PENERAPAN ALGORITMA ASIMETRIS RSA UNTUK KEAMANAN DATA PADA APLIKASI PENJUALAN CV. SINERGI COMPUTER LUBUKLINGGAU BERBASIS WEB

Susanto
Program Studi Teknik Informatika
STMIK MUSIRAWAS
Email: susanto@muralinggau.ac.id

Andri Anto Tri Susilo
Program Studi Teknik Informatika
STMIK MUSIRAWAS
Email: andri.lubuklinggau@gmail.com

ABSTRAK

Masalah keamanan data merupakan masalah yang sangat serius dalam kegiatan bisnis di era digital. kegiatan bisnis di era digitalmerupakan kegiatan bisnis yang sebagian besar menggunakan teknologi aplikasi komputer serta menjadikan komputer *server* sebagai tempatmenyimpan data-data dalam kegiatan bisnis sehingga dapat disimpulkan media komputer menjadi faktor utama di dalam kegiatan bisnis yang dilakukan. Keamanan data yang menjadi masalah utama bukan hanya data yang tersimpan di komputernya saja, namun juga keamanan data yang dikirimkan lewat jaringan komputer dan aplikasi komputertetapi juga keamanan data yang disimpan di dalam *database.* Penerapan algoritma kriptografi RSA menjadi solusi yang baik pada sistem penjualan yang akan dibangun CV. Sinergi *Computer* Lubuklinggau untuk menjamin kerahasiaan data-data penjualan yang disimpan didalam *database*, dengan penggunaan algoritma RSA ke dalam sistem penjualan tersebut maka data yang disimpan di dalam *database* berupa penjumlahan angka sehingga isi datanya tidak dapat dimengerti oleh pihak lain.

Kata kunci: algoritma RSA; *database*; keamanan.

ABSTRACT

Data securyty issues are a very serious problem in business activities in the digital era. Business activities in the digital era are business activities that mostly use computer application technology and make server computer a place to store data in business activities so that it can be concluded that computer media is a mojar factor in business activities. Data security is the main problem not only data stored on the computer, but also data securyty that is sent through computer network and computer application but also the securyty of data stored in the data base. The application of RSA cryptographic algorithm is a good solution for the sales system that will be built by CV. Lubuklinggau Computer Synergy to ensure the confidentiality of sales data stored in the database, by using the RSA algorithm into the sales system, the data stored in the database is in the form of a sum of numbers so that the contents of the data cannot be understood by other parties.

Keywords: *RSA algorithm; database; security.*

1. PENDAHULUAN

Masalah keamanan data merupakan masalah yang sangat serius dalam kegiatan bisnis di era digital. kegiatan bisnis di era digital merupakan kegiatan bisnis yang sebagian besar menggunakan teknologi aplikasi komputer serta menjadikan komputer *server*sebagai tempat menyimpan data-data dalam kegiatan bisnis sehingga dapat disimpulkan media komputer menjadi faktor utama di dalam kegiatan bisnis yang dilakukan. Keamanan [1]data yang menjadi masalah utama bukan hanya data yang tersimpan di komputernya saja, namun juga keamanan data yang dikirimkan lewat jaringan komputer dan aplikasi komputertetapi keamanan data yang disimpan di dalam *database.*

Database [2]merupakan sekumpulan informasi yang disimpan di dalam komputer secara sistematik yang dapat digunakan melalui sebuah program komputer tertentu untuk menjalankannya. Keamanan *database* menjadi solusi terakhir pada saat aplikasi komputer mengalami gangguan yang disebabkan oleh pihak luar setelah berhasil melewati keamanan jaringan komputer dan keamanan aplikasi komputer. Dalam

sebagian kegiatan bisnis, keamanan *database* menjadi masalah utama setelah menjamin keamanan pada jaringan komputer dan aplikasi komputernya. Contohnya pada kegiatan bisnis penjualan peralatan elektronik yaitu*database* akan menyimpan data-data penjualan, seperti data produk dan data pelanggan serta hak akses pelanggan, dan jika kegiatan bisnis tersebut terintegrasi dengan identitas data lainya antara lain kartu kredit maka harus menjamin kerahasiaan identitas data karena menyangkut privasi pelanggan. Semua yang menyangkut data pribadi pelanggan harus dijamin kerahasiaannya bahkan dari karyawan sekalipun tidak mempunyai hak untuk mengakses atau melihat data identitas pelanggang tersebut. *Database* yang aman akan menjaditolok ukur sebuah perusahaan dalam keberlangsungan kegiatan bisnis yang dilakukan perusahaan tersebut.

Keamanan *database* dapat dilakukan dengan beberapa cara contohnya pembatasan hak akses pada*database* tersebut, pengunaan nama *field*data yang hanya pahami oleh pemilik aplikasi dan tidak terdapat pegawai yang dapat mengakses *database* dan memahami alur *database* yang ada sehingga terhindar dari manipulasi data dan lainnya, serta menerapkan metode *kriftografi* pada aplikasi[3] terhadap *field* data di dalam *database*nya dengan tujuan *field* data yang disimpan menjadi lebih terjamin privasinya dan tidak dapat dimengerti oleh pihak luar mapun pihak dalam.

