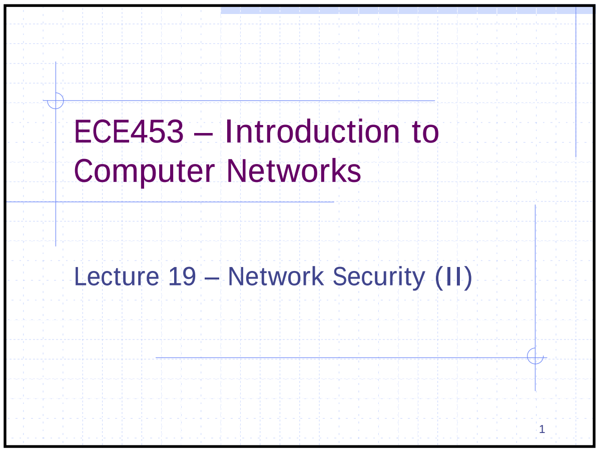
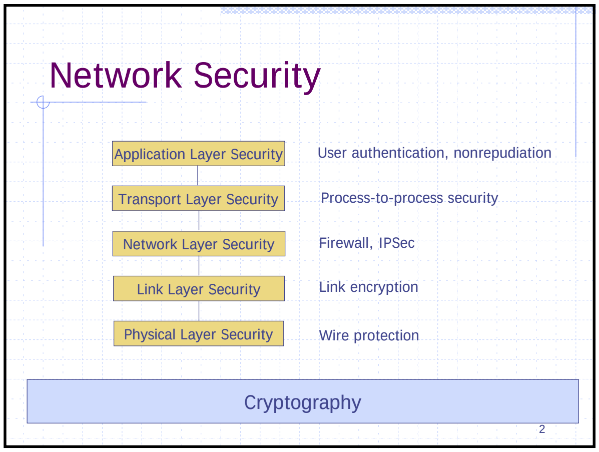


ECE453 – Introduction to Computer Networks

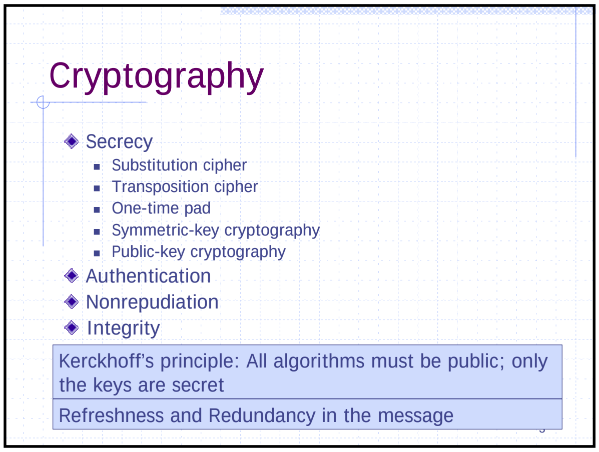
Lecture 19 – Network Security (II)



Network Security

Application Layer Security	User authentication, nonrepudiation
Transport Layer Security	Process-to-process security
Network Layer Security	Firewall, IPSec
Link Layer Security	Link encryption
Physical Layer Security	Wire protection

Cryptography



Cryptography

- Secrecy
  - Substitution cipher
  - Transposition cipher
  - One-time pad
  - Symmetric-key cryptography
  - Public-key cryptography
- Authentication
- Nonrepudiation
- Integrity

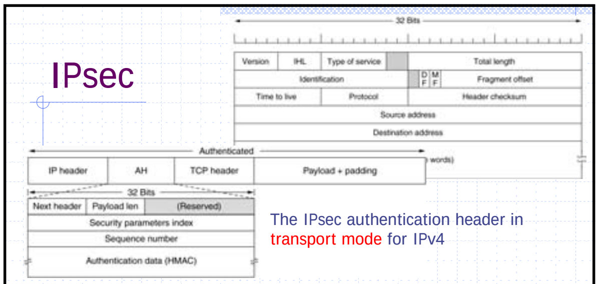
Kerckhoff's principle: All algorithms must be public; only the keys are secret

Refreshness and Redundancy in the message

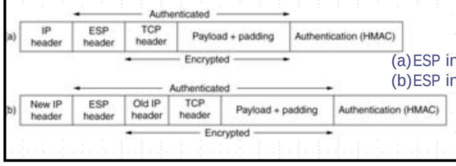
IPsec

- Where to put security?
- A framework for multiple services, algorithms, and granularities
  - Services: secrecy, integrity, prevent replay attack
- Connection-oriented
  - SA (Security Association)

IPsec

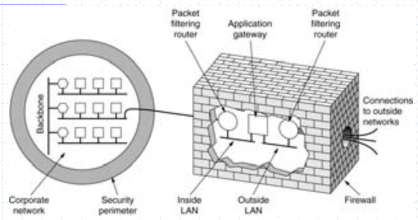


The IPsec authentication header in transport mode for IPv4



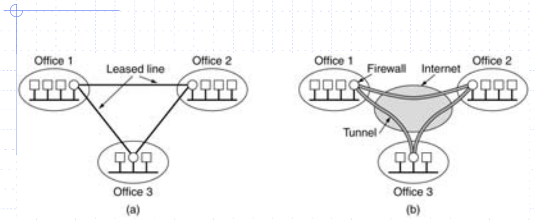
(a)ESP in transport mode.
(b)ESP in tunnel mode.

