# CS 725/825 & IT 725

# Lecture 11

# **Network Security**

October 1, 2025

# Security

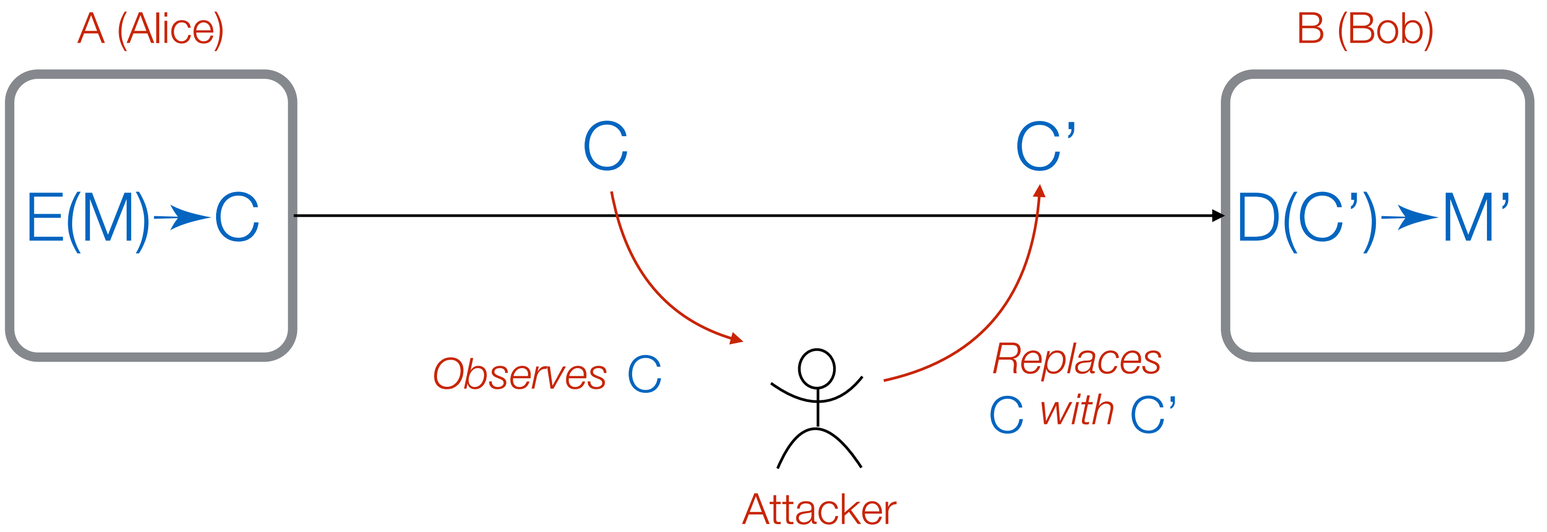
- A broad problem, we will look at securing communication protocols
- Objectives:
  - confidentiality
  - authentication
  - message integrity
  - non-repudiation

    *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 $D_{privk}$( )

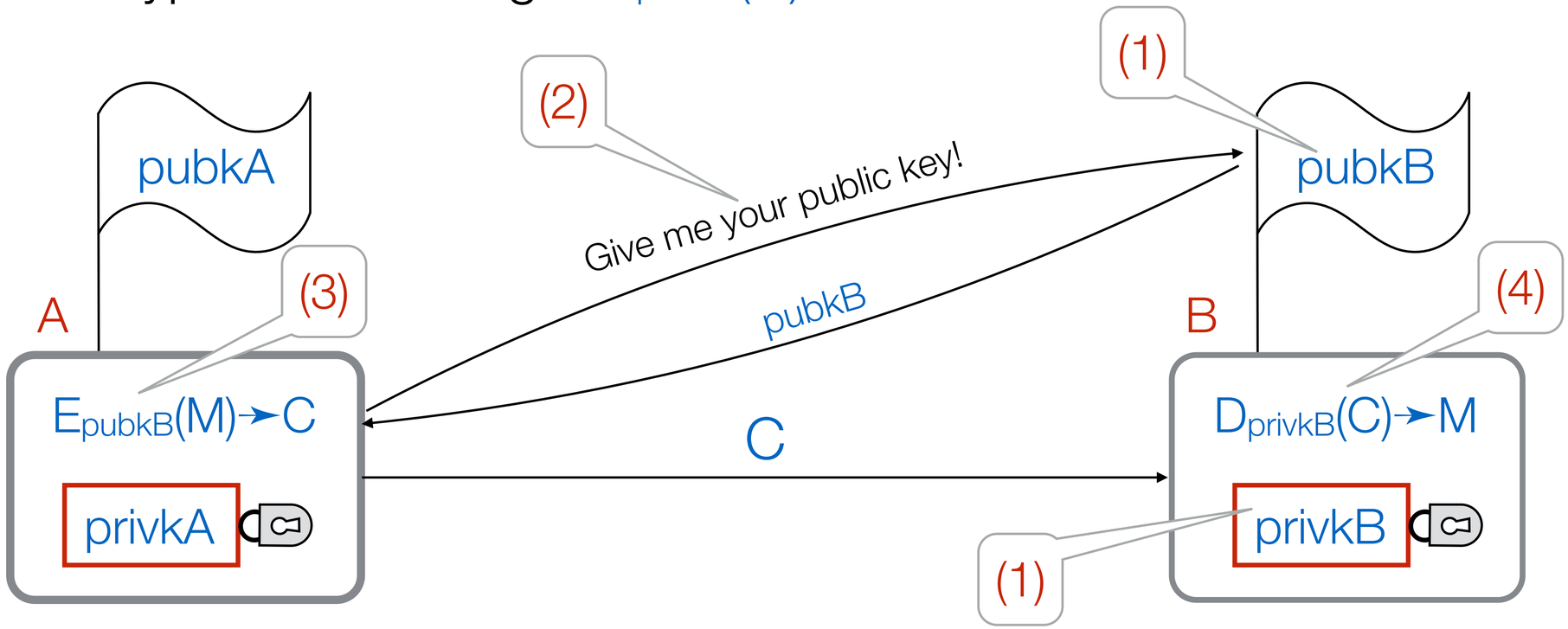
# Public Private Key Cryptography

(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

# 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

# Encryption Methods

- (Diffie-Hellman key exchange)
  - a method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.
- RSA - Rivest, Shamir, and Adleman
  - 1978, public/private key algorithm, 1,024 to 4,096- bit keys (typically)
- Elliptic-curve cryptography (ECC)
  - 2005, allows shorter keys while providing equivalent security