CSCI368
Network Security

Subject Revision

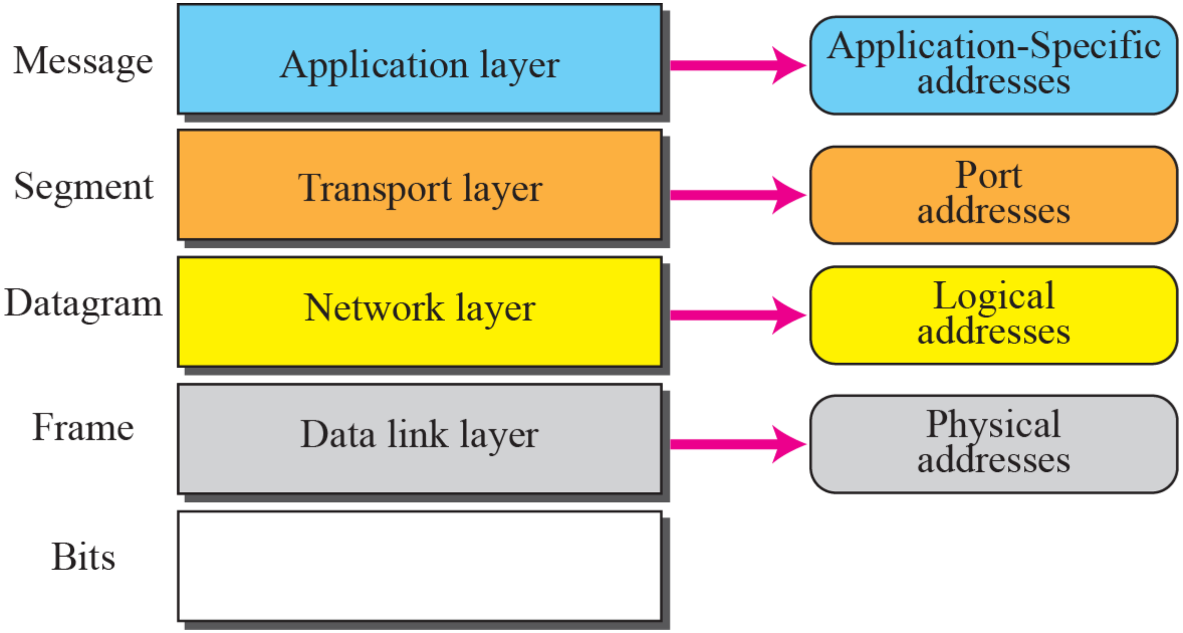
Main Topics

- Network Basics
- Cryptography Basics
- PKI
- Authentication & Key Establishment
- Email Security
- Centralised authentication – Kerberos
- IPSec, SSL/TLS, SSH & VPN
- Wireless Security
- Mobile Security

