CS 725/825 & IT 725

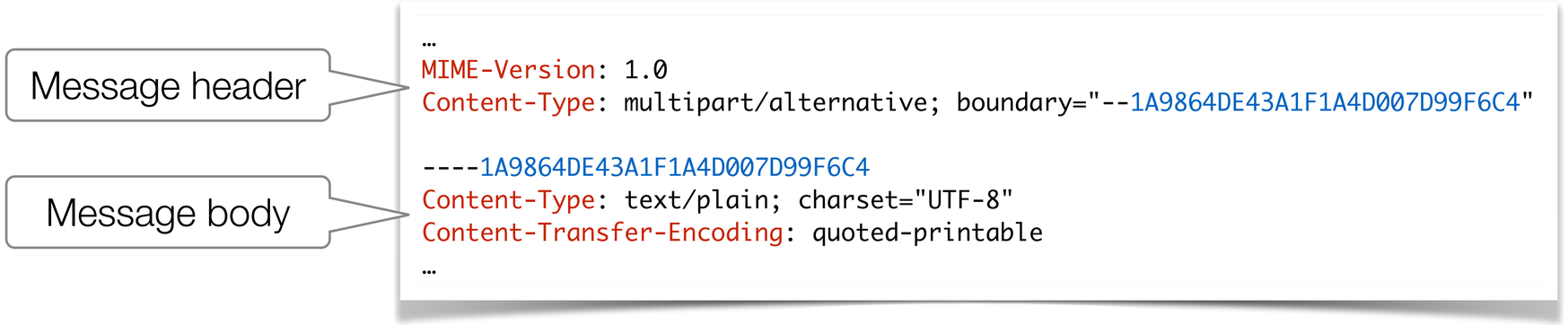
Lecture 13

Network Security

October 18, 2023

MIME

- Problem: SMTP was designed to deliver limited length, English text
- Solution: MIME (Multipurpose Internet Mail Extensions)
  - encode content to look like text
  - mark it with content type so it can be unpacked and rendered on the receiving end
  - package components of the message



Network Security

Security

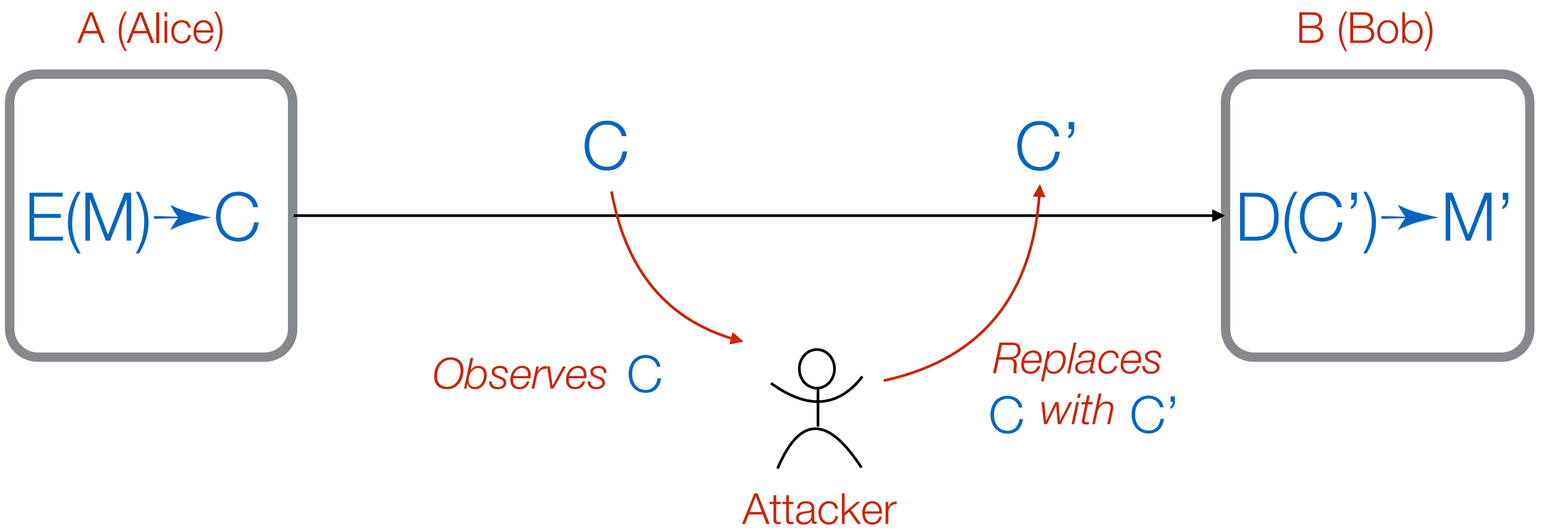
- A broad problem, we will look at securing communication protocols
- Objectives:
  - confidentiality
  - authentication
  - message integrity
  - non-repudiation

    Non-repudiation is the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract...

