Public-Key Cryptography and RSA

An approach of asymmetric cipher

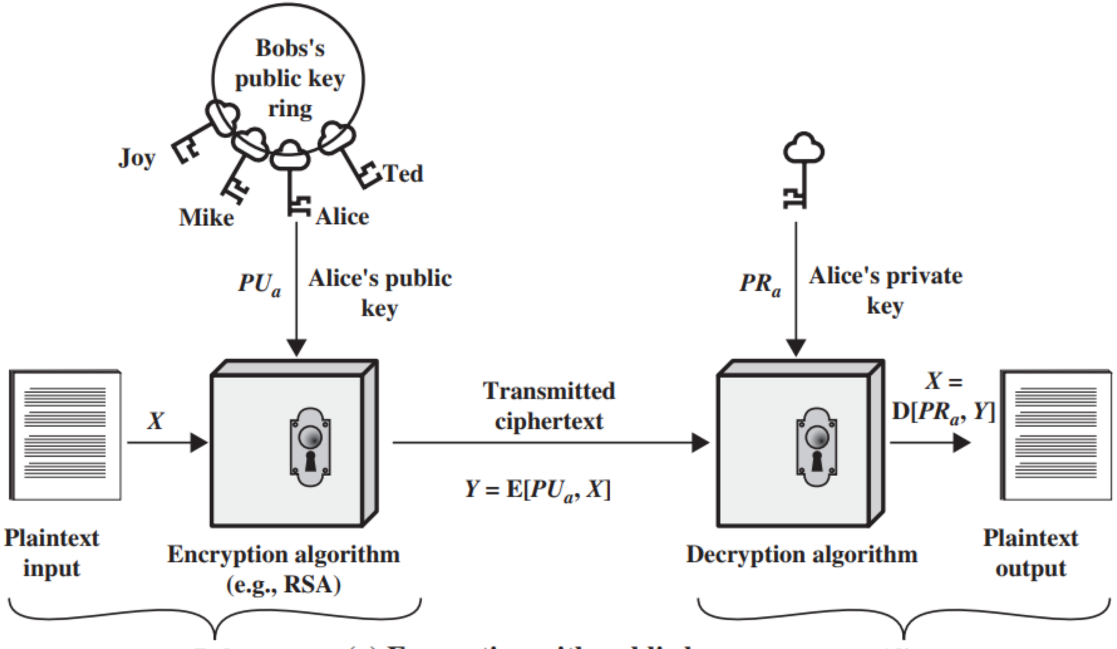
Public-Key Cryptography

- Also known as Asymmetric Cryptography.
- Two related keys, a public key and a private key, that are used to perform encryption-decryption:
  - Public Key: shared openly; used for encryption.
  - Private Key: kept secret; used for decryption.

A public-key encryption

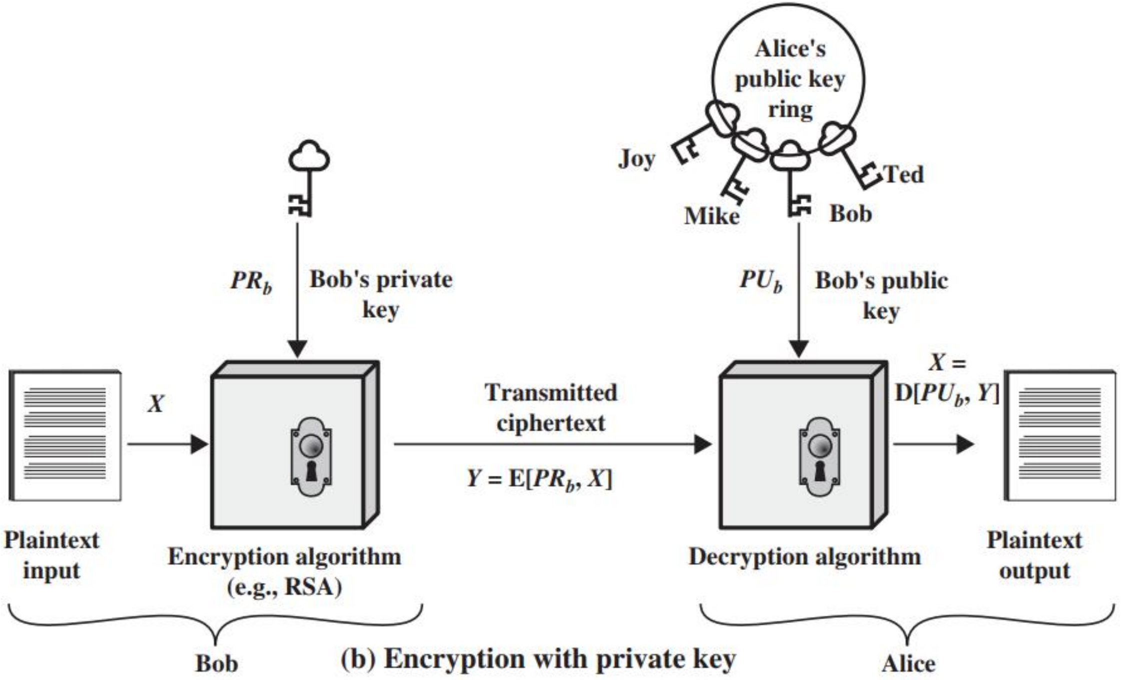
- Asymmetric algorithms rely on one key for encryption and a different but related key for decryption.
- Either of the two related keys can be used for encryption, with the other used for decryption.