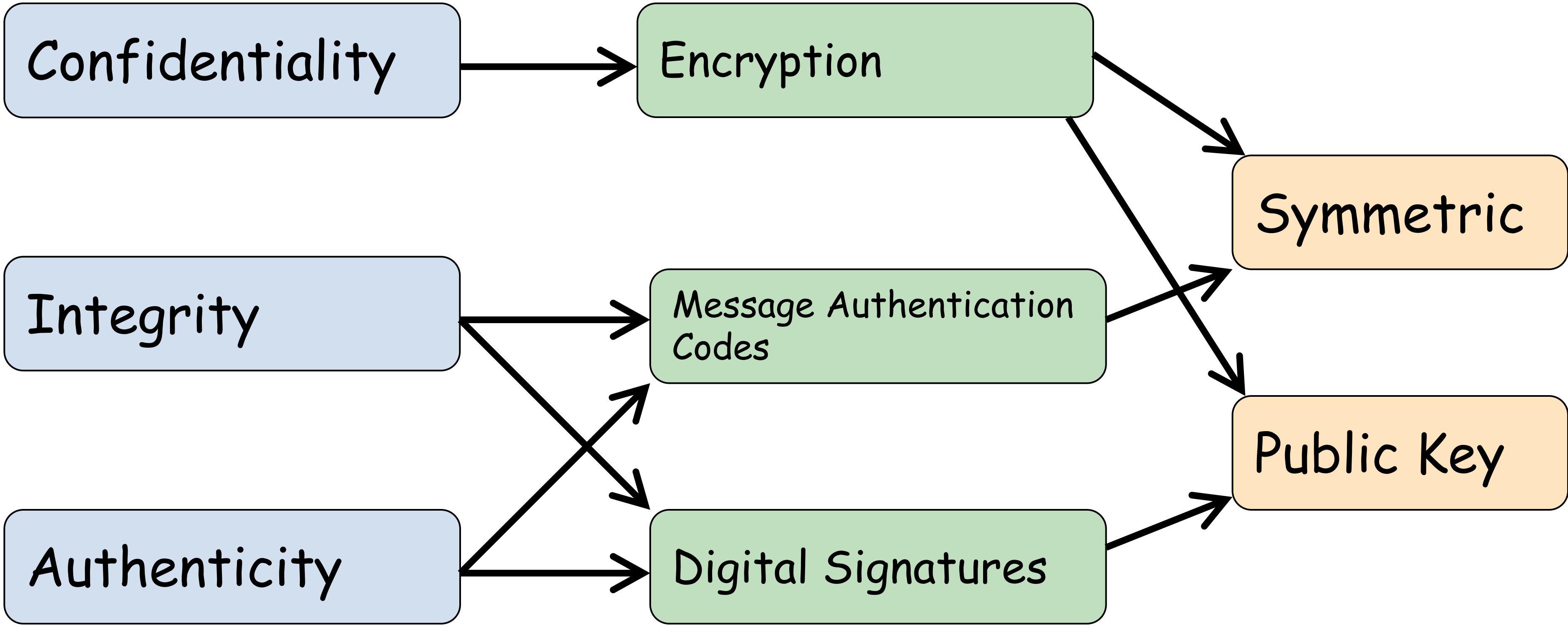
Network Basics

❑ 7-layer OSI Reference Model

❑ 5-layer TCP/IP Internet model



Cryptography and Security Assurance



Confidentiality

Integrity

Authenticity

Encryption

Message Authentication Codes

Digital Signatures

Symmetric

Public Key

PKI

- Public key certificates
- CA
- Revocation
- X.509
- PKI trust models

Authentication and Key Establishment Protocols

- **Common network attacks**
- **Assumptions on attacker capability**
- **Remote identification/authentication**
- **Key establishment protocols:** Key freshness, Key authentication, Forward secrecy
- **Key transport VS Key Agreement**
- **Diffie-Hellman protocol & MITM**
- **Unknown key share attack, DH with Authentication**
- **Password-based protocols**

Email Security

- PGP
  - **Operation: authentication, confidentiality, both**
  - Radix-64 conversion
  - **Key rings**
  - **Public key management**
- S/MIME
  - Operation
  - Public key management

Centralised Authentication and Kerberos

- Motivation
- NTLM
- **Needham-Schroeder protocol**
- **Kerberos Architecture**
- Kerberos V4
  - Basic protocol
  - Inter-realm authentication
  - Limitations
- Kerberos V5
  - Improvements on V4

IPSec

- Security goals
- **Security protocols**
  - **AH vs ESP**
- **Operation modes**
  - **Transport vs Tunnel**
- Security association
- Internet Key Exchange (IKE)
  - Two Phases
  - Phase 1: Aggressive vs Main mode
- IKEv2

SSL/TLS

- Architecture
  - Record protocol
  - Change Cipher Spec protocol
  - Alert protocol
  - Handshake protocol
- **SSL/TLS connection vs session**
- **SSL/TLS Handshake Key Exchange Methods**
- SSL/TLS key derivation
  - Premaster secret, master secret, connection keys
- TLS 1.3

SSH

- SSH Architecture
  - **Transport layer protocol**
  - User authentication protocol
  - Connection protocol
- **Port forwarding**
- VPN

Wireless LAN Security

- WEP
  - Encryption process
  - **Weaknesses of WEP**
- WPA
  - **802.1x authentication**
    - **Port-based access control**
    - **EAP**
  - TKIP
    - **Improvements on WEP**
  - CCMP

Mobile Security

- **GSM AKE**
  - **Weakness**
- **3GPP AKA**
  - **SQN-based server authentication**

Final Exam

- Date & Time: **September 4th (check with SIM)**
- Duration: **3 hours**
- **Closed book exam**

Final Exam

- Total: **60 marks**
- You must **score at least 40% (i.e., 24 marks)** to avoid a TF.
- Question types:
  - Multiple choice: 12 questions (2 marks each)
  - Short-answer & protocol-analysis: 11 questions

MCQ Question

- Which ones would be the most suitable protocols/tools for securing e- mail?

  A. PGP
  B. IPSec and IKE
  C. S/MIME
  D. SSL/TLS
  E. SSH

MCQ Question

- Which ones would be the most suitable protocols/tools for securing e- mail?

A. PGP (+50%)
B. IPSec and IKE (-33.3333%)
C. S/MIME (+50%)
D. SSL/TLS (-33.3333%)
E. SSH (-33.3333%)

MCQ Question

- PGP uses which of the following algorithms to encrypt the content of an email?

  A. A public-key encryption algorithm

  B. A symmetric-key encryption algorithm

  C. Both PKE and SKE algorithms

  D. ZIP

  E. Radix-64

MCQ Question

- PGP uses which of the following algorithms to encrypt the content of an email?

A. A public-key encryption algorithm (-25%)

B. A symmetric-key encryption algorithm (+100%)

C. Both PKE and SKE algorithms (-25%)

D. ZIP (-25%)

E. Radix-64 (-25%)

MCQ Question

- Which of the following cryptographic algorithms provide message confidentiality?

A. RSA signature
B. SHA-1
C. Diffie-Hellman key exchange
D. HMAC
E. None of the listed options

MCQ Question

- Which of the following cryptographic algorithms provide message confidentiality?

A. RSA signature (-100%)

B. SHA-1 (-100%)

C. Diffie-Hellman key exchange (-100%)

D. HMAC (-100%)

E. None of the listed options (+100%)

MCQ Question

- Which of the following cryptographic algorithms provide message confidentiality?

A. RSA encryption

B. SHA-1

C. AES

D. HMAC

E. None of the listed options

MCQ Question

- Which of the following cryptographic algorithms provide message confidentiality?

  A. RSA encryption (+50%)
  B. SHA-1 (-50%)
  C. AES (+50%)
  D. HMAC (-50%)
  E. None of the listed options (-100%)