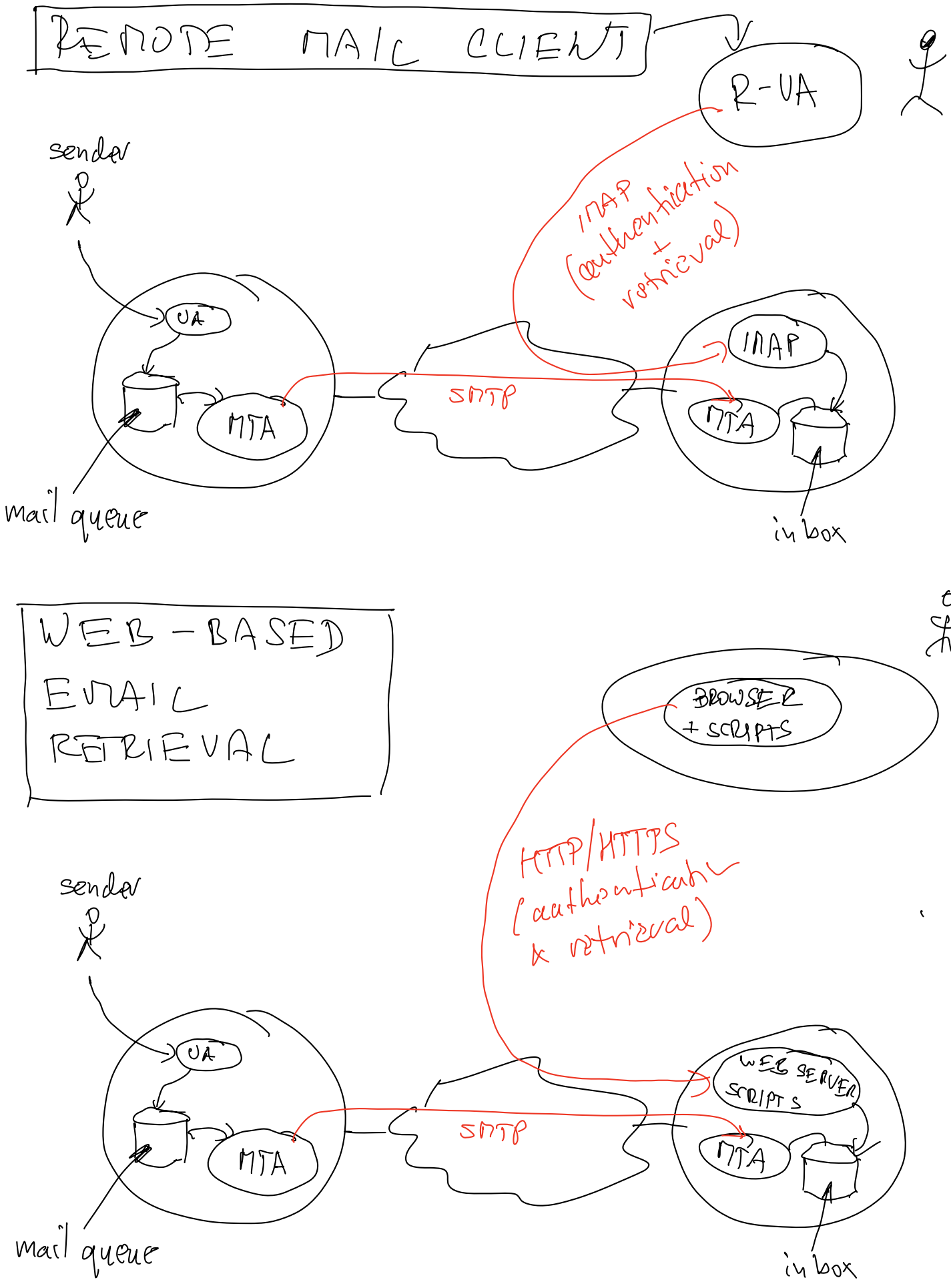
CS 725/825 & IT 725

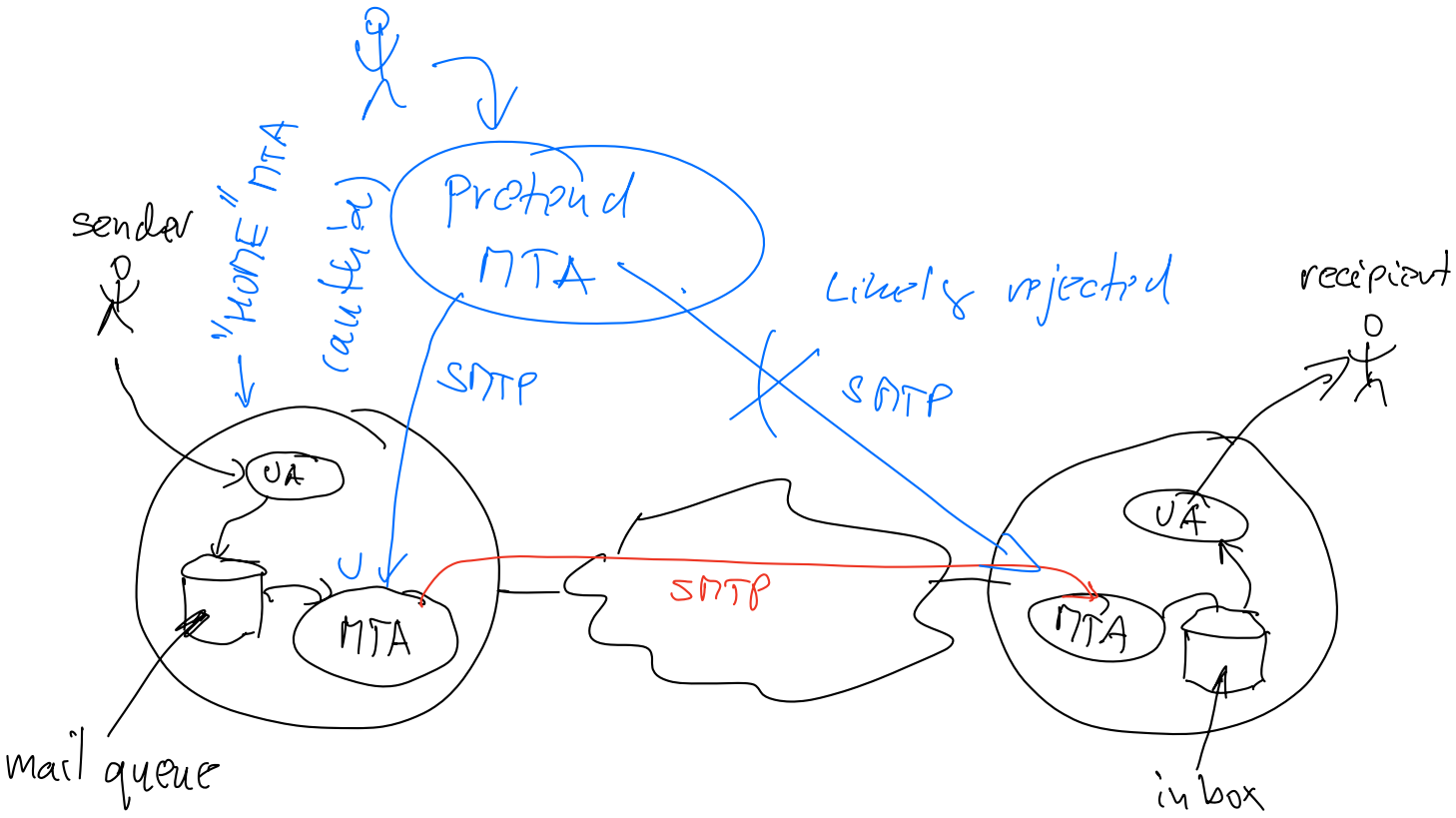
Lecture 10

Application Layer

September 30, 2024


REMOTE MAIL CLIENT
R-UA
sender
IMAP (authentication + retrieval)
UA
MTA
SMTP
IMAP
MTA
mail queue
inbox
WEB-BASED EMAIL RETRIEVAL
BROWSER + SCRIPTS
HTTP/HTTPS (authentication & retrieval)
sender
UA
MTA
SMTP
WEB SERVER SCRIPTS
MTA
mail queue
inbox

REMOTE SENDER



UA to MTA Communication

- UA and MTA on the same host (the old days)
  - UA and MTA communicate using files
  - use of host's authentication methods
- UA and MTA communicate over a network (today)
  - SMTP was not designed for this
  - sending mail: SMPT with authentication
  - retrieving mail: IMAP (includes authentication) or "remote authenticated access via HTTP" (webmail)

