Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.

Implementasi Metode Kriptografi RSA Pada Priority Delaer Untuk Layanan Penjualan Dan Pemesanan Handphone Berbasis J2ME

Arinta Nugrahani Ayuningtyas [1] Mike Yuliana [2] M Zen Samsono Hadi [2]
[1] Mahasiswa Politeknik Elektronika Negeri Surabaya, Jurusan Teknik Telekomunikasi
[2]Dosen Politeknik Elektronika Negeri Surabaya Institut Teknologi Sepuluh Nopember
Kampus ITS, Surabaya 60111
e-mail : arintz_tha_dw@yahoo.co.id

Abstrak – Distributor adalah perantara yang menyalurkan produk dari pabrik (*manufacturer*) ke priority dealer. Sebuah distributor memiliki beberapa *priority dealer* yang melakukan penjualan *handphone* langsung pada konsumen (*end user*). Pada kenyataannya pembelian dari *priority dealer* ke distributor dilakukan secara langsung. Laporan hasil penjualan *handphone*, akan dituliskan pihak *priority dealer* di sebuah buku yang nantinya akan dilaporkan kepada distributor. Untuk itu diperlukan suatu layanan yang bisa mempermudah sistem itu yaitu komunikasi dengan *mobile device* secara *online* dan untuk keamanan datanya digunakan kriptografi *Riverst Shamir Adleman* (RSA).

Pada proyek akhir ini dibuat suatu sistem layanan penjualan dan pemesanan handphone pada *priority dealer* dimana ini merupakan interaksi antara *server* yang berbasis PHP dengan *client* yang berbasis J2ME. Data yang dikirimkan dari *client* ke *server* dienkripsi menggunakan algoritma RSA, lalu oleh *server* data tersebut didekripsi sehingga kembali seperti bentuk data awalnya dan bisa diolah untuk diinformasikan ke *client*.

Hasil yang didapatkan pada proyek akhir ini adalah sebuah layanan penjualan dan pemesanan untuk *priority dealer* dengan menggunakan kriptografi RSA. Metode enkripsi RSA merupakan metode enkripsi yang non linier karena jumlah karakter asli dan hasil proses enkripsi memiliki panjang atau jumlah karakter yang tidak sama. Waktu yang diperlukan untuk proses enkripsi/dekripsi RSA dari client ke server adalah 63 detik sampai 149 detik .

Kata kunci : Kriptografi, Enkripsi, Dekripsi, RSA

1. PENDAHULUAN

Distributor adalah perantara yang menyalurkan produk dari pabrik (*manufacturer*) ke *priority dealer*. Sebuah distributor memiliki beberapa *priority dealer* yang melakukan penjualan *handphone* langsung pada konsumen (*end user*). Pada kenyataannya untuk pembelian dari priority dealer ke distributor dilakukan secara langsung. Untuk laporan hasil penjualan handphone, pihak *priority dealer* akan menuliskan hasil penjualannya disebuah buku yang nantinya akan dilaporkan kepada distributor.

Saat ini banyak sistem pejualan yang berbasis online dengan tujuan memudahkan proses pembelian bagi pelanggan, namun kelemahannya yaitu banyak *hacker* yang akan menyadap informasi secara diam-diam, sehingga keamanan data benar-benar menjadi permasalahan yang sangat penting terutama pada jaringan komputer. Oleh karena itu perlu diberikannya sistem pengamanan data.

Pada tugas akhir ini dibuat implementasi metode kriptografi RSA pada *prioity dealer* untuk layanan penjualan dan pemesanan handphone berbasis J2ME. Dalam pembuatan J2ME diperlukan suatu program yang mana dapat melayani penjualan dan pemesanan yang terintegrasi dengan database MySQL dan server apache. Pada sistem pengamanan data yang dikirim dari sisi *priority dealer* ke sisi *server* menggunakan metode RSA. Metode RSA digunakan untuk mengenkripsi data informasi pemesanan dan penjualan *handphone* dalam bentuk teks dan mendekripsikannya agar menjadi data teks yang asli sehingga data tersebut kemudian akan dapat diakses oleh *priority dealer*

2. TEORI PENUNJANG

2.1 J2ME

Teknologi Java merupakan sebuah teknologi yang berkembang sangat pesat akhir-akhir ini. Bahkan belakangan ini dikabarkan berusaha mengalahkan Microsoft yang terkenal sebagai kampiun dari produsen *operating system* dimuka bumi ini.

Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.

2.2 PHP MySQL

PHP merupakan suatu program yang dapat dikoneksikan dengan program yang lain seperti java dan database MySQL. Berikut ini adalah langkah-langkah koneksi PHP-MySQL:

1. Membuka koneksi ke *server* MySQL
   mysql_connect()
2. Memilih *database* yang akan digunakan di *server*
   mysql_select_db()
3. Mengambil sebuah query dari sebuah *database*
   mysql_query()
4. Mengambil *record* dari tabel
   a. mysql_fetch_array()
   b. mysql_fetch_assoc()
   c. mysql_fetch_row()
   d. mysql_num_rows()

2.3 Algoritma RSA

RSA adalah salah satu contoh kriptografi yang menerapkan konsep public key. Kunci pada RSA mencakup dua buah kunci, yaitu public key dan private key. *Public key* digunakan untuk melakukan enkripsi, dan dapat diketahui oleh orang lain. Sedangkan *private key* tetap dirahasiakan dan digunakan untuk melakukan dekripsi.

Pembangkitan kunci atau key generation dari RSA adalah sebagai berikut :

1. Pilih dua buah bilangan prima sembarang a dan b. Jaga kerahasiaan a dan b ini.
2. Hitung n = a * b. Besaran n ini tidak perlu dirahasiakan.
3. Hitung m = (a-1) * (b-1). Sekali m telah dihitung, a dan b dapat dihapus untuk mencegah diketahuinya oleh pihak lain.
4. Pilih sebuah bilangan bulat untuk kunci publik, sebut namanya e, yang relatif prima terhadap m (relatif prima berarti GCD(e, m) = 1) dengan syarat e ≠ (p-1), e ≠ (q-1), dan e < n
5. Hitung kunci dekripsi, d, dengan kekongruenan ed ≡1 (mod m).

$$d = \frac{1 + km}{e}$$

Proses enkripsi dapat dilakukan dengan :

$$C = P^e \bmod n$$

Proses dekripsi dapat dilakukan dengan :

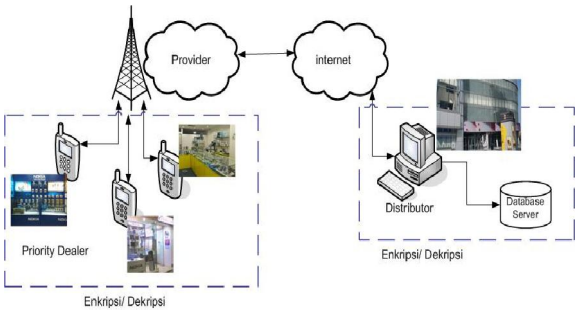
$$P = C^d \bmod n$$

3. Perencanaan Sistem

3.1 Cara kerja

3.1.1 Perancangan Sistem

Pada proyek akhir ini digunakan satu buah PC *(Personal Computer)* dan dapat menggunakan hanya satu buah *handphone* saja. PC ini bertindak sebagai *server* sedangkan *handphone* bertindak sebagai *client* yang dapat digunakan oleh *priority dealer*.



Gambar 1 Blok Diagram Sistem

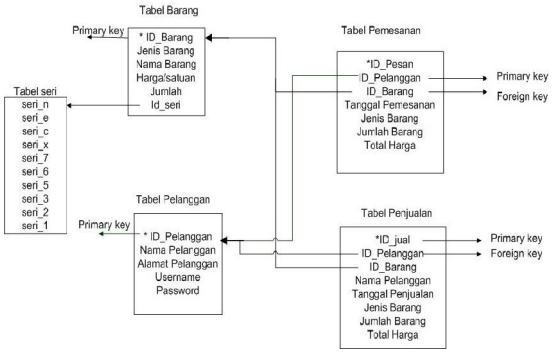
6.1.2 Perancangan Program Interaksi Client Server

Pada *handphone priority dealer* akan dibuat sebuah aplikasi untuk input data maupun mengakses *database server*. Untuk tampilannya akan dibuat 3 buah menu utama yaitu pesan barang, laporan penjualan dan menu untuk keluar. Pada menu pesan barang akan ditampilkan menu pemesanan dan cek stok, dimana dalam menu pemesanan ini terbagi dalam 10 jenis menu yaitu seri N, seri E, sri X, seri C, seri 7, seri 6, seri 5, seri 3, seri 2 dan seri 1. Dan Pada menu laporan penjualan, terbagi dalam 10 jenis menu juga yaitu seri N, seri E, seri X, seri C, seri 7, seri 6, seri 5, seri 3, seri 2 dan seri 1.

3.1.3 Perancangan Database

Pada proyek akhir ini database terdapat 2 tabel utama yaitu tabel barang dan tabel pelanggan. Dari tabel barang dan tabel pelanggan ini dibuat suatu relasi sehingga dibuat tabel baru yaitu tabel pemesanan dan tabel penjualan, selain itu tabel barang juga dibuat relasi tabel baru yaitu tabel seri.

Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.



Gambar 2 Relasi Antar Tabel

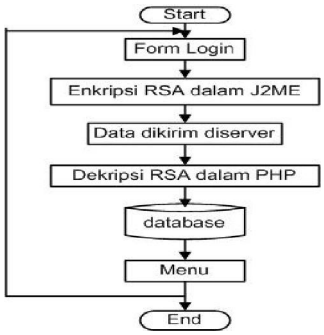
4. Implementasi, Hasil dan Analisa

Pada tahap ini metode enkripsi/dekripsi RSA diimplementasikan pada *handphone priority dealer* yang berbasis J2ME yang terintegrasi dengan PC *server* yang berbasis php.

4.1 Impelementasi Metode Enkripsi /Dekripsi RSA yang terintegrasi antara Client Berbasis J2ME dan Server Berbasis PHP

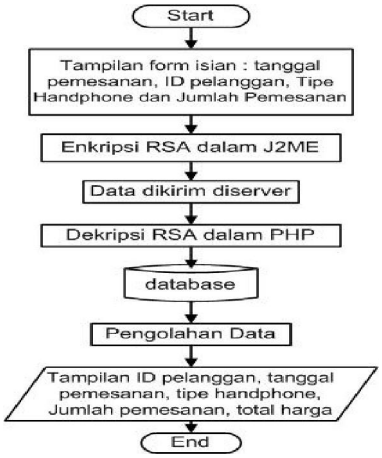
Pada bagian ini metode enkripsi RSA diimplementasikan pada *handphone client* untuk proses enkripsi data *string* dan metode dekripsi RSA diimplementasikan pada PC *server* untuk proses dekripsi data.

Flowchart implementasi enkripsi / dekripsi RSA pada login ditunjukkan pada gambar 3.



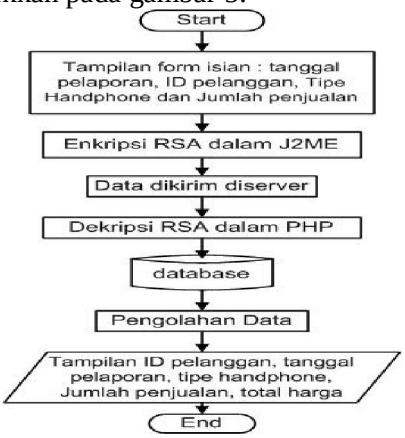
Gambar 3 *Flowchart* Imlementasi Enkripsi/ Dekripsi RSA Pada Login

Flowchart implementasi enkripsi/ dekripsi RSA pada menu pemesanan barang ditunjukkan pada gambar 4.



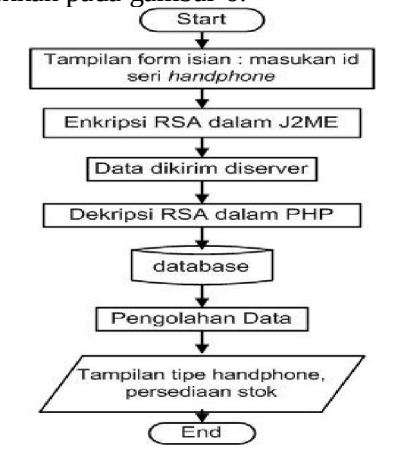
Gambar 4 *Flowchart* Imlementasi Enkripsi/ Dekripsi RSA Pada Pemesanan Barang

Flowchart implementasi enkripsi / dekripsi RSA pada menu laporan penjualan ditunjukkan pada gambar 5.



Gambar 5 *Flowchart* Imlementasi Enkripsi/Dekripsi RSA Pada Laporan Penjualan.

Flowchart implementasi enkripsi / dekripsi RSA pada menu pengecekan stok ditunjukkan pada gambar 6.



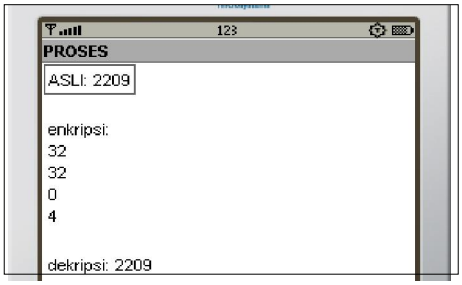
Gambar 6 *Flowchart* Imlementasi Enkripsi/Dekripsi RSA Pada Pengecekan Stok.

Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.

4.2 Pengujian dan Analisa

7.2.1 Pengujian dan Analisa Implementasi Metode Enkripsi/ Dekripsi RSA pada handphone, PC , dan Integrasi Client Server

Pada data *string* yang diisikan di *textfield*, pengujian dilakukan dengan menampilkan simbol hasil enkripsi, dan hasil dekripsi kemudian dibandingkan dengan teks aslinya menggunakan metode RSA untuk karakter angka. Perbandingan data sebelum dan sesudah enkripsi serta sesudah dekripsi untuk karakter dalam j2me bisa dilihat pada gambar 7.



Gambar 7 Hasil Enkripsi/Dekripsi Karakter di *Handphone*

Dari proses enkripsi/dekripsi RSA pada data string berupa huruf , angka dan metakarakter tersebut terlihat bahwa metode enkripsi/dekripsi yang dibuat telah teruji kebenarannya, karena *string* yang terenkripsi setelah didekripsi kembali ke *string* aslinya.

4.2.2 Pengujian, Perbandingan dan Analisa Linieritas Hasil Enkripsi

Tujuan dari pengujian ini adalah untuk mengetahui panjang dari simbol hasil enkripsi apakah panjangnya sama dengan dengan panjang karakter yang dikirimkan atau tidak. Dikatakan linier jika panjang hasil enkripsi sama dengan dengan panjang karakter teks aslinya. Kemudian linieritas metode RSA ini dibandingkan dengan *software* enkripsi lain dari *open source*

a. Pengujian dan Analisa Linieritas Hasil Enkripsi Menggunakan Metode RSA

Pengujian ini dilakukan dengan mengamati panjang dari simbol yang dihasilkan dari proses enkripsi menggunakan metode RSA dan membandingkannya dengan panjang teks aslinya. Berikut ini adalah gambar hasil simbol enkripsi RSA :

Tabel 1 . Panjang karakter asli dan simbol enkripsi metode RSA

Karakter Asli	Jumlah Karakter	Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi
1	1	1	1
12	2	132	3
123	3	13233	5
1234	4	132339	6
12345	5	13233910	8
123456	6	132339106	9
1234567	7	1323391067	10
12345678	8	13233910678	11
123456789	9	132339106784	12
1234567890	10	1323391067840	13

Dari tabel 1 dapat diketahui bahwa metode enkripsi RSA ini adalah non linier karena panjang karakter teks asli yang dikirimkan tidak sama panjangnya dengan panjang karakter hasil proses enkripsi.

b. Pengujian dan Analisa Linieritas Hasil Enkripsi Menggunakan Software Enkripsi PGP

Pada pengujian ini *software* PGP digunakan sebagai pembanding terhadap linieritas panjang karakter hasil enkripsi. Perbandingan ini dilakukan dengan mengamati panjang dari simbol yang dihasilkan dari proses enkripsi menggunakan metode PGP dan membandingkannya dengan panjang teks aslinya. Untuk lebih jelasnya dapat dilihat pada tabel hasil enripsi dibawah ini :

Tabel 2 . Panjang karakter asli dan simbol enkripsi metode PGP

Karakter Asli	Jumlah Karakter	Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi
1	1	QAgPHyyDJgCThi1mWr1KANti41pM2vcFxBNGcQPFFDbiq	45

Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.

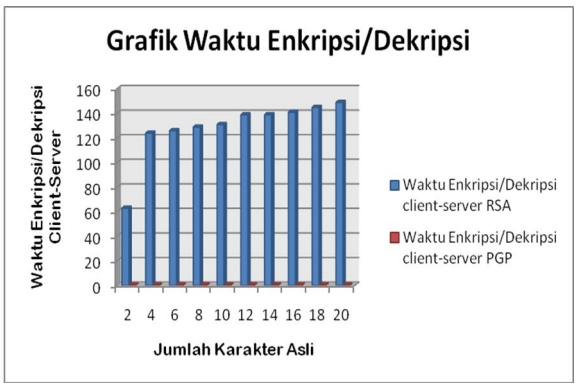
12	2	P/TA4q61 BDc1Cj4N bKxOVxe uBPiM71 KxPPOQO v64xpeRf	45
123	3	P8c7k2Dv 6BjWJ/eO BuynlvAZ ++ljQ96m BDcdthYa HB9Da	45
1234	4	P8D5502tc mRorT6M KzQznk7Z 3lgg2c8xc Ki4ZJ5vP 2EINT	45

Dari tabel 2 dapat diketahui metode enkripsi PGP ini adalah non linier karena panjang karakter teks asli yang dikirimkan tidak sama panjangnya dengan panjang karakter hasil proses enkripsi.

Dari tabel 1 dan tabel 2 dapat disimpulkan bahwa algoritma enkripsi RSA merupakan metode enkripsi yang non linier, dan begitu juga dengan kriptografi PGP merupakan enkripsi yang non linier juga.

4.2.3 Pengujian, Perbandingan dan Analisa Waktu Enkripsi/Dekripsi

Pada pengujian ini dihitung waktu proses enkripsi di client dan proses dekripsi di server hingga data tersebut ditampilkan kembali pada client kembali. Kemudian waktu proses enkripsi/dekripsi akan dibandingkan antara algoritma RSA dengan software enkripsi yang lain mana yang lebih cepat prosesnya.



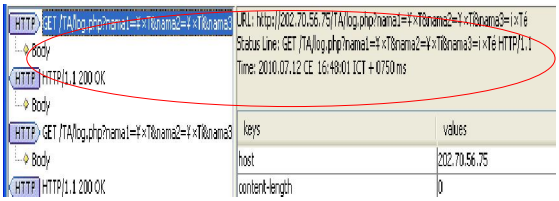
Gambar 8 Grafik Waktu Enkripsi/Dekripsi

Berdasarkan hasil pengujian terhadap lamanya waktu proses enkripsi antara metode RSA dan kriptografi PGP dapat disimpulkan bahwa kriptografi PGP memiliki waktu enkripsi/dekripsi yang lebih cepat karena kriptografi PGP dapat mengenkripsi dan mendekripsi *file* dengan jumlah karakter yang banyak dalam waktu yang singkat dibandingkan metode enkripsi RSA

4.2.4.Pengujian dan Analisa Menggunakan Monitoring Tool Sun Java Wireless Toolkit

Pada proses pengujian ini menggunakan Monitoring Tool Sun Java Wireless Toolkit sehingga dapat diamati autentikasi data hasil enkripsi yang dikirimkan dari client ke server.

Berikut ini adalah hasil yang ditunjukkan oleh tool monitoring *sun java wireless toolkit* :



Gambar 9. Autentikasi Data Login Pada Monitoring Tool Sun Java Wireless Toolkit

Dari gambar 9 dapat dilihat bahwa menu client server telah terenkripsi dengan baik, sehingga saat dilakukkan monitoring data maka pada tool yang digunakan attacker akan nampak simbol-simbol yang tidak dapat dibaca.

5. Kesimpulan

Dari hasil pengujian dan analisa pada bab sebelumnya, maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Algoritma enkripsi RSA dan PGP merupakan metode enkripsi yang non linier karena jumlah karakter asli dan hasil proses enkripsi memiliki panjang atau jumlah karakter yang tidak sama.
2. Waktu yang diperlukan oleh algoritma RSA untuk mengenkripsi dan mendekripsi dari client ke server adalah 63 detik -149 detik. Hal ini menunjukkan bahwa panjang karakter berpengaruh terhadap waktu proses enkripsi/dekripsi RSA. Sedangkan waktu proses enkripsi/dekripsi menggunakan software PGP adalah 0,3-0,4 detik. Hal

Generated by Foxit PDF Creator © Foxit Software
http://www.foxitsoftware.com For evaluation only.

ini menujukkan bahwa panjang karakter tidak berpengaruh signifikan terhadap waktu proses enkripsi/dekripsi *kriptografi* PGP.

3. Pengujian dari hasil enkripsi data pada kriptografi RSA hanya berupa angka, sedangkan huruf dan metakarakter tidak bisa dienkripsi.

6. Daftar Pustaka

[1] Krida Kusuma, "Keamanan Data Pada GPRS Menggunakan Algoritma RSA Berbasis J2ME", Proyek akhir STT-Telkom, 2007.

[2] Laili Aidi, "Perancangan dan Implementasi Aplikasi Layanan *Delivery Service* Pemesanan Makanan berbasis J2ME Studi Kasus di Hoka-Hoka Bento",Proyek akhir STT-Telkom, 2007.

[3] Zen S Hadi,*"Modul Teori PHPInternet Programming"*, PENS-ITS, Surabaya, 2009.

[4] Zen S Hadi,*"Modul Teori MySQL Internet Programming"*, PENS-ITS, Surabaya, 2009.

[5] Zen S Hadi,*"Modul Praktikum J2ME Internet Programming"*, PENS-ITS, Surabaya, 2009.

[6] Muhammad Iqbal, "Studi Teknis Metode Enkripsi RSA dalam Perhitungannya", Proyek akhir ITB, 2008.

[7] Rinaldi Munir, "*Kriptografi*", Informatika, Bandung, 2006.

[8] Dyah Retnowulan, " Pembuatan Sistem Pengamanan Informasi Pemesanan Barang Toko Komputer Berbasis J2ME Menggunakan Algoritma RC4", Proyek akhir PENS-ITS, Surabaya, 2010.