CS 725/825 & IT 725

Lecture 12

Network Security

October 19, 2026

Network Security

Security

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

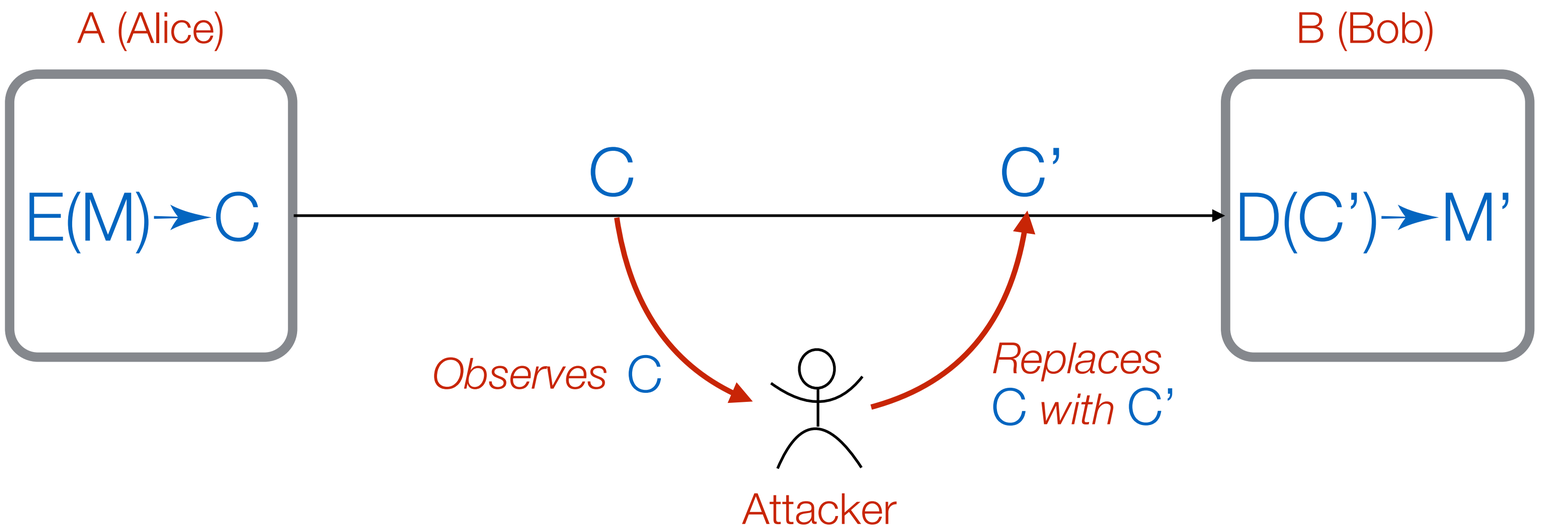
    Non-repudiation is the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract...

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}( )



