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

"बेटी बचाओ, बेटी पढ़ाओ"

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.: 21

Session Name- Multi-Precision Arithmetic

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 **– RSA public key cryptosystem**

Topic to be discussed today- Today We will discuss about **Multi-Precision Arithmetic**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

Introduction & Brief Discussion about the Topic**– Multi-Precision Arithmetic**

Multi-Precision Arithmetic

This involves libraries of functions that work on multiword (multiple precision) numbers and multiplication digit by digit. Also, it does exponentiation using square and multiply are a number of well-known multiple precision libraries available - so don't reinvent the wheel.

We can use special tricks when doing modulo arithmetic, especially with the modulo reductions

Faster Modulo Reduction

Chivers (1984) noted a fast way of performing modulo reductions whilst doing multi-precision arithmetic calcs.

Given an integer A of n characters (a0, ... , an-1) of base b

$$A = \sum_{i=0}^{n-1} a_i b^i.$$

then

$$A \equiv \left\{ \sum_{i=0}^{n-2} a_i\ b^i + a_{n-1}\ b^{n-1} \ (\mathrm{mod}\ jm) \right\} (\mathrm{mod}\ m)$$

ie: this implies that the MSD of a number can be removed and its remainder mod m added to the remaining digits will result in a number that is congruent mod m to the original.

* Chivers algorithm for reducing a number is thus:

```
Construct an array R = (bd, 2.bd, ... , (b-1).bd)(mod m)

FOR i = n-1 to d do

WHILE A[i] != 0 do

j = A[i];

A[i] = 0;
```

```
A = A + bi-d.R[j];

END WHILE

END FOR
```

where A[i] is the ith character of number A R[j] is the jth integer residue from the array R n is the number of symbols in A, d is the number of symbols in the modulus

Speeding up RSA - Alternate Multiplication Techniques

- conventional multiplication takes O(n2) bit operations, faster techniques include the Schönhage-Strassen Integer Multiplication Algorithm:
- breaks each integer into blocks, and uses them as coefficients of a polynomial
- evaluates these polynomials at suitable points, & multiplies the resultant values
- interpolates these values to form the coefficients of the product polynomial
- combines the coefficients to form the product of the original integer
- the Discrete Fourier Transform, and the Convolution Theorem are used to speed up the interpolation stage
- can multiply in O(n log n) bit operations

the use of specialized hardware because:

- conventional arithmetic units don't scale up, due to carry propogation delays
- so can use serial-parallel carry-save, or delayed carry-save techniques with O(n) gates to multiply in O(n) bit operations, or can use parallel-parallel techniques with O(n2) gates to multiply in O (log n) bit operations

Reference-

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

QUESTIONS: -

Q1. Explain Multi-Precision Arithmetic.

Next, we will discuss more about RSA and the Chinese Remainder Theorem.

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