur paling penting pada *e-commerce*. *Secure Socket Layer* (SSL) adalah protokol yang digunakan untuk *browsing web* secara aman. Kedua protokol ini memfasilitasi penggunaan enkripsi untuk data yang rahasia dan membantu menjamin integritas informasi yang dipertukarkan antara *website* dan *web brwoser* (misalnya *Netscape*, *Interner Explorer*, dsb).

SSL adalah contoh protokol *client-server*, yang dalam hal ini *web browser* adalah *client* dan *website* adalah *server*. *Client* yang memulai komunikasi, sedangkan *server* memberi respon terhadap permintaan *client*. Fungsi paling dasar yang digunakan SSL adalah membentuk saluran untuk mengirimkan data terenkripsi, seperti data kartu kredit, dari *browser* ke *website* yang dituju.

2. Ancaman pada *E-commerce*

Karena berbagai informasi penting seperti identitas, alamat, nomor kartu kredit, dan informasi lainnya dipertukarkan pada fasilitas *E-commerce*, teknologi ini pun tidak lepas dari perhatian para penjahat cyber yang berusaha mendapatkan banyak keuntungan meskipun harus melanggar hukum. Metodenya pun bermacam-macam, seperti penyerangan pada teknologi internet umumnya.

Salah satu yang cukup sering dilakukan adalah *phishing*. Phishing berarti meniru suatu halaman website hingga menyerupai aslinya dengan tujuan mendapatkan informasi penting dari pelanggan situs asli. Para pelaku phishing membuat situs palsu ini semirip mungkin dengan aslinya. Tidak hanya isinya, nama domainnya pun dibuat mirip hingga pengguna yang salah memasukkan domain ke web browser akan memasuki situs palsu (misalnya memalsukan situs **http://www.klikbca.com** dengan membuat situs **http://www.click-bca.com**; perhatikan namanya yang hanya berbeda tipis dan dapat membingungkan masyarakat umum) dan informasi-informasi pribadinya akan dapat jatuh ke tangan pihak-pihak yang tidak berhak.

Cara mencegah kejahatan *E-commerce* tidak jauh dengan pencegahan teknologi informasi lainnya, yaitu dengan menitikberatkan pada faktor sumber daya manusia yang menggunakannya. Meskipun manusia dapat mambuat teknologi secanggih-canggihnya dan seaman-amannya, teknologi tersebut akan lumpuh ketika penggunanya tidak berhati-hati dalam menggunakannya.

3. Kriptografi Kunci Publik pada *E-commerce*

Kriptografi kunci publik digunakan dalam sistem *e-commerce* untuk otentikasi (tanda tangan elektronik) dan komunikasi yang aman (enkripsi). Keamanan saat menggunakan kriptografi kunci publik pusat pada kesulitan untuk memecahkan masalah kelas tertentu. Skema RSA bergantung pada kerumitan pengolahan bilangan bulat besar, sedangkan kesulitan pemecahan logaritma diskrit memberikan dasar bagi ElGamal dan prosesor kurva aritmatika.

Mengingat bahwa keamanan skema kunci publik tersebut bergantung pada sejumlah kecil masalah yang saat ini dianggap keras, penelitian tentang skema baru yang didasarkan pada kelas-kelas lain dari masalah yang bermanfaat. Pekerjaan tersebut memberikan keragaman yang lebih besar dan karenanya kekuatan *cryptanalysts* untuk berkonsentrasi lebih pada jenis baru benar-benar masalah. Selain itu, hasil penting pada potensi kelemahan yang ada skema kunci publik yang muncul sebagai teknik untuk faktorisasi dan pemecahan logaritma diskrit terus meningkat.

Kuantum waktu polinomial algoritma dapat digunakan untuk memecahkan kedua masalah dan karenanya, keberadaan komputer kuantum pada kisaran 1.000 bit akan menjadi ancaman dunia nyata untuk sistem berbasis pada anjak atau masalah log diskret. Hal ini menunjukkan pentingnya penelitian menjadi algoritma baru untuk enkripsi asimetris. Pada saat ini tidak ada banyak hasil yang diketahui tentang kerentanan masalah keras terhadap algoritma kriptografi kuantum. Oleh karena itu, banyak penelitian upaya ke arah ini tampaknya menjadi keharusan jika kita mengandaikan adanya komputer kuantum dalam dekade mendatang.