Firewalls

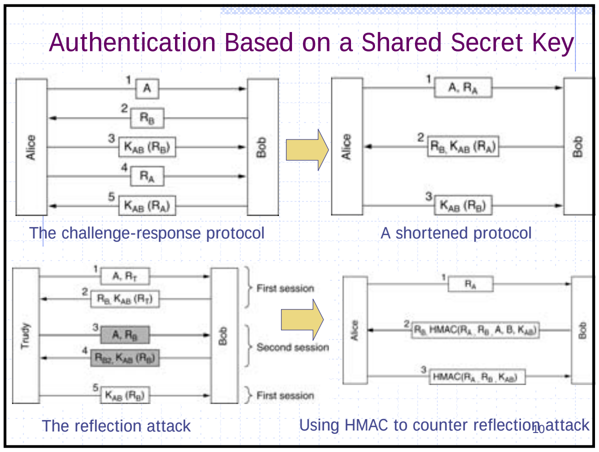


A firewall consisting of two packet filters and an application gateway

Virtual Private Networks



(a) A leased-line private network. (b) A virtual private network



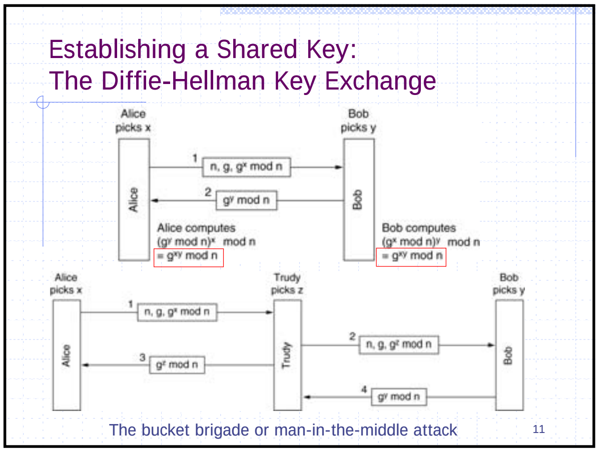
Authentication Based on a Shared Secret Key

The challenge-response protocol

A shortened protocol

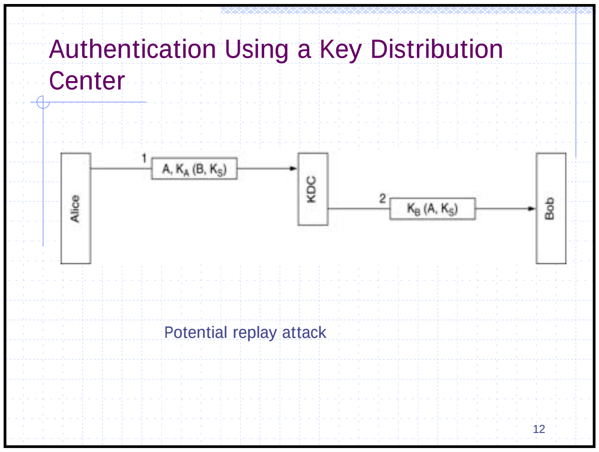
The reflection attack

Using HMAC to counter reflection attack



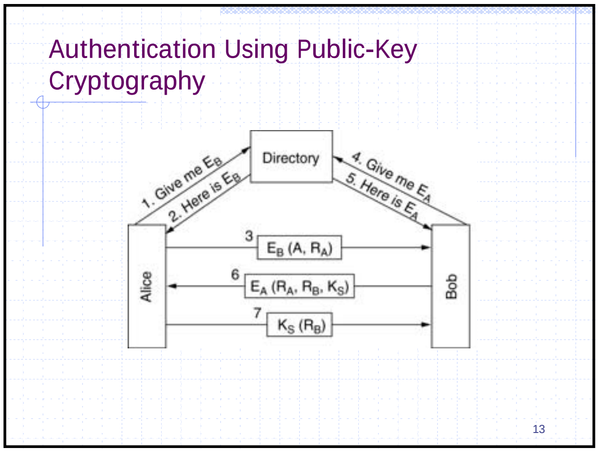
Establishing a Shared Key: The Diffie-Hellman Key Exchange

The bucket brigade or man-in-the-middle attack



Authentication Using a Key Distribution Center

Potential replay attack



Authentication Using Public-Key Cryptography