Secure Network File Transfer using Hybrid Cryptographic Algorithms

Thin Thin Swe
Computer University (Pyay)
thinswe01@gmail.com

Abstract

Security requirement is extremely needed to prevent various types of network attacks in some environment such as banking, exam question distribution, and military information exchange process. Files and data are transferred through networks in such environments. These networks are more vulnerable to network attacks. This paper presents a system to support secure network file transfer. The proposed system uses hybrid cryptosystem; Asymmetric RSA and Symmetric PBE (Password- Based Encryption). PBE uses password to generate encryption and decryption key. AES algorithm is used for the file encryption and RSA algorithm is used for key encryption . This system is more secure than generating keys from storage media. The entire system is implemented by Java Programming Language.