Dual Signature pada Proses Pembayaran Elektronik

Christabella Chiquita B. 13509050[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]*christabella.c.b@std.stei.itb.ac.id*

***Abstract*— Dual signature adalah teknologi utama yang digunakan pada protokol SET (Secure Electronic Transaction) dan sudah diterapkan oleh Visa dan MasterCard. Dual signature secara umum bekerja dengan cara menggabungan (konkatenasi) dua message yang diterima oleh dua pihak, namun masing – masing pihak hanya dapat membaca message yang memang berhak untuk dilihatnya. Ini berhubungan dengan salah satu keamanan informasi yang cukup penting, yaitu otorisasi. Pada dual signature ini digunakan digital signature, yang membutuhkan tiga jenis algoritma, yaitu general algoritma, signature alogithm, dan algoritma verifikasi. Untuk enkripsinya dapat dengan algoritma kunci publik atau algoritma simetris. Saat ini sudah banyak algoritma yang digunakan untuk digital signature, seperti RSA, DSA, dll.**

***Index Terms*—dual signature, SET, otorisasi, digital signature, RSA**

I. INTRODUCTION

Perkembangan zaman menuntut manusia untuk melakukan semua aktivitasnya dengan seefektif dan seefisien mungkin. Hal – hal yang dulunya dilakukan harus dengan tatap muka dan secara manual, kini mulai bergeser ke cara yang lebih otomatis dan dapat dilakukan tanpa tatap muka secara langsung. Salah satu yang sedang meningkat saat ini adalah adanya kegiatan e-commerce. Pada e-commerce, dikenal suatu istilah pembayaran elektronik (e-payment), yaitu pembayaran secara elektronik (melalui internet). Sistem pembayaran elektronik saat ini sudah diterima sebagai cara yang lebih sederhana dan mudah untuk digunakan. Namun, tidak bisa dihindari pula, masalah keamanan informasi pun patut diberi perhatian lebih, salah satunya adalah masalah kontrol akses.

E-payment sendiri saat ini sudah banyak metodenya, salah satunya adalah menggunakan kartu kredit atau debit. Setiap metode memiliki protokolnya masing – masing, seperti pada pembayaran menggunakan VISA atau MASTERCARD, ada sebuah protokol yang diterapkan, yaitu protocol SET (Secure Electronic Transaction). Protokol SET ini memiliki sebuah teknologi untuk keperluan otorisasinya, yaitu teknologi dual signature. Dual signature memiliki prinsip menggabungkan (konkatenasi) dua buah message yang akan dikirimkan kepada dua pihak, namun masing – masing pihak hanya diperkenankan mengambil informasi yang sesuai dengan hak akses mereka. Pada makalah ini diajukan judul yaitu Penerapan Teknologi Dual Signature untuk Otorisasi pada Sistem E-Payment untuk membahas mengenai salah satu penggunaan kriptografi yaitu digital signature yang dimodifikasi sedemikian rupa sehingga membentuk dual signature yang digunakan dalam kehidupan sehari – hari, yaitu pada protocol SET dari Visa dan MasterCard .

II. SECURE ELECTRONIC TRANSACTION (SET)

Sistem pembayaran merupakan sistem yang digunakan untuk mengirimkan sejumlah uang. Saat ini sistem pembayaran elektronik yang sudah digunakan mencakup penggunaan kartu kredit, kartu debit, internet banking, dll. Setiap jenis sistem pembayaran elektronik memiliki prosedur dan protokol masing – masing. Salah satu protokol yang dikeluarkan oleh Visa dan MasterCard adalah SET (Secure Electronic Transaction). Protokol SET melibatkan empat entitas utama, yaitu pemegang kartu (cardholder / customer), merchant, acquirer (bank merchant), issuer (bank customer). Pemegang kartu dan merchant harus mendaftar CA (Certificate Authority) terlebih dahulu. Langkah - langkah transaksi pada protokol SET berdasarkan referensi [1] secara sederhana adalah sebagai berikut :

