Software Defined Networks

Motivation:
- many protocols, vendors, management platforms
- virtualization, cloud, … (fill the buzzword of a day)
- scale up in size and bandwidth

Goals:
- flexibility, agility, …
- central management, programatically configured (API)
- open and vendor-independent
SDN Architecture

Grossly simplified:

- **Application Layer**
  - Application
  - Application
  - APIs

- **Control Layer**
  - Network Service
  - Network Service
  - Open Flow

- **Infrastructure**
Network Security
Security

- A broad problem, we will look at securing communication protocols

- Objectives:
  - encryption
  - 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** - ciphertext (encrypted text)
- Encryption: $E(M) \rightarrow C$
- Decryption: $D(C) \rightarrow M$
Encryption - Attacks

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

![Diagram showing encryption and attacks]
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

- **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