Pembuatan Sistem Pengamanan Informasi Pemesanan Barang Toko Komputer Berbasis J2ME Menggunakan Algoritma RC4

Dyah Retnowulan [1] M Zen Samsono Hadi [2] Mike Yuliana [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 : dyah@student.eepis-its.edu e-mail : zenhadi@eepis-its.edu, mieke@eepis-its.edu

Abstrak

Saat ini sebagian besar toko-toko baik di perkotaan maupun di pedesaan masih menggunakan cara yang manual untuk melakukan transaksi jual beli yaitu dengan datang langsung ke toko tersebut maupun melalui telepon, padahal di era globalisasi sekarang teknologi *online* melalui internet telah berkembang pesat. Akan tetapi masih sangat jarang digunakan sebagai media transaksi jual beli di sebagian besar toko yang ada di Indonesia. Akan tetapi keamanan jaringan internet masih kurang diperhatikan dan metode pengaman data yeng melewati jaringan internet masih sedikit dan jarang diterapkan oleh karena itu banyak *hacker* akan menyadap informasi secara diam-diam.

Pada proyek akhir ini dibuat interaksi antara *server* yang berbasis PHP dengan *client* yang berbasis J2ME. Data yang dikirimkan dari *client* ke *server* dienkripsi menggunakan algoritma RC4. 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 bahwa metode enkripsi RC4 merupakan metode enkripsi yang linier karena jumlah karakter asli dan hasil proses enkripsi memiliki panjang atau jumlah karakter yang sama, sedangkan software enkripsi AES merupakan metode yang non linier. Waktu yang diperlukan untuk proses enkripsi/dekripsi RC4 searah dari client ke server adalah 1,125 detik sampai 1,492 detik . Sedangkan waktu enkripsi/dekripsi bolak-balik yaitu dari client ke server dan server ke client adalah 1,265 detik sampai 1,625 detik. Sedangkan waktu proses enkripsi/dekripsi untuk karakter huruf, angka, dan metakarakter menggunakan software AES adalah 0,3-0,4 detik. Aplikasi integrasi *client server* tidak dapat mensupport karakter huruf kapital dan form choicegroup.

Kata Kunci : J2ME, Kriptografi, Enkripsi, Dekripsi, Algoritma RC4

1. Pendahuluan

Saat ini sebagian besar toko-toko baik di perkotaan maupun di pedesaan masih menggunakan cara yang manual untuk melakukan transaksi jual beli yaitu dengan datang langsung ke toko tersebut maupun melalui telepon, padahal di era globalisasi sekarang teknologi *online* melalui internet telah berkembang pesat. Akan tetapi masih sangat jarang digunakan sebagai media transaksi jual beli di sebagian besar toko yang ada di Indonesia.

Dalam proyek akhir ini dibuat suatu sistem pemesanan barang online melalui handphone yang aman serta disajikan analisis kinerja sistem pengamanan data yang dikirim dari sisi *client* (*handphone* pelanggan) ke sisi *server* menggunakan metode RC4 dengan menggunakan kunci simetrik. Metode RC4 digunakan untuk mengenkripsi data informasi pemesanan barang dalam bentuk teks dan mendekripsikannya agar menjadi data teks yang asli sehingga data tersebut kemudian akan dapat diakses oleh pemilik toko

2. Tinjauan Teori

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.

2.2. PHP (*Personal Home Page*)

PHP adalah skrip bersifat *server-side* yang ditambahkan ke dalam HTML. PHP merupakan *Hypertext Processor*. Skrip yang terdapat pada PHP akan membuat suatu aplikasi yang dapat terintegrasi ke dalam HTML, sehingga suatu halaman web tidak lagi bersifat statis, namun menjadi bersifat dinamis.

Ada beberapa cara untuk memulai menulis skrip PHP, yaitu :

1. <?php
   Script php anda
   ?>
2. <?
   Script php anda
   ?>

2.3 Database MySQL

MySQL sebenarnya merupakan turunan salah satu konsep utama dalam database sejak lama, yaitu *SQL (Structure Query Language)*. SQL adalah sebuah konsep pengoperasian *database*, terutama untuk seleksi dan pemasukan data, yang memungkinkan pengoperasian data dikerjakan dengan mudah secara otomatis.

