Sistem Keamanan Jual Beli Online Menggunakan Algorithma RSA dan MD5 Berbasis Web

Slamet Widodo[1],Raden Abdul Hadi Hag[2]
Jurusan Teknik Komputer
Politeknik Negeri Sriwijaya
Jalan Srijaya Negara, Palembang 30139
Telp.0711-353414 Fax.0711-355918
E-mail : slamet_widodo2003@yahoo.com

Abstrak

Kemajuan teknologi informasi jaman sekarang ini mendorong seseorang atau organisasi untuk melakukan kegiatan bisnis melalui media internet. Pada saat ini jumlah pengguna situs jual beli online sangat berkembang sangat cepat sehingga memudahkan transaksi bisnis antara penjual dan pembeli melalui media internet. Sehingga bisnis jual beli online mempunyai manfaat yang sangat menguntungkan bagi penjual dan pembeli.

Dari segi bisnis jual beli online mempunyai manfaat yang sangat menguntungkan bagi penjual dan pembeli produk-produk yang ditawarkan sesuai kebutuhan konsumen.Namun jual beli online mengandung resiko yang ditimbulkan melalui transaksi tersebut. Salah satu resiko yang ditimbulkan adannya penipuan-penipuan yang mengatas namakan seseorang atau organisasi tertentu untuk mendapatkan keuntungan secara mudah dengan melalui situs-situs jual beli online sehingga akan berdampak kerugian bagi penjual atau pembeli yang benar-benar memanfaatkan transaksi jual beli online.

Kriptography adalah salah satu cara untuk mengurangi atau mengatasi tidak amannya transaksi jual beli online melalui media internet. Penerapan sistem keamanan jual beli online adalah dengan melakukan enkripsi penyandian data pada identitas *credit card*(kartu kredit) pembeli dan menambahkan tanda tangan digital (validasi) untuk mengecek keabsahannya. Algorithma RSA***(Rivest—Shamir—Adleman)*** dan MD5 **(*Message-Digest algortihm 5*)** tampaknya menjanjikan untuk mengatasi keamanan data transaksi jual beli online. Dengan menggunakan algorithma RSA dan MD5 sistem akan melakukan proses pengamanan data transaksi jual beli online tersebut dengan melakukan pengenkripsian dikirim ke server.

Kata kunci: Kriptografi, tanda tangan digital, RSA, MD5.

---

1. LATAR BELAKANG

Kemajuan teknologi informasi jaman sekarang ini mendorong seseorang atau organisasi untuk melakukan kegiatan bisnis melalui media internet. Pada saat ini jumlah pengguna situs jual beli online sangat berkembang sangat cepat sehingga memudahkan transaksi bisnis antara penjual dan pembeli melalui media internet. Sehingga bisnis jual beli online mempunyai manfaat yang sangat menguntungkan bagi penjual dan pembeli.

Dari segi bisnis jual beli online mempunyai manfaat yang sangat menguntungkan bagi penjual dan pembeli produk-produk yang ditawarkan sesuai kebutuhan konsumen.Namun jual beli online mengandung resiko yang ditimbulkan melalui transaksi tersebut. Salah satu resiko yang ditimbulkan adannya penipuan-penipuan yang mengatas namakan seseorang atau organisasi tertentu untuk mendapatkan keuntungan secara mudah dengan melalui situs-situs jual beli online sehingga akan berdampak kerugian bagi penjual atau pembeli yang benar-benar memanfaatkan transaksi jual beli online.

Salah satu cara untuk mengurangi atau mengatasi tidak amannya transaksi jual beli online melalui media internet adalah dengan melakukan penyandian data pada identitas *credit card*(kartu kredit) pembeli dan menambahkan tanda tangan digital (validasi) untuk mengecek keabsahannya yaitu menggunakan teknik enkripsi deskripsi dan tanda tangan digital.