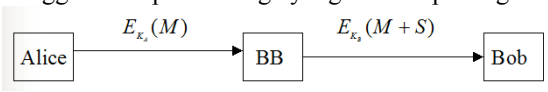
- Customer melakukan browsing di situs e-commerce dan menentukan barang / jasa apa yang akan dibelinya
- Customer mengirimkan order / pesanan dan informasi pembayaran, berupa message dengan dua bagian, yaitu Purchase Order (PO) untuk merchant dan informasi kartu kredit untuk acquirer. Merchant mengirimkan informasi kartu kredit ke acquirer.
- Acquirer memeriksa issuer untuk keperluan otorisasi pembayaran
- Issuer mengirimkan hasil otorisasi ke acquirer, acquirer mengirimkan otorisasi ke merchant
- Merchant memfinalisasi pesanan dan mengirim konfirmasi ke customer
- Merchant memperoleh transaksi dari acquirer

- Issuer mencetak bill kartu kredit (invoice) kepada customer

2.1. Tanda-tangan Digital

Tanda tangan digital adalah tanda-tangan untuk data digital. Tanda-tangan digital berfungsi sebagai otentikasi pada data digital (pesan, dokumen elektronik). Tanda tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci. Tanda-tangan digital ini selalu berbeda-beda antara satu isi dokumen dengan dokumen lain. Tanda tangan digital dapat dilakukan dengan dua cara yaitu enkripsi pesan dan menggunakan kombiansi fungsi hash dan kriptografi kunci-publik.

Jika menggunakan cara melalui enkripsi pesan maka pesan dienkripsi dengan algoritma simetri. Namun, cara ini tidak menyediakan mekanisme untuk anti-penyangkalan. Kelemahan ini dapat diatasi dengan menggunakan pihak ketiga yang disebut penengah.



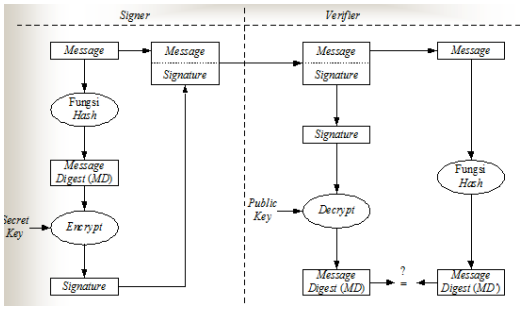
Gambar 2.1 : Tanda Tangan Digital dengan Cara Enkripsi.

Jika menggunakan cara kedua, maka pesan terlebih dienkripsi dengan kunci privat pengirim. Pesan kemudian didekripsi oleh penerima dengan kunci public pengirim. Dengan cara ini, maka kerahasian pesan dan otentikasi keduanya tercapai sekaligus dengan demikian tidak perlu lagi penengah. Algoritma kunci-publik untuk digunakan pada tanda-tangan digital harus memenuhi sifat:

$$D_{SK}(E_{PK}(M)) = M \text{ dan } D_{PK}(E_{SK}(M)) = M$$

Gambar 2.2 : Sifat Kunci-publik untuk Tanda Tangan Digital.

Untuk kasus tertentu dimana kerahasian pesan tidak diperlukan melainkan hanya memerlukan informasi keotentikan pesan saja, pemanfaatan algoritma kriptografi kunci-publik dan fungsi hash dapat digunakan seperti pada diagram di bawah ini.



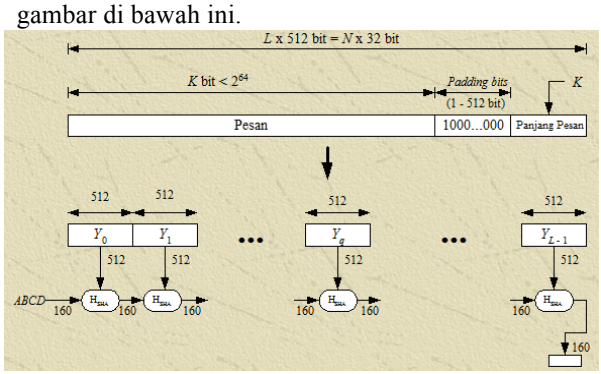
Gambar 2.3 : Diagram Penggunaan Tanda Tangan Digital sebagai Alat Otentikasi Pesan

2.2. SHA (Secure Hash Algorithm)

SHA adalah fungsi hash satu-arah yang digunakan bersama DSS (Digital Signature Standard). SHA memiliki enam varian dan salah satunya adalah SHA-1. Langkah-langkah pemuatan message digest dengan SHA-1 sebagai berikut:

1. Penambahan bit-bit pengganjal
2. Penambahan nilai panjang pesan semula
3. Inisialisasi penyangga MD
4. Pengolahan pesan dalam blok berukuran 512 bit.

