PENERAPAN ALGORITMA GABUNGAN RC4 DAN BASE64 PADA SISTEM KEAMANAN E-COMMERCE

Febrian Wahyu. C[1], Adriana. P Rahangiar[2], Febry de Fretes[3]
[1, 2, 3] Program Studi Magister Sistem Informasi
Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga, Jawa Tengah,50711
E-mail: febrian_wahyu_christanto@yahoo.co.id, petronel1978@yahoo.com, bentar_etes@yahoo.com

ABSTRAK
Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Setiap penyedia layanan jasa E-commerce berusaha untuk menyediakan suatu sistem yang dapat menjaga keamanan data dari transaksi-transaksi yang dilakukan oleh setiap pelanggan. Proses transaksi pembayaran penggunaan jasa e-commerce dilakukan melalui bank secara online. Keamanan pelaksanaan proses pembayaran masih mengalami masalah yaitu sering terjadi cyber crime terhadap data pelanggan di bank yang menimbulkan berkurangnya kepercayaan pelanggan untuk menggunakan jasa layanan e-commerce. Penelitian ini dimaksudkan untuk membuat suatu sistem keamanan e-commerce dengan menggunakan gabungan algoritma RC4 dan Base64. Algoritma RC4 dan Base64 adalah jenis algoritma kriptografi yang mengubah data plainteks menjadi chipher text. Enkripsi data yang dilakukan dengan menggunakan dua algoritma ini dapat mengenkripsi data password nasabah di bank sehingga password dari nasabah tidak dapat diketahui oleh pihak-pihak yang tidak berkepentingan saat nasabah melakukan transaksi dengan menggunakan e-commerce. Penerapan dua algoritma ini di sisi penyedia e-commerce diharapkan akan meningkatkan kepercayaan pelanggan untuk bertransaksi menggunakan sistem e-commerce.

Kata kunci: Algortima RC4, Base64, Sistem keamanan e-commerce.

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini mengharuskan setiap perusahaan untuk dapat meningkatkan kualitas kinerjanya dalam upaya menghadapi persaingan global yang semakin pesat. E-commerce merupakan salah satu teknologi yang digunakan untuk melakukan proses perdagangan atau jual beli yang dilakukan melalui World Wide Web. Dalam hal ini perusahaan dapat melakukan proses penjualan produk dan customer dapat membeli sekaligus melakukan proses pembayaran lewat internet.

Penggunaan E-Commerce mulai meningkat di Indonesia disebabkan karena beberapa faktor yaitu akses internet yang semakin murah dan cepat mendorong pertumbuhan pengguna internet, dukungan dari sektor perbankan Indonesia yang menyediakan fasilitas untuk melakukan transaksi lewat internet, biaya web hosting yang semakin murah dan mulai banyak software open source untuk membantu membangun sebuah website e-commerce, seperti osCommerce, Magento, joomla dll. E-commerce juga memberikan banyak manfaat bagi perusahaan yaitu revenue stream baru, melebarkan jangkauan pemasaran, menurunkan biaya promosi, marketing, distribusi, memperpendek waktu perputaran produk, meningkatkan loyalitas customer dan meningkatkan value chain.

Dalam penerapan E-commerce ada sebagian masyarakat yang masih meragukan pelaksanaan transaksi melalui E-commerce, hal ini disebabkan karena pada umumnya masyarakat belum terlalu paham bagaimana melakukan transaksi online melalui internet, mereka masih meragukan tingkat keamanan untuk melakukan transaksi pembayaran online melalui internet karena besarnya jumlah kasus-kasus penipuan yang dilakukan melalui internet baik berupa pemalsuan identitas, manipulasi data transaksi, dll. Hal-hal di atas menimbulkan rendahnya minat masyarakat untuk menggunakan E-commerce sebagai salah satu teknologi yang memudahkan customer untuk melakukan proses pembelian dan pembayaran suatu produk lewat internet.