2. TINJAUAN PUSTAKA

2.1 Jual Beli Online

Pengertian Jual Beli Online yaitu (sebuah akad jual beli yang dilakukan dengan menggunakan sarana eletronik (internet) baik berupa barang maupun berupa jasa). Atau " akad yang disepakati dengan menentukan ciri-ciri tertentu dengan membayar harganya terlebih dahulu sedangkann barangnya diserahkan kemudian".Masalah jual beli online merupakan masalah fiqih kontemporer yang belum pernah dibahas dalam kitab-kitab fiqih klasik. Oleh karena itu dalam pembahasan yang berhubungan dengan jual beli online banyak dikaitkan dengan item-item jual beli yang ada dalam kitab- kitab fiqih, terkait dengan ketentuan pokok atau lazim disebut rukun dan syarat jual beli. (http://azzuracie.wordpress.com)

2.2 Kriptografi

"Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya" (Munir, 2006:02).

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu:

a. Kerahasiaan pesan *(confidentiality/ secrecy)*.
b. Otentikasi *(authentication)*.
c. Keaslian pesan *(data integrity).*
d. Nirpenyangkalan *(non-repudiation).*

2.3 Digital Signature

Tandatangan digital atau sering disebut dengan *Digital Signature* merupakan sebuah teknik otentikasi pesan yang digunakan untuk keperluan *message integrity*, *user authentication, non repudiation*. *Message integrity* adalah menjaga keaslian pesan dikirim dan diterima oleh pihak yang berhak. *User authentication* bertujuan untuk menjamin keaslian identitas pengirim, dan *non repudiation* adalah pengirim pesan tidak dapat menyangkal isi pesan (Munir, 2006: 239).

Tanda tangan digital dengan mudah dapat dipindahkan, tidak bisa ditiru oleh orang lain, dan dapat secara otomatis dilakukan *time-stamp*. Kemampuan itu untuk memastikan bahwa pesan asli yang tiba di pengirim tidak bisa dengan mudah diganti. Suatu tanda tangan digital dapat digunakan di segala macam pesan, apakah itu terenkripsi atau tidak, sehingga penerima dapat memastikan identitas pengirim itu dan pesan tiba secara utuh.

Terdapat 3 cara dalam proses pemberian *digital signature*, yaitu:

1. Menggunakan algoritma kunci simetri
2. Menggunakan algoritma kunci asimetri
3. Menggunakan Fungsi *hash*

Dari ketiga cara tersebut, yang akan penulis gunakan dalam proses pemberian *digital signature* adalah fungsi *hash.* Salah satu algoritma yang menggunakan fungsi *hash* dalam metode enkripsinya adalah *MD5*.

2.4 *MD5(Message Digest 5)*

MD5 adalah fungsi hash satu arah yang diuat oleh Ronald Rivest pada tahun 1991. *MD5* adalah perbaikan dari *MD4* setelah *MD4* berhasil diserang oleh kriptanalis. MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan message digest yang panjangnya 256bit. (Munir, 2006:220)

Selain penggunaan *MD5* untuk pemberian *digital signature*-nya, dignakan juga algoritma kunci publik untuk proses pengamanan datanya salah satu algoritma kunci publik yang digunakan adalah RSA.

2.5 Algoritma RSA

”Algoritma RSA dibuat oleh tiga orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, yaitu: Ron Rivest, Adi Shamir, dan Leonard Adleman. Huruf **RSA** itu sendiri berasal dari inisial nama mereka **R**ivest—**S**hamir—**A**dleman” (Munir,2006:179).

RSA di bidang kriptografi adalah sebuah algoritma pada enkripsi *public key*. Algoritma di sebut kunci publik karena kunci enkripsi dapat dibuat publik yang berarti semua orang boleh mengetahuinya. RSA masih digunakan secara luas dalam protokol electronic commerce, dan dipercaya dalam mengamankan dengan menggunakan kunci yang cukup panjang.

Terdapat tiga proses dalam penggunaan algoritma RSA, yaitu:

1. Proses Pembangkitan Kunci

Pada bagian ini, terdapat tujuh tahapan. Proses ini dilakukan oleh pihak server.

