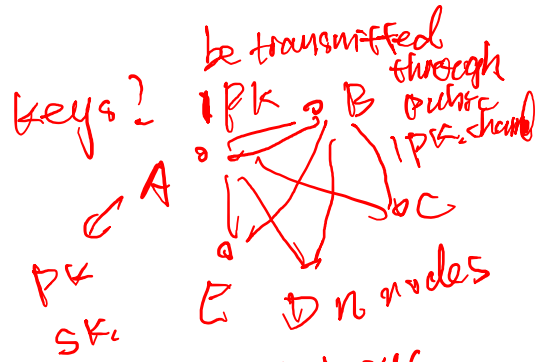
Public-Key Cryptography



- 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
  - 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 → pk can be sent through public channel.
- **Drawback:** Much slower than symmetric-key cryptography
  - Number theory calculations are much slower than XORs and bit-shifts

· speed.

64 bits AES ⇒ 2¹⁵ RSA. ✗ quantum computer

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

Public-key cryptography

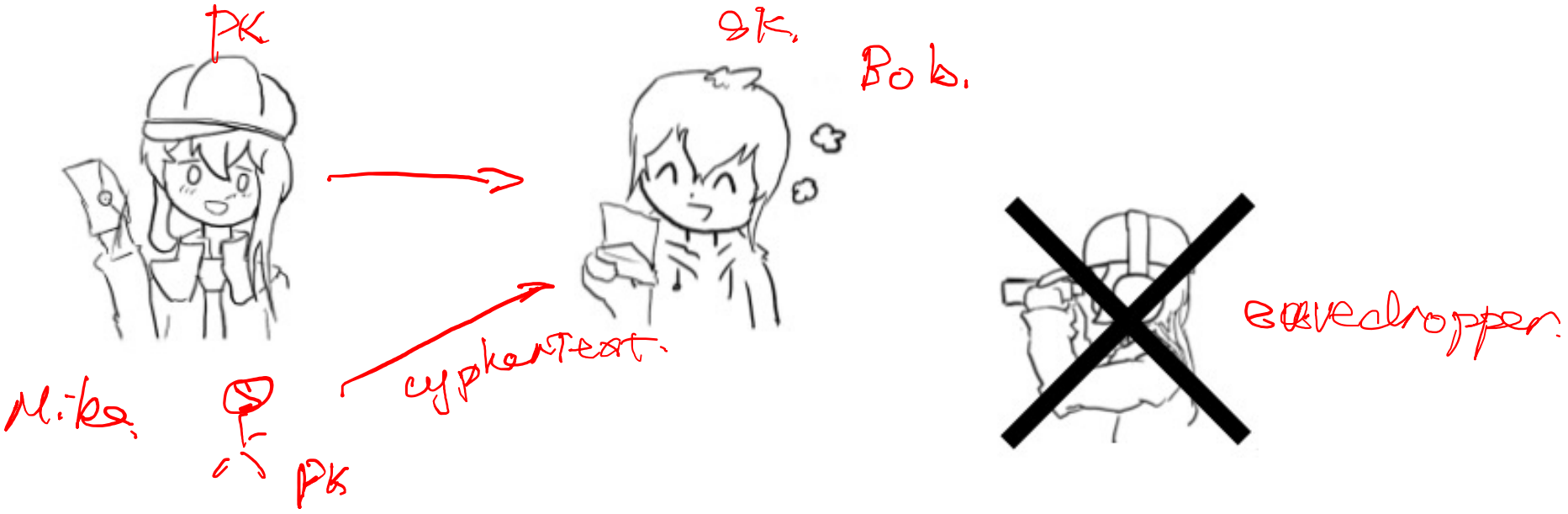
- **public-key/two-key/asymmetric** cryptography involves the use of **two** keys:
  - a **public-key**, which may be known by anybody, and can be used to **encrypt messages**, and **verify signatures**
  - a **private-key**, known only to the recipient, used to **decrypt messages**, and **sign** (create) **signatures**
- is **asymmetric** because
  - Not the same key
  - those who encrypt messages or verify signatures **cannot** decrypt messages or create signatures