MTA to MTA communication

- Simple Mail Transfer Protocol (SMTP)
  - covers single hop
  - no encryption
  - no authentication
  - there was supposed to be a “not so simple” mail transfer protocol
  - some problems were addressed by ESMTP (extended SMTP) and other procedural methods

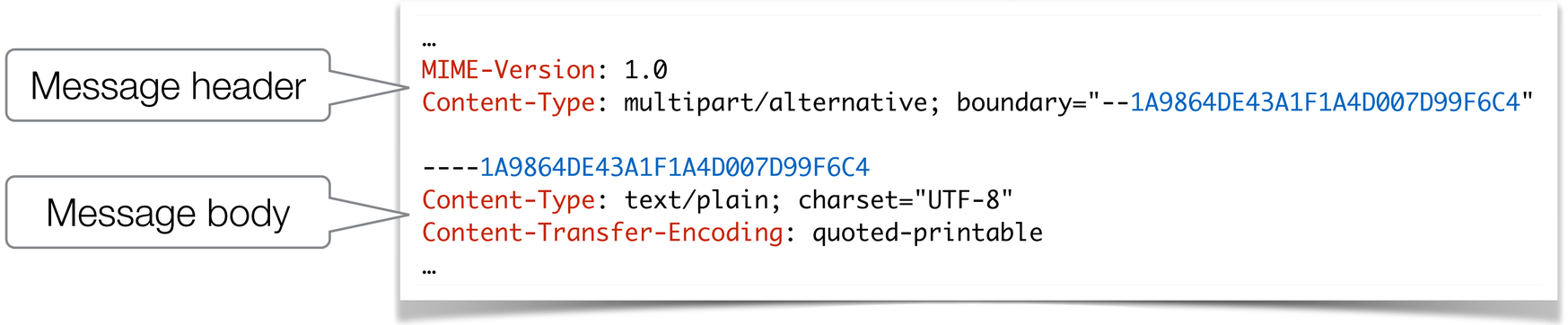
SMTP Server Actions

- SMTP server is deciding whether to accept an email message for delivery
  - Local: recognized user of the organization that runs the server:
    - by IP address
    - authenticated
  - Global: everyone else

To: / From:	Local	Global
Local	Deliver	Deliver
Global	Deliver (with caution)	Deny (unless authenticated)

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

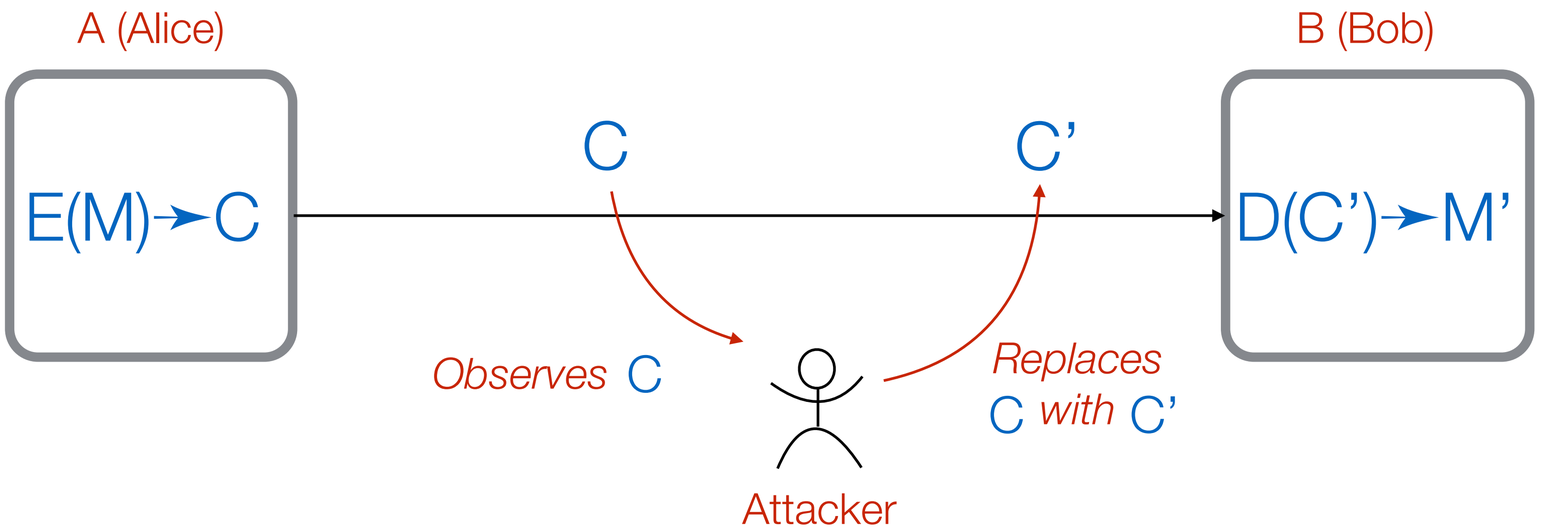
- A broad problem, we will look at securing communication protocols
- Objectives:
  - confidentiality
  - authentication
  - message integrity
  - non-repudiation

