BAB V

KESIMPULAN DAN SARAN

Kesimpulan

Dalam penerapan Algoritma RSA *digital signature* untuk transaksi *digital* cash ini, dapat memberikan jaminan keamanan untuk otentikasi setiap serial number yang di-*release* oleh bank. Hal tersebut dikarenakan *serial number digital signature* yang memiliki jumlah blok 11 ini hanya dapat diverifikasi dengan menggunakan *public key* dan variabel n yang diberikan oleh bank, dalam hal ini adalah pihak yang menandatangani *serial number* tersebut. Jika *hacker/cracker* berhasil mencuri *public key* dan variabel n ini, maka tentunya proses verifikasinya tidak semudah dilakukan, karena *hacker/cracker* harus mengetahui nilai bilangan prima p dan q dari variabel n tersebut, proses pemfaktoran variabel n menjadi bilangan prima p dan q ini sangat sulit mengingat pemfaktoran untuk bilangan prima ini sangat besar, terdapat 570 kemungkinan untuk menentukan kedua bilangan prima tersebut. Tidak hanya itu, hacker/cracker juga harus mengetahui perhitungan modifikasi konversi dari string *message digest* ke ASCII tersebut, Yang dalam hal ini penulis menggunakan modifikasi pengurangan 30 angka untuk setiaphasil konversi ASCII desimalnya.

Dalam penerapan algoritma RSA *digital signature* dalam transaksi *digital cash* ini memiliki beberapa kelebihan seperti :

1. Transaksi ini dapat lebih menjaga privasi kustomer dalam transaksinya, karena dalam transaksinya tidak membutuhkan data privasi kustomer seperti informasi kustomer, nomor rekening, PIN atau data kartu kredit yang diberikan kepada vendor disaat transaksi dilakukan seperti dalam tansaksi *online* sekarang ini. Yang dibutuhkan dalam transaksi *digital cash* ini hanya *serial number* dan *serial number digital signature* saja.
2. Karena variabel yang digunakan dalam menandatangani *serial number* ini menggunakan fungsi random untuk bilangan prima p dan q dengan 570 kemungkinan, maka tentunya di setiap penandatanganan akan memiliki nilai *serial number digital signature* yang berbeda pula meskipun serial number tersebut sama.
3. Uang digital ini terputus hanya sampai dengan nominal yang terkandung dalam uang digital tersebut, tidak seperti transaksi yang melibatkan no rekening atau kartu kredit misalnya. jika terjadi pencurian tehadap no rekening atau kartu kredit misalnya dan dipergunakan oleh pihak yang bukan haknya, maka akan berpengaruh pada saldo akun yang terdapat di bank kustomer yang dicuri, sedangkan untuk uang digital ini hanya terbatas untuk nominal yang terkandung dalam uang digital tersebut.

Adapun kekurangan dalam sistem ini adalah :

1. Uang digital ini lebih direkomendasikan untuk jumlah nominal yang tidak terlalu besar yang ditujukan untuk kebutuhan tertentu.

2. Karena transaksinya anonim dan portabel, maka perlu untuk menyimpan baik-baik setiap serial number dan serial number digital signature yang dimilikinya.
3. Dalam transaksi yang penulis rancang ini, tidak membahas secara terperinci mengenai interaksi antar *external entity* di luar sistem informasi *digital cash* yang terdapat pada dokumen teknis perangkat lunak mengenai interaksi antar bank dan deposit.

Saran

1. Dalam implementasi RSA *digital signature* pada transaksi *digital cash* ini untuk penggunaan algoritma dalam proses penandatanganannya dapat juga digunakan algoritma asimetrik lain selain dari pada algoritma RSA, seperti Algoritma DSA, Algoritma Elgamal, algoritma Schnorr.
2. Agar lebih mengoptimalkan keamanan dalam transaksinya, gunakan *sertificate* SSL versi terbaru.
3. Transaksi *digital cash* ini dapat dikembangkan hingga *include* ke berbagai *pheriperal* untuk *serial number digital signature* seperti : *smart card* dan *mobile phone* misalnya. Selain itu menurut penulis transaksi *digital cash* ini dapat juga diimplementasikan secara *offline* untuk transaksi di supermarket tertentu dengan mengkonversi *serial number digital signature* ke dalam kode *barcode* agar dapat dibaca oleh alat pembaca *barcode*.