Kriptografi [4]sendiri merupakan ilmu dan sekaligus seni untuk mengamankan data yang didalamnya terdapat algoritma tertentu yang bertujuan sebagai *confusion* atau pembingungan, dengan cara mengubah teks polos *(plaintext)* menjadi teks yang tidak bisa dibaca artinya secara langsung oleh manusia atau teks rahasia *(ciphertext).* Kriptografi mempunyai proses *enkripsi* dimana dapat mengubah teks atau data *(plaintext)* menjadi teks rahasia *(ciphertext),* kemudian sebaliknya proses deskripsi yang dapat mengembalikan teks rahasia *(ciphertext)* menjadi teks atau data *(plaintext)*. Dalam proses ini digunakan kunci rahasia, semakin banyak kunci rahasia yang digunakan maka semakin bagus. Algoritma kriptografi diklasifikasikan menjadi dua yaitu algoritma simetris dan algoritma asimetris. Contoh algoritma kriptografi Asimetris yaitu algoritma *RSA* (Rivest, Shamir, Adleman)[5].

Penerapan algoritma kriptografi RSA menjadi solusi yang baik pada sistem penjualan yang akan dibangun CV. Sinergi *Computer* Lubuklinggau untuk menjamin kerahasiaan data-data penjualan yang disimpan didalam *database*, dengan penggunaan algoritma RSA ke dalam sistem penjualan tersebut maka data yang disimpan di dalam *database* berupa penjumlahan angka sehingga isi datanya tidak dapat dimengerti oleh pihak lain.

2. METODOLOGI PENELITIAN

Dalam melakukan penelitian ini, peneliti memilih metode yang digunakan untuk pengembangan sistem yaitu metode *Waterfall*[6], Alasan digunakan metode ini dikarenakan langkah-langah metode *waterfall* sesuai dengan rancangan peneliti. Dimana dalam pengembangan ini peneliti merancang dan membangun sistem secara selangkah demi selangkah. Adapun langkah-langkah yang dilaksanakan dalam metode *Waterfall*antara lain:

a. Analisis Sistem
   Pada langkah ini peneliti melakukan analisis data.
b. Desain Sistem
   Pada langkah ini peneliti membuat desain dari aplikasi berupa struktur data, diagram blok proses keamanan pada *database*, representasi antarmuka, dan membuat algoritma RSA, yang akan diterapkan langkah selanjutnya.
c. Pembuatan Kode Program *(Coding)*
   Disini peneliti melakukan pengkodean *(coding),* untuk membuat program sesuai dengan desain sistem sebelumnya. Pada langkah ini adalah aplikasi komputer yang telah dikerjakan sesuai dengan desain sistem.
d. Pengujian
   Langkah selanjutnya sistem baru yang telah dibuat, maka akan dilakukan pengujian guna memperbaiki kesalahan *(error)* dan hasil aplikasi yang dibuat sesuai dengan kebutuhan.

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Penerapan algoritma asimetris *RSA*untuk keamanan data pada aplikasi penjualan cv. sinergi computer lubuklinggau berbasis webmerupakan penelitian yang dimulai dari:

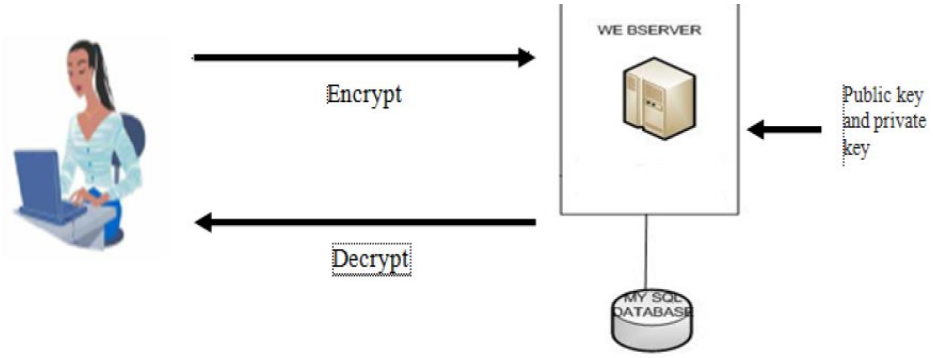
3.1.1 Analisis Sistem

Pada tahap ini dilakukan penelitian langsung ke tempat penelitian dan wawancara dengan pimpinan untuk mencari masalah-masalah yang muncul yang ada di CV. Sinergi.

3.1.2 Desain Sistem

Pada langkah ini dilakukan pembuatan desain dari aplikasi antara lain

a. *Block* diagram
   Block diagram keamanan pada *database* menggunakan algoritma RSA ini digunakan untuk menggambarkan cara kerja algoritma RSA pada sistem dan *database* yang disajikan pada gambar 1. Pada block diagram menggambarkan bahwa kunci privat dan kunci publik dimasukkan pada *source code*.