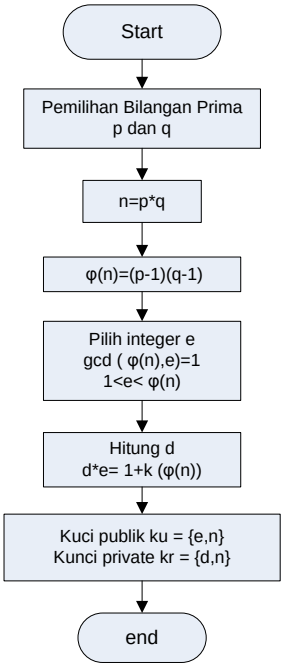
a. Pilih bilangan prima sembarang p dan q. Kedua nilai ini harus dirahasiakan.Misal bil. prima p = 7 dan q = 11,
b. Hitung n = p.q, Besaran n ini tidak perlu dirahasiakan .n = 7.11 =77
c. Hitung φ(n) = (p - 1)(q - 1) . φ(n) = (7 - 1)(11 -1)= 6.10 = 60
d. Pilih sebarang bilangan e, $1 < e < \phi(n)$, $\Phi(n)=\{1,2,3,4,6,8,..,76\}=\{x|gcd(x, n)=1\}$ misalnya e=17
e. dengan $gcd(\phi(n), e) = 1$. Pilih e dalam $\{x|gcd(x, 60)=1\}$
f. Hitung invers dari e, yaitu $d*e = 1+ k(\phi(n))$.

d . e = 1mod 60, d =53

53 . 17 mod 60 = 901 mod 60 = 1 mod 60

g. Kunci publik: (n, e) dan kunci rahasia: (n, d).

Berikut ini *flowchart* proses pembangkitan kuncinya:



Gambar 1. Pembangkitan Kunci

2. Proses Enkripsi

Proses enkripsinya dilakukan oleh pihak pengirim. Seluruh perhitungan pemangkatan bilangan modulo dilakukan menggunakan metode fast exponentiation.

1. Ambil kunci publik (n,e).
2. Pilih plainteks m, dengan $0 \leq m \leq n - 1$.
3. Hitung $c = m^e \bmod n$.
4. Diperoleh cipherteks c, dan kirimkan.

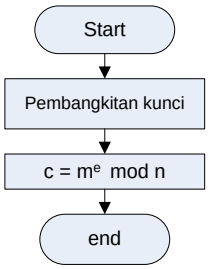
M = “PESAN”, m = 16 5 19 1 14

- Enkripsi: c = me mod n
- c1 = 1617 mod 77 = 25
- c2 = 517 mod 77 = 3
- c3 = 1917 mod 77 = 24
- c4 = 117 mod 77 = 1

- c5 = 1417 mod 77 = 42

c = 25 03 24 01 42, C = “YCXAp”

Berikut ini *flowchart* proses enkripsinya:



Gambar 2. Proses Enkripsi

3. Proses Dekripsi

Proses dekripsi dilakukan oleh pihak penerima cipherteks.

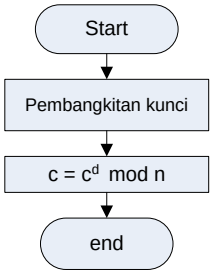
1. Ambil kunci publik (n,e) dan kunci rahasia (n,d).
2. Hitung $m = c^d \bmod n$.
3. Diperoleh plainteks m.

C = “YCXAp”, c = 25 03 24 01 42

- Dekripsi: m = cd mod n
- m1 = 2553 mod 77 = 16
- m2 = 353 mod 77 = 5
- m3 = 2453 mod 77 = 19
- m4 = 153 mod 77 = 1
- m5 = 4253 mod 77 = 14

m = 16 5 19 1 14 , M = “PESAN”

Berikut ini *flowchart* proses dekripsinya:



