{tag} {/tag}
IJCA Special Issue on Communication Security
© 2012 by IJCA Journal

comnetcs - Number 1

Year of Publication: 2012

Authors:
Neetesh Saxena

Narendra S. Chaudhari

{bibtex}comnetcs1002.bib{/bibtex}

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

- Steven M. Bellovin, Michael Merritt “Augmented Encrypted Key Exchange: A Password-Based Protocol Secure against Dictionary Attacks and Password File Compromise” (1993).
- Xun Yi and Kwok Yan Lam “Hash function based on block cipher” IEE 1997 Electronics Letters Online No: I9971336.
- Luo Zhong Zhao Zhongining Zhu Chongguang “The Unfavourable Effects of Hash Coding on CMAC Convergence and Compensatory Measure” Instilutc of Rcmotc Scnsing Applications .CAS Dept Image Processing.P 0.Box 9718 Beijing china.
- H.E. Michail, A.P. Kakarountas, G. Selimis, C.E. Goutis “Throughput Optimization of the Cipher Message Authentication Code” VLSI Design Laboratory, Dpt. of Electrical & Computer Engineering, University of Patras, Greece.
- 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