UCS2602 SOFTWARE SYSTEM SECURITY

Public Key Cryptography - RSA

Unit-II

Session Objectives

- Study the working of public-key cryptographic algorithm RSA.

Session Outcomes

At the end of this session, participants will be able to:

- Discuss the working of RSA.

Agenda

1. RSA
2. RSA Example - En/Decryption
3. Summary

Presentation Outline

RSA

- By Rivest, Shamir & Adleman of MIT in 1977
- Best known & widely used public-key scheme
- Based on exponentiation in a finite (Galois) field over integers modulo a prime
- Uses large integers (e.g., 1024 bits)
- Security due to cost of factoring large numbers

RSA Encryption - Decryption

- To encrypt a message M the sender:
  - Obtains public key of recipient $PU = \{e, n\}$
  - Computes: $C = M^e \mod n$, where $0 \leq M \leq n$
- To decrypt the ciphertext C the owner:
  - Uses their private key $PR = \{d, n\}$
  - Computes: $M = C^d \mod n$
- Note that the message M must be smaller than the modulus n (block if needed)

RSA Key Setup

- Each user generates a public/private key pair by:
  - Selecting two large primes at random: p, q
  - Computing their system modulus $n = p \cdot q$
  - Note: $\phi(n) = (p-1)(q-1)$
  - Selecting at random the encryption key e where $1 < e < \phi(n)$, $\gcd(e, \phi(n)) = 1$
  - Solve following equation to find decryption key d: $e \cdot d = 1 \mod \phi(n)$ and $0 \leq d \leq n$
  - Publish their public encryption key: $PU = \{e, n\}$
  - Keep secret private decryption key: $PR = \{d, n\}$

Why RSA Works

- Because of Euler's Theorem:

$$a^{\phi(n)} \mod n = 1 \text{ where } \gcd(a, n) = 1$$

- In RSA, we have:

$$n = p \cdot q$$

$$\phi(n) = (p - 1)(q - 1)$$

- Carefully chose e & d to be inverses mod $\phi(n)$
- Hence $e \cdot d = 1 + k \cdot \phi(n)$ for some k
- Therefore:

$$C^d = M^{e \cdot d} = M^{1+k \cdot \phi(n)} = M \cdot (M^{\phi(n)})^k$$

$$= M \cdot 1^k = M \mod n$$

RSA Example - Key Setup

1. Select primes: $p = 17$ & $q = 11$
2. Calculate $n = p \cdot q = 17 \times 11 = 187$
3. Calculate $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$
4. Select e: $\gcd(e, 160) = 1$; choose $e = 7$
5. Determine d: $d \cdot e = 1 \mod 160$ and $d \leq 160$. Value is $d = 23$ since $23 \times 7 = 161 = 10 \times 160 + 1$
6. Publish public key $PU = \{7, 187\}$
7. Keep secret private key $PR = \{23, 187\}$

RSA Example - En/Decryption

- Sample RSA encryption/decryption:
- Given message $M = 88$ (note: $88 < 187$)
- Encryption:

$$C = 88^7 \mod 187 = 11$$

- Decryption:

$$M = 11^{23} \mod 187 = 88$$

RSA Security

- Possible approaches to attacking RSA:
  - Brute force key search - infeasible given size of numbers
  - Mathematical attacks - based on difficulty of computing $\phi(n)$, by factoring modulus n
  - Timing attacks - on running of decryption
  - Chosen ciphertext attacks - given properties of RSA

Summary

Discussed:

- RSA algorithm
- RSA implementation and security