3.1. Aspek Keamanan

Aspek keamanan pada aplikasi *e- commerce* dengan ancaman keamanan seperti yang telah dijelaskan diatas dapat diatasi dengan kriptografi karena kriptografi menyediakan beberapa aspek keamanan berikut :

a. Kerahasiaan (*confidentiality*)

Layanan yang digunakan untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya. Layanan ini umumnya direalisasikan dengan cara mengenkripsi pesan menjadi bentuk yang tidak dapat dimengerti.

b. Integritas Data (*data integrity*)

Layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain aspek keamanan ini dapat diungkapkan sebagai pertanyaan : "Apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?".

Istilah lain yang serupa dengan *data integrity* adalah otentikasi pesan (*message authentication*). Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubstitusian data lain kedalam pesan yang sebenarnya.

c. Otentifikasi (*authentication*)

Otentifikasi adalah layanan yang untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*) dan untuk mengidentifikasi kebenaran sumber pesan (*data origin authentication*). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan : "Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar? ".

Otentikasi sumber pesan secara implisit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu layanan integritas data selalu dikombinasikan dengan layanan otentikasi sumber pesan.

d.* Nirpenyangkalan (*Nonrepudiation)

Nirpenyangkalan adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan. Menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

3.2. Tanda Tangan *Digital*

Serangan umum yang terjadi pada kunci publik tanpa identitas adalah penyamaran (*impersonation attack*). Seseorang yang memiliki kunci publik orang lain dapat menyamar seolah-olah dialah pemilik kunci itu. Serangan semacam ini adalah masalah yang muncul dari penggunaan kriptografi kunci publik. Contohnya, dalam teknologi *e-commerce*, pembayaran transaksi dilakkan dengan menggunakan kartu kredit. Pelanggan mengiriman informasi kartu kreditnya yang bersifat rahasia melalui website pedagang online. Selama pengiriman, informasi kartu kredit tersebut dilindungi dengan cara mengenkripsinya dengan kunci publik pedagang online. Bagaimana pelanggan itu memastikan bahwa website pedagang online tersebut memang benar milikpedagan online dan bukan website pihak lain yang menyamar sebagai *website* pedagang asli dengan tujuan untuk mncuri informasi kartu kredit.

Untuk menjawab masalah di atas, solusinya adalah dengan memberikan sertifikat *digital* pada kunci publik. Sertifikat *digital* dikeluarkan oleh pemegang otoritas sertifikasi (*Certification Authority* atau CA). CA biasanya merupakan institusi keuangan (seperti bank) yang terpercaya. Sertifikat *digital* adalah dokumen *digital* yang berisi informasi sebagai berikut:

i. Nama subjek (perusahaan/individu yang disertifikasi),
ii. Kunci publik si subjek,
iii. Waktu kedaluarsa sertifikat (*expire time),*
iv. Informasi relevan lain seperti nomor seri sertifikat, dan lain-lain.

CA membangkitkan nilai *hash* dari sertifikat *digital* tersebut (misalnya dengan fungsi *hash* satu arah MD5 atau SHA), lalu menandatangani nilai *hash* tersebut dengan menggunakan kunci privat CA.

Contoh sebuah sertifikat *digital*:
Penulis membawa kunci publiknya dan mendatangi CA untuk meminta sertifikat *digital*. CA mengeluarkan sertifikat *digital* dan menandatangani sertifikat tersebut dengan cara mengenkripsi nilai *hash* dari kunci publik penulis (atau nilai *hash* dari sertifikat *digital* keseluruhan) dengan menggunakan kunci privat CA. Misalnya sebuah aplikasi pembuat kunci

publik seperti yang penulis buat menghasilkan tanda tangan *digital* untuk transaksi *e-commerce* seperti pada gambar 1 di bawah ini.