public-key encryption with public key



(a) Encryption with public key

public-key encryption with private key



(b) Encryption with private key

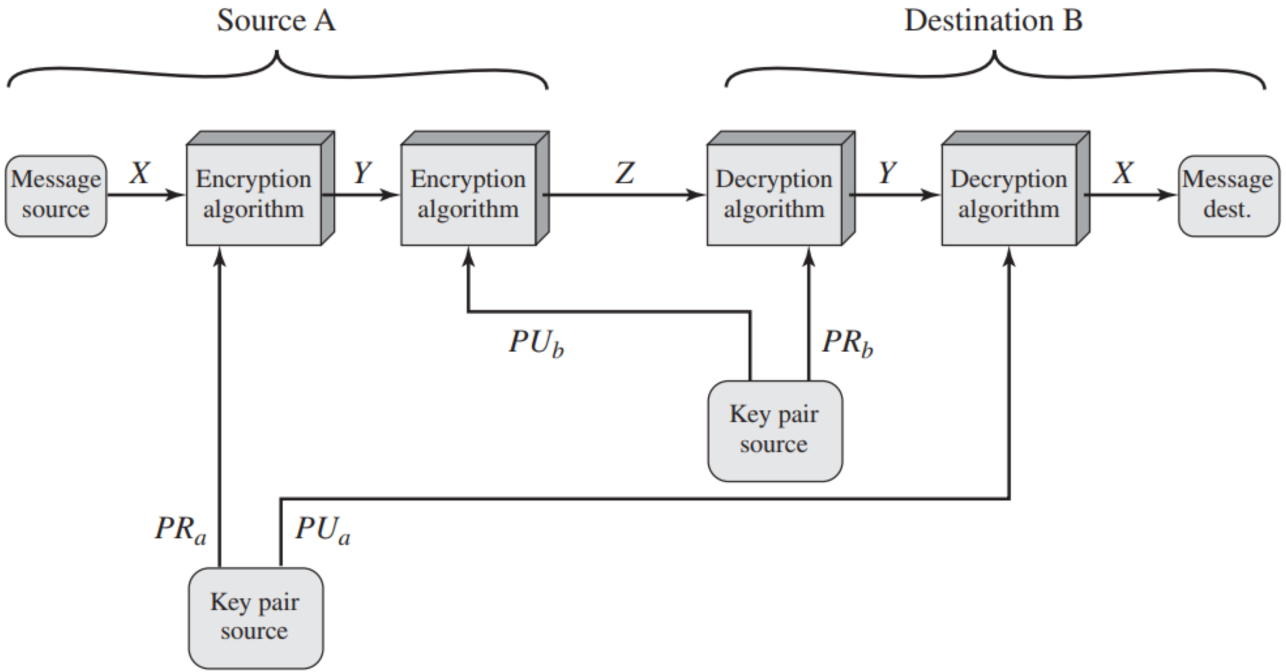
The essential steps of public-key encryption

Each user generates a pair of keys to be used for the encryption and decryption of messages.

Each user places one of the two keys in a public register or other accessible file.

This is the public key. The companion key is kept private. Each user maintains a collection of public keys obtained from others.

Public-Key Cryptosystem: Authentication and Secrecy



RSA Algorithm

- Developed by Rivest, Shamir, and Adleman in 1977.
- Based on the mathematical difficulty of factoring large prime numbers.
- Most widely used public-key algorithm.
- RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n

RSA Key Generation Steps

- Choose two large prime numbers, p and q.
- Compute $n = p \times q$ (modulus).
- Compute $\varphi(n) = (p - 1)(q - 1)$ (Euler's totient).
- Choose an encryption key *e*, such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.
- Compute the decryption key d, such that $d \times e \equiv 1 \pmod{\varphi(n)}$.
- The public key = (e, n); the private key = (d, n).

5 11

7

Example

1. Select two prime numbers, $p = 17$ and $q = 11$.
2. Calculate $n = pq = 17 \times 11 = 187$.
3. Calculate $\phi(n) = (p - 1)(q - 1) = 16 \times 10 = 160$. 40
4. Select e such that e is relatively prime to $\phi(n) = 160$ and less than $\phi(n)$; we choose $e = 7$.
5. Determine d such that $de \equiv 1 \pmod{160}$ and $d < 160$. The correct value is $d = 23$, because $23 \times 7 = 161 = (1 \times 160) + 1$;

RSA Encryption Process

- To encrypt a message M:
- Convert the message into a numerical value m.
- Compute $c = m^e \bmod n$.
- The result c is the cipher text.

