



International Journal on Recent Researches In Science, Engineering & Technology

A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy.

It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in DIIF and SJIF.

Research Paper

Available online at: www.ijrrset.com

Chief Editors 1 : Dr. M.Narayana Rao, Ph.D., Rtd. Professor, NIT, Trichy.

(Engg.&Technology division)

2 : Dr. N.Sandyarani, Ph.D., Professor,

Chennai based Engg.College, (Science division)

ISSN (Print) : 2347-6729

ISSN (Online) : 2348-3105

Volume 2, Issue 4,

April 2014

DIIF IF :1.46

SJIF IF: 1.329

A Secure Key exchange protocol

R . Balakrishna

Abstract - Literature review revealed that remote user authentication and key agreement system through credit card is a viable practical solution to validate the eligibility of a remote user and thus to provide a secure communication . This paper suggest a Secure Authenticated Key Exchange Protocol (SAKEP) for Credential Services . The intrinsic worth of this scheme include that , the system do not require any verification table and the user is at liberty to choose and change the password .further , with this system , the computation and communication cost are lower as the scheme adopts one - way hash functions , block siphers and credit card. In addition the proposed scheme offers mutual authentication between server and user by a nonce based plan and is free from time- synchronization problem . The proposed cheme is secured against id -theft , also resists to replay attacks, stolen verifier attacks, guessing attacks, reflection attack and offers forward secrecy and known -key security .