2.4. 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()

2.5. Algoritma RC4

RC4 merupakan stream cipher yang didesain oleh Rivest untuk RSA Data *Security* (sekarang *RSA Security*) pada 1987. RC4 menggunakan panjang variabel kunci dari 1 s.d 256 byte untuk menginisialisasi *state* tabel. *State table* digunakan untuk pengurutan menghasilkan *byte pseudo-random* yang kemudian menjadi *stream pseudo-random*. Setelah di-XOR dengan *plaintext* sehingga didapatkan *ciphertext*. Tiap elemen pada *state table* di *swap* sedikitnya sekali. Kunci RC4 sering dibatasi sampai 40 bit, tetapi dimungkinkan untuk mengunakan kunci 128 bit. RC4 memiliki kemampuan penggunaan kunci antara 1 sampai 2048 bit.

3. Perencanaan Sistem

3.1 Bahan dan Alat

Pada bagian ini dilakukan perencanaan dari pembuatan sistem pengamanan pemesanan barang pada toko komputer menggunakan RC4 yang meliputi:

- Perencanaan perangkat keras
- Perencanaan perangkat lunak

3.1.1 Perencanaan Perangkat keras

Peralatan-peralatan yang dibutuhkan dalam sistem, yaitu :

- Satu buah komputer
- Satu buah *handphone support java*

3.1.2 Perencanaan perangkat lunak

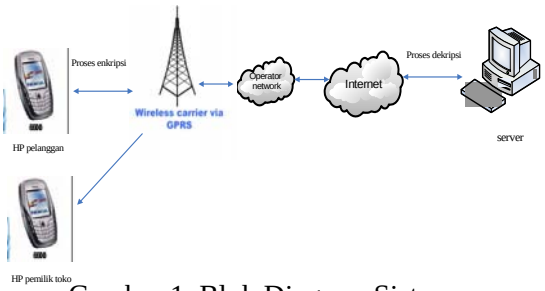
Perangkat lunak yang dibutuhkan dalam sistem ini, adalah :

1. *Sun java TM Wireless Toolkit 2.5.2 For CLDC*
2. *XAMPP*

3.2 Cara kerja

3.2.1 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* pelanggan dan *client* pemilik toko.



Gambar 1. Blok Diagram Sistem

3.2.2 Perancangan Program Interaksi Client Server

Pada Sistem yang dibuat ada suatu interaksi antara *server* dengan *client. Client* dibagi menjadi 2 yaitu pelanggan dan pemilik toko.

3.2.2.1 Interaksi *Server* dengan *Client (Handphone* Pelanggan*)*

Pada *handphone* pelanggan akan dibuat sebuah aplikasi untuk input data maupun mengakses *database server*. Untuk tampilannya akan dibuat 4 buah menu utama yaitu lihat barang, pesan barang, peraturan pemesanan dan menu untuk keluar.

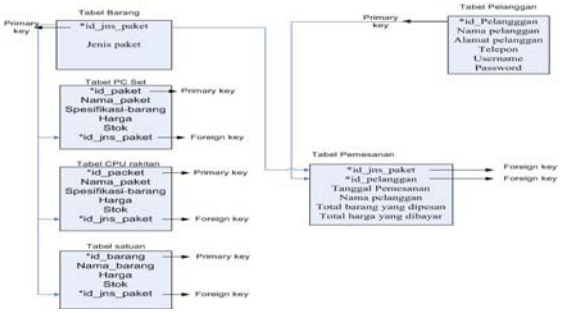
3.2.2.2 Interaksi *Server* dengan *Client (Handphone* Pemilik Toko*)*

Pada *handphone* pemilik toko akan dibuat aplikasi untuk mengakses melihat stok barang yang tersedia setelah ada pemesanan barang dan melihat data pesanan sesuai tanggal yang diinginkan.

3.2.3 Perancangan Database

Pada proyek akhir ini data diperoleh dengan cara *survey* ke toko komputer yang berada di HI Tech mall Surabaya. Setelah didapatkan data pelanggan dan data barang, data tersebut kemudian diolah dalam database MySQL.

Relasi antar tabel dalam *database* ditunjukkan pada Gambar 2 dibawah ini



Gambar 2. Relasi Antar Tabel

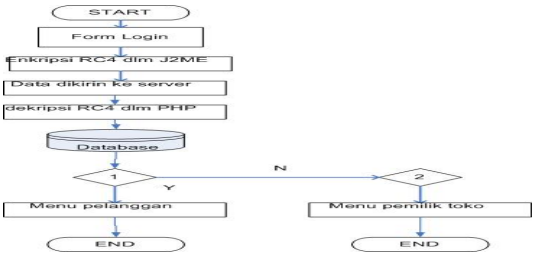
4. Implementasi, Hasil dan Analisa

Pada tahap ini metode enkripsi/dekripsi RC4 diimplementasikan pada *handphone* pelanggan yang berbasis J2ME yang terintegrasi dengan PC *server* yang berbasis php, kemudian dianalisa.

