International J. of Engg. Research & Indu. Appls. (IJERIA).
ISSN 0974-1518, Vol.2, No. VII (2009), pp 73-90

PREPARATION OF BIGNUMBER LIBRARY FOR CRYPTOGRAPHY AND LARGE POSITIVE INTEGER CALCULATIONS

D. T. MANE, P. R. DEVALE, V. R. PAWAR AND S. B. JAVHERI

Abstract

Organizations in both public and private sectors have become increasingly dependent on electronic data processing. Protecting these important data is of utmost concern to the organizations and cryptography is one of the primary ways to do the job. Public Key Cryptography is used to protect digital data going through an insecure channel from one place to another.

This paper is concerned primarily with preparation of a cryptographic library BigNumber in Java**,** which used in implements various mathematical algorithms used in Cryptography for Encryption and Decryption such as RSA, IDEA, DES etc. We also implement these algorithms on universal base system. Therefore these algorithms works not only familiar Binary, Decimal or HexaDecimal number system but also work on any user defined number system. Since many of the most widely implemented techniques emphasis is placed on efficient algorithms for performing the basic arithmetic operations in this structure (addition, subtraction, multiplication, division, and exponentiation). In some cases, several algorithms will be presented which perform the same operation. For such algorithms efficiency can be measured in numerous ways such as Time requirement for execution and memory space (Heap and Non Heap) requirement.

R Library is implemented irrespective of any Radix base number representation. It is used in any Cryptographic or large calculation system. The results are also useful to design efficient implementation of large calculation system.

Keywords - RSA, Key, Public Key, Private Key, GCD, Exponentiation