Gambar 1 : Digest Transaksi melalui Aplikasi SHA yang Dibuat

Dari hasil digest itulah yang dibuat menjadi sertifikat *digital*. Contoh isi sertifikat *digital* dan tanda tangan *digital* dari CA kira-kira seperti pada gambar 2.

```
Saya menyatakan bahwa kunci publik :
d483ed285cc72e9ffa4e435d5a6ac12dac77fc80

Merupakan kepemilikan dari :
   Gressia Melissa
   Jalan Ganesha no.10
   Bandung, Indonesia
   e-mail :
   if16017@students.if.itb.ac.id
   waktu kadaluarsa : 1 Juni 2010
```

Gambar 2 Sertifikat *Digital*

Jadi, sertifikat *digital* menyatakan kunci publik sebagai pengikat identitas pemilik kunci publik. Sertifikat ini dapat dianggap sebagai surat pengantar dari CA. Supaya sertifikat *digital* itu dapat diverifikasi, maka kunci publik CA harus diketahui secara luas. Seseorang yang memiliki kunci publik CA dapat memverifikasi bahwa tanda tangan di dalam suatu sertifikat itu sah dan arena itu mendapat jaminan bahwa kunci publik di dalam sertifikat itu memang benar.

Sertifikat *digital* sendiri tidak rahasia, tersedia secara publik, dan disimpan oleh CA di dalam repositori sertifikat. Salinan sertifikat tersebut juga dimiliki oleh pemohon sertifikat. Penulis mungkin meletakkan sertifikat tersebut di dalam *homepage*-nya, dengan pranala ke halaman web yang menyatakan: klik ini untuk melihat sertifikat kunci publik saya. Hasil pengeklikan akan memperlihatkan sertifikat *digital* dan tanda tangan dari CA. Misalkan sewaktu-waktu Alice mengakses *homepage* penulis untuk mendapatkan kunci publik penulis.

Misalkan juga Carol berhasil memintas request Alice (*client*) ke *homepage* penulis (*server*), sehingga *request* tersebut masuk ke *homepage* penulis palsu (yang dibuat oleh Carol, tujuan memintas adalah agar Alice mengira Carol adalah penulis, sehingga Carol dapat memperoleh informasi rahasia dari Alice, misalnya kunci). Carol sudah meletakkan sertifikat *digital*-nya di dalam halaman web palsu, tetapi jika Alice membaca sertifikat tersebut dia langsung paham bahwa dirinya sedang tidak berkomunikasi dengan penulis karena identitas penulis tidak terdapat di dalam sertifikat tersebut.

Misalkan Carol berhasil mengubah *homepage* penulis, mangganti kunci publik penulis di dalam sertifikat *digital* dengan kunci publiknya. Tetapi, jika Alice meng-*hash* sertifikat *digital* tersebut, dia memperoleh nilai *hash* yang tidak sama dengan nilai *hash* yang dihasilkan jika tanda tangan *digital* diverifikasi dengan kunci publik CA. Karena Carol tidak mempunyai kunci privat CA, maka Carol tidak dapat membangkitkan tanda tangan *digital* dari sertifikat penulis yang sudah diubah tersebut. Dengan cara ini, Alice dapat meyakini bahwa dia memiliki kunci publik penulis dan bukan kunci publik Carol.

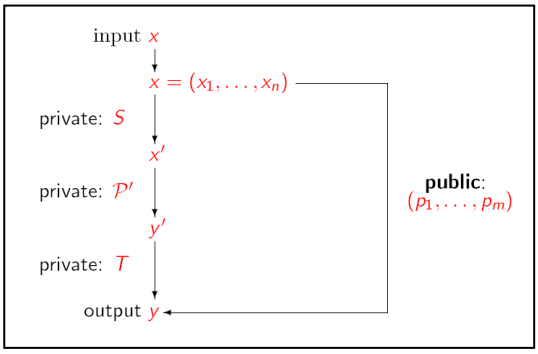
Skema ini juga tidak membutuhkan CA harus *online* untuk melakukan verifikasi. Adanya atribut waktu kadaluarsa pada sertifikat *digital* dimaksudkan agar pengguna mengubah kunci publik (dan kunci privat pasangannya) secara periodik. Makin lama penggunaan kunci, makin besar peluang kunci diserang dan dikriptanalisis. Jika pasangan kunci tersebut diubah, maka sertifikat *digital* yang lama harus ditarik kembali. Pada sisi lain, jikakunci privat berhasil diketahui pihak lain sebelum waktu kadaluarsanya, sertifikat *digital* harus dibatalkan dan ditarik kembali, dan pengguna harus mengganti pasangan kuncinya.