Gambar 3. Proses Dekripsi

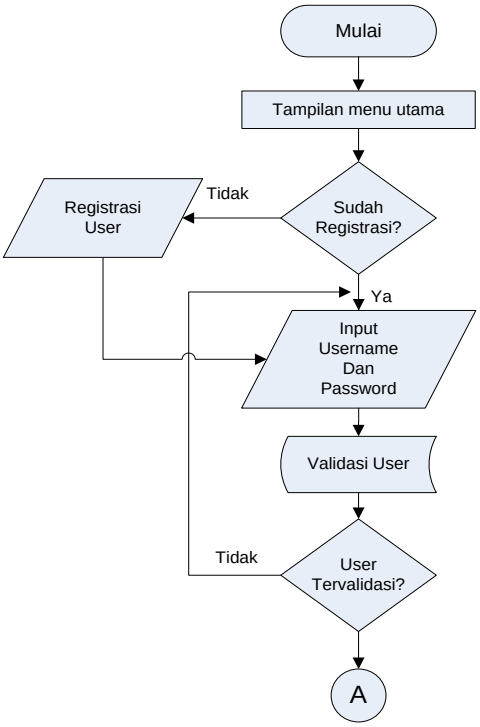
3. Metodologi Penelitian

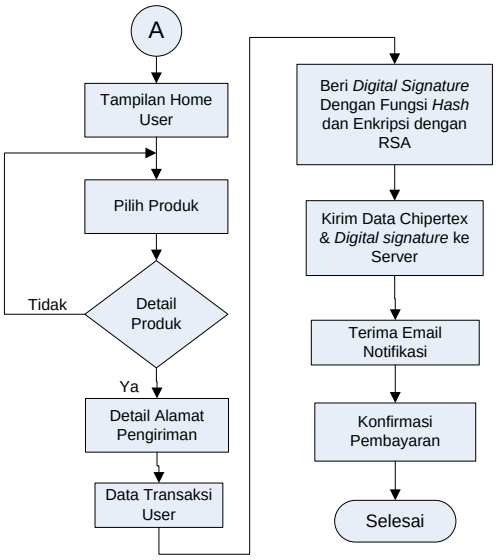
3.1 Perancangan Sistem

Pada perancangan sistem ini metodologi penelitian yang digunakan adalah :

Studi literatur,alat dan bahan penelitian ,hash data transaksi online dengan algorithma MD5*(Message Digest)* dan enkripsi data transaksi serta tanda tangan digital menggunakan algorithma RSA.Berikut cara kerja diagram alir sistem :

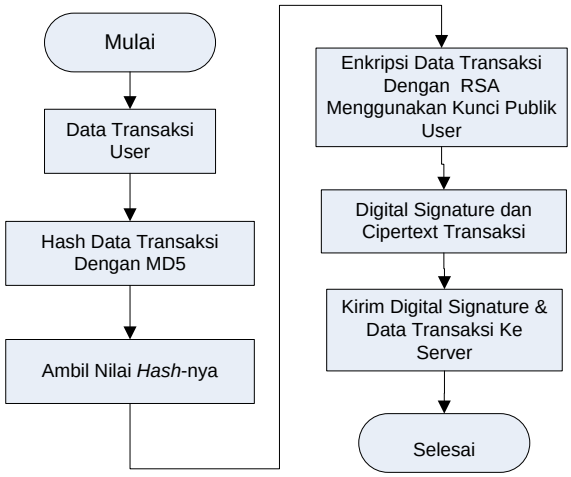
Gambar 3.1 menjelaskan pengguna jual beli online melakukan registrasi dengan mengisikan username dan password,kemudian user melakukan pilih produk yang akan diorder dan melakukan transaksi order barang dimana sistem akan mengenkripsi identitas pemesan barang yaitu credit card





Gambar 3.1 Flowchat pada *user*

Selanjutnya Gambar 3.2 Flowchart Enkripsi transaksi Data Order dijelaskan gambar dibawah ini :