Dalam upaya untuk mengatasi permasalahan keamanan terhadap proses bisnis e-commerce. Banyak cara telah dilakukan untuk meningkatkan keamanan data yang berada dalam jaringan, salah satunya dengan menggunakan teknik kriptografi. Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Salah satu contoh penerapannya yaitu penggunaan Certificate Authority (CA) melalui pendekatan PKI (Public Key Infrastruktur), Ipsec, Pretty Good Privacy, dll.

Dalam penelitian ini dibahas tentang bagaimana penerapan algoritma kriptografi RC4 dan Encoding Base64 dalam menyelesaikan dan mengatasi masalah keamanan dalam E-Commerce yang dimodelkan melalui interaksi antara Website Rental Mobil dan Bank. Algoritma RC4 dan Base64 adalah jenis algoritma kriptografi yang mengubah data

plainteks menjadi chipher text. Enkripsi data yang dilakukan dengan menggunakan dua algoritma ini dapat mengenkripsi data password nasabah di bank sehingga password dari nasabah tidak dapat diketahui oleh pihak-pihak yang tidak berkepentingan saat nasabah melakukan transaksi dengan menggunakan e-commerce. Penerapan dua algoritma ini di sisi penyedia e-commerce diharapkan akan meningkatkan kepercayaan pelanggan untuk bertransaksi menggunakan sistem e-commerce.

2. TINJAUAN PUSTAKA

Kajian terdahulu diambil dari penelitian dengan judul " Implementasi Pengamanan Dokumen pada *Microsoft Office* Dengan Algoritma Kriptografi RC4 *Stream Chiper* Dan SHA-1" yang menghasilkan sebuah aplikasi untuk pengamanan data pada *Microsoft Office.* Hasil dari penelitian menghasilkan sebuah program aplikasi yang dapat mengubah isi suatu dokumen (*plainteks*) yang berupa teks, tabel dan gambar menjadi kode-kode yang tidak dikenal (*cipherteks*) menjadi dokumen aslinya (*plainteks*). Juga dapat digunakan untuk dokumen dengan ekstensi *.doc*, *.txt*, *.rtf*, *.xls*, *.pp*t, dan *.mdbl*. Selain itu, dapat menghasilkan *file* enkripsi dan deskripsi sama dengan ekstensi *file* sebelumnya yaitu *plainteks* dan *cipherteks* (Andri, 2007).

Pada penelitian yang berjudul "Pemanfaatan MIME *Base64* Untuk menyembunyikan *Source Code* PHP" menghasilkan sebuah aplikasi yang dapat melakukan *encoding* terhadap sekumpulan *file* (*folder*), dapat menentukan *folder* tujuan (untuk *encoding* kumpulan *file*), dapat membuang *white space*, memiliki masukan waktu kadaluarsa selain itu aplikasi ini dapat digunakan untuk aplikasi demo (Teguh, 2007).

2.1 Kriptografi *RC4*

Algoritma kriptografi *RC4* adalah enkripsi dengan kategori *stream* simetrik yang dibuat oleh *RSA Data Security, Inc* (RSADSI). Proses enkripsi deskripsi mempunyai proses yang sama sehingga hanya ada satu fungsi yang dijalankan untuk menjalankan kedua proses tersebut. *RC4* mempunyai sebuah *S-Box* dan *key* dalam bentuk array 256 byte yaitu : S_0, S_1, ..., S_{255} yang berisi permutasi dari bilangan 0 sampai 255, K0, K1, …, K255 (Ekklesia, 2005).