Gambar 1. Block Diagram Keamanan *Database*

b. Desain database yang terdiri dari tabel admin, tabel kategori, tabel konsumen, tabel produk, order produk dan pemesanan produk.
c. Membuat algoritma RSA
   Pada algoritma RSA ini di pilih nilai bilangan prima untuk p = 11 dan q = 29. Algoritma tersebut yaitu

```
<?php
$n = gmp_mul(11, 29);
$valn = gmp_strval($n);
    $m = gmp_mul(gmp_sub(11, 1),gmp_sub(29, 1));
 for($e = 2; $e < 1000; $e++){
    $fpb = gmp_gcd($e, $m);
    if(gmp_strval($fpb)=='1')
    break;}
$i=1;
 do {
    $key = gmp_div_qr(gmp_add(gmp_mul($m,$i),1), $e);
    $i++;
    if($i==1000)
        break;}
while(gmp_strval($key[1])!='0');
$d = $key[0];
$vald =gmp_strval($d);
?>
```

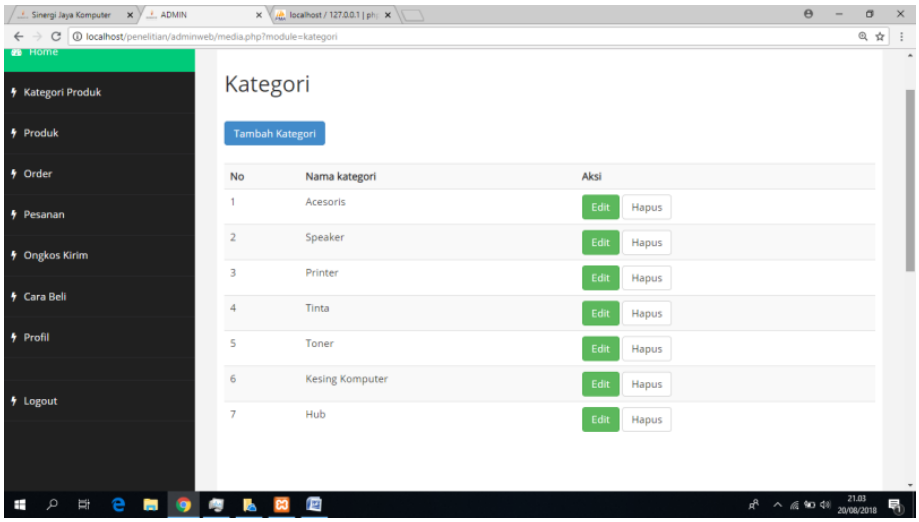
d. Mendesain tampilan *input* dan *output*, desain ini terdiriaa dari desain untuk admin dan desain untuk konsumen.

3.1.3 Pembuatan Kode Program

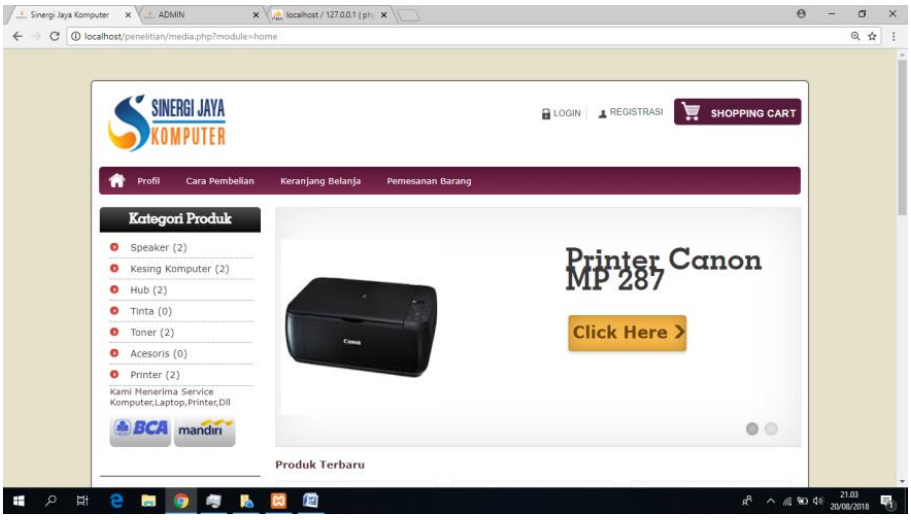
Proses pembuatan kode program menggunakan bahasa pemrograman PHP. Program yang dibuat menyesuaikan dari rancangan database, rancangan input dan rancangan output.