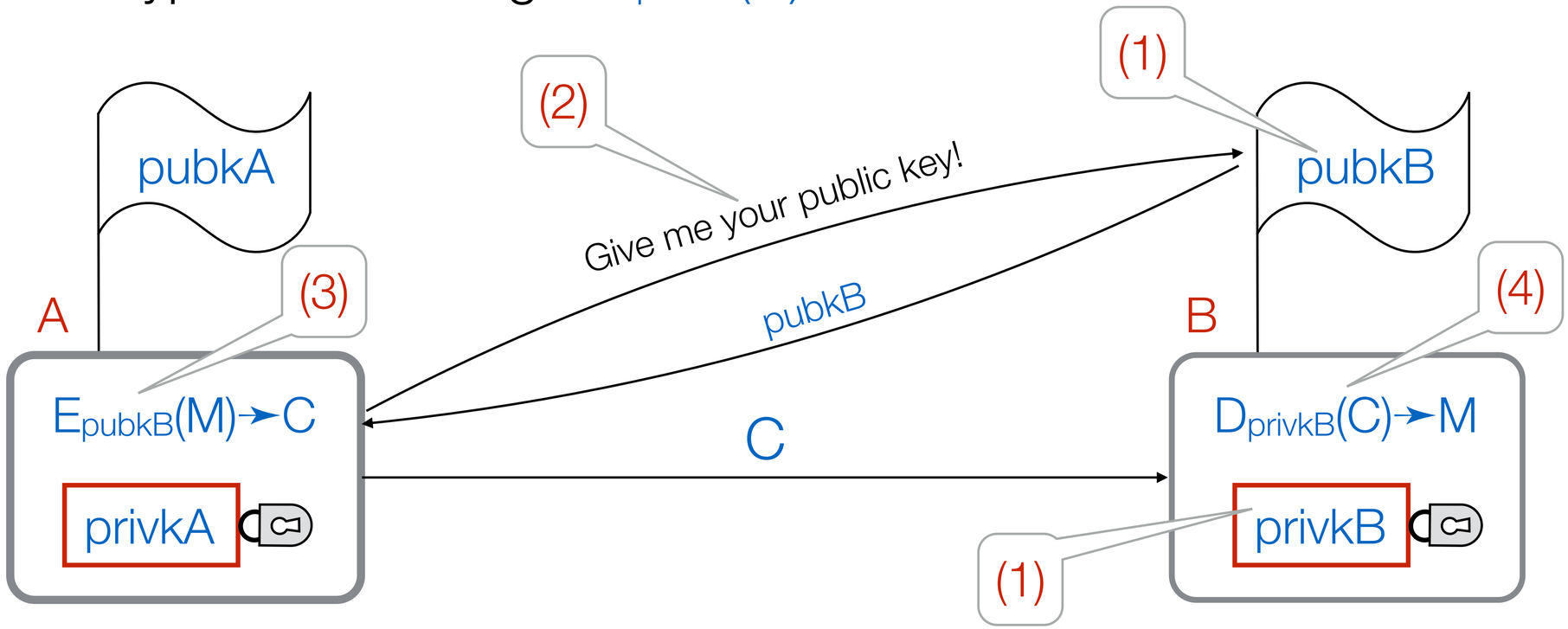
Public Private Key Cryptography

(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

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

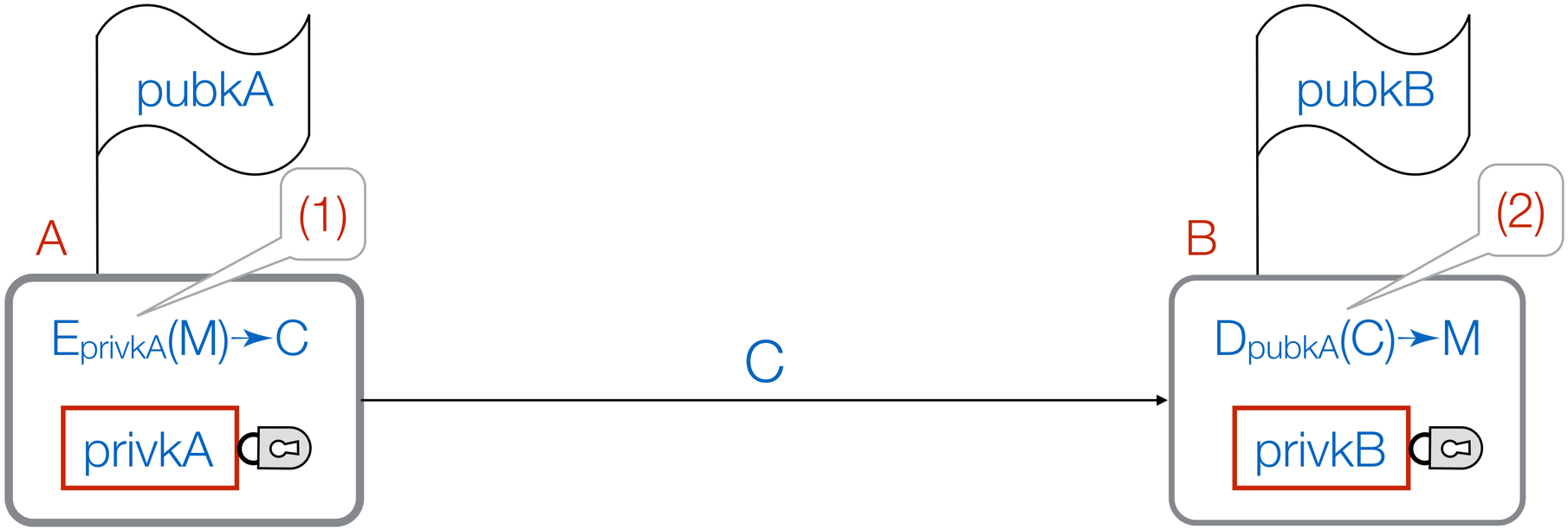
Encryption Methods

- (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

Authentication

- Basic idea:
  - use “flipped” public/private key cryptography
  - only possessor of private key could have encrypted something that decrypts using its public key
- Problem: Replay Attack
  - solution: use of a nonce
- Still unaddressed: We need a trusted way to obtain someone’s public key

Authentication - Basics



(1) A “encrypts” the message: $E_{privkA}(M) \rightarrow C$ and sends it to B

(2) B “decrypts” the message: $D_{pubkA}(C) \rightarrow M$

(3) if M “looks OK”*, its sender is authenticated

* the assumption is that recipient can tell the difference between a valid message and a random string of bits that would be the result of decryption with a wrong key