Sedangkan untuk inisialisasi *S-Box* yaitu dengan mengisikan nilai 1 sampai dengan 255 dimulai dari S0 sampai dengan S255, isi *S-Box* secara berurutan, yaitu S0=0, S1=1, ... , S255=255 (Scheiner, 2001). Untuk inisialisasi *key* yaitu dengan mengisikan *array* K255 *byte* dengan kunci yang diulangi sampai seluruh *array* K0,K1, ... K255 terisi seluruhnya. *Pseudocode* yang terbentuk untuk menciptakan *initialisasi key* adalah sebagai berikut.

```
For I = 0 to 255
Ki = I mod length (key)
```

(Jakd, 2008)

Menurut Jakd, *pseudorandom* adalah nilai yang dibangkitkan dari nilai *S-Box* dan *Key* yang telah diinisialisasi. Caranya *set* indeks *j* dengan nol, dan melakukan penukaran nilai *S-Box* yang sudah diinisialisasi sebelumnya dengan nilai perulangan ditambah dengan *S-Box* awal ditambah dengan nilai dari array K yang dapat digambarkan dan dijelaskan dalam *Pseudocode* sebagai berikut.

```
j = 0
for i = 0 to 255
j = (j + Si + Ki) mod 256
swap Si dan Sj
```

Fungsi *swap* merupakan fungsi yang menukarkan nilai S ke-i dengan nilai S ke-j. Kemudian membangkitkan nilai *pseudorandom key* berdasarkan indeks dan nilai *S-Box*. Terdapat 2 indeks yaitu i dan j, yang diinisialisasi dengan bilangan nol. Untuk menghasilkan random *byte* langkahnya adalah sebagai berikut.

```
i = 0
j = 0
for idx = 0 to len-1
i = (i + 1) mod 256
j = (j + Si) mod 256
swap Si dan Sj
t = (Si + Sj) mod 256
k = St
buffidx = k XOR buffidx
```

Keterangan:

- *buff* merupakan pesan yang akan dienkripsi atau dekripsi
- *len* merupakan panjang dari *buff*

Nilai *pseudorandom key* inilah yang akan di XOR dengan *plainteks* untuk menghasilkan *cipherteks* atau XOR dengan *cihperteks* untuk menghasilkan *plainteks.* Untuk menghasilkan *cipherteks* yaitu dengan rumus "*Cipherteks = Plainteks XOR K*" sedangkan untuk menghasilkan *plainteks* yaitu dengan rumus "*Plainteks = Cipherteks XOR K*" (Fauzan, 2008).

Contoh lain dari implementasi algoritma *RC4* adalah saat proses *key scheduling algorithm* didapatkan *S-Box* terakhir 54, 157, 62, 162, 25, 135, 195, 103, 208, 8, 188, 42, 165, 13, 141, 253, 35, 231, 108, 134, 93, 82, 49, 9, 83, 139, 147, 38, 87, 193, 22, 219, 113, 248, 155, 117, 64, 123, 154, 67, 53, 94, 46, 102, 133, 170, 106, 194, 24, 246, dan 45 maka penyelesaiannya terdapat di dalam Tabel.1.

Tabel 1. Proses *Key Schedulling Algorithm RC4*

Iterasi	Pesan	Ascii	i=(i+1)mod 256	j=(j+SBox[i]) mod 256	Pertukaran	SBox[(Sbox[i]+ Sbox[j])mod 256]	Pesan ^ K	Ascii
			i	j		K	Hasil	
			Nilai awal 0	Nilai awal 0				
0	i	105	(0+1)mod 256= 1	(0+157)mod 256=157	sbox ke-1 dengan Sbox ke - 157	SBOX[144]+157 mod 256] = SBOX[301%256] = SBOX[45] = 170	105 ^ 170=195	Ã
1	b	98	(1+1) mod 256 = 2	(157+62) mod 256 = 219	sbox ke-2 dengan sbox ke-219	SBOX[15+62 mod 256]=SBOX[77]=236	98 ^ 236 = 142	ž
2	u	117	(2+1) mod 256 = 3	(219+162) mod 256 = 125	sbox ke-3 dengan sbox ke-125	SBOX[47+162 mod 256]=SBOX[209]=158	117 ^ 158 = 235	ë

