World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:10, No:07, 2016

Secure Proxy Signature Based on Factoring and Discrete Logarithm

Authors : H. El-Kamchouchi, Heba Gaber, Fatma Ahmed, Dalia H. El-Kamchouchi

Abstract : A digital signature is an electronic signature form used by an original signer to sign a specific document. When the original signer is not in his office or when he/she travels outside, he/she delegates his signing capability to a proxy signer and then the proxy signer generates a signing message on behalf of the original signer. The two parties must be able to authenticate one another and agree on a secret encryption key, in order to communicate securely over an unreliable public network. Authenticated key agreement protocols have an important role in building a secure communications network between the two parties. In this paper, we present a secure proxy signature scheme over an efficient and secure authenticated key agreement protocol based on factoring and discrete logarithm problem.

Keywords : discrete logarithm, factoring, proxy signature, key agreement
Conference Title : ICCSCS 2016 : International Conference on Cryptography and Security in Computing Systems
Conference Location : Zurich, Switzerland
Conference Dates : July 21-22, 2016

Open Science Index, Computer and Information Engineering Vol:10, No:07, 2016 publications.waset.org/abstracts/51597.pdf