Encryption

- M - message, C - cyphertext (encrypted text)
- Encryption: E(M)➔C
- Decryption: D(C)➔M

Encryption - Attacks



- Passive attack: message observed
- Active attack: message replaced or modified

Encryption Categories

Secret method: E( ) and D( )

Public method, secret key: E_k( ) and D_k( )

Public method, public and private keys: E_{pubk}( ) and D_{privk}( )

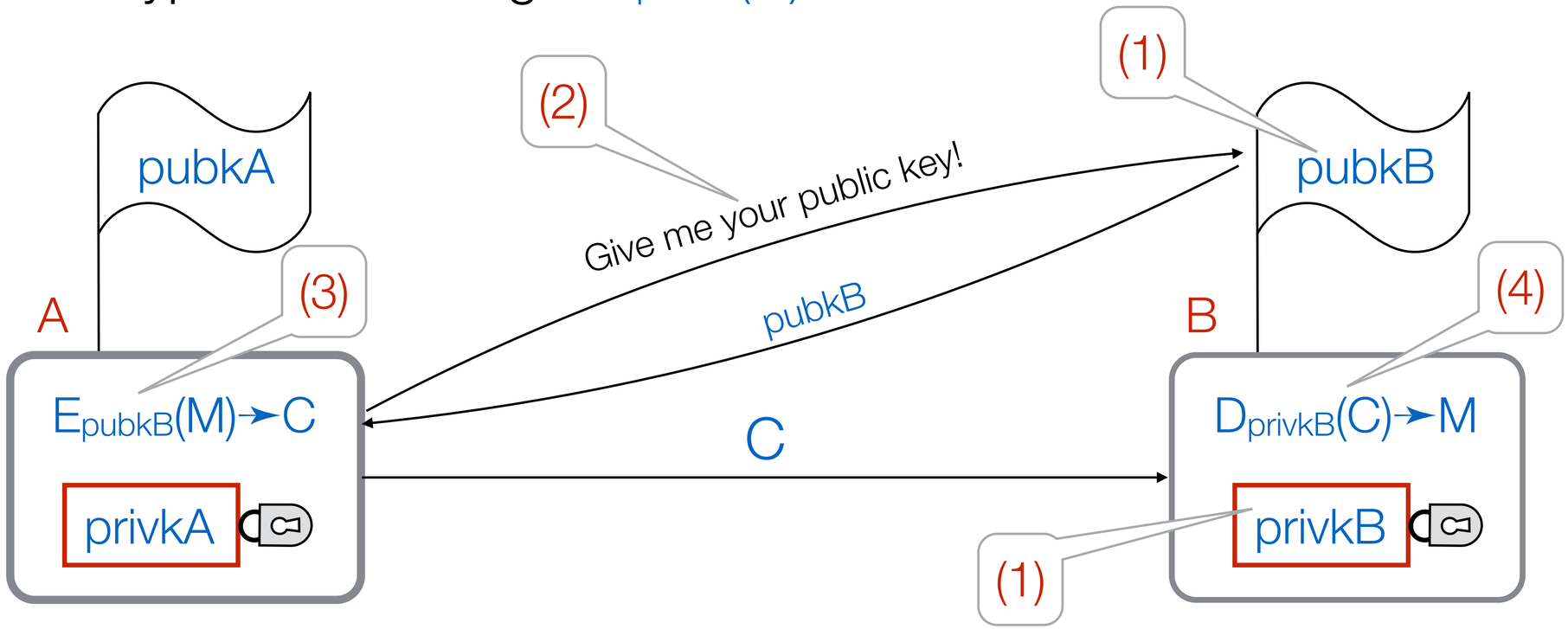
Public Private Key Cryptography

(1) B generates public/private key pair: pubkB and privB

(2) A gets B's public key

(3) A encrypts the message: $E_{pubkB}(M) \rightarrow C$ and sends it to B

(4) B decrypts the message: $D_{privkB}(C) \rightarrow M$



Key Exchange Problem

- Everything hinges on A getting B's public key...
  - once that's done, all is set
- Man-in-the-middle (MITM) attack
- Needed:
  - authentication
  - message integrity