2.2 Algoritma Base64

Transformasi *Base64* merupakan salah satu algoritma untuk *Encoding* dan *Decoding* suatu data ke dalam format ASCII, yang didasarkan pada bilangan dasar 64 atau bisa dikatakan sebagai salah satu metoda yang digunakan untuk melakukan encoding (penyandian) terhadap data binary. Karakter yang dihasilkan pada transformasi *Base64* ini terdiri dari A..Z, a..z dan 0..9, serta ditambah dengan dua karakter terakhir yang bersimbol yaitu + dan / serta satu buah karakter sama dengan (=) yang digunakan untuk penyesuaian dan menggenapkan data binary atau istilahnya disebut sebagai pengisi pad. Karakter simbol yang akan dihasilkan akan tergantung dari proses algoritma yang berjalan.

Kriptografi Transformasi *Base64* banyak digunakan di dunia internet sebagai media data format untuk mengirimkan data, ini dikarenakan hasil dari *Base64* berupa *Plaintext*, maka data ini akan jauh lebih mudah dikirim, dibandingkan dengan format data yang berupa bineri. Dalam Implementasinya beberapa contoh dalam Transformasi *Base64*, yang antara lain adalah sebagai berikut(Wahana Komputer, 2010).

- PEM (*Privacy-Enhaced Mail*) adalah protokol pertama dengan teknik Base64 yang didasarkan pada RFC 989, yang terdiri dari 7 karakter (7-bit) yang digunakan pada SMTP dalam transfer data tapi untuk sekarang PEM sudah tidak menggunakan RFC 989 tapi sudah di ganti dengan RFC 1421 yang menggukana karakter A_Z, a-z, 0..9.
- MIME (*Multi Purpose Mail Extension*) didasarkan pada RFC 2045. Teknik encoding Base64 MIME, mempunyai konsep yang berdasarkan RFC 1421 versi PEM. Sedangkan MIME diakhiri dengan Padding "=" pada hasil akhir encodingnya.
- UTF-7 didasarkan pada RFC 2152, yang umumnya disebut "MODIFICATION BASE" UTF-7 menggunakan karakter MIME, tidak memakai padding"=", karakter "=" digunakan sebagia escape untuk encoding.
- OpenPGP (*PGP Prety Good Privacy*) dirancang pada RFC 2440, yang menggukan Coding 64 Radix atau ASCI Amor. Teknik encodingnya didasarakan pada MIME tetapi ditambah dengan 24 bit CRC Cheksum. Nilai Cheksum dihitung dari data Input sebelum dilakukan Proses Encoding.

Dalam *Encoding Base64* dapat dikelompokkan dan dibedakan menjadi beberapa kriteria yang tertera dan dapat dilihat di dalam Tabel 2

Tabel 2. *Encoding Base64* (Josefsson, 2003)

Data 6 bit	Karakter Encoding 64	Data 6 bit	Karakter Encoding 64
0	A	33	h
1	B	34	i
2	C	35	j
3	D	36	k
4	E	37	l
5	F	38	m
6	G	39	n
7	H	40	o
8	I	41	p
9	J	42	q
10	K	43	r
11	L	44	s
12	M	45	t
13	N	46	u
14	O	47	v
15	P	48	w
16	Q	49	x
17	R	50	y
18	S	51	z
19	T	52	0
20	U	53	1
21	V	54	2
22	W	55	3
23	X	56	4
24	Y	57	5
25	Z	58	6
26	A	59	7
27	B	60	8
28	C	61	9
29	D	62	+
30	E	63	/
31	F	(pad)	=
32	G		

Teknik *encoding Base64* sebenarnya sederhana, jika ada satu (*string*) *bytes* yang akan disandikan ke *Base64* maka caranya adalah(Ariyus, 2008).