3.1.4 Pengujian

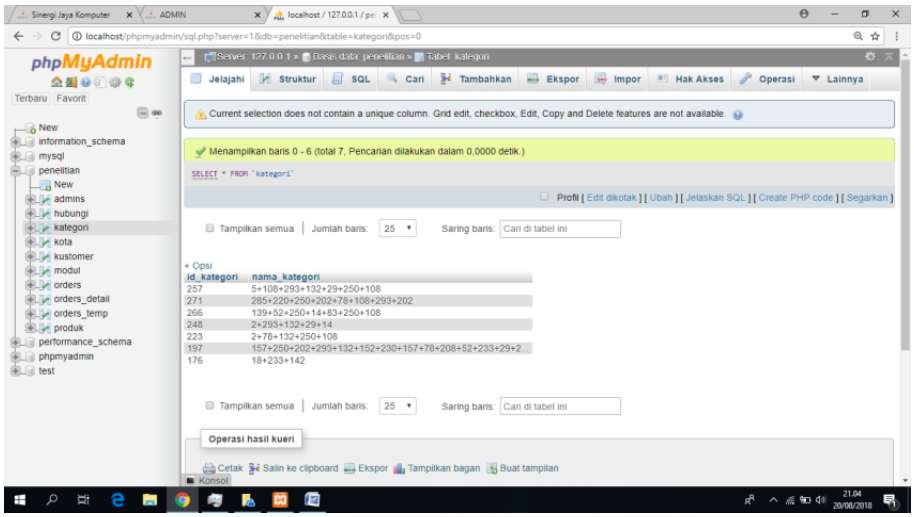
Proses pengujian ini dilaksanakan guna menguji algoritma RSA dapat diterapkan pada aplikasi yang direncanakan. Pada saat proses pengujian seperti pada gambar 2 sampai dengan gambar 14, terlihat bahwa agoritma RSA yang digunakan dapat berjalan sesuai dengan yang direncanakan yaitu informasi yang masukkan ke dalam aplikasi tersimpan di database dalam bentuk enkripsi angka. Proses pengujian ini terdiri dari data admin, data konsumen, data kategori barang, data produk, dan data order produk.



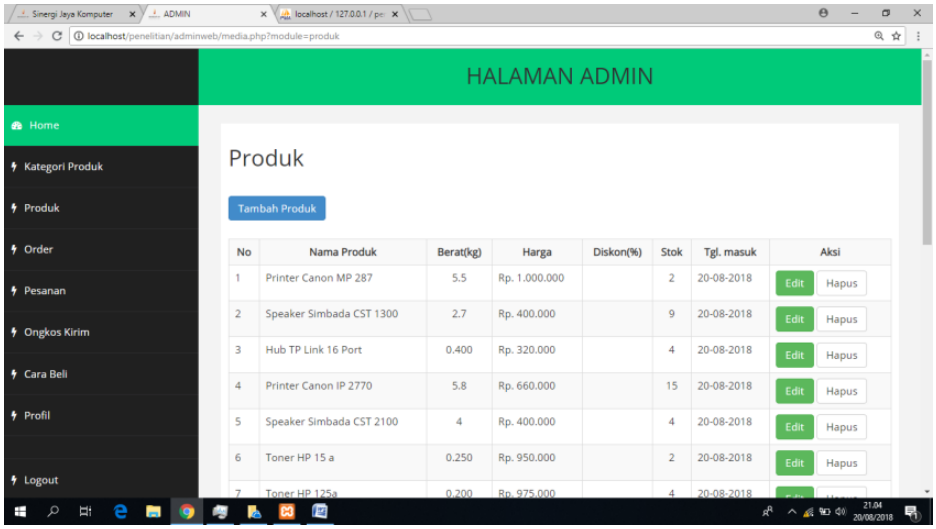
Gambar 2. Tampilan Data Kategori Produk Yang Sudah Didekrip Pada Halaman Admin



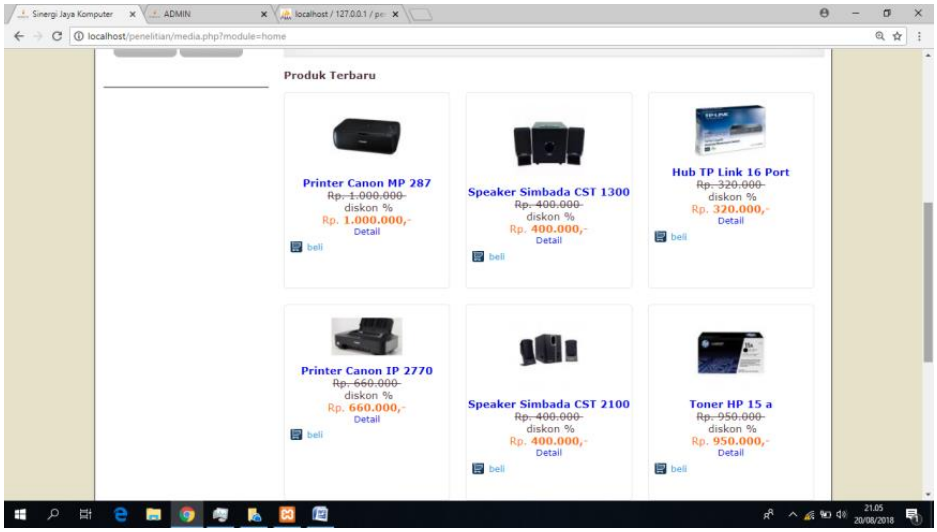
Gambar 3. Tampilan Data Kategori Produk Yang Sudah Didekrip Pada Halaman Konsumen