Bagaimana CA memberitahu ke publik bahwa sertifikat *digital* ditarik? Caranya dengan CA secara periodik mengeluarkan CRL (*Certificate Rovocation List*) yang berisi nomor seri sertifikat *digital* yang sudah ditarik. Sertifikat *digital* yang sudah kedaluarsa otomatis

dianggap tidak sah lagi dan ia juga dimasukkan dalam CRL. Dengan cara ini, maka CA tidak perlu memberitahu perubahan sertifikat *digital* kepada setiap orang. Sayangnya, keberadaan CRL menyebabkan pengguna yang memakai sertifikat *digital* harus memiliki CRL untuk memvalidasi apakah sertifikat tersebut telah ditarik. Sebagai alternatif CRL adalah *Online Certification Status Protocol* (OCSP), yang memvalidasi sertifikat secara *real time*.

Untuk penggunaan *e-commerce*, setiap transaksi yang dilakukan secara cepat berpengaruh terhadap kebutuhannya untuk memutakhirkan sertifikat *digital*-nya. Keuntungannya, durasi waktu kadaluarsa dapat diatur seminimal mungkin agar mereduksi kemungkinan adanya serangan. Durasi waktu kadaluarsa yang relatif singkat tidak akan menjadi masalah bagi transaksi yang dilakukan melalui *e-commerce* karena keberlakuannya memang sampai pembayaran dilakukan. Biasanya penjual tidak akan memberikan waktu yang lama untuk proses pembayaran, sehingga ia mempunyai alasan untuk membatasi waktu kadaluarsa transaksi.

3.3. Skema *Multivariate Quadratic*



Gambar 3 Skema Umum

Algoritma *Multivariate Quadratic* dikembangkan oleh tim peneliti dari Norwegian University of Science and Technology (NTNU). Ditinjau dari mekanisme kerjanya, MQ mengaplikasikan *secure key exchange* (pertukaran kuci). Skema itu menjamin keamanan proses penandatanganan kunci publik.

Sebagai ilustrasi, jika Alice ingin mengirim data ke Bob, mereka memiliki kata kunci masing-masing. Pembuatan kata kunci itu biasa dilakukan dengan dua cara, yakni dengan algoritma simetris dan algoritma asimetris. Algoritma simetris kerap disebut algoritma konvensional, yaitu algoritma yang menggunakan kunci yang sama pada proses enkripsi dan deskripsinya. Algoritma itu mengharuskan pengirim dan penerima data menyetujui satu kunci tertentu. Kelebihan algoritma simetris ialah memiliki proses enkripsi dan deskripsi yang jauh lebih cepat dibandingkan dengan algoritma asimetris. Sedangkan kelemahannya terletak pada permasalahan distribusi kunci. Hal itu menyebabkan kunci sangat rentan dibajak oleh peretas jika pengirimannya dilakukan melalui Internet.

Persoalan menganai keamanan pengiriman melalui jaringan publik dapat diatasi dengan mengaplikasikan algoritma asimetris yang dikenal dengan kriptografi kunci publik. Sebutan asimetris (tidak simetris) memperlihatkan adanya perbedaan kunci yang digunakan pada proses enkripsi dan deskripsi. Kunci publik digunakan untuk proses enkripsi data, sedangkan proses deskripsi menggunakan kunci yang biasa disebut dengan kunci rahasia (*private key*).

Berdasarkan konsep itu, kunci yang didistribusikan merupakan kunci publik yang tidak diperlukan kerahasiaannya, sedangkan kunci rahasia tetap disimpan atau tidak didistribusikan. Jadi, setiap orang yang memiliki kunci publik dapat melakukan proses enkripsi yang hanya bisa dibaca oleh orang yang memiliki kunci rahasia.

Skema konsep di atas juga digunakan pada algoritma RSA. Yang membedakannya ialah pada RSA, proses enkripsi dinyatakan dalam persamaan

$$y = x^e \pmod n$$

Sedangkan pada algoritma MQ, digunakan proses berlapis untuk enkripsinya.