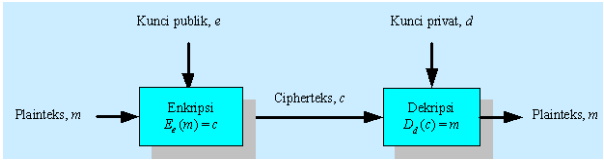
Skema pembuatan message digest ditunjukkan pada gambar di bawah ini.



Gambar 2.3 : Skema Pembuatan Message Digest

2.3. Kriptografi Kunci-Publik

Kriptografi ini muncul untuk mengatasi kekurangan kunci-simetri yaitu bagaimana mengirimkan kunci rahasia kepada penerima. Pada kriptografi ini, masing-masing pengirim dan penerima mempunyai sepasang kunci yaitu kunci public untuk mengenkripsi pesan dan kunci privat untuk mendekripsi pesan. Kelebihan kriptografi ini adalah tidak diperlukan pengiriman kunci rahasia dan jumlah kunci dapat ditekan. Kriptografi ini didasarkan pada fakta bahwa komputasi untuk enkrip/dekrip pesan mudah dilakukan dan secara komputasi hampir tidak mungkin menurunkan kunci privat bila diketahui kunci publik. Pasangan kunci ini pun tidak perlu diubah bahkan dalam periode waktu yang panjang. Namun, proses enkripsi dan dekripsi memakan waktu yang besar karena melibatkan operasi perpangkatan yang besar. Selain itu, ukuran chiperteks lebih besar daripada plainteks sehingga bisa dua sampai empat kali ukuran plainteks. Oleh karena itu, kripto ini biasa digunakan untuk pertukaran kunci.



Gambar 2.4 Diagram Proses Enkripsi/Dekripsi Kriptografi Kunci Publik

III. OTORISASI PADA PROTOKOL SET

Berdasarkan kamus, authorization berarti tindakan untuk mengotorisasi, di mana mengotorisasi berarti memberikan wewenang tertentu. Otorisasi dapat

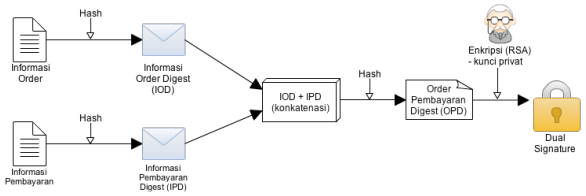
diartikan sebagai proses pemberian hak / wewenang kepada suatu pihak untuk melakukan atau memiliki sesuatu. Misalnya pada sistem komputer multiuser, otorisasi dilakukan oleh administrator sistem dengan mendefinisikan pengguna mana yang boleh mengakses ke sistem dan kepentingan apa yang dimilikinya (termasuk akses ke file atau direktori mana, batasan waktu akses, dll.) Otorisasi mencakup segala fungsi yang mendefinisikan hak akses terhadap resources yang ada, dan secara lebih spesifiknya untuk keperluan kontrol akses. Jadi, otorisasi berhubungan dengan penentuan apakah pengguna tertentu (yang sudah diotentikasi) memiliki hak atau izin untuk mengakses, memanipulasi, maupun menghapus resource tertentu.Pada protokol SET, otorisasi diperlukan untuk memastikan bahwa merchant dan bank hanya dapat melihat informasi yang dibutuhkan dan diizinkan saja. Oleh karena itu, salah satu kunci utama teknologi SET adalah dual signature yang digunakan untuk kepentingan privasi informasi order dan pembayaran.

Sedangkan kontrol akses sendiri merupakan bagian dari otorisasi. Kontrol akses merupakan mekanisme di mana sistem memberikan hak untuk mengakses data atau melakukan aksi tertentu. Mekanisme ini mengendalikan operasi apa yang boleh dan tidak boleh dilakukan oleh pengguna tertentu, misalnya dengan melihat user ID-nya. Kontrol akses pada sistem secara umum mencakup hak akses file (create, read, edit, deleteserver file), hak akses program (hak mengeksekusi program pada server aplikasi), dan hak akses data (hak mengambil dan mengubah informasi pada basis data). Kontrol akses terdiri dari dua fase, yaitu fase pendefinisian kebijaksanaan (policy definition) dan fase pelaksanaan kebijaksanaan (policy enforcement). Pada fase pertama dilakukan otorisasi akses, sedangkan pada fase kedua dilakukan persetujuan atau penolakan terhadap akses tersebut. Beberapa model kontrol akses yang ada adalah sebagai berikut