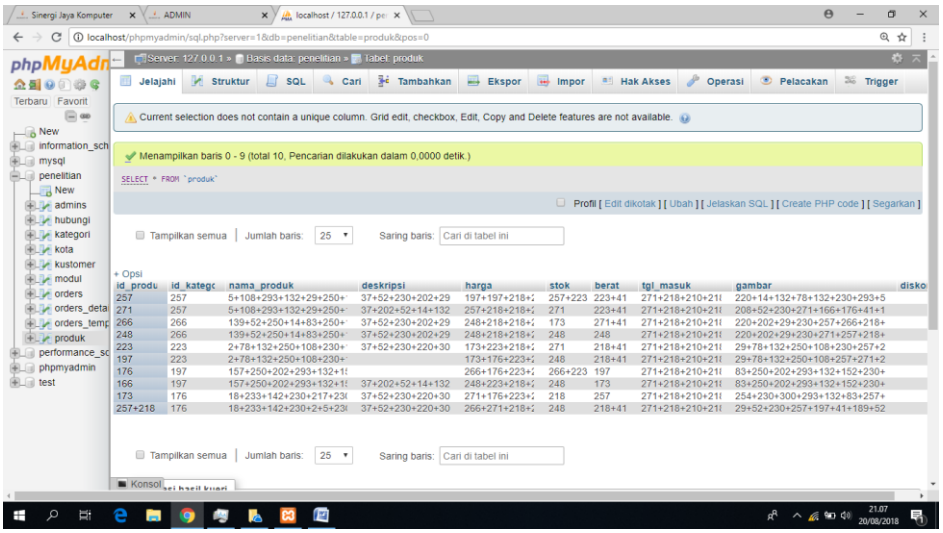
Gambar 4. Tampilan Data Kategori Produk Yang Terenkripsi Pada *Database*



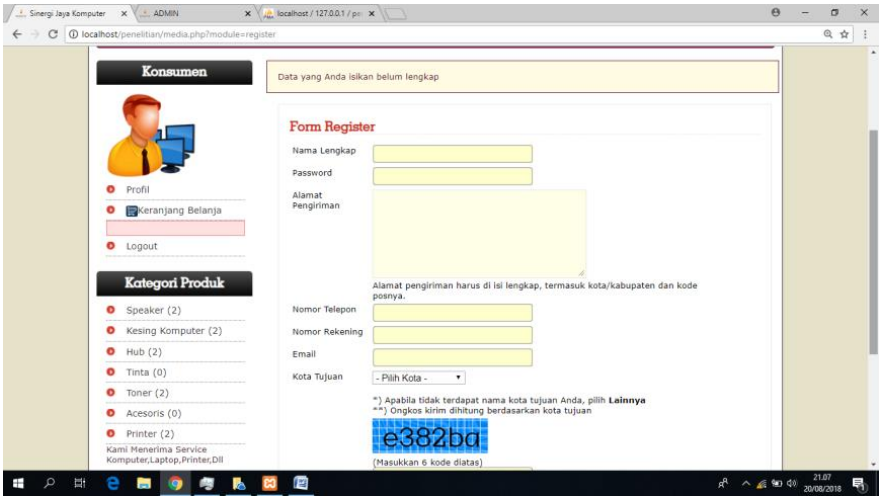
Gambar 5. Tampilan Data Produk Yang Sudah Didekrip Pada Halaman Admin



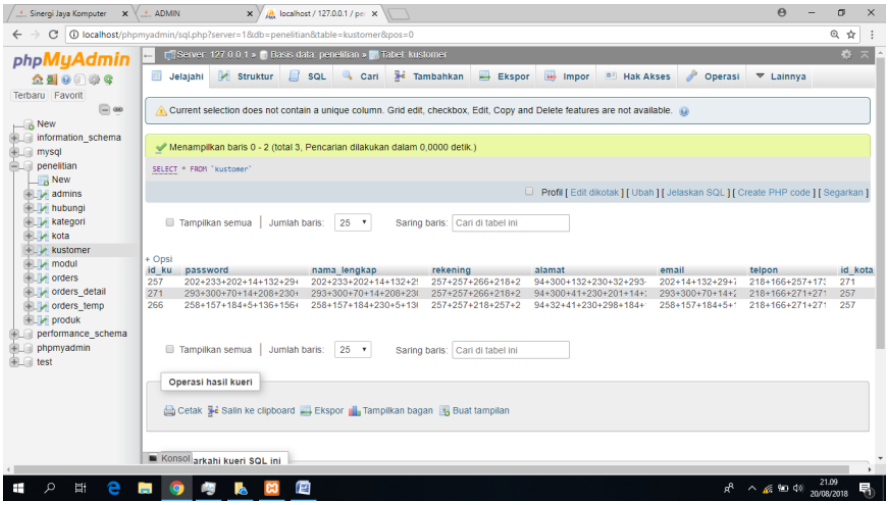
Gambar 6. Tampilan Data Produk Yang Sudah Didekrip Pada Halaman Konsumen