a. Pecah *string bytes* tersebut ke per-3 *bytes*.
b. Gabungkan 3 *bytes* menjadi 24 *bit*. Dengan catatan 1 *bytes* = 8 bit, sehingga 3 x 8 = 24 *bit*.
c. Lalu 24 *bit* yang disimpan di-*buffer* (disatukan) dipecah-pecah menjadi 6 *bit*, maka akan menghasilkan 4 pecahan.
d. Masing masing pecahan diubah ke dalam nilai *decimal*, imana maksimal nilai 6 *bit* dalah 63.
e. Terakhir, jadikan nilai nilai desimal tersebut menjadi indeks untuk memilih karakter penyusun dari *base64* dan maksimal adalah 63 atau indeks ke 64.

Dan seterusnya sampai akhir *string bytes* yang mau kita konversikan. Jika ternyata dalam proses *encoding* terdapat sisa pembagi, maka tambahkan sebagai penggenap sisa tersebut karakter =. Maka terkadang pada *base64* akan muncul satu atau dua karakter = ().

Penerapan pengamanan data transaksi dengan algoritma Base64 terdapat pada *user name* (nama pada kartu kredit), PIN dan pembayaran seperti contoh berikut ini :

User Name : Edsel
PIN : 4587

Pada contoh diatas, *user name* Edsel diganti menjadi RWRzZWw= sedangkan PIN 4587 diganti

menjadi NDU4Jw= =. Pada tabel ASCII, huruf E, d, s, e, l disimpan sebagai 69, 100, 115, 101, 108. Pada bilangan berbasis dua menjadi 01000101, 01100100, 01110011, 01100101, 01101100. Jika kelima byte digabungkan, akan menghasilkan 40 *bit*. Angka tersebut harus dikonversi sehingga berbasis 64, dengan membagi 40 *bit* tersebut dengan 6 *bit*. Maka akan dihasilkan 7 bagian yang masing-masing terdiri dari 6 *bit*. Kemudian masing-masing bagian tersebut dikonversi ke nilai yang ada pada base64, seperti pada penyelesaian berikut.

Encoding untuk *User Name* :

Huruf : E d s e l

ASCII : 69 100 115 101 108

Bit : 01000101 01100100 01110011 01100101 01101100

: 010001 010110 010001 110011 011001 010110 110000 000000

Index : 17 22 17 51 25 22 48

Base64 : R W R z Z W w = W 2

Sedangkan untuk *PIN*

Huruf : 4 5 8 7

ASCII : 52 53 56 55

Bit : 00110100 00110101 00111000 00100111

: 001101 000011 010100 111000 001001 110000 000000 000000

Index : 13 3 20 56 9 48

Base64 : N D U 4 j w = =

Pada penyelesaian tersebut terdapat *padding*, yaitu proses dimana akan dilakukan apabila sekelompok karakter yang dimiliki tidak penuh 6bit. Proses *padding* dilakukan dengan menambahkan karakter "=" pada encoding base64. Sehingga hasil encoding dari username dan PIN diatas adalah sebagai berikut.

User name : RWRzZWw=

PIN : NDU4Jw= =

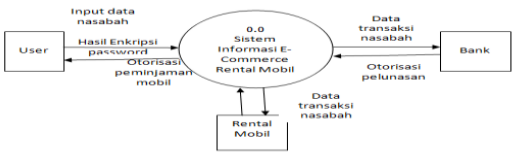
3. PERANCANGAN SISTEM

Perancangan sistem merupakan sebuah proses yang terdiri dari beberapa kegiatan. Pertama adalah menentukan secara tepat dan rinci operasional manajemen yang berkaitan dengan kegiatan pengolahan data yang dikehendaki. Kedua adalah mengatur semua kebutuhan tadi, serta membagi-baginya secara sistematis pada beberapa tahap dan bagian, yang nantinya akan dioperasionalkan. Ketiga menentukan cara-cara pelaksanaan dari masing-masing jenis tugas tersebut, dan keempat menentukan tingkat ukuran mutu untuk menilai keberhasilan (dan ketidakberhasilan) dari masing-masing tugas tersebut (Solamo, 2003). Untuk dapat mencapai keinginan yang di maksud maka perlu dilakukan perancangan sistem sebagai berikut.

