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

R.SA.

- Uses number theory
 - Examples: Modular arithmetic, factoring, discrete logarithm problem, which is a 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 of can be sent through plathic channel.
- Drawback: Merch slower than symmetric-key cryptography
 - Number theory calculations are much slower than XORs and bit-shifts

Speed.

64 bits

RSA.

RSA.

Quantum computer

Reading materials

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

 **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

PKI

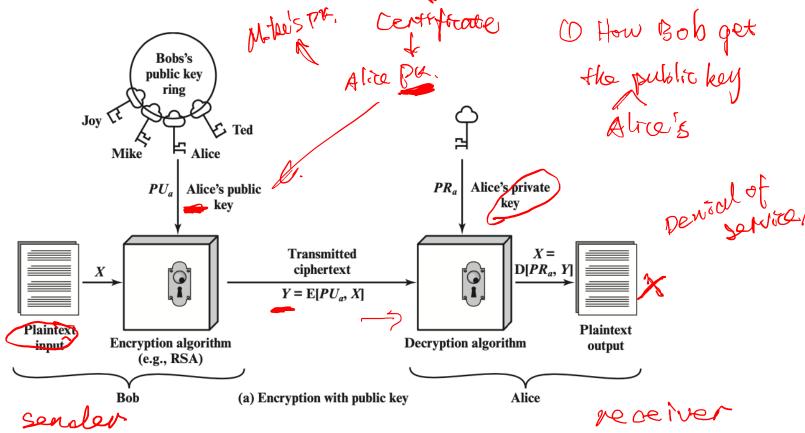
SK As energyt & verify

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

25 SS H. Remote Login
Create password
RSA Rey An example of key distribution Server PK, SK SSH server SSH client ~ 195h /-d-rsa-pub ~ [.shh/id-rsa Generates a public and PK. G(N, PK) Sends the public key of number private key pair. the client to the server. Encrypts the Initiates a login request. random number using Returns an encrypted corresponding random number. public key. Uses the private key to decrypt Sends decrypted data. 4 information. Verifies that the HARPSIN client's decryption information is correct. 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.