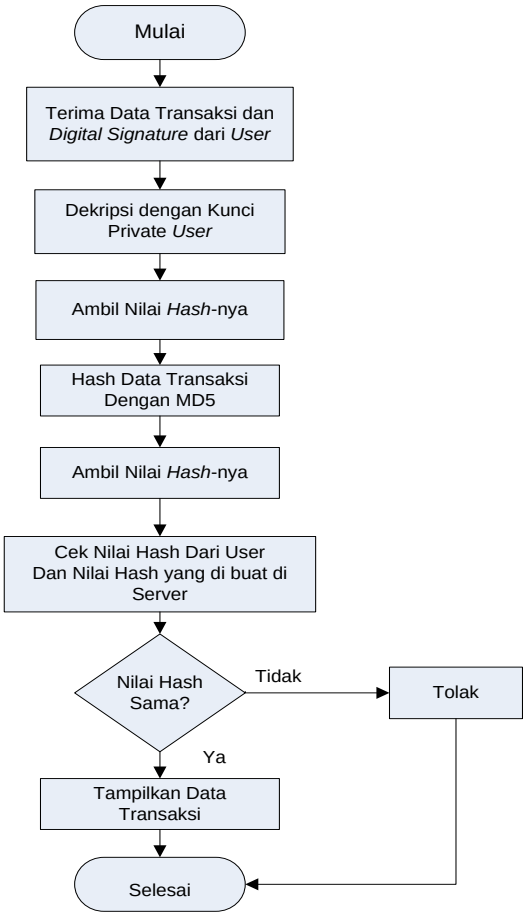


Gambar 6. *Flowchart* Enkripsi Data

Data transaksi terlebih dahulu di enkripsi dengan fungsi *hash Message Digest*, sehingga menghasilkan nilai *hash*. Kemudian nilai *hash* tersebut di enkripsi dengan algoritma RSA dan menggunakan kunci privat *user*. Hasil Enkripsi inilah yang merupakan tanda tangan digitalnya-nya.

Setelah *tanda tangan digital* tersebut di bentuk, data transaksi yang asli di kirim bersamaan dengan *tanda tangan digital*-nya. Hasil dari proses transaksi data order yang sudah disimpan di server selanjutnya dilakukan proses deskripsi data hasil enkripsi (ciphertext). Gambar 3.3 Flowchart Dekripsi Transaksi data order

Berikut ini merupakan *flowchart* proses dekripsi data transaksi yang diterima pada server admin:



Gambar 3.3. *Flowchart* Dekripsi Data

Data transaksi *user* yang sudah diterima, akan di dekripsi terlebih dahulu menggunakan

kunci publik *user* dan akan di ambil nilai *hash*-nya. Kemudian data transaksi akan di *hash* lagi dengan *Message Digest* sehingga menghasilkan nilai *hash* juga.

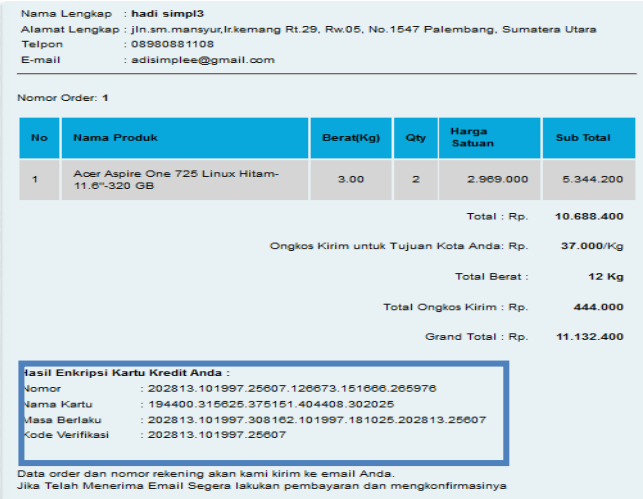
Nilai *hash* yang dikirim dari *user* akan di cocokkan dengan nilai *hash* yang dibuat di server. Jika nilai hash sama, maka data akan di tampilkan dalam mode terdekripsi, dan jika tidak maka data akan di tolak dan dikirim pemberitahuan ke halaman user secara langsung.

4. Hasil dan Pembahasan

4.1 Implementasi Hasil

Dengan menggunakan program PHP dan database Mysql dihasilkan aplikasi untuk keamanan data transaksi produk yang akan di order dikirim dari pengguna ke server dengan cara mengenkripsi dan membubuhi tanda tangan digital pada identitas credit card calon pembeli order barang melalui transaksi online seperti dijelaskan Gambar 4.1 berikut ini :

Berikut ini merupakan halaman selesai transaksinya :


Nama Lengkap : **hadi simpl3**
Alamat Lengkap : jln.sm.mansyur,lr.kemang Rt.29, Rw.05, No.1547 Palembang, Sumatera Utara
Telpon : 08980881108
E-mail : adisimplee@gmail.com

