ABSTRACT

Most important aspect to be considered in the SMS Banking service is the level of its security where the great number of data communications that occur in the banking network, an informations to be very vulnerable to attacks from parties that are not eligible. Other obstacle is how both user and server in a bank know that the identity of the connection into the network, really concerned. In other words, an authentication of a short-message transmitted through end-to-end SMS Banking network being a factor which determines a smooth second-deal parties.

Method security standard which is always used to do authentication in a banking deal is to use a password, for example, a user trying to login with the first to enter a PIN (Personal Identifier Number). But, if you use the same password (static password) several times to enter into a system, easily will be the target of sniffer attacks.

Therefore, in this Final Project will be discussion of the design of security system that combines the application of the technique encryption/decryption 128-bit AES (Rinjdael algorithm) with the authentication method One-Time Password (OTP) based Challenge/Response with Changeable-Rules as business-optimizing SMS Banking services available, to ensure the authenticity and integrity of the message content, as well as short transactions clear identification of the sender. All will be implemented in simulation using NetBeans 6.5.

The desired results from this form of SMS Banking security steps in the deal by using the SMS service (Short Message Service) Plain which secure, fast, and user-friendly.

Keywords: optimization, SMS Banking, SMS Plain, security, authentication, Rinjdael (AES), One-Time Password.