PK

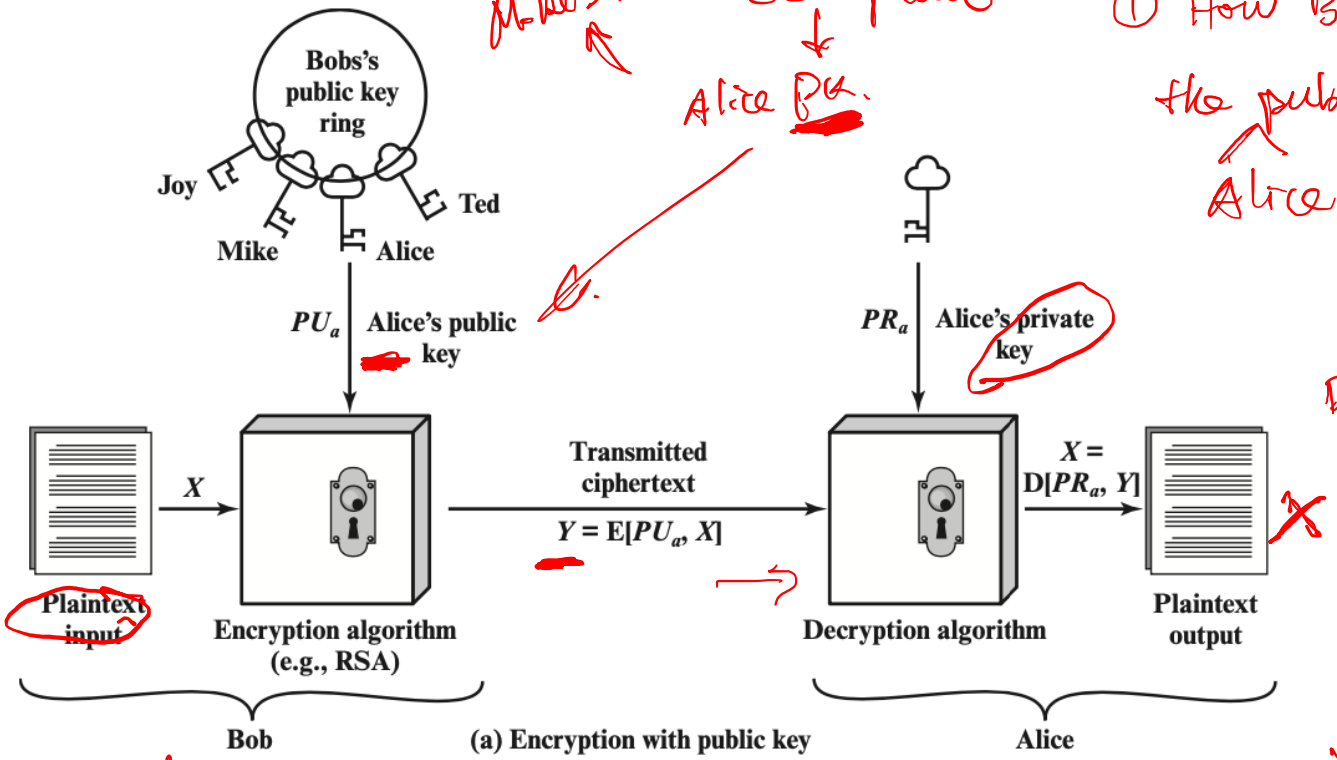
SK ↛ encrypt & verify

Public-Key Encryption

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



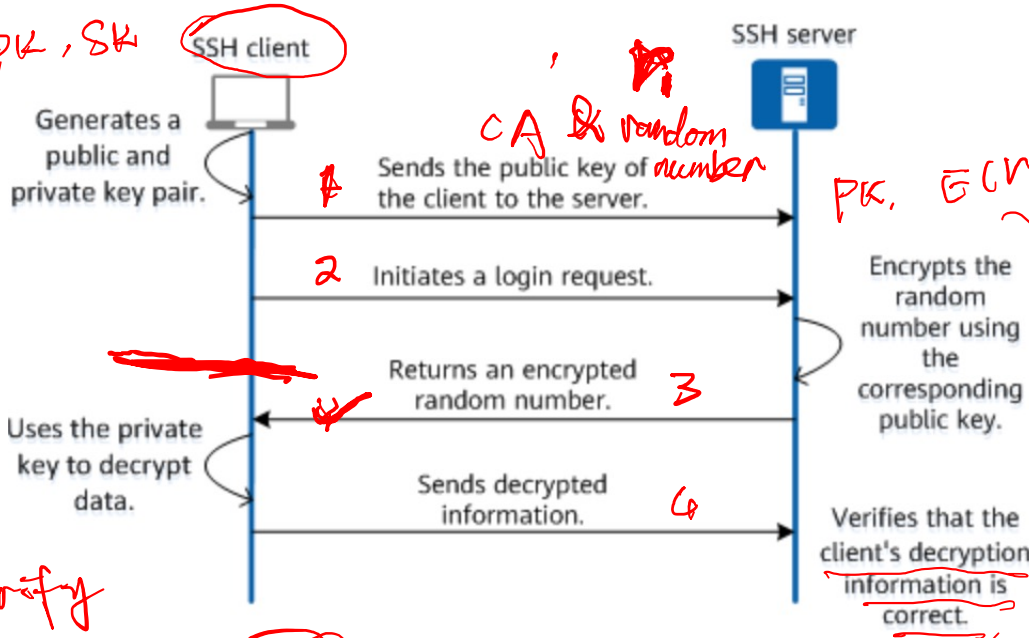
Public-Key Cryptography - Encryption



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

An example of key distribution



SSH key-based client authentication. Source: Peiyue and Yuanyuan 2021.

1.Peiyue, G. and F. Yuanyuan. 2021. "What Is SSH?" Info-Finder, Huawei, July 22. Updated 2021-12-14. Accessed 2023-04-18.