Message Integrity

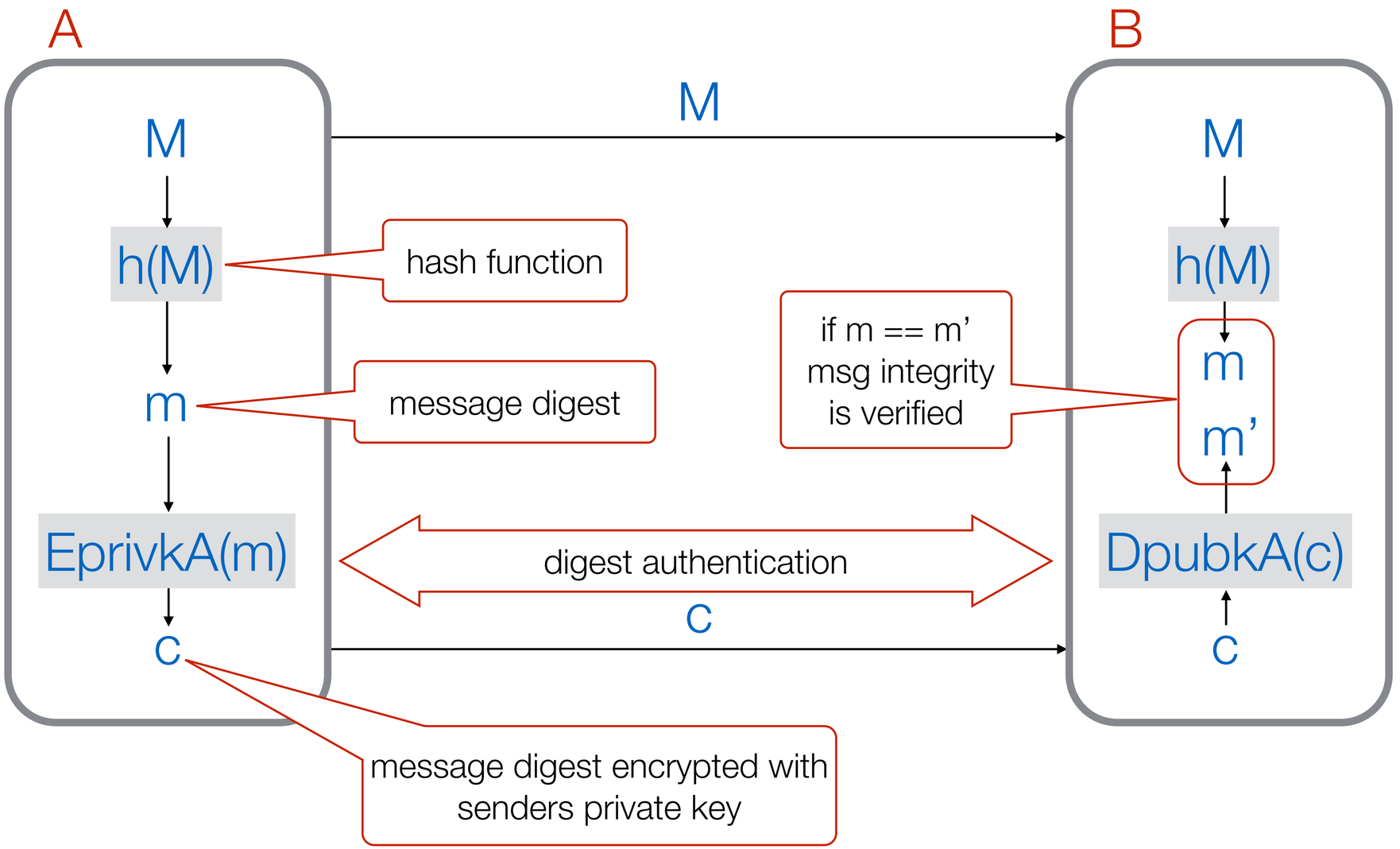
- Basic idea:
  - use public/private key cryptography
  - send a hash of a message (aka message digest) …
  - … encrypted using sender's private key
  - if hash of the received message agrees with decrypted received hash, it is assumed that the message was not altered in transit
- Problems:
  - need a cryptographic hash function
  - need a secure method for public key distribution

Cryptographic hash function

$H(M) \rightarrow m$

- Even the smallest change in message M results in a significant "unpredictable" change of the hash value m
- It is infeasible to find two distinct messages, M_1 and M_2, with the same hash value: $H(M_1) = H(M_2)$
- It is infeasible to modify a message M to get M' in a way that the hash value remains the same: $H(M) = H(M')$
- … must be easy to compute
  - M is arbitrarily large, m is small and fixed-size (100's of bits)

Message Integrity



Cryptographic hash functions

- MD5 - Message Digest Algorithm
  - 1992, R. Rivest, digest size 128 bits
- SHA-1 - Secure Hash Algorithm
  - 1995, NSA, digest size 160 bits
- SHA-2
  - 2001 NSA designed, variants SHA-256 and SHA-512
- SHA-3
  - 2012 public competition winner, 2015 NIST-designated hashing standard (SHAKE variant allows arbitrary output length)

Certificates

- Solving the public key distribution problem
- Shared trust (having somebody's public key) helps:
  - When both A and B trust C
    ⇒ A can establish trust with B (and vice versa)
- Where to start?
  - who to trust
  - how is the initial trust established
- Solution: Certificate Authority (CA)