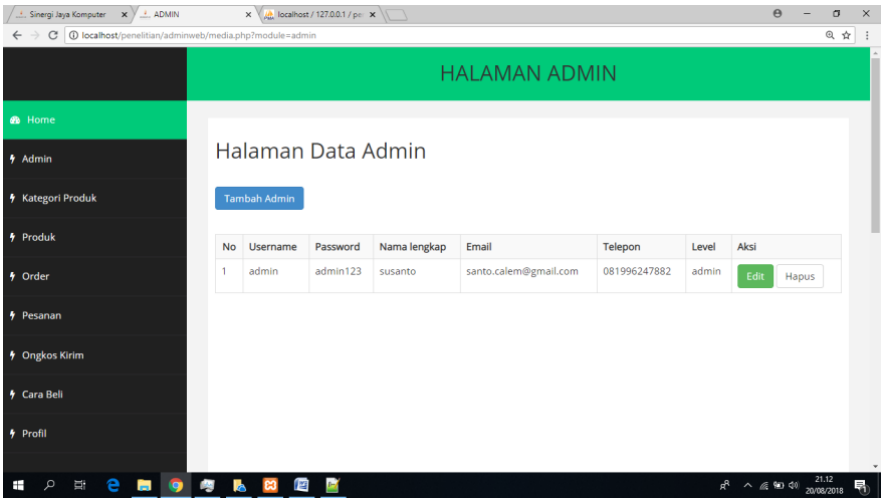
Gambar 7. Tampilan Data Produk Yang Dienkripsi Pada *Database*



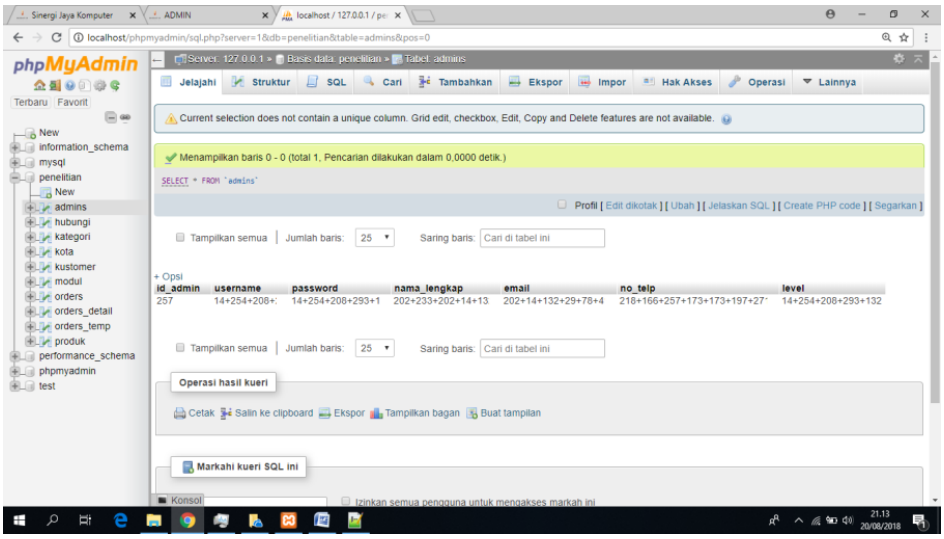
Gambar 8. Tampilan Data Registrasi Pada Halaman Konsumen



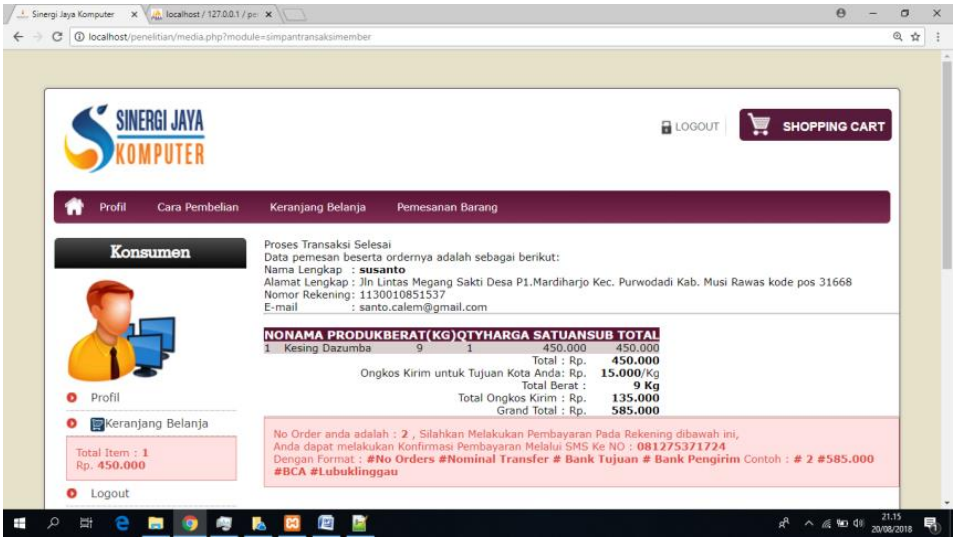
Gambar 9. Tampilan Data Konsumen Yang Dienkripsi Pada Database