Nomor Order: **1**

No	Nama Produk	Berat(Kg)	Qty	Harga Satuan	Sub Total
1	Acer Aspire One 725 Linux Hitam-11.6"-320 GB	3.00	2	2.969.000	5.344.200

Total : Rp. **10.688.400**
Ongkos Kirim untuk Tujuan Kota Anda: Rp. **37.000**/Kg
Total Berat : **12 Kg**
Total Ongkos Kirim : Rp. **444.000**
Grand Total : Rp. **11.132.400**

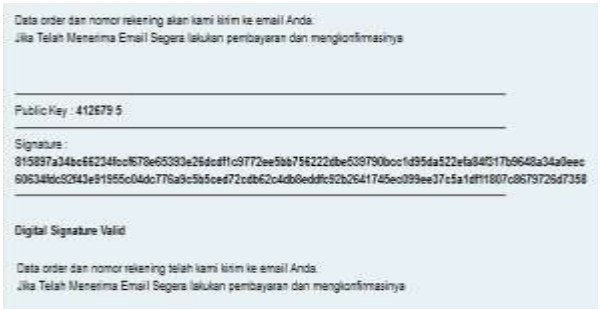
Hasil Enkripsi Kartu Kredit Anda :
Nomor : 202813.101997.25607.126673.151666.265976
Nama Kartu : 194400.315625.375151.404408.302025
Masa Berlaku : 202813.101997.308162.101997.181025.202813.25607
Kode Verifikasi : 202813.101997.25607

Data order dan nomor rekening akan kami kirim ke email Anda.
Jika Telah Menerima Email Segera lakukan pembayaran dan mengkonfirmasinya

Gambar 4.1 Enkripsi Identitas Kartu Kredit Order Transaksi Barang

Pada halaman *user*, proses pengamanan data dijalankan saat *user* melakukan *Check Out*. Pada saat *user* mengklik *button Check Out* maka secara otomatis data transaksi yang telah ada akan dienkripsi dengan RSA dan diberi *digital signature*.

Kunci Publik yang digunakan untuk mengenkripsi data transaksi tersebut akan ditampikan pada halaman selesai transaksi. Pada halaman selesai transaksi tersebut, ditampilkan juga hasil enkripsi dari penginputan cara pembayaran menggunakan kartu kredit dan *Signature-nya*.


Data order dan nomor rekening akan kami kirim ke email Anda.
Jika Telah Menerima Email Segera lakukan pembayaran dan mengkonfirmasinya

Public Key : 412679 5

Signature :
815897a34bc66234fcc1678e65383e26dcdf1c9772ee5bb756222dbe639790bcc1d95da522efa84f317b9648a34a9eec
6063486c82f43e91955c04dc776a9c5b5ced72cdb62c4db8eddfc92b2641745ec099ee37c5a1dff1807c8579726d7358

Digital Signature Valid

Data order dan nomor rekening telah kami kirim ke email Anda.
Jika Telah Menerima Email Segera lakukan pembayaran dan mengkonfirmasinya

Gambar 4.2 Tanda Tangan Digital Identitas Kartu Kredit Order Transaksi Barang.

Gambar 4.3 menjelaskan hasil tanda tangan digital dari identitas kartu kredit menggunakan public key pengguna transaksi data jual beli online. Publik Key yang digunakan untuk mengenkripsi data menggunakan Algorithma RSA dan tanda

tangan digital yang dibentuk dengan menggunakan fungsi hash menggunakan algorithma MD5 data hasil enkripsi dan *tanda* tangan digital yang akan dikirim ke server admin. Pada server admin ini data tersebut akan didekripsi dan di verifikasi tanda tangan digitalnya.

