Abstract

Key management is the hardest part of cryptography. Designing secure cryptographic algorithms and protocols isn’t easy. As the Intranet becomes popular, it is important to consider the system security. This is because the data flowing through the network is susceptible to be intercepted and modified by a cracker or hacker. So, how to protect personal privacy and preserve a safe online commerce? These are challenges for security protocols. In this paper, a protocol has been developed that depends on the Elliptic key cryptosystem to provide a robust mechanism for key exchange. Also the confidentiality is provided using AES and RC4 with random selection. To satisfy message integrity, SHA1 technique is considered.

References

- Benjamin Tobler. "A Structures Approach to Network Security Protocol Implementation"; a Dissertation, Faculty of Science, University of Cape Town, 2005

**Index Terms**

Computer Science  
Security

**Keywords**

Security protocol  
Transport layer  
Intranet  
Key exchange.