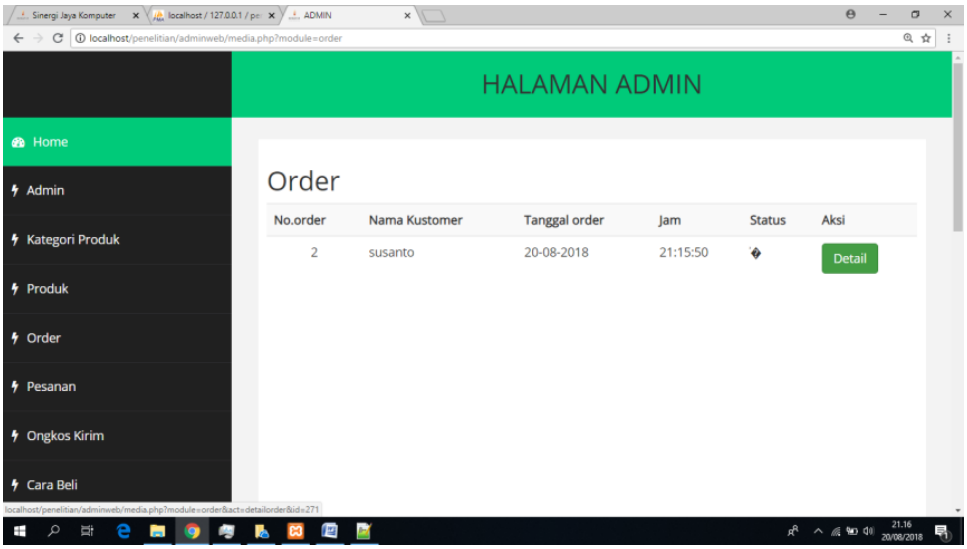
Gambar 10. Tampilan Data Admin Yang Sudah Didekrip Pada Halaman Admin



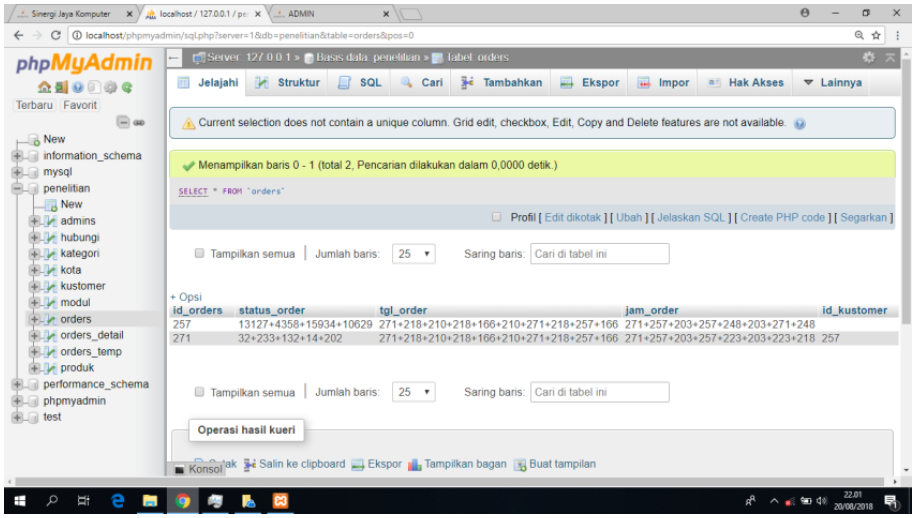
Gambar 11. Tampilan Data Admin Yang Sudah Dienkripsi Pada Database



Gambar 12. Tampilan Data Order Produk Yang Sudah Didekrip Pada Halaman Konsumen



Gambar 13. Tampilan Data Order Produk Yang Sudah Didekrip Pada Halaman Admin



Gambar 14. Tampilan Data Order Produk Yang Sudah Dienkrip Pada Database

3.2 Pembahasan

Pembahasan penerapan algoritma RSA pada proses pengamanan data adalah sebagai berikut

a. Dipilih 2 bilangan prima yaitu nilai p dan nilai q dimana nilai p tidak sama dengan nilai q, disini peneliti memilih nilai$p = 11$ dan nilai $q = 29$.

b. Dihitung nilai

$$m = p\ x\ q \quad (1)$$

Sehingga hasilnya adalah $11\ x\ 29 = 319$.

c. Dihitung nilai

$$n = (p - 1)\ x\ (q - 1) \quad (2)$$

Sehingga hasilnya adalah (11-1)* (29-1) = 280

d. Pilih nilai $e$yang relatively prime terhadap nilai n, $e$yang relatively prime terhadap nilai $n$artinya faktor pembagi terbesar kedua adalah 1, secara matematis dinotasikan $\gcd(e, n) = 1$.

Nilai e dapat dihitung dengan cara $\gcd(3,280) = 1$, maka nilai $e = 3$

e. Pilih nilai d, nilai d merupakan nilai integer dapat dihitung dengan menggunakan rumus

$$d = (1 + mn)/e \quad (3)$$

Sehingga didapat $d = \frac{(1+2.280)}{3} = 187$

f. Proses enkripsi dengan rumus

$$C = n^e mod\ m \quad (4)$$

Nilai C adalah bentuk enkripsi, nilai nadalah karakter dalam bentuk bilangan ASCII yang akan di enkripsi, e adalah kunci publik yang didapat dari proses $\gcd(e,n) = 1$, sedangkan madalah nilai perkalian p dan q

g. Proses dekripsi dengan rumus

$$M = C^d mod\ m \quad (5)$$

Nilai M adalah bentuk dekripsi berupa Nilai karakter ASCII, C adalah bentuk enkripsi, d adalah kunci privat sedangkan madalah nilai perkalian p dan q.

