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- RSA Public-key cryptosystem

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 **– Substitution-Permutation Ciphers**

Topic to be discussed today- Today We will discuss about **RSA public key cryptosystem**

Lesson deliverance (ICT, Diagrams & Live Example)-

- Diagrams

Introduction & Brief Discussion about the Topic**– RSA**

RSA Public-Key Cryptosystem

It is best known and widely regarded as most practical public-key scheme was proposed by Rivest, Shamir & Adleman in 1977:

It is a public-key scheme which may be used for encrypting messages, exchanging keys, and creating digital signatures and it is based on exponentiation in a finite (Galois) field over integers modulo a prime nb exponentiation takes O((log n)3) operations. Its security relies on the difficulty of calculating factors of large numbers nb factorization takes O(e log n log log n) operations (same as for discrete logarithms). The algorithm is patented in North America (although algorithms cannot be patented elsewhere in the world) and this is a source of legal difficulties in using the scheme

RSA is a public key encryption algorithm based on exponentiation using modular arithmetic, to use the scheme, first generate keys:

Key-Generation by each user consists of:

- selecting two large primes at random (~100 digit), p, q
- calculating the system modulus R=p.q p, q primes
- selecting at random the encryption key e,
- e < R, gcd(e, F(R)) = 1
- solving the congruence to find the decryption key d,
- e.d [[equivalence]] 1 mod [[phi]](R) 0 <= d <= R
- publishing the public encryption key: K1={e,R}
- securing the private decryption key: K2={d,p,q}

Encryption of a message M to obtain ciphertext C is:

- C = Me mod R 0 <= d <= R

Decryption of a ciphertext C to recover the message M is:

- M = Cd = Me.d = M1+n.[[phi]](R) = M mod R

the RSA system is based on the following result:

if R = pq where p, q are distinct large primes then X [[phi]](R) = 1 mod R

for all x not divisible by p or q and [[Phi]](R) = (p-1)(q-1)

Security of RSA

The security of the RSA scheme rests on the difficulty of factoring the modulus of the scheme R

best known factorization algorithm (Brent-Pollard) takes:

$$O\left(\frac{e^{\sqrt{2 \ln p \ln \ln p}}}{\ln p}\right)$$

operations on number R whose largest prime factor is p

Decimal Digits in R	#Bit Operations to Factor R
20	7200
40	3.11e+06
60	4.63e+08
80	3.72e+10
100	1.97e+12
120	7.69e+13
140	2.35e+15
160	5.92e+16
180	1.26e+18
200	2.36e+19

This leads to R having a length of 200 digits (or 600 bits) given that modern computers perform 1-100 MIPS the above can be divided by 106 to get a time in seconds

> **nb**: currently 1e+14 operations is regarded as a limit for computational feasibility and there are 3e+13 usec/year

but most (all!!) computers can't directly handle numbers larger than 32-bits (64-bits on the very newest). Hence, need to use multiple precision arithmetic libraries to handle numbers this large

Reference-

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

QUESTIONS: -

Q1. Give an overview about RSA algorithm.

Q2. Explain Key-Generation in RSA.

Q3. Write about security of RSA algorithm.

Next, we will discuss more about Multi-Precision Arithmetic.

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