3.1 Dual Signature

Dual signature secara umum merupakan menggabungan (konkatenasi) dua message yang diterima oleh dua pihak, namun masing – masing pihak hanya dapat membaca message yang memang berhak untuk dilihatnya. Secara umum, tahap pembentukan dual signature pada pembayaran elektronik dengan protokol SET dapat dilihat pada gambar III.1 dan dapat dibaca secara lebih rinci pada referensi Implementation of Dual Signature in Java [2].

Hasil dual signature inilah yang akan diterima baik oleh merchant maupun oleh bank. Yang berbeda adalah, merchant diberikan Informasi Order beserta IPD, sedangkan bank diberikan Informasi Pembayaran beserta IOD. Untuk kebutuhan verifikasi, merchant melakukan hash pada konkatenasi antara IO (InformasiOrder) dengan IPD, bila hasilnya sama dengan hasil dekripsi dari dual signature, berarti verifikasi sukses. Begitu pula untuk bank, untuk verifikasi, bank melakukan hash terhadap konkatenasi antara IP (InformasiPembayaran) dengan IOD, dan dibandingkan dengan dekripsi dual signature. Pada tahap ini dapat dilihat bahwa otorisasi dilakukan untuk memastikan merchant hanya memiliki Informasi Order, IPD, dan dual signature, sedangkan bank hanya boleh memiliki Informasi Pembayaran, IOD, dan dual signature.



Gambar III.2 Proses pembentukan Dual Signature pada SET

3.2 Mekanisme Otorisasi pada SET

Mekanisme otorisasi ini terdiri dari tahap request dan response. Request otorisasi dilakukan oleh merchant kepada Payment Gateway, di mana pesan request tersebut terdiri dari :

1. Informasi berkaitan dengan pembayaran : Informasi Pembayaran, dual signature, IOD, dan amplop digital
2. Informasi berkaitan dengan otorisasi : blok yang terdiri dari ID transaksi yang ditandai dengan kunci privat merchant dan dienkripsi dengan one-time session key
3. Sertifikat : sertifikat signature key cardholder, sertifikat signature key merchant, sertifikat pertukaran kunci merchant.

Dan yang dilakukan oleh Payment Gateway adalah sebagai berikut :

1. Memverifikasi semua sertifikat di atas
2. Mendekripsi amplop digital otorisasi untuk memperoleh kunci simetris dan blok dekripsi
3. Memverifikasi signature merchant pada blok otorisasi
4. Mendekripsi amplop digital pembayaran untuk memperoleh kunci simetris dan blok dekripsi
5. Memverifikasi dual signature pada blok pembayaran
6. Memverifikasi ID transaksi dari merchant dicocokkan dengan Informasi Pembayaran dari kostumer
7. Meminta dan menerima otorisasi Issuer

Tahap berikutnya adalah respon terhadap otorisasi, yang pesannya terdiri dari tiga informasi, yaitu informasi berkaitan dengan otorisasi, capture token information, sertifikat. Secara umum, protokol SET memiliki kelemahan yaitu banyaknya transaksi yang

berlangsung sehingga membutuhkan waktu yang agak lama. Transaksi – transaksi yang berlangsung mencakup 4 message antara merchant dan cardholder, 2 message antara merchant dan payment gateway, 6 kali sertifikasi sertifikat digital, 9 siklus enkripsi/dekripsi RSA, 4 kali verifikasi sertifikat, 4 kali enkripsi/dekripsi DES. Secara lebih rinci, transaksi yang terjadi pada protokol ini dapat dilihat pada gambar II.3 sampai gambar II.6 dan pembentukan message yang terjadi dapat dilihat pada tabel III.1. Selain itu, untuk mengimplementasikan dual signature, cardholder harus menginstal aplikasi khusus, yang sering disebut e-wallet. E-wallet ini adalah kebutuhan mutlak pada SET karena e-wallet bertugas membuat semua message yang digunakan selama transaksi berlangsung.

