Programme: B.Sc.
Subject: Computer Science
Semester: VI
Course Code: CSD105
Course Title: NETWORK SECURITY

Unit : II
Module Name: Asymmetric Key Cryptography, RSA En/Decryption algorithm
Name of the Presenter: Ms. Dipti Nene

Overview of Asymmetric Key Cryptography (Public Key Cryptography)

- 2 different keys are used
- One key used for encryption and the other corresponding key used for decryption
- No other key can decrypt the message, not even the one used for encryption
- Every communicating party needs just a key pair for communicating with any number of other communicating parties
- One of the 2 keys is the public key and the other is the private key

Eg;
Suppose A wants to send a message to B
A and B should each have a private and public key
1.When A wants to send a message to B A encrypts the message using B's public key.
2.A sends this encrypted message to B
3.B decrypts A's message using B's private key no one else can make any sense of the message since it can be decrypted only by B who has the private key.
When B wants to send a message to A, exactly reverse steps take place.

RSA En/Decryption

- Invented by Rivest, Shamir and Adleman in year 1978
- RSA algorithm is asymmetric/public key cryptography algorithm.
- Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key
- Public Key can be given to anyone. The other key must be kept private.
- It is based on the principle that it is easy to multiply large numbers, but factoring large numbers is very difficult.

RSA Key Setup

Each user generates a public/private key pair by:

1.Select two large primes at random: P, Q

2.Compute N = P X Q.

3.Select a public key(encryption key) E such that it is not a factor of (P-1) and (Q-1) i.e.$\Phi(N) = (P-1)\ (Q-1)$ such that $\gcd(E, \Phi(N)) = 1$, $1<e<\Phi$

[Select a private key(decryption key) D such that following is true :

(D X E) mod (p – 1) X (q – 1) = 1]

5.For encryption, calculate cipher text CT from plain text PT as follows :

CT = PTE mod N

6.Send CT as cipher text to the receiver

7.For decryption, calculate plain text PT from cipher text CT as follows :

PT = CTD mod N

publish their public encryption key: PU={e,n} keep secret private decryption key: PR={d,n}

RSA En/Decryption

- to encrypt a message M the sender:
- obtains public key of recipient PU={e,n}
- computes: C = Me mod n, where 0 ≤ M <n M=PT
- to decrypt the ciphertext C the owner:
- uses their private key PR={d,n}
- computes: M = Cd mod n C=CT

- note that the message M must be smaller than the modulus n (block if needed)

RSA Example 1
Step 1: In this step, we have to select prime numbers. suppose P is 7 and Q is 17
Step 2: Calculate N N = P * Q = 7 * 17 ◊ N = 119
Step 3: Select public key such that it is not a factor of (P – 1) and (Q – 1).
ø(n) = (7 – 1) * (17 – 1)= 6 * 16= 96
[factor of 96 is 2 * 2 * 2 * 2 * 2 *3 ,So here we can select encryption key E as 5 because it is not a factor of both 2 & 3] Step 4: Select private key in such way that it match following equation

(D * E) mod (P – 1) * (Q – 1) = 1.

(D * 5) mod (7 – 1) * (17 – 1) = 1
(D * 5) mod (6) * (16) = 1.
(D * 5) mod 96 = 1 select D as 77
(77 * 5) mod 96 = 1.
385 mod 96 = 1
1 = 1 Hence the equation is equal.

RSA Example 2

1. Select primes: p=17 & q=11
2. Calculate n = p.q =17 x 11=187
3. Calculate ø(n) =(p–1)(q-1)=16x10=160
4. Select E: gcd(e,160)=1; choose e=7
5. Determine d: d*e=1 mod 160 and d < 160 Value d=23 since 23*7=161= 10x160+1

1. Publish public key PU={7,187}
2. Keep secret private key PR={23,187}

Four possible approaches to attacking the RSA algorithm are :

- Brute force: This involves trying all possible private keys.

- Mathematical attacks: There are several approaches, all equivalent in effort to factoring the product of two primes.
- Timing attacks: These depend on the running time of the decryption algorithm.
- Chosen ciphertext attacks: This type of attack exploits properties of the RSA algorithm.