Abstract

Paper introduced RSA cryptosystem and its security aspects. RSA is a public key algorithm that applied widely in the field of information security in the Internet-Banking and E-Commerce applications. The proposed scheme for RSA cryptosystem contains three prime numbers and overcome several attack possible on RSA. The proposed scheme has speed improvement on RSA decryption side by using the Chinese Reminder Theorem (CRT) and the scheme is semantically secure also.

References


\textbf{Index Terms}

Computer Science \hspace{1cm} Security

\textbf{Keywords}

Cryptography \hspace{0.5cm} Prime Numbers \hspace{0.5cm} RSA Cryptosystem \hspace{0.5cm} Security analysis