Implementation of Secure Online Shopping System by using Digital Signature

Naing Linn Ko Ko, Khin Than Mya

University of Computer Studies, Yangon

konaing.lkk@gmail.com

Abstract

The growth of the Internet and e-commerce has presented businesses; these have also been exposed to the various threats. So, network security is necessary to counter the threats and make networks safe to use. The main security concern of applications are addressed b cryptography. Public key cryptography can be used for confidentiality, authentication or both. Proving identity is called authentication. Authentication is one of the most important factors in online systems. RSA algorithm is extensively used in the popular implementation of Public Key Infrastructures. Digital signature is a user authentication method to prevent impersonations. Sales and marketing people need to understand crypto in order to prove the products they are selling are secure. In this paper, we have implemented secure online shopping system by using Public key authentication, (Rivest-Shamir-Adleman) RSA Digital signature and Secure Hash Algorithm (SHA-512) to ensure security of not only the data but also network of online shopping.