4.1. Impelementasi Metode Enkripsi /Dekripsi RC4 yang terintegrasi antara Client Berbasis J2ME dan Server Berbasis PHP

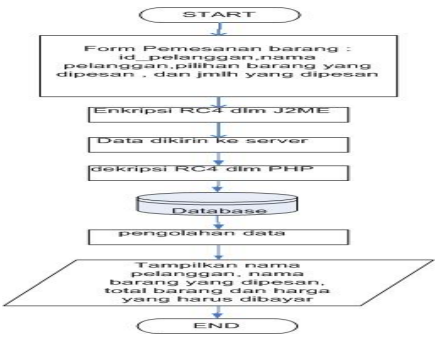
Pada bagian ini metode enkripsi RC4 diimplementasikan pada *handphone client* untuk proses enkripsi data *string* dan metode dekripsi RC4 diimplementasikan pada PC *server* untuk proses dekripsi data.

Flowchart implementasi enkripsi / dekripsi RC4 pada login ditunjukkan pada gambar dibawah ini :



Gambar 3 . *Flowchart* Imlementasi Enkripsi/Dekripsi RC4 Pada Login

Flowchart implementasi enkripsi / dekripsi RC4 pada menu pemesanan barang ditunjukkan pada gambar dibawah ini :

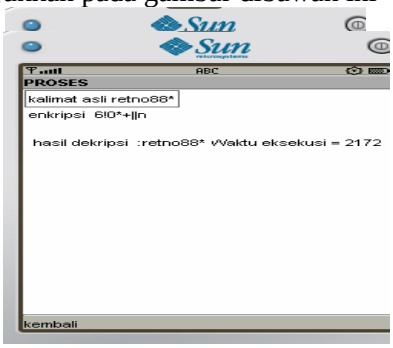


Gambar 4 . *Flowchart* Imlementasi Enkripsi/Dekripsi RC4 Pada Pemesanan Barang

4.2 Pengujian dan Analisa

4.2.1 Pengujian dan Analisa Implementasi Metode Enkripsi/Dekripsi RC4 pada handphone, PC , dan Integrasi Client Server

Pada proses pengujian ini metode enkripsi/dekripsi RC4 digunakan untuk mengirim data dari *client* yang berbasis J2ME ke *server* yang berbasis PHP, dimana proses enkripsi data dilakukan di sisi client dan proses dekripsi data di sisi *server*. Kemudian diuji kebenaran hasil dekripsinya. Hasil enkripsi/dekripsi pada *client server* ditunjukkan pada gambar dibawah ini



Gambar 5. Hasil Enkripsi/Dekripsi Pada *Client Server*

Dari proses enkripsi/dekripsi RC4 data *string* pada *client server* tersebut terlihat bahwa metode enkripsi/dekripsi yang dibuat telah teruji kebenarannya, karena teks yang terenkripsi di client yang berbasis J2ME setelah didekripsi di server PHP kembali ke teks 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 RC4 ini dibandingkan dengan *software* enkripsi lain dari *open source*.

a. Pengujian dan Analisa Linieritas Hasil Enkripsi Menggunakan Metode RC4

Pengujian ini dilakukan dengan mengamati panjang dari simbol yang dihasilkan dari proses enkripsi menggunakan metode RC4 dan membandingkannya dengan panjang teks aslinya. Berikut ini adalah gambar hasil simbol enkripsi RC4 :

Untuk lebih jelasnya dapat dilihat pada tabel hasil enripsi dibawah ini :

Tabel 1 . Panjang karakter teks asli dan simbol enkripsi metode RC4

Karakter Asli	Jumlah Karakter	Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi
@	1	„	1
r*	2	¶‘	2
r2*	3	¶‰	3
qr2*	4	µÉ ¢	4
qr2*^	5	µÉ ¢x	5
qr23^8	6	µÉ »x—	6
qr23^8*	7	µÉ »x— È	7
qr23^8*y	8	µÉ »x— È=	8
qr23^8*yx	9	µÉ »x— È=_	9
qr23^8*yx5	10	µÉ »x— È=_q	10

Dari tabel 1 dapat diketahui bahwa jumlah karakter teks asli dan jumlah karakter hasil enkripsi dari teks tersebut sama panjangnya. Sehingga dapat dikatakan bahwa metode enkripsi RC4 ini adalah linier.

