IMPACT: International Journal of Research in Engineering & Technology (IMPACT: IJRET)
ISSN(E): 2321-8843; ISSN(P): 2347-4599
Vol. 2, Issue 6, Jun 2014, 143-150
© Impact Journals

UNIQUE INFORMATION BASED SECURE RSA

NEHA GUPTA[1], RAVI KUMAR GUPTA[2] & SHIPRA GUPTA[3]

[1,2]Research Scholar, Department of Computer Science & Engineering, Mewar University, Chittorgarh, Rajasthan, India

[3]Assistant Professor, Department of Computer Science & Engineering, WIT, Sohna, Haryana, India

ABSTRACT

Computer security is one of the most important parameters considered in any computer system to prevent any data misuse by an unauthorized/ outside intrusion. Cryptography is one technique for data/ computer security. In this paper, we have proposed a technique for a more secure data transfer which is a alteration to the classical public key crytogarphy method known as Unique Information Based Secure RSA. This method is based on public key cryptography scheme. In Unique Information Based Secure (UI SECURE) RSA public key of a user is derived from his/her unique identity such as email id, phone number. With the use of UI SECURE RSA, there is no need of public key certificates. It has a special entity called SEM. SEM is an on-line partially trusted server. For using services of SEM, a user needs to obtain an identity based token from SEM. A message cannot be encrypted or decrypted without this token. UI SECURE RSA divides the private key of the user in two parts: one part is given to the user and the other to the SEM. Both parts of the key are used to encrypt/decrypt the message. This technique is very secure as the key cannot be derived using half key.

KEYWORDS: Cryptography, Public Key, Private Key, Encryption, Decryption