JAYOTI VIDYAPEETH WOMEN'S UNIVERSITY, JAIPUR
Government of Rajasthan established
Through ACT No. 17 of 2008 as per UGC ACT 1956
NAAC Accredited University

Faculty of Education and methodology

Department of Science and Technology

Faculty Name- Jv'n Narendra Kumar Chahar (Assistant Professor)

Program- B.Tech 8thSemester

Course Name– Cryptography and Network Security

Session no.: 22

Session Name- RSA and the Chinese Remainder Theorem

Academic Day starts with –

- Greeting with saying **'Namaste'** by joining Hands together following by 2-3 Minutes Happy session, Celebrating birthday of any student of respective class and **National Anthem**.

Lecture starts with- quotations' answer writing

Review of previous Session **– Multi-Precision Arithmetic**

Topic to be discussed today- Today We will discuss about **RSA and the Chinese Remainder Theorem**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

Introduction & Brief Discussion about the Topic**– RSA and the Chinese Remainder Theorem**

RSA and the Chinese Remainder Theorem

A significant improvement in decryption speed for RSA can be obtained by using the Chinese Remainder theorem to work modulo p and q respectively.

Since p,q are only half the size of R=p.q and thus the arithmetic is much faster

CRT is used in RSA by creating two equations from the decryption calculation:

M = Cd mod R as follows:

M1 = M mod p

= (C mod p)d mod (p-1)

M2 = M mod q

= (C mod q)d mod (q-1)

then the pair of equations

M = M1 mod p M = M2 mod q has a unique solution by the CRT, given by:

M = [((M2 +q - M1)u mod q] p + M1

where

p.u mod q = 1

Primality Testing and RSA

The first stage of key-generation for RSA involves finding two large primes p, q

Because of the size of numbers used, must find primes by trial and error and modern primality tests utilize properties of primes eg:

an-1 = 1 mod n where GCD(a,n)=1

all primes' numbers 'n' will satisfy this equation but some composite numbers will also satisfy the equation, and are called pseudo-primes.

Most modern tests guess at a prime number 'n', then take a large number (eg 100) of numbers 'a', and apply this test to each. If it fails the number is composite, otherwise it is is probably prime.

There are a number of stronger tests which will accept fewer composites as prime than the above test. eg:

$$\text{GCD}(a,n) = 1, \quad \text{and} \quad \left(\frac{a}{n}\right) (\text{mod } n) = a^{\frac{(n-1)}{2}} (\text{mod } n)$$

$$\text{where } \left(\frac{a}{n}\right) \text{ is the Jacobi symbol}$$

RSA Implementation in Practice

Software implementations: Generally, perform at 1-10 bits/second on block sizes of 256-512 bits

two main types of implementations:

- on micros as part of a key exchange mechanism in a hybrid scheme
- on larger machines as components of a secure mail system

Hardware Implementations

Generally, perform 100-10000 bits/sec on blocks sizes of 256-512 bits and all known implementations are large bit length conventional ALU units.

Reference-

1. **Book:** William Stallings, “Cryptography & Network Security”, Pearson Education, 4th Edition 2006.

QUESTIONS: -

Q1. Explain RSA and the Chinese Remainder Theorem.

Next, we will discuss more about ElGamal

.

- Academic Day ends with-
  National song ‘Vande Mataram’