Dual signature memiliki beberapa karakteristik yang membuatnya penting dan cocok diterapkan pada sistem e-payment menggunakan kartu kredit, yaitu :

1. Karena sifat hash yang aman, maka tidak layak untuk menemukan informasi order maupun informasi pembayaran lain yang berarti yang memiliki hash ke nilai yang sama namun namun dual signature membantu dalam mendapatkan hash dari knkatenasi hasil hash dari order information dan payment information.
2. Karena cardholder menandatangani hash, maka tidak memungkinkan ada orang lain yang dapat menemukan tanda tangan yang mengacu pada value yang sama. Bagaimanapun, ada hanya satu pasangan informasi order dan informasi pembayaran sebagai input dari berbagai dual signature yang diberikan. Selain itu, tidak memungkinkan untuk memalsukan tanda tangan orang lain, yang akan mengakibatkan dual signature mengikat secara tidak ambigu terhadap informasi order dan payment.
3. Ketika merchant melakukan validasi dual signature, mereka akan merasa yakin bahwa dual signature tersebut memang dibuat oleh cardholder itu. Selain itu, merchant mengecek apabila informasi order yang digunakan sebagai input ke dual signature terurut dengan benar jika dibandingkan dengan data yang disupply oleh cardholder dengan kopian lokal dari deskripsi order.
4. Merchant tidak bisa mengecek apabila informasi pembayaran pada dual signature adalah valid, ini mungkin diakibatkan dengan hubungan dengan payment gateway
5. Payment gateway juga melakukan pengecekan terhadap dual signature untuk kebenarannya. Jika valid, maka payment gateway yakin mengenai autentikasi dan integritas dari dual signature. Setelah merchant mengecek bahwa pembayaran itu memang valid milik orang (cardholder) tersebut, dan payment gateway sudah mengecek kebenarannya, maka tidak ada jalan sama sekali bagi cardholder dan merchant untuk melakukan penipuan

PInitReq,PInitRes	Purchase initialization request/response.
PReq,PRes	Purchase request/response.
AuthReq,AuthRes	Authorization request/response.
AuthRevReq,AuthRevRes	Authorization reversal request/response.
InqReq,InqRes	Inquiry request/response.
CapReq,CapRes	Capture request/response.
CapRevReq,CapRevRes	Capture reversal request/response.
CredReq,CredRes	Credit request/response.
CredRevReq,CredRevRes	Credit reversal request/response.
PCertReq,PCertRes	Payment gateway's certificate request/response.
BatchAdminReq,BatchAdminRes	Batch Administration request/response.
CardCInitReq,CardCInitRes	Cardholder's certificate initialization request/response.
Me-AqCInitReq,Me-AqCInitRes	Merchant's or acquirer's certificate initialization request/response.
RegFormReq,RegFormRes	Registration form request/response.
CertReq,CertRes	Certificate request/response.
CertInqReq,CertInqRes	Certificate inquiry request/response.

Tabel III.1 Message pada protokol SET
(Sumber : Goichiro Hanaoka, Yuliang Zheng, Hideki Imai, LITESET : a Light-Weight Secure Electronic Transaction Protocol [3])

IV. IMPLEMENTASI

Pada tahap implementasi, terdapat tiga tahap utama, yaitu :

1. GUI
2. Membuat Fungsi Hash
3. Menyusun Algoritma enkripsi

Masing – masing tahap tersebut akan dijelaskan pada subbab 4.1 dan 4.2

4.1 GUI

Untuk memahami konsep dual signature dengan lebih baik, dibuat sebuah GUI untuk pengguna dan akan digunakan untuk pengguna memasukkan informasi order, seperti ID, nama, dll. Di bawah ini merupakan screenshoot implementasi GUI pada sistem pembayaran elektronik (e-payment) :

Gambar 4.1 Screenshot Program

4.2 Pembuatan Fungsi Hash

Setelah menekan tombol Procees Payment pada layer GUI, dibentuk sebuah message digest untuk informasi order. Algoritma MD yang digunakan adalah SHA-1. Ketika useer menekan tombol Pay, dibentuk sebuah message digest dari informasi pembayaran seperti nomor kartu kredit, nama, CCV, tanggal expired, dll. Berikut ini adalah source code untuk pembentukan message digest.

```
public static String message (string msg){
    MessageDigest MD =
MessageDigest.getInstance("SHA-1");
    md.update(msg.getBytes);
    byte[] mb = md.digest;
```

```
        printed = "";
        for (int i=0; i<mb.length(); i++){
          byte temp = mb[i];
          String s = Integer.toHexString(new
Byte(temp));
          while (s.length() <2){
            s="0"+s;
          }
          s=s.substring(s.length()-2);
          printed+=s;
        }
        return printed;
        }
    }
```

