Archana B.Kadga, International Journal of Computer Science and Mobile Applications,
Vol.1 Issue. 6, December- 2013, pg. 27-33 **ISSN: 2321-8363**

Implementing Asymmetric-Key Cryptography using Parallel-Key Cryptographic Algorithm (PCA)

Archana B.Kadga
Assistant Professor at SMSMPITR, Akluj Dist.Solapur (Maharastra)
archanabk20@gmail.com; kadgaarchana@gmail.com

Abstract

In this day, the necessity of security and protection of computer information on network has become more and more important. In cryptography, asymmetric-key is the framework with high flexibility which can be applied to most of cryptographic systems using today. To reduce the encryption and decryption time which is the main drawback of asymmetric-key cryptography, we have proposed a new mechanism called "Parallel-key Cryptographic Algorithm (PCA)" which accelerates the cryptographic system in encryption and decryption process and strengthens the system against Brute force attack. We have shown that, in our practical experiment results, our proposed algorithm can perform faster in encrypting and decrypting message than other asymmetric-key cryptographic algorithm; RSA (Rivest, Shamir and Adleman). In our theoretical analysis, we have shown that PCA can provide the security against Brute force attack better than other algorithms. Furthermore, PCA can be applied to parallel computing and cryptographic mode such as Cipher Block Chaining (CBC) and Interleaved Cipher Block Chaining (ICBC) for higher efficiency.

Keywords: PCA; RSA; Brute force attack; Cipher block Chaining

Full Text: www.ijcsma.com/publications/december2013/V1I609.pdf