Cryptography Course Project Abstract

Submitted to : Mr. Alwyn Roshan Pais

Submitted by: Lokananda D M (09CO43), Nishanth P (09CO63), Soumya Mathew (09CO94)

Title:

Implementation and comparison of variants of RSA algorithm.

Abstract:

In this project we plan to implement and compare five variations of the RSA algorithm as analysed by Cesar Alison Monteiro Paixao & Decio Luiz Gazzoni Filho [1] and Boneh & Shacham [2]. The five variants are:

- Batch RSA: This variant does a number of decryptions for approximately the cost of one.
- Mprime RSA: It is a multifactor RSA algorithm based on modifying the structure of the RSA modulus, i.e. it uses a modulus of the form N = pqr, to speed up decryption.
- Mpower RSA: It is a multifactor RSA algorithm based on modifying the structure of the RSA modulus, i.e. it uses a modulus of the form $N = p^2q$, to speed up decryption.
- Rebalanced RSA: This variant improves decryption performance at the expense of encryption performance by choosing d such that d mod p − 1 and d mod q − 1 are small (on the order of s bits usually s = 160)
- Rprime RSA: It is a combination of Mprime RSA and Rebalanced RSA where the key generation procedure of Rebalanced RSA (modified for k primes) is employed together with the decryption procedure of Mprime RSA.

References:

[1] Cesar Alison Monteiro Paixao and D´ecio Luiz Gazzoni Filho. (2005). An efficient variant of the RSA cryptosystem.

[2] Boneh, D. and Shacham, H. (2002). Fast variants of RSA. RSA Laboratories.