ABSTRAK

Aspek paling penting yang harus diperhatikan dalam layanan *e-payment* adalah tingkat keamanannya dimana dengan banyaknya komunikasi data yang terjadi pada jaringan perbankan, suatu informasi menjadi sangat rentan terhadap serangan-serangan dari pihak-pihak yang tidak berhak. Kendala lainnya adalah bagaimana baik *user* maupun *server* di bank mengetahui bahwa suatu identitas yang masuk kedalam koneksi jaringan tersebut, benar-benar yang bersangkutan. Dengan kata lain, keotentikan suatu data tertransmisi didalam jaringan *e-payment* yang *end-to-end* menjadi faktor yang turut menentukan kelancaran bertransaksi kedua-belah pihak.

Metode keamanan standar yang selalu digunakan untuk melakukan otentikasi dalam bertransaksi perbankan adalah menggunakan *password*, misalnya seorang user hendak melakukan login dengan terlebih dahulu memasukkan sebuah PIN (*Personal Identifier Number*). Tetapi, jika menggunakan password yang sama (password statis) beberapa kali untuk masuk ke dalam suatu sistem, maka akan mudah menjadi target serangan *sniffer*.

Program ini belum berhasil diselesaikan dengan sempurna, karena masih terdapat *bug (error)* yang terjadi, dan bug tersebut merupakan halangan terbesar karena benar-benar menyalahi landasan teori dari algoritma Rijndael ini sendiri yang mana hanya boleh dan hanya dapat memproses 8 bit dalam satu kolom pada *array state*. Hal ini disebabkan karena adanya kekurangan pada library Java yang tidak mensupport perhitungan *checksum* dan *carry overflow* sehingga dibutuhkan library tambahan. Karena itu program ini belum bisa dilanjutkan.

Key words: Personal Identification Number, One-Time Password, AES 128 dan Carding.