Modified RSA Cryptosystem Based on Offline Storage and Prime Number

NTC Mini Project (CO313)

By:
Mehnaz Yunus 16CO124
Sharanya Kamath 16CO140

Submitted to:
Prof. B.R.Chandravarkar
Asst. Professor CSE Dept, NITK

Abstract

This project suggests a new algorithm concept to presents the modified form of RSA algorithm in order to speed up the implementation of RSA algorithm during data exchange across the network.

This includes the architectural design and enhanced form of RSA algorithm through the use of third prime number in order to make a modulus n which is not easily decomposable by intruders

Modified RSA Method

An algorithm is developed which is based on modified RSA cryptosystem. Considering these assumptions for algorithm-

- p , q, and r are prime numbers.
- n is common modulus.
- e is public key.
- d is private key.
- M is message.

RSA Proposed Method:

- Select the random values p, q, and r.
- Calculate $n=pqr$.
- Calculate $\O(n) = (p-1)(q-1)(r-1)$.
- Calculate e such that $\gcd(e, \O(n))=1$ and $1<e<\O(n)$.
- Encrypt the message M where $M<n$ and encrypt with public key e such that $C=M^e \bmod n$.
- Calculate private key $d = e^{-1} \pmod{\O(n)}$.
- Decrypt the message M such that $M=C^d \bmod n$.

Offline Storage

First table contains the values of p, q, Ø(N). Second table contain the values of e, d, r. We use the third prime r thus if anyone want to hack the database table to guess the value of modulus n, he cannot get success because value of n depends on all three prime numbers n= p*q*r. Therefore it is hard to hack both the table simultaneously.

Advantages of Modified RSA

- The strength of large prime number depend on three variables p, q and r. It is difficult to break the large prime number into three as compare in existing RSA algorithm.
- p, q, d and e are stored in two database tables before algorithm starts. We take the index value correspond the values of e and d from the database table and exchange at the time of encryption and decryption rather than original key (e, d). Hence security is increased.
- In proposed method keys are stored offline before the process start. Thus, the speed of process increased as compared to original RSA method.

Future Scope

This method will provide more security and it is reliable to use in networks and cloud computing environment.

In future some security concepts can be applied in the existing RSA algorithm for providing more efficiency and security.

Thank You