    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}( )

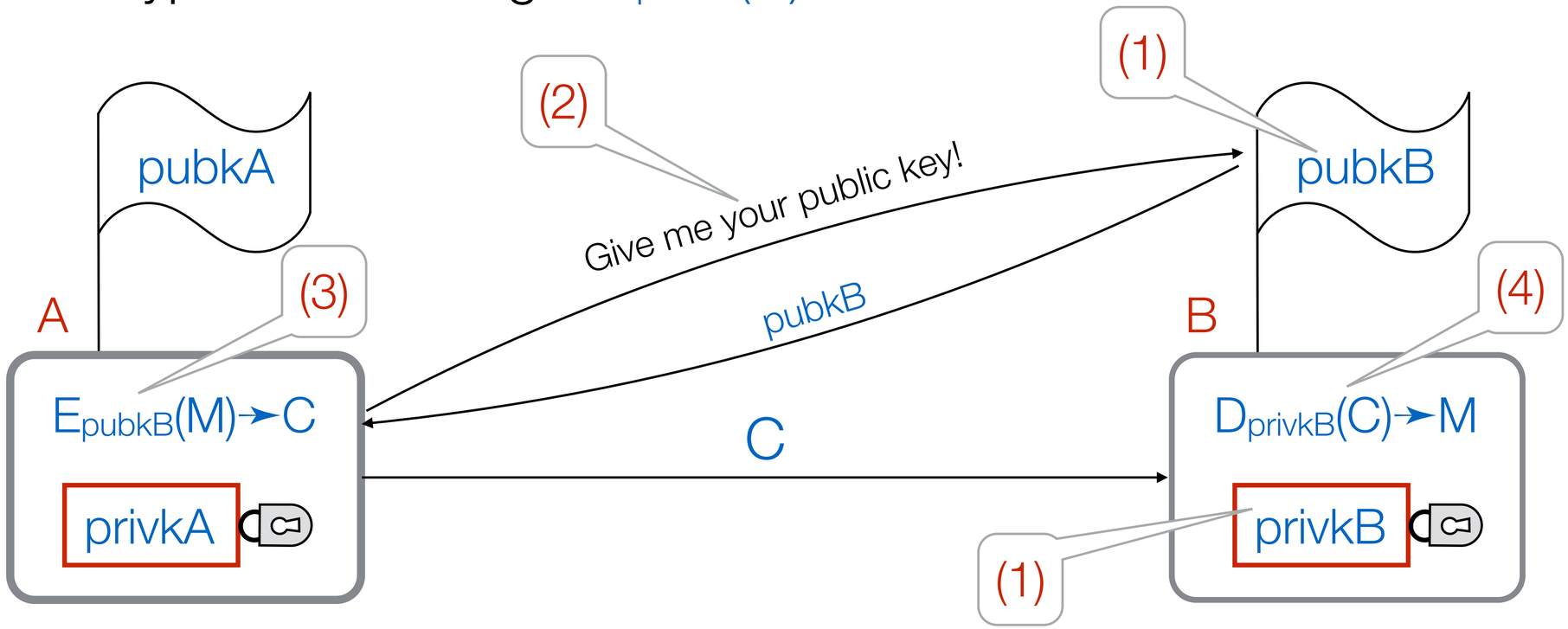
Public Private Key Cryptography

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

(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

Encryption Methods

- Cæsar (substitution) cipher
  - … frequency analysis
- “Unbreakable” cipher: One Time Pad
- DES - Data Encryption Standard
  - 1977, symmetric key, 56-bit key, 64-bit data blocks
- AES - Advanced Encryption Standard
  - 1998, symmetric key, 128,192, and 256-bit keys, 128-bit data blocks