Policy for Secure Communication using Hybrid Encryption Algorithm

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 125
Number 10
Year of Publication: 2015

Authors:
Amrita Jain, Vivek Kapoor

10.5120/ijca2015906035

Abstract

Secure communication in network environment is primary requirement to access remote resources in a controlled and efficient way. For validation and authentication in e-banking and e-commerce transactions, digital signatures using public key cryptography is extensively employed. To maintain confidentiality, Digital Envelope, which is the combination of the encrypted message and signature with the encrypted symmetric key, is also used. This research paper has proposed to develop a hybrid technique using Symmetric & Asymmetric key cryptography. It will also include Message authentication code to maintain integrity of message. Therefore, proposed model will not only help to maintain confidentiality and authentication of message and user but integrity of data too. Java technology has been proposed to validate the performance of proposed model in context of message length, key length, cipher text length and computational time for encryption and decryption.

References
1. Elichiro Fujisaki, Tatsuaki Okamoto, David Pointcheval and Jacques Stern, RSAOAEP is secure under the RSA assumption, Journal of Cryptology, 2002
5. CRC Press. This book may downloaded from http://www.cacr.math.uwaterloo.ca/hac/

Index Terms

Computer Science

Algorithms
Keywords

Hybrid Secure Communication, RSA, MAC, Symmetric Key.