a. Perancangan *User Interface*
   Aplikasi sistem pengamanan data teks menggunakan algoritma kriptografi *Base64* dan *RC4* mempunyai beberapa halaman yang memudahkan pengguna dalam mengoperasikannya, halaman tersebut adalah:
   - Halaman Enkripsi dan Dekripsi *Base64*
   - Halaman Enkripsi dan Dekripsi *RC4*
   - Halaman Enkripsi dan Dekripsi gabungan *RC4* dan *Base64*
b. Perancangan Aplikasi Sistem Keamanan pada Data Teks
   Sistem yang dihasilkan berupa aplikasi Sistem Keamanan Data Teks pada aplikasi web form. Sistem ini pada intinya merupakan sarana kriptografi data teks secara aman karena telah dienkripsi dan didekripsi menggunakan dua algoritma kriptografi *Base64* dan *RC4*, yang terdiri dari desain *User Interface*, Perancangan *Input*, *p*erancangan Proses dan perancangan *Output*
c. Data Flow Diagram (DFD)
   Dalam mendesain aplikasi Sistem Pengamanan Data Teks menggunakan Algoritma Kriptografi *Base64* dan *RC4* ini menggunakan *Data Flow Diagram* (DFD). DFD digunakan untuk menyajikan sebuah sistem atau perangkat lunak pada setiap tingkatan abstraksi.

3.1 Diagram Konteks

Diagram Konteks pada aplikasi pengamanan data teks menggunakan algoritma kriptografi *Base64* dan *RC4* terdapat pada Gambar 1.



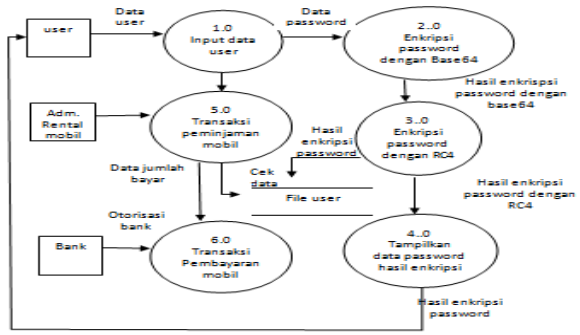
Gambar 1. Diagram Konteks Sistem Kriptografi

Dalam Gambar 1 dijelaskan konteks dari sistem kriptografi dalam aplikasi pengamanan terhadap proses transaksi pembayaran peminjaman mobil di Rental Mobil. Dimana user akan melakukan pendaftaran data user berupa data pribadi disertai dengan data password. Data password user akan dienkripsi oleh sistem sehingga, data password yang tersimpan di database Rental Mobil adalah data hasil enkrispi dengan menggunakan algoritma Base64 dan RC4 untuk untuk kemudian ditampilkan kembali kepada *user* dalam bentuk data teks hasil kriptografi.

3.2 DFD *Level* 0

DFD *Level* 0 merupakan dekomposisi dari diagram konteks yang sudah ada.

 ISSN: 1907-5022



Gambar 2. DFD *Level* 0

Gambar 2 dijelaskan mengenai proses yang terjadi dalam aplikasi sistem E-commerce Rental Mobil, dimana pelanggan yang ingin meminjam mobil harus terlebih dahulu melakukan pendaftaran data pribadinya beserta password yang diinginkan. Sistem akan melakukan enkripsi terhadap password tersebut dengan menggunakan algortima Base64 setelah hasil enkripsi tersebut kemudian dienkrispsi lagi dengan menggunakan algoritma RC4, kemudian hasi enkripsi tersebut akan ditampilkan kepada user dan disimpan dalam database pelanggan milik Rental Mobil. Proses selanjutnya pelanggan dapat melakukan peminjaman mobil dan secara langsung melakukan proses pembayaran kepada Bank dengan memasukan data password sebenarnya untuk diotorisasi pembayarannya oleh pihak Bank.