$y_1 = x_1x_2 + x_1x_3 + x_1x_5 + x_2x_5 + x_2x_6 + x_3x_5 + x_5x_6 \pmod p$
$y_2 = x_1x_3 + x_2x_4 + x_3x_5 \pmod p$
$y_3 = x_1x_3 + x_1x_5 + x_2x_3 + x_3x_4 + x_3x_6 + x_5x_6 \pmod p$
$y_4 = x_1x_2 + x_3x_5 \pmod p$
$y_5 = x_1x_3 + x_1x_4 + x_1x_5 + x_2x_4 + x_3x_4 + x_3x_6 \pmod p$
$y_6 = x_1x_3 + x_1x_4 + x_2x_3 + x_2x_5 + x_3x_4 + x_4x_5 + x_4x_6 \pmod p$
...
y_n

MQ melibatkan kunci publik dan kunci privat. Kunci privat terdiri dari tiga buah transformasi, yaitu S, P', dan T. P' merupakan transformasi privat yang dirancang untuk dilakukan pada tiap skema. P' memetakan elemen dari $GF^n \rightarrow GF^m$. S mentransformasikan dari $GF^n \rightarrow GF^n$ dan T mentransformasikan $GF^m \rightarrow GF^m$. Setiap transformasi harus dapat dibalikkan (*invertible*). Perlu dicatat bahwa elemen-elemen dipetakan pada bidang enkripsinya masing-masing, bukan pada kelompok proses enkripsi. Sedangkan kunci publik dihasilkan dari transformasi privat. Kunci publik dapat dinyatakan sebagai

$$P = S \,.\, P' \,.\, T$$

Untuk tanda tangan *digital*, dihasilkan dari penggunaan kunci privat dan diverifikasi menggunakan kunci publik.

i. Pertama, pengirim mengambil pesan dan menginterpretasikannya sebagai vektor pada ranah nilai kecil (contohnya apabila ranah hanya memiliki dua elemen, maka vektor yang dibuat berupa *bit vector*).
ii. Kemudian, S mengambil masukan berupa
$$x = <x_1, x_2, \ldots x_n>. S$$
iii. Selama transformasi S, x dimultiplikasi dengan matriks M_S. Penambahan vektor v_S dengan panjang n dilakukan. Maka dimensi M_S adalah n x n. Persamaan transformasi S ialah
$$S = M_S * x + v_S$$
iv. T merupakan transformasi yang serupa dengan S. Transformasi tersebut dinyatakan dengan
$$T = M_T * y' + v_T$$
v. Kemudian, hasil dari S adalah masukan baru bagi transformasi privat P'.

Tanda tangan lengkap terdiri dari elemen (x, y) sebagai *bit vector*. Penerima *tuple* ini harus memiliki kunci publik. Karena ia memiliki kunci, maka ia dapat memvalidasi keabsahan tanda tangan x. Dengan demikian, penerima mengisi himpunan persamaan publik dengan elemen-elemen pada *bit vector* tersebut. Contoh himpunan persamaan publik dapat berbentuk seperti di bawah ini :

$$y_1 = x_1x_2 + x_1x_4 + x_3x_4$$
$$y_2 = x_1x_3 + x_2x_4$$
$$y_3 = x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$
$$y_4 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$$

4. Kesimpulan

Keamanan aplikasi *e-commerce* dapat ditangani dengan implementasi algoritma asimetris untuk memverifikasi transaksi melalui tanta tangan *digital*. Proses awal yaitu pembentukan kunci dapat menggunakan fungsi *hash* satu arah untuk kemudian menghasilkan tanda tangan *digital*-nya melalui algoritma asimetris.

Algoritma asimetris MQ melalui proses enkripsi yang berlapis, sehingga keamanannya lebih tinggi dibandingkan dengan algoritma RSA untuk mengotentikasi identitas transaksi *e-commerce*.

5. Daftar Pustaka

[1] Munir, Rinaldi. 2004. *Bahan Kuliah IF3054, Kriptografi*. Bandung : Departemen Teknik Informatika, Institut Teknologi Bandung.

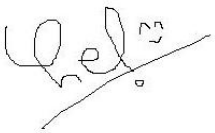
[2] Wolf, Christopher; Bart Preneel. 2005. *Multivariate Quadratic Public Key System*. Leuven-Heverlee : Cryptology ePrint Archive.

[3] _____. 2001. *E-commerce* Security. [Online] Tersedia : http://www.upu.int (Tanggal akses : 28 April 2010).

6. Pernyataan

Makalah yang dibuat untuk pemenuhan ujian akhir semester mata kuliah Kriptografi ini bukan merupakan plagiasi.

Bandung, 17 Mei 2010



Gressia Melissa