Pengujian selanjutnya adalah proses perhitungan algoritma Rives Shamir Adleman (RSA) dengan cara menghitung manual untuk mendapatkan bentuk enkripsi dan bentuk dekripsi. Pada proses perhitungan ini akan mencari bentuk enkripsi dan dekripsi "Printer".

Tabel 1. Nilai desimal pada tabel ASCII dari karakter "Printer"

Kareakter	***P***	***r***	***i***	***n***	***t***	***e***	***r***
ASCII	80	114	105	110	116	101	114

Dari perhitungan pada langkah b dan d yang telah dilakukan maka di peroleh nilai $m = 319, n = 280, e = 31, d = 271$ Sehingga untuk proses enkripsi yang terjadi sebagai berikut:

$C = 80^3 mod\ 319 = 5$
$C = 114^3 mod\ 319 = 108$
$C = 105^3 mod\ 319 = 293$
$C = 110^3 mod\ 319 = 132$
$C = 116^3 mod\ 319 = 29$
$C = 101^3 mod\ 319 = 250$
$C = 114^3 mod\ 319 = 108$

Dari hasil perhitungan di atas jika digabungkan maka bentuk enkripsi dari "Printer" yaitu 5+108+293+132+29+250+108. Bentuk enkripsi dipisahkan oleh karakter + antara karakter. Bentuk penggunaan algoritma RSA pada aplikasi untuk mengekripsi data "Printer " dapat dilihat di gambar 2 dan 3 pada bagian kategori dan gambar 4 untuk *database*.

Pengujian selanjutnya adalah Mendekripsi data enkripsi "5+108+293+132+29+250+108", pada proses dekripsi pemisah karakter enkripsi tanda "+" diabaikan. Proses dekripsi data sebagai berikut:

$M = 5^{187} mod\ 319 = 80$
$M = 108^{187} mod\ 319 = 114$
$M = 293^{187} mod\ 319 = 105$
$M = 132^{187} mod\ 319 = 110$
$M = 29^{187} mod\ 319 = 116$
$M = 250^{187} mod\ 319 = 101$
$M = 108^{187} mod\ 319 = 114$

Jika hasil perhitungan dekripsi dikumpulkan maka enkripsi dari "5+108+293+132+29+250+108" adalah 80 114 105 110 116 101 114. Hasil dekripsi tersebut jika dilihat dari tabel ASCII, merupakan karakter dari Printer.

4. KESIMPULAN

Berdasarkan hasil pengujian pada penerapan algoritma asimetris *rsa* untuk keamanan data pada aplikasi penjualan cv. sinergi computer lubuklinggau berbasis web yang telah dilakukan oleh peneliti, setiap data yang diinputkan ke dalam aplikasi penjualan, data atau karakter yang dimasukkan tersebut disimpan di *database*berbentuk enkripsi penjumlahan angka jika data yang dimasukan lebih dari satu karakter tetapi jika data yang dimasukan hanya satu karakter makadata atau karakter yang dimasukkan tersebut disimpan di *database*berbentuk enkripsi angka, dengan data yang tersimpan di dalam *database* ini dalam bentuk penjumlahan angka maka data konsumen, data produk dan data pendukung lainnya aman tersimpan di dalam database tersebut karena sulit dimengerti oleh pihak lain. Semakin besar nilai bilangan prima yang dimasukan pada nilai$p$ dan q dari algoritma asimetris RSA ini maka semakin terjamin keamanan datanya.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada Kemenristek Dikti dalam rangka pemberian hibah penelitian dosen pemula, sehingga penelitian ini dapat terlaksana.

DAFTAR PUSTAKA

[1] W. Lestari and Dkk, "Aplikasi Algoritma Kriptografi dan Steganografi Untuk Kemanan Informasi Berbasis Teks," Politeknosains, vol. Vol. 15, no. No. 2, 2016.
[2] B. Rahajo, Belajar Otodidak Membuat Database Menggunakan MySq. Bandung: Informatika, 2011.
[3] P. Edy, Sistem Informasi Geografis: Konsep-Konsep Dasar (Perspektif Geodesi & Geomatika). Bandung: Informatika, 2014.
[4] R. Sadikin, Kriptografi untuk Kemanan Jaringan. Yogyakarta. Yogyakarta: CV Andi Offset, 2012.
[5] H. Listiyono, "Implementasi Algoritma Kunci Piblic Pada Algoritma RSA," Din. Inform., vol. Vol.1, no. No.2, 2009.
[6] M. Sukamto, A, R, and Shalahuddin, Rekayasa Perangkat Lunak. Bandung: Informatika, 2013.