4. PERMODELAN DAN IMPLEMENTASI ALGORITMA RC4 & BASE 64

Proses perancangan sistem yang telah dilakukan di atas digunakan sebagai dasar untuk mengimplementasikan gabungan algoritma yaitu RC4 dan Base64 ke dalam sistem dalam hal ini adalah sistem E-Commerce antara Website Rental Mobil "Maju Jaya" dan Bank "Jaya". Nasabah Bank "Jaya" akan melakukan transaksi peminjaman mobil menggunakan kartu kredit mereka. Keamanan yang terjamin dalam proses transaksi diharapkan dapat membuat kenyamanan pelanggan rental maupun nasabah bank dalam melakukan transaksi karena jauh dari resiko pencurian data pelanggan kartu kredit yang dilakukan oleh pihak yang tidak bertanggungjawab.

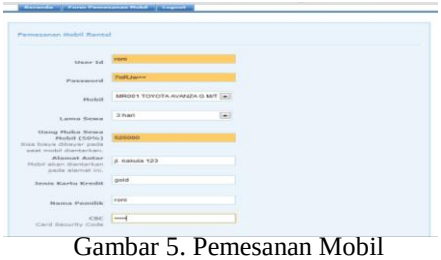
Dalam implementasi dan permodelan ini didukung dengan fasilitas web service sehingga dalam transaksi yang dilakukan oleh pelanggan rental, maka pada saat itu Website Rental Mobil "Maju Jaya" akan melakukan pemeriksaan ke dalam basis data Bank "Jaya" untuk menentukan kebenaran data kartu kredit yang dimasukkan oleh pelanggan.

Gambar 3. Register Nasabah

Dimulai dengan pembuatan akun nasabah oleh Admin Bank, maka sistem ini akan dapat berjalan. Selain nomor rekening, nama, telp, jenis kartu kredit, dan masa berlaku kartu, maka di dalam halaman ini disimpan pula Card Security Code (CSC) sebagai nomor pin nasabah. Dalam hal ini CSC berlaku seperti password yang digunakan oleh nasabah dalam melakukan transaksi peminjaman mobil. Untuk halaman dalam pendaftaran member terdapat di dalam Gambar 4.

Gambar 4. Pendaftaran Pelanggan Rental

Dalam Gambar 4 adalah form pendaftaran untuk menjadi member pelanggan dalam rental. Dalam hal ini informasi yang disimpan adalah informasi umum yang menerangkan tentang data pelanggan.



Gambar 5. Pemesanan Mobil

Setelah melakukan pendaftaran. Maka dalam Gambar 5 pelanggan akan dapat login ke dalam sistem rental dan melakukan transaksi peminjaman mobil. Dalam halaman ini disediakan jenis mobil dan lama meminjam. Untuk password pelanggan sudah terenkripsi menggunakan algoritma RC4 yang digabung dengan Base64 sehingga menjadi suatu Cipher Text yang sangat berbeda dari Plain Text nya. Untuk pembayaran, maka diminta jenis kartu, nama pemilik kartu, serta CSC untuk nantinya sistem Website rental akan memeriksa ke basisdata bank melalui Web Service. Apabila informasi yang dimasukkan benar, maka transaksi akan berhasil dilakukan, apabila informasi salah, maka transaksi tidak berhasil.

