Abstract

Asymmetric algorithm like Diffie-Hellman can be used to encrypt the SMS message in M-commerce or mobile banking system. Password key exchange protocol based on Diffie-Hellman key exchange algorithm allows users to exchange a secret key that can be used in message encryption. The security of this protocol can be increased by using the MAC (message authentication code) or hash function with the encryption. These functions act as an error detecting code or checksum. This paper throws a light on the comparative analysis of both the authentication functions separately in password key exchange protocol. By analyzing some of the security issues viz. (i) brute force attach and (ii) cryptanalysis, it can be very well shown that the MAC function is more secure than hash.
References

- C.J. Mitchell “Truncation attacks on MACs” IEE 2003 Electronics Letters Online No: 20030921DOI: 10.1049/el: 20030921

Index Terms

Computer Science

Keywords

GSM  SMS security  authentication function  public key cryptography