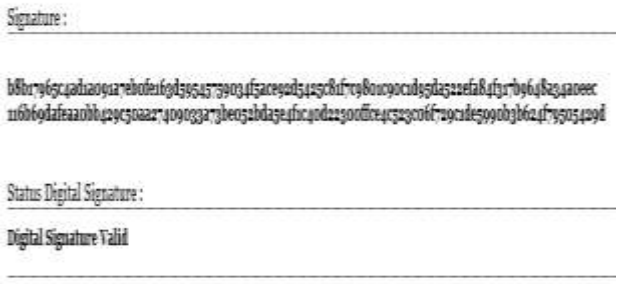
Gambar 4.3 Hasil Transaksi Order Barang Jual Beli Online Enkripsi Menggunakan Private Key

Gambar 4.3. menjelaskan data order yang sudah dienkripsi dan tanda tangan digital yang dikirim ke server dalam bentuk *ciphertext* yaitu data yang terenkripsi, akan didekripsi menggunakan kunci privat dari pengirim *(user).*

Pada gambar 4.4 Berikut ini merupakan hasil email notifikasi yang telah dikirim ke *email user :*

Gambar 4.4 Kiriman Notifikasi Mail Pemesan Hasil Transaksi Data Order Barang Online.

Selanjutnya hasil pengiriman data dari pengirim pembeli online dilakukan proses validasi tanda tangan digital yang sudah didekripsi . Berikut ini merupakan tampilan hasil validasi dari tanda tangan digital :



Gambar 4.5 Tanda Tangan Digital yang sudah divalidasi

Berikut ini merupakan pengujian saat dekripsi dari data transaksi lamannya pengujian waktu dekripsinya pada gambar 4.6 dibawah ini:

Waktu Dekripsi

Waktu Dekprisi Nama :	**0.20156097412109** /ms
Waktu Dekprisi Alamat :	**1.259831905365** /ms
Waktu Dekprisi Telpon :	**0.19487500190735** /ms
Waktu Dekprisi Email :	**0.34901595115662** /ms
Waktu Dekprisi Ongkoskirim :	**0.12546491622925** /ms
Waktu Dekprisi Total Bayar :	**0.15000104904175** /ms
Waktu Dekprisi Nomor Kartu :	**0.10414886474609** /ms
Waktu Dekprisi Nama dikartu:	**0.086683988571167** /ms
Waktu Dekprisi Masa Berlaku :	**0.12360286712646** /ms
Waktu Dekprisi Kode Verifikasi :	**0.050757884979248** /ms

Gambar 4.6 menjelaskan waktu dekripsi nama yaitu **0.201ms**,dekripsi alamat **1.259ms**, dekripsi telephone **0.194ms**, deskripsi email **0.349ms,**deskripsiOngkos kirim **0.125ms**,deskripsi total bayar **0.125ms** ,deskripsi Nomor kartu **0.104ms**, dekripsi nama kartu **0.0866ms** ,deskripsi masa berlaku **0.123ms**, dan deskripsi kode verifikasi **0.050ms** Dari hasil waktu enkripsi diatas disimpulkan bahwa semakin panjang karakter yang terenkripsi maka akan semakin lama pula proses pendekripsiannya.

5. KESIMPULAN

Dari penelitian ini dapat penulis simpulkan metode enkripsi dan deskripsi menggunakan algorithma RSA membuat kemanan data transaksi order barang secara online akan lebih aman dari orang yang tidak berhak selain penyedia jual beli online dan pengguna transaksi dengan melakukan enkripsi kartu kredit pembeli. Keabsahan transaksi juga akan lebih valid dengan adannya tanda tangan digital untuk verifikasi pembeli dan penjual order barang secara online dengan membubuhi tanda tangan digital.

6. DAFTAR PUSTAKA

Munir, Rinaldi. 2006. *Kriptografi*. Penerbit Informatika: Bandung.

Sadikin, Rifki. 2012, *Kriptografi untuk kemanana jaringan*. C.V ANDI OFFSET (Penerbit ANDI): Yogyakarta.

Nugroho, Bunafit. 2009. *Aplikasi Pemrograman Web Dinamis dengan PHP dan Mysql*. Gava Media: Yogyakarta.

Oktaviani, Diar puji. 2010. *Menjadi Programer Jempolan Menggunakan PHP* . MediaKom: Yogyakarta

Stakur, Stendy. 2005. *Aplikasi Web Database dengan Dreamwever MX 2004* . Andi: Yogyakarta.

Zaki, Ali. 2008. *36 Menit Belajar Komputer PHP dan MySQL* . PT. Alex Media Komputindo: Jakarta

http://azzuracie.wordpress.com/2013/04/25/hukum-jual-beli-online/

.

7.