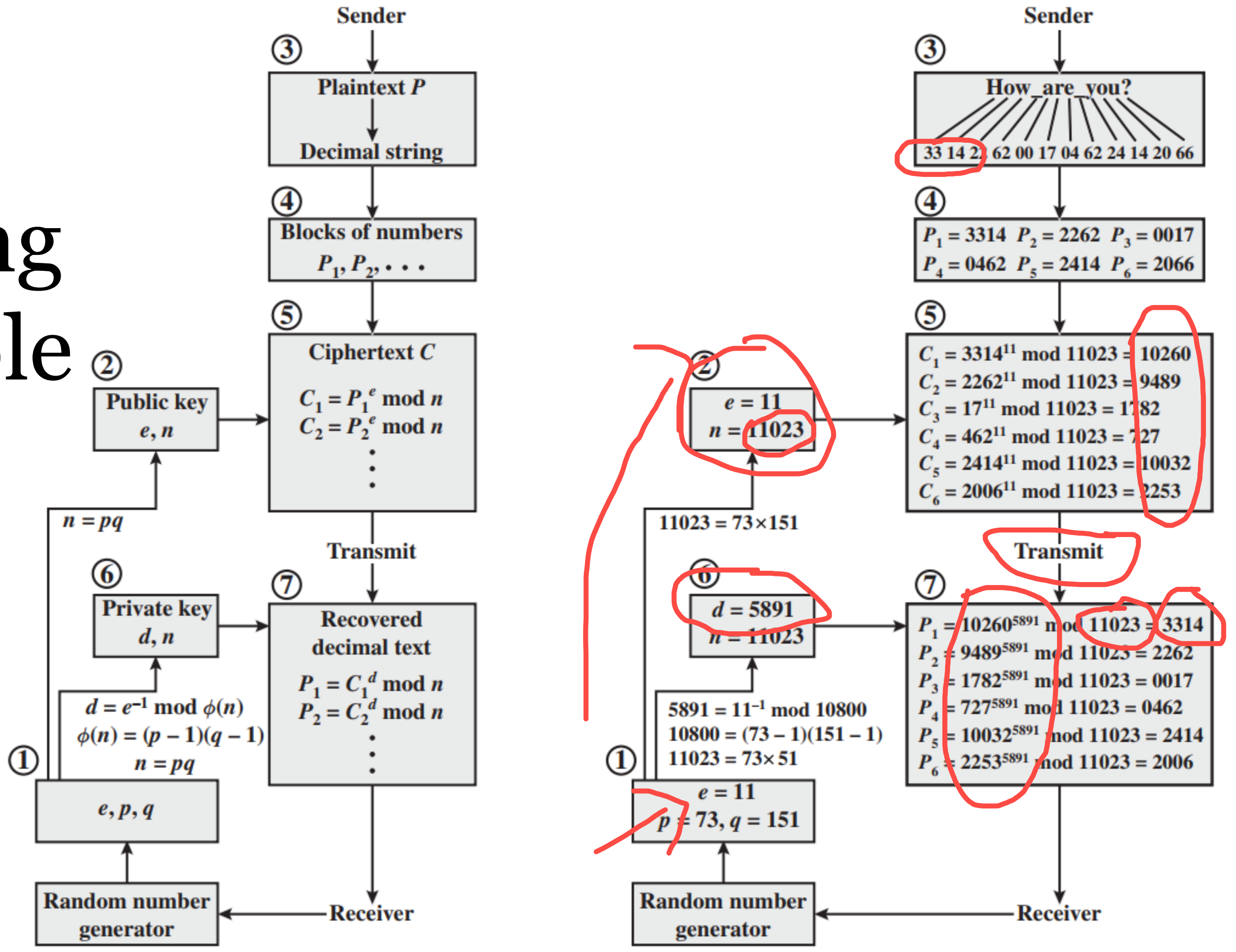
RSA Decryption Process

- To decrypt ciphertext c:
- Compute $m = c^d \mod n$.
- Convert the numeric message m back to text.

RSA Example (Small Numbers)

- Choose primes: **$p = 3$**, **$q = 11$**
- Compute **$n = 3 \times 11 = 33$**
- Compute **$\varphi(n) = (3-1)(11-1) = 20$**
- Choose **$e = 3$** (since $\gcd(3, 20) = 1$)
- Compute **$d = 7$** (since $3 \times 7 \equiv 1 \bmod 20$)
- Public key = **(3, 33)**, Private key = **(7, 33)**
- **Encryption:**
  Message $m = 4 \rightarrow c = 4^3 \bmod 33 = 64 \bmod 33 = 31$
- **Decryption:**
  $\rightarrow m = 31^7 \bmod 33 = 4$ (original message restored)

RSA Processing of Multiple Blocks



Strengths and Weaknesses of RSA

- **Strengths:**
  - Proven mathematical foundation.
  - Supports both encryption and authentication.
  - Widely trusted and implemented.
- **Weaknesses:**
  - Slower than symmetric ciphers.
  - Vulnerable if key sizes are too small (< 2048 bits).
  - Quantum computing poses future risks.

Thank You