Network Security

Chapter 3

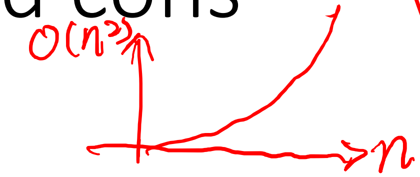
Public-Key Cryptography and Message Authentication

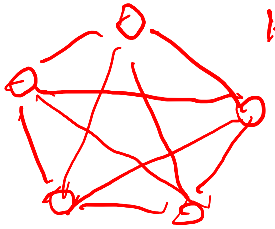
Public-Key Cryptography

Conventional cryptography

- traditional **private/secret/single-key** cryptography uses **one** key
- shared by both sender and receiver
- if this key is disclosed, communications are compromised
- also is **symmetric**, parties are equal

Pros and cons





How many keys? $\frac{n \cdot (n-1)}{2} \approx O(n^2)$

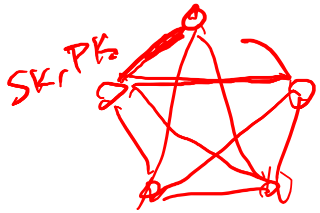
64 bits = 215 bits
AES RSA

- Pros:
  - Encryption is fast for large amounts of data
  - Provide the same level of security with a shorter encryption key
  - By now, it's unbreakable to quantum computing

Cyphertext:

- Cons
  - Key distribution assumes a secure channel
  - Does not protect sender from receiver forging a message & claiming it's sent by sender
  - $\rightarrow n\uparrow$ It does not scale well for large networks. It requires a separate key for each pair of communicating parties, which can result in a large number of keys to manage and protect.

Public-Key Cryptography



How many keys?

$n \cdot (1SK + 1PK)$

$= n \cdot 2$

$\approx O(n)$

- In public-key schemes, each person has two keys
    - **Public key**: Known to everybody
    - **Private key**: Only known by that person
    - Keys come in pairs: every public key corresponds to one private key
- Uses number theory

  NP RSA DH
    - Examples: Modular arithmetic, factoring, discrete logarithm problem, Elliptic logs over Elliptic Curves
    - Contrast with symmetric-key cryptography (uses XORs and bit-shifts)
- Messages are numbers
    - Contrast with symmetric-key cryptography (messages are bit strings)

Public-key Cryptography

- **Benefit:** No longer need to assume that Alice and Bob already share a secret
- **Drawback:** Much slower than symmetric-key cryptography
  - Number theory calculations are much slower than XORs and bit-shifts

Reading materials

- Encryption: Strengths and Weaknesses of Public-key Cryptography
- Public-key cryptography is a public invention due to Whitfield Diffie & Martin Hellman at Stanford Uni in 1976 History

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
  - Not the same key
  - those who encrypt messages or verify signatures **cannot** decrypt messages or create signatures

Public-Key Encryption

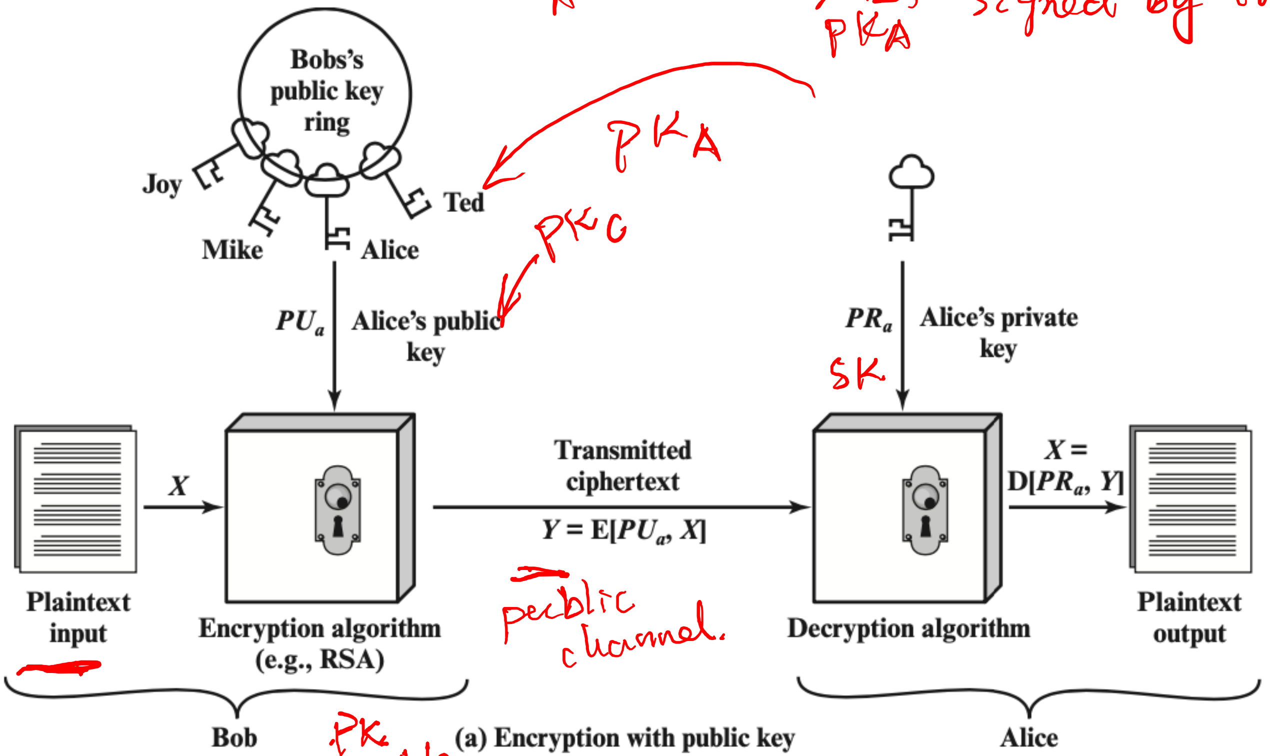
- Everybody can encrypt with the public key
- Only the recipient can decrypt with the private key

PK
SK,
~~SK~~
eavesdropper
Attacker
PK

Public-Key Cryptography - Encryption

Attacker

PKA certificate Signed by third party's SK



(a) Encryption with public key

Encryption steps

- step1: generate a pair of keys
- step2: keep the private key / secret key (SK) and distribute the public key (PK) – place PK in a public register or other accessible file

~/.ssh/ ~~authorized~~ authorized_keys

- step3: Bob encrypts the message with Alice’s PK
- step4: upon receiving the ciphertext (CT), Alice decrypt CT with SK

Review & Quiz I

- Chapter 1 & 2
- Friday (Oct. 10, 2025), in class
- Please ensure your participation