BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan rumusan masalah dan hasil penelitian dapat diambil beberapa kesimpulan:

1. Penelitian ini telah berhasil mengimplementasikan *blind signature* menggunakan algoritma RSA dalam transaksi *digital cash*, hal ini terbukti dengan dihasilkannya *digital cash* dengan *signature* **11690041 9413863 20358004 2196839 1013569 5409521 20604743 2243615 20001304 11394742 20604743 13289899** dari *serial number* **RvcNtQ056901** melalui proses *blinding*, *signing* dan *unblinding.*
2. Sistem *blind signature digital cash* telah berhasil dibangun dengan adanya aplikasi *system blind signature digital cash* yang terintegrasi pada website Bank Aman Sentosa. *Digital cash* yang dihasilkan juga memenuhi syarat *property anonimity digital cash*, karena privasi *customer* tetap terjaga dari bank. Bank tidak dapat mengetahui trasaksi *digital cash* yang dilakukan oleh *customer*, bahkan bank tidak bisa secara pasti menghubungkan antara suatu *digital cash* dengan *customer*. Di lain pihak,*vendor* juga tidak mengetahui identitas *customer* yang membeli produknya.

3. Penelitian ini berhasil membuat *digital cash* yang valid digunakan dalam transaksi pembayaran, hal ini terbukti karena hanya *digital cash* dengan nominal yang cukup saja yang bisa digunakan sebagai alat pembayaran.
4. Skema untuk menjaga keamanan *digital cash* telah berhasil dibangun, dengan adanya proses *update digital cash* untuk *digital cash* yang masih memiliki sisa nominal saat transaksi pembayaran.
5. *Property transfer ability digital cash* juga terpenuhi dalam penelitian ini. Nominal *digital cash* dapat ditransfer ke rekening *vendor* saat proses pembayaran atas pembelian sejumlah produk miliknya.
6. Selain dua *property* utama tersebut, *digital cash* hasil juga memenuhi *property independece*, yaitu dapat di kirim melalui jaringan atau *network*. *Property security*, yaitu *digital cash* tidak dapat di duplikasi, karena baik *serial number* maupun *signature* yang menjadi *digital cash* bersifat unikserta masing-masing *digital cash* memiliki atribut yang berbeda-beda. Selain itu setiap *digital cash* yang masih aktif setelah proses pembayaran akan di *update* menjadi *digital cash* baru yang berbeda dengan atribut yang berbeda pula dari yang semula, sehingga pencurian atau penggunaan kembali *digital cash* tidak akan valid dalam proses pembayaran.
7. Proses enkripsi dan dekripsi menggunakan algoritma RSA (dalam penelitian ini proses *blinding, signing* dan *unblinding* serta *validasi*) pada

plainteks (***Serial Number***) menggunakan kunci publik dan privat yang di *generate* secara *random* menghasilkan 100% nilai validasi *true.*

8. Proses enkripsi dan dekripsi (*blinding, signing* dan *unblinding* serta *validasi*) pada *plainteks* (***Digital Cash***) menggunakan kunci publik dan privat yang di *generate* secara *random* menghasilkan 67% nilai validasi *true* dan 33% nilai validasi *false.*

5.2 Saran

System blind signature digital cash yang merupakan hasil penelitian ini memiliki beberapa kelebihan di antaranya:

1. Penggunaan *digital cash* dalam transaksi pembelian *online* lebih aman, karena penggunaannya terbatas sampai dengan jumlah nominalnya saja. Tidak seperti transaksi yang melibatkan rekening atau kartu kredit, jika terjadi pencurian maka akan langsung berpengaruh pada saldo rekening.
2. Setiap *digital cash* yang masih aktif setelah proses pembayaran akan di *update* menjadi *digital cash* baru yang berbeda dengan atribut yang berbeda pula dari yang semula.
3. *Digital cash* yang masih aktif tapi nilai nominalnya tidak mencukupi untuk transaksi pembelian dapat ditambah nilai nominalnya, atau *claim* untuk memasukan sisa nominal tersebut ke saldo rekening *customer*.

4. *Digital cash* sulit untuk dipalsukan atau diduplikasi, karena masing-masing *digital cash* memiliki atribut yang berbeda-beda yang didapatkan melalui proses *blinding, signing, dan unblinding* terlebih dahulu.

Adapun kekurangan dari sistem ini adalah:

1. Sistem ini belum menerapkan kepemilikian kunci privat dan publik bagi masing-masing *customer*.
2. *Digital cash* yang dihasilkan tidak memiliki batas masa aktif.
3. Customer tidak bisa melakukan *claim* nominal *digital cash* dalam jumlah tertentu.

Untuk mengembangkan penelitian ini, dapat dipertimbangkan beberapa hal berikut berdasarkan kelebihan dan kekurangan dari sitem yang telah dibangun:

1. Membuat skema baru, dengan memberikan kunci bagi *customer*. Masing-masing *customer* memiliki kunci publik dan kunci privat yang berbeda-beda, dan untuk penggunaan *digital cash* disertai dengan kunci milik *customer*. Hal ini akan menambah keamanan dan kekuatan *digital cash*.
2. Membuat fungsi *expire* untuk *digital cash* atau masa aktif *digital cash* setelah proses *withdrawal*.
3. Membuat fungsi *claim* nominal *digital cash* dalam jumlah tertentu.
4. Implementasi *blind signature* menggunakan algoritma lain seperti DSA atau elgalmal.
5. Membangun sistem *digital cash* protokol *ofline*