Dalam field CSC informasi yang dimasukkan adalah bersifat Plain Text, untuk kemudian dienkripsi oleh Web Service menjadi suatu Cipher Text. Cipher Text inilah yang akan disesuaikan dengan basisdata di dalam bank untuk menentukan kesuksesan transaksi peminjaman mobil. Jadi pada intinya yang mengetahui Cipher Text dari CSC ini adalah pelanggan Rental Mobil "Maju Jaya" yang merupakan nasabah dari Bank "Jaya" karena di dalam basisdata bank, informasi CSC ini sudah dienkripsi pula, sehingga Admin bank pun tidak dapat mengetahui CSC milik nasabah.

Gambar 6. Admin Rental View Transaksi

Gambar 6 adalah fasilitas yang dimiliki oleh Admin Rental Mobil "Maju Jaya" dalam meluhat transaksi pelanggannya. Dalam halaman ini password pengguna sistem telah dienkripsi pula untuk menjamin keamanan dari pelanggan. Sedangkan untuk fasilitas Admin Bank "Jaya" dalam melihat transaksi nasabah terdapat di dalam Gambar 7 .

Gambar 7. Lihat Transaksi Pelanggan

Gambar 7 dijelaskan proses saat Admin Bank "Jaya" melakukan pemeriksaan terhadap transaksi yang telah dilakukan pelanggan. Dalam hal ini, Admin bank hanya dapat melihat informasi tersebut bahwa nomor rekening dari seorang nasabah telah meminjam mobil dari rental mobil dengan total transaksi yang diketahui.

Gambar 8. Web Service Rental dan Bank

Gambar 8 adalah source code Web Sevice yang menghubungkan antara dua Website dalam permodelan ini yaitu Website Rental Mobil "Maju Jaya" dan Bank "Jaya". Dalam Gambar 8 dijelaskan bahwa informasi yang diambil oleh Website rental kepada bank adalah informasi tentang nama, jenis kartu kredit, masa berlaku kartu, serta CSC (sudah terenkripsi). Apabila informasi yang diminta benar terdapat di dalam basisdata bank dan sesuai, maka transaksi akan berhasil. Sedangkan apabila masa berlaku kartu sudah habis, maka akan muncul pesan kepada pelanggan bahwa "Kartu Kredit Habis Masa Berlaku", dan apabila informasi yang dimasukkan pelanggan untuk membayar tidak benar, maka akan muncul pesan "Kartu Kredit Tidak Ditemukan".

5. KESIMPULAN

Sistem keamanan menggunakan Algoritma Kriptografi *RC4* dan *Base64* dapat menjamin keamanan data transakis pembayaran online yang dilakukan oleh pelanggan karena password pelanggan di Bank telah disamarkan dengan proses enkripsi dan sangat sulit dipecahkan apabila kunci dan perhitungan algoritma berbeda. selain itu, disisi penyedia jasa e-commerce dapat menjamin kenyamanan bagi para pelanggan yang menggunakan jasa layanan e-commerce.

Sistem e-commerce yang dibuat dengan dukungan Web Service yang bersifat multi tier dan multi platform memungkinkan sistem berlaku untuk semua model protokol.

PUSTAKA

Andri, Yuli. (2007). Implementasi Pengamanan Dokumen Pada *Microsoft Office* Dengan Algoritma *RC4 Stream Chiper* dan *SHA-1*. Yogyakarta : Teknik Informatika Universitas Ahmad Dahlan.

Ariyus, Dony. (2008). Pengantar Ilmu Kriptografi Teoti, Analisis, dan Implementasi. Yogyakarta : Andi Offset.

Ekklesia Dicky (2005). Studi dan Implementasi Pengamanan Basis Data dengan Teknik Kriptografi RC4. Badung.

Fauzan, M. F. (2008). Pengamanan Transmisi dan Data *Query* Basis Data dengan Algoritma Kriptografi. Bandung : Teknik Informatika.

Solamo, Weng. (2003). *Software Engineering*. San Fransisco : JEDI.

Teguh, Salman. (2007). Pemanfaatan *MIME Base64* untuk Menyembunyikan *Source Code PHP*. Bandung : Teknik Elektro dan Informatika Institut Teknologi Bandung.