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

Pada pengujian ini *software* AES digunakan sebagai pembanding terhadap linieritas panjang karakter hasil enkripsi. Pada *software* AES ini yang diinputkan adalah file teks yang berekstensi *.txt yang didalamnya berisi sejumlah karakter tertentu. Hasil dari proses enkripsi ditaruh dalam suatu *file* yang berekstensi *.aes dan simbol karakter enkripsinya dapat dilihat juga pada notepad. Berikut ini adalah tabel 2 dibawah ini :

Tabel 2. Panjang karakter teks asli dan simbol enkripsi software AES

Karakter Asli	Jumlah Karakter	Hasil Enkripsi	Jumlah Karakter Hasil Enkripsi
@	1	CHS ñP / ¬9o£nRØ Çüà Èà ¶>8 ö,; å™$¤ƒ 4 ÄM¨©æ´u ö¯õÉÐ-Þ Ð1¥Xç,ó× s. ›° ˜‡@– ôF Íp} Ç_™°à‡ ”0´ñY	97
r*	2	CHS ¾a 0 3ße˜¡Ñ4ôì öv£Ð¶{p# š³Š3 5_” $ ô="Lh*w $d¹ å01 ÷ iÏ*°'n– ©PÈ é¼º ~›¶t 8v ‘I òl< 7B:m:cL(Ñ Ç µ Œ (ùS 8êÀ	97
r2*	3	CHS)a 1 Ä[«óFœk …V¾ €” v@)¯ âš wê`e'ffñ | »? !Ë;G ´û o ™è8^Û BóF&Ñ ÏMj¼ ï· Wé TE¯öi ‰ƒx´Käñ k ÍÈB M£„4Y 9d’7}Y	97

Pada tabel 2 software AES tidak 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 RC4 merupakan metode enkripsi yang linier, sedangkan *software* enkripsi AES merupakan metode enkripsi yang non linier.

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 RC4 dengan software enkripsi yang lain mana yang lebih cepat prosesnya.

a. Pengujian dan Analisa Waktu Enkripsi/Dekripsi Enkripsi Menggunakan Metode RC4

Berikut ini adalah tabel hasil pengukuran waktu enkripsi/dekripsi untuk karakter huruf sepanjang 20 karakter

Tabel 3. Waktu Enkripsi/Dekripsi 8 karakter

Karakter Asli	Jumlah Karakter	Waktu Enkripsi/Dekripsi Searah (detik)	Waktu Enkripsi/ Dekripsi Bolak-Balik (detik)
r*	2	1,125	1,265
t4*g	4	1,141	1,313
t>k98*	6	1,219	1,360
retno88*	8	1,297	1,391
wulan7^8 *4	10	1,312	1,437
wulan88 >*kl9	12	1,390	1,467
wulan88^ kl*t5o	14	1,396	1,521
retno88*t >k98$hk	16	1,408	1,568
retno88*t >k98$hk 9%	18	1,456	1,607
retno88*t >k98$hk 9%k&	20	1,492	1,625

Dari tabel 3 dapat diketahui bahwa pada metode enkripsi RC4, waktu yang diperlukan untuk proses enkripsi/dekripsi serarah dari client ke server adalah 1,125 detik sampai 1,492 detik . Sedangkan waktu enkripsi/dekripsi bolak-balik yaitu dari client ke server dan server ke client adalah 1,265 detik sampai 1,625 detik

b. Pengujian dan Analisa Waktu Enkripsi/Dekripsi Enkripsi Menggunakan *Software* Enkripsi AES

Hasil pengukuran waktu proses enkripsi/dekripsi dapat dilihat pada tabel 4 dibawah ini :

Tabel 4. Waktu proses enkripsi/dekripsi software karakter huruf AES

Karakter Asli	Jumlah Karakter	Waktu Enkripsi/Dekripsi (detik)
r*	2	0,3
t4*g	4	0,3
t>k98*	6	0,3
retno88*	8	0,3
wulan7^8*4	10	0,3
wulan88>*kl9	12	0,3
wulan88^kl*t5o	14	0,4
retno88*t>k98$ hk	16	0,4
retno88*t>k98$ hk9%	18	0,4
retno88*t>k98$ hk9%k&	20	0,4

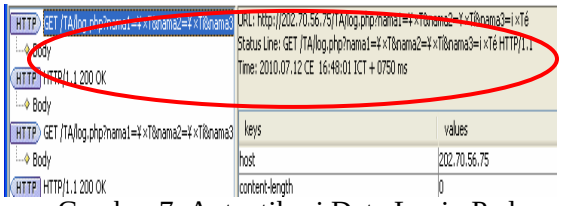
Dari tabel 4 dapat dilihat bahwa waktu proses enkripsi/dekripsi untuk karakter huruf, angka, dan metakarakter menggunakan software AES adalah 0,3-0,4 detik. Hasil ini tidak presisi karena dalam software tidak terdapat tool untuk pengukuran waktu proses enkripsi/dekripsi, sehingga pengukuran waktu dilakukan menggunakan stopwatch.