Gambar 4.2 Metode implementasi SHA-1

4.3 Pembuatan Algoritma Enkripsi

Pada dual signature, digunakan algoritma enkripsi kunci publik. Pada implementasi ini, digunakan algoritma enkripsi kunci publik yaitu RSA-1024 bit key size. Untuk menerapkan algoritma RSA, ddilakukan tiga tahap sebagai berikut :

1. Memilih dua angka prima (P dan Q)
2. Hitung N menggunakan rumus

$$N = P \times Q$$

3. Pilih secara acak kunci publik tersebut (i.e, kunci enkripsi) E di mana bukan merupakan faktor (P-1) dan (Q-1)
4. Pilih sebuah kunci privat (i.e. description key), D, yang rumusnya sebagai berikut. hitung text CT nyaa fro

$$(D \times E) \bmod (P-1) \times (Q-1) = 1$$

5. Untuk enkripsi, hitung teks cipher CT dari plaintext PT sebagai berikut

$$CT = PTE \bmod N$$

6. Kirim CT sebagai cipher text kepada penerima
7. Untuk dekripsi, hitung plaintext Plaintext PT dari ciphertext (CT) dengan rumus sebagai berikut :

$$PT = CT^{D} \bmod N$$

Source code untuk implementasi algoritma enkripsi adalah sebagai berikut :

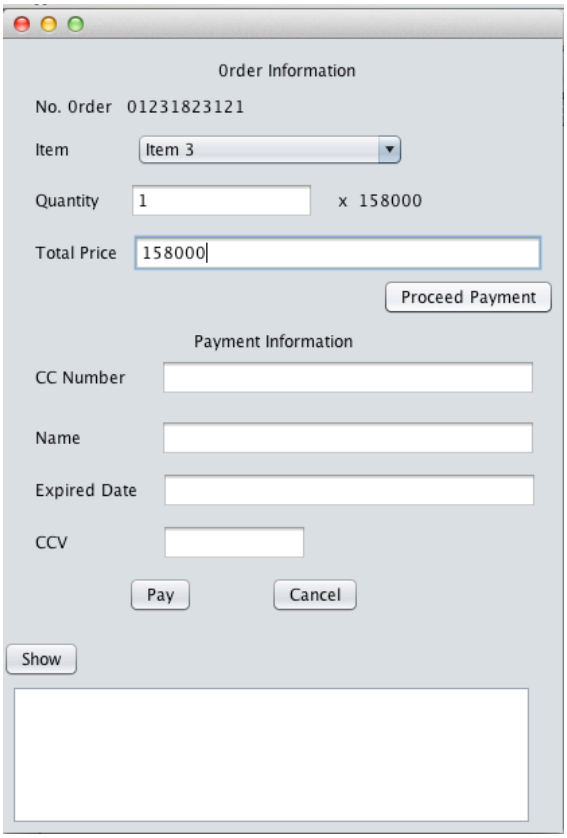
```
        public Set (int N){
BigInteger p = BigInteger.probabalePrime (N/2,
random);
BigInteger q = BigInteger.probabalePrime (N/2,
random);
        N = P multiply (Q)
        BigInteger m = (p subtract (BigIntegerONE))
multiply (q.subtract (BigInteger ONE);
        E = new BigInteger("5");

while (m.gcd(e).intValue()>1){
        e = e.add(new BigInteger("2"));
d = e.modInverse (m);
System.out.println ("Private : "+d);
System. out.println (modulus (N) start "N");
}

public BigInteger Encrypt(BigInteger message)
{
        return message.modPow(e,N);
}


public BigInteger Decrypt(BigInteger encrypted)
{
        return encrypted.modPow(D,A);
}
```

Gambar 4.2 Metode implementasi algoritma enkripsi

V. RESULT

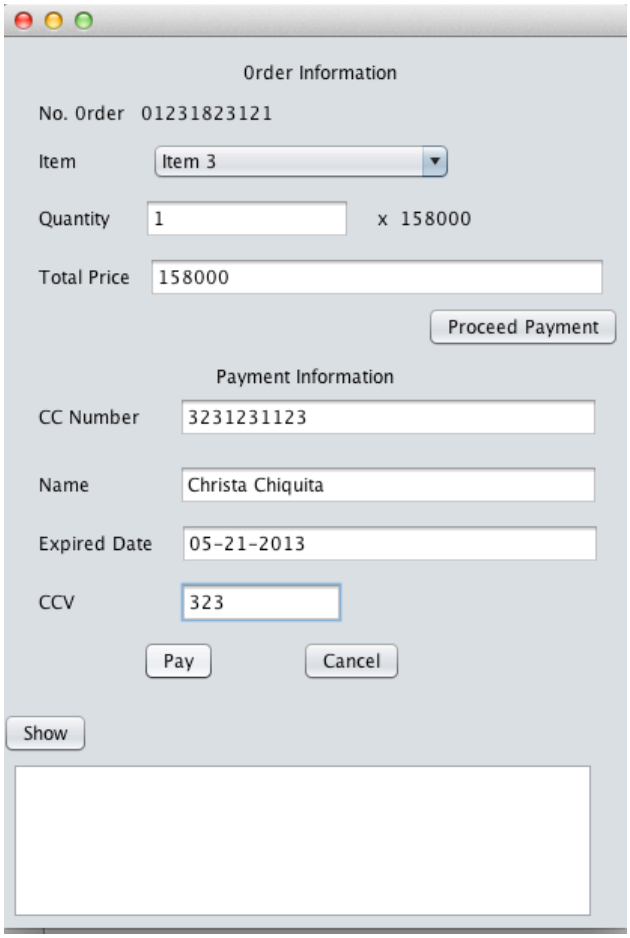
Untuk memverifikasi kebenaran dual signature maka dilakukan step – step berikut ini.

Step 1 :Pengguna memilih barang dari dropdown list kemudian menginput jumlah item yang diinginkan, kemudian klik "Proceed Payment".



Gambar 5.1 Step 1

Step 2 : Masukkan informasi pembayaran dan klik "Pay"



Gambar 5.2 Step 2

Step 3 : Ketika tombol "Pay" ditekan, sistem akan melakukan pembentukan message digest. Dan jika ditekan tombol Show maka akan ditampilkan seperti berikut ini.

No. order : 01231823121
Item Name : Item 3
Item Price : 158000
Quantity : 1
Total Price : 158000

CC Number : 3231231123
Name : Christabella Chiquita
Exp Date : 21 Mei 2013
CCV : 323

Message : 236472384635182926409283
Encrypted :
328174357814370134796536631737235703703174130740163483147801364817402709568650873863773727329183916366463478279180219018402894737438481685914193791273914791823010474756275932414914801402709568650873863773727329183916366463478279180219018402838418237104683
Decrypt : 236472384635182926409283

VI. SIMPULAN

Digital signature merupakan suatu metode yang diterapkan untuk membuat dual signature yang dimanfaatkan oleh VISA dan MASTER CARD. Karena pada dual signature ini menerapkan bahwa kedua informasi penting (informasi order dan informasi pembayaran masing – masing dibuat menjadi message digest terlebih dahulu, sehingga dengan mekanisme ini, dapat disimpulkan bahwa keamanan sistem terutama di bagian otorisasi.

REFERENCES

[1] Li, Y., & Wang, Y. (n.d.). Secure Electronic Transaction (SET protocol), 1–16
[2] [11] Singh, S., & Prema, K. V. (2012). Implementation of Dual Signature in Java, 2(3), 302–307.
[3] Hanaoka, G., Zheng, Y., & Imai, H. (n.d.). LITESET : a Light-Weight Secure Electronic Transaction Protocol.
[4] SET. Secure Electronic Transaction Specification - Book1: Business Description. http://www.setco.org/download.html/set_bk1.pdf, May 1997
[5] SET. Secure Electronic Transaction Specification – Book3: Formal Protocol Definition. http://www.setco.org/download.html/set_bk3.pdf, May 1997
[6] [7] S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., 1999 pp553- 554.
[7] [8] An Introduction to Cryptology Prentice-Hall, ISBN 0-13- 030369-0web services
[8] [9] Java GUI Applications Learning Trails:‖http://netbeans.org/kb/trails/matisse.html‖.

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, 20 Mei 2013

Christabella Chiquita 13509050