Public Key Cryptography - RSA

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

1 RSA

2 RSA Example - En/Decryption

3 Summary

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 (eg. 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: $\mathbf{C} = M^e$ **mod n**, where $0 \leq M \leq n$
- To decrypt the ciphertext **C** the owner:
  - uses their private key **PR=**$\{$**d,n**$\}$
  - computes: $\mathbf{M} = C^d$ **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.q**
  note ϕ**(n)=(p-1)(q-1)**
- Selecting at random the encryption key e where
  $1 < e < ø(n)$, **gcd(e,**ϕ**(n))=1**
- Solve following equation to find decryption key **d**
  e.d=1 mod ϕ **(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 where gcd(a,n)=1**
- in RSA have:
  n=p.q
  $\boldsymbol{\phi}$**(n)=(p-1)(q-1)**
  carefully chose e & d to be inverses mod ø(n)
- hence **e.d=1+k.**$\boldsymbol{\phi}$**(n)** for some k
  hence :
  $C^d = M^{e.d} = M^{1+k.\phi(n}) = M^1.(M^{\phi(n)})^k$
  $= M^1.(1)^k = M^1 =$ M mod n

RSA Example - Key Setup

1. Select primes: p=17 & q=11
2. Calculate **n = pq** =17 x 11=187
3. Calculate ϕ(n)=(p–1)(q-1)=16x10=160
4. Select e: **gcd(e,160)=1**; choose e=7
5. Determine d: **de=1 mod 160** and d $\leq$ 160 Value is d=23 since 23x7=161= 10x160+1
6. Publish public key PU={7,187}
7. Keep secret private key PR={23,187}

Presentation Outline

1 RSA

2 RSA Example - En/Decryption

3 Summary

RSA Example - En/Decryption

- sample RSA encryption/decryption is:
- given message M = 88 (note. 88¡187)
- encryption:
  $C = 88^7 \bmod 187 = 11$
- decryption:
  $M = 11^{23} \bmod 187 = 88$

RSA Security

possible approaches to attacking RSA are:

- brute force key search - infeasible given size of numbers
- mathematical attacks - based on difficulty of computing ϕ(n), by factoring modulus n
- timing attacks - on running of decryption
- chosen ciphertext attacks - given properties of RSA

Presentation Outline

1 RSA

2 RSA Example - En/Decryption

3 Summary

Summary

Discussed:

- RSA algorithm
- RSA implementation and security