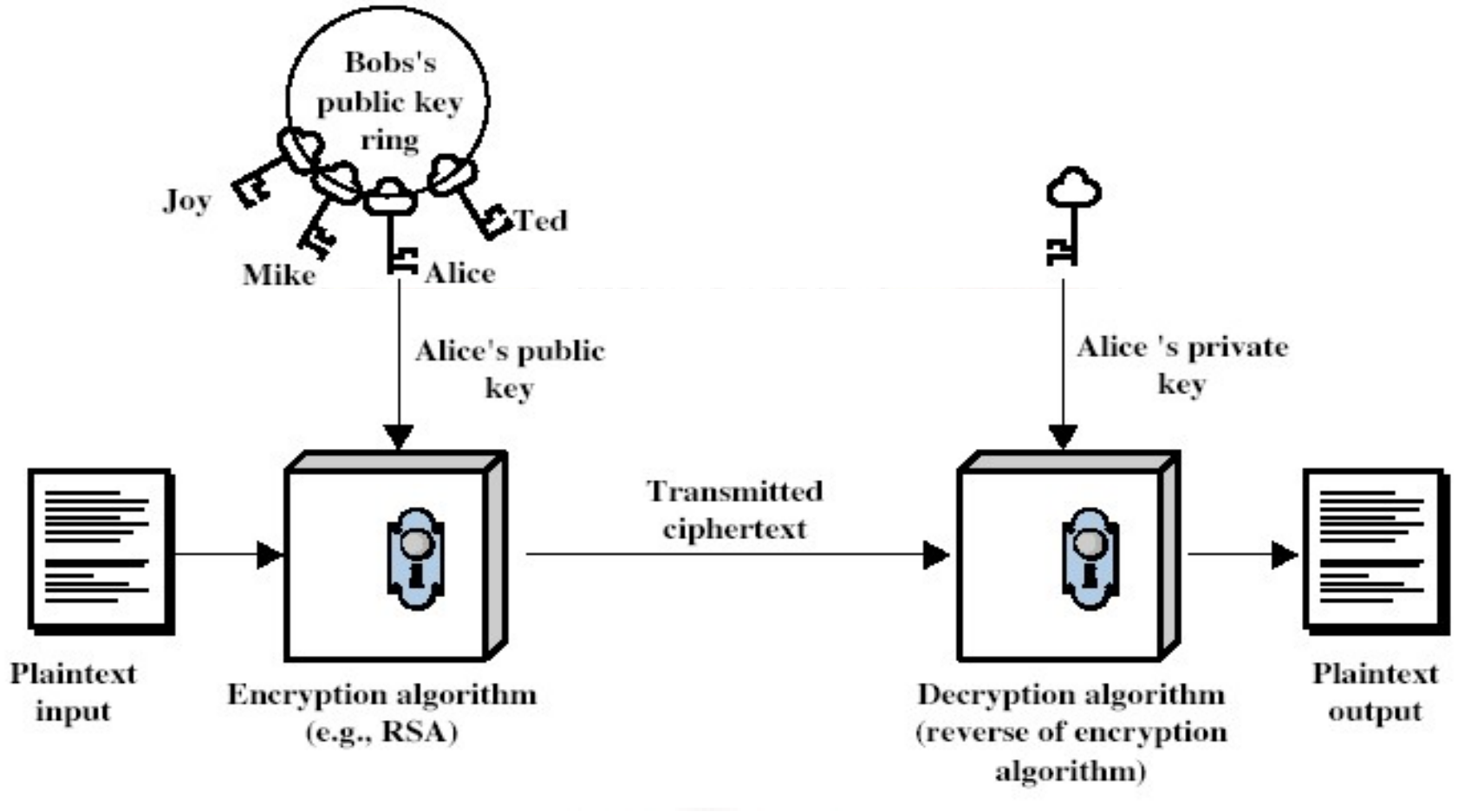
RSA Algorithm

Public-Key Cryptography

- **public-key/two-key/asymmetric** cryptography involves the use of **two** keys:
  - a **public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**
  - a **private-key**, known only to the recipient, used to **decrypt messages**, and **sign** (create) **signatures**

- is **asymmetric** because
  - those who encrypt messages or verify signatures **cannot** decrypt messages or create signatures

Public-Key Cryptography



RSA Algorithm

- Rivest, Shamir & Adleman who first publicly described it in 1977.
- It is an algorithm for public-key cryptography.
- RSA algorithm involves three steps
  - Key Generation
  - Encryption
  - Decryption

Key Generation

1. Select p, q where p & q both prime, $p \neq q$
2. Calculate $n = p \times q$
3. Calculate $\emptyset(n) = (p-1) \times (q-1)$
4. Select integer e such that $\gcd(\emptyset(n),e)=1$; $1<e<\emptyset(n)$
5. Calculate d, $d \equiv e^{-1} \pmod{\emptyset(n)}$ or $d.e \equiv 1 \pmod{\emptyset(n)}$

Public Key : PU = { e, n }

Private Key : PR = { d, n }

Encryption

Plaintext : $M < n$

Ciphertext : $C = M^e \bmod n$

Decryption

Ciphertext : C

Plaintext : $M = C^d \bmod n$

RSA Example

1. Select primes: $p=17$ & $q=11$
2. Compute $n = pq = 17 \times 11 = 187$
3. Compute $\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$
4. Select e : $\gcd(e,160)=1$; choose $e=7$
5. Determine d: $de=1 \bmod 160$ and $d < 160$
   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 cont.

RSA encryption/decryption

- message $M = 88$ $(88<187)$
- encryption:

  $C = 88^{7} \bmod 187 = 11$
- decryption:

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

References

- William Stallings, *Cryptography and Network Security*, 1999.


Thanks
S.S JAIN SUBODH P.G. COLLEGE