

# Secure connections

Peter Levinsky, Roskilde, Datamatiker

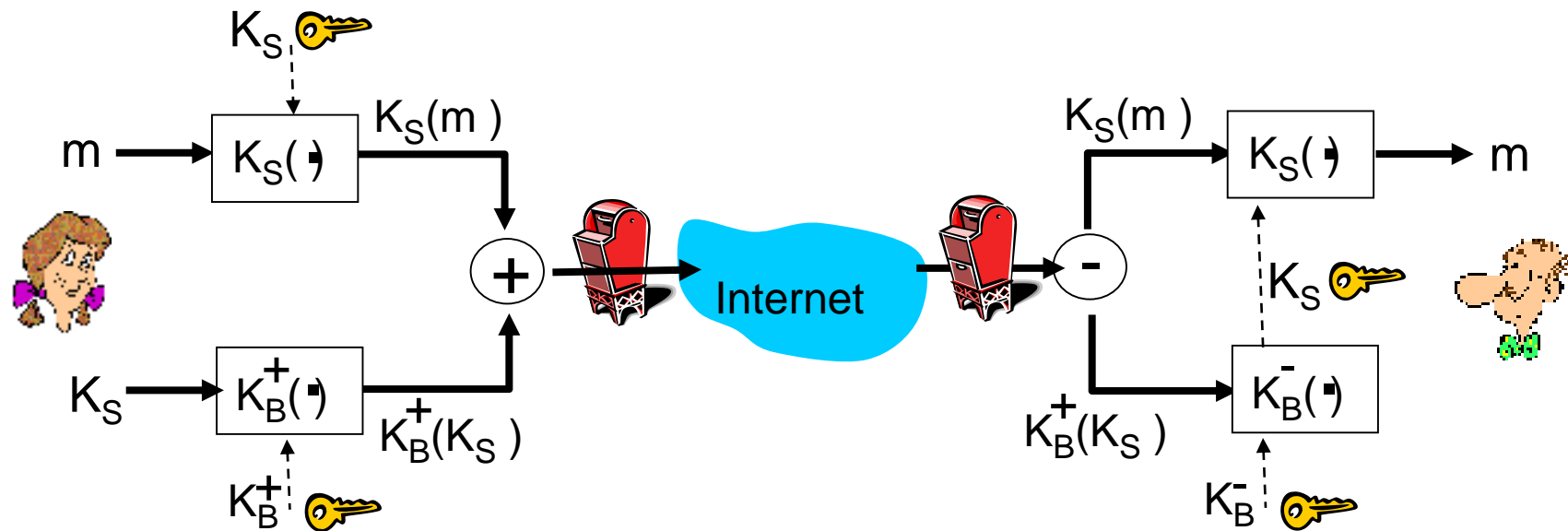
14.11.2022

# Secure connections examples

Application Layer	Email – Pretty Good Privacy
Transport Layer	Secure Socket Layer
Network Layer	Ipssec (VPN)
DataLink Layer	Wifi – WEP (not part of curriculum)
Physical Layer	N/A

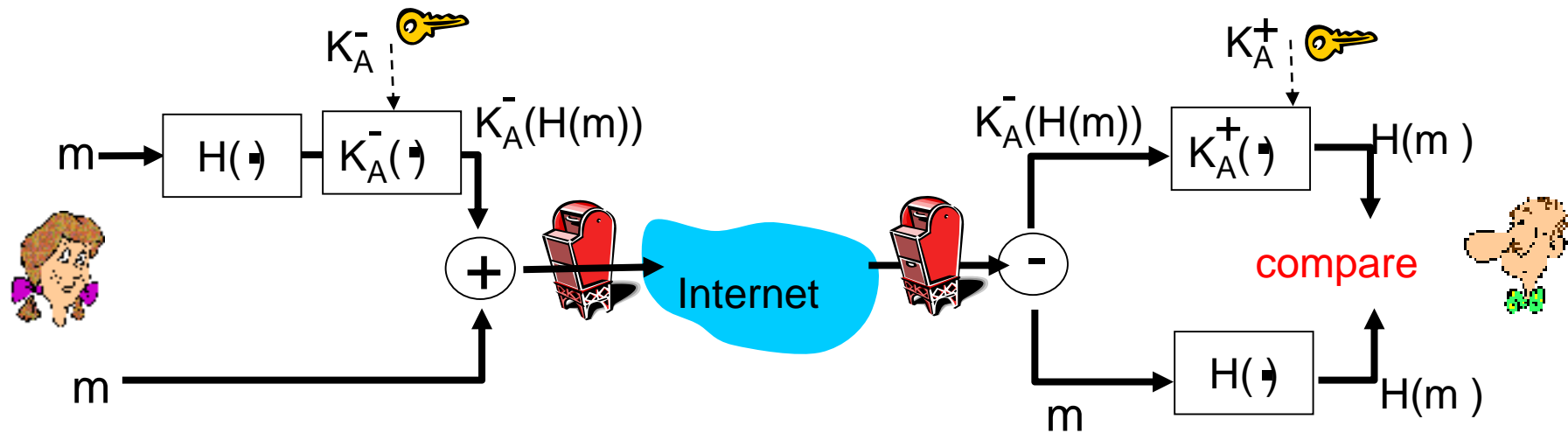
# Secure Application layer email - PGP (Pretty Good Privacy)

**Alice wants to  
send confidential e-mail,  $m$ , to Bob**



