Journal of Computer Science Engineering and Information Technology Research (JCSEITR)
ISSN(P): 2250-2416; ISSN(E): Applied
Vol. 6, Issue 2, Dec 2016, 15-22

AN EFFICIENT AND ROBUST MODIFIED RSA BASED SECURITY ALGORITHM IN MODERN CRYPTOGRAPHY

RAMKRISHNA GHOSH

Haldia Institute of Technology, India

ABSTRACT

In modern world, security plays a significant role to transmit confidential information over the network. Security is also demanding in wide range of applications. Cryptographic algorithms play a significant role in providing the data security against malevolent attacks.RSA algorithm is applied in the popular implementations of Public Key communications. Asymmetric key cryptography, also called Public Key cryptography uses two different keys. One key is used for encryption and other corresponding key must be used for decryption. No other key can decrypt the message not even the original key used for encryption. The importance of this method is that every communicating party requires a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he/she can communicate with anyone else. In our research paper, we have performed an efficient implementation of RSA algorithm and compared it with existing RSA algorithm.

KEYWORDS: Public Key, RSA Algorithm, Encryption & Decryption

Received: Nov 06, 2016; **Accepted:** Dec 13, 2016; **Published:** Dec 17, 2016; **Paper Id.:** JCSEITRDEC20162

Original Article