Berdasarkan hasil pengujian terhadap lamanya waktu proses enkripsi antara metode RC4 dan software AES dapat disimpulkan bahwa *software* AES memiliki waktu enkripsi/dekripsi yang lebih cepat karena *software* AES dapat mengenkripsi dan mendekripsi *file* dengan jumlah karakter yang banyak dalam waktu yang singkat dibandingkan metode enkripsi RC4.

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 sunjava wireless toolkit :

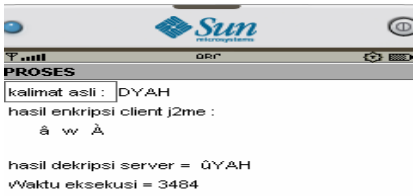


Gambar 7. Autentikasi Data Login Pada Monitoring Tool Sun Java Wireless Toolkit

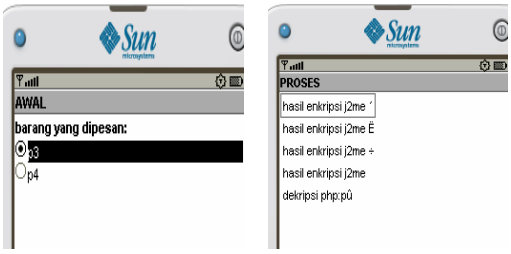
Dari gambar 7 dapat dilihat bahwa menu client server telah terenkripsi dengan baik, sehingga saat dilakukkan monitoring data maka pada tool yang digunakan attacker akan nampak simbol-simbol yang tidak dapat dibaca.

4.2.5 Karakter dan Bentuk Form Yang Tidak Support Dalam Integrasi J2ME dan PHP

Berikut ini adalah gambar karakter dan bentuk form yang tidak dapat disupport oleh integrasi program J2ME dan PHP



Gambar 8. Hasil Enkripsi/Dekripsi Karakter Huruf Kapital Pada Integrasi J2ME dan PHP



Gambar 9. Hasil Enkripsi/Dekripsi Choicegroupl Pada Integrasi J2ME dan PHP

5. Kesimpulan

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

1. Algoritma enkripsi RC4 merupakan metode enkripsi yang linier , sedangkan software enkripsi AES merupakan metode enkripsi non linier.
2. Waktu yang diperlukan oleh algoritma RC4 untuk mengenkripsi dan mendekripsi waktu yang diperlukan untuk proses enkripsi/dekripsi serarah dari client ke server adalah 1,125 detik -1,492 detik . Waktu enkripsi/dekripsi bolak-balik yaitu dari client ke server dan server ke client adalah 1,265 detik - 1,625 detik. Hal ini menujukkan bahwa panjang karakter berpengaruh terhadap waktu proses enkripsi/dekripsi RC4. Sedangkan waktu proses enkripsi/dekripsi menggunakan software AES adalah 0,3-0,4 detik. Hal ini menujukkan bahwa panjang karakter tidak berpengaruh signifikan terhadap waktu proses enkripsi/dekripsi *software* AES.
3. Aplikasi integrasi *client server* tidak dapat mensupport karakter huruf kapital dan form choicegroup. Hal ini disebabkan karena dalam pemrograman J2ME perlu dilakukan konvert data beberapa kali untuk memasukan data inputan ke dalam fungsi enkrip dan dekrip, sedangkan pada PHP dapat langsung mengenali berbagai tipe data tanpa mengkonvert

Daftar Pustaka

[1] Muriyanto,*"Perancangan dan Pembuatan Aplikasi Kriptografi Bwrbasis Metode RC4"*, PENS-ITS, Surabaya, 2008

[2] Arif Mardiyansah, *"Pembuatan Sistem Informasi PENS ITS Yang Dapat Diakses Melalui WAP"*, PENS-ITS, Surabaya, 2008

[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] William Stalling,*"Cryptography and Network Security,Prinsiples and Pratices"*, 3rd Edition, 2003, Pearson Education Inc

[7] Concepts Of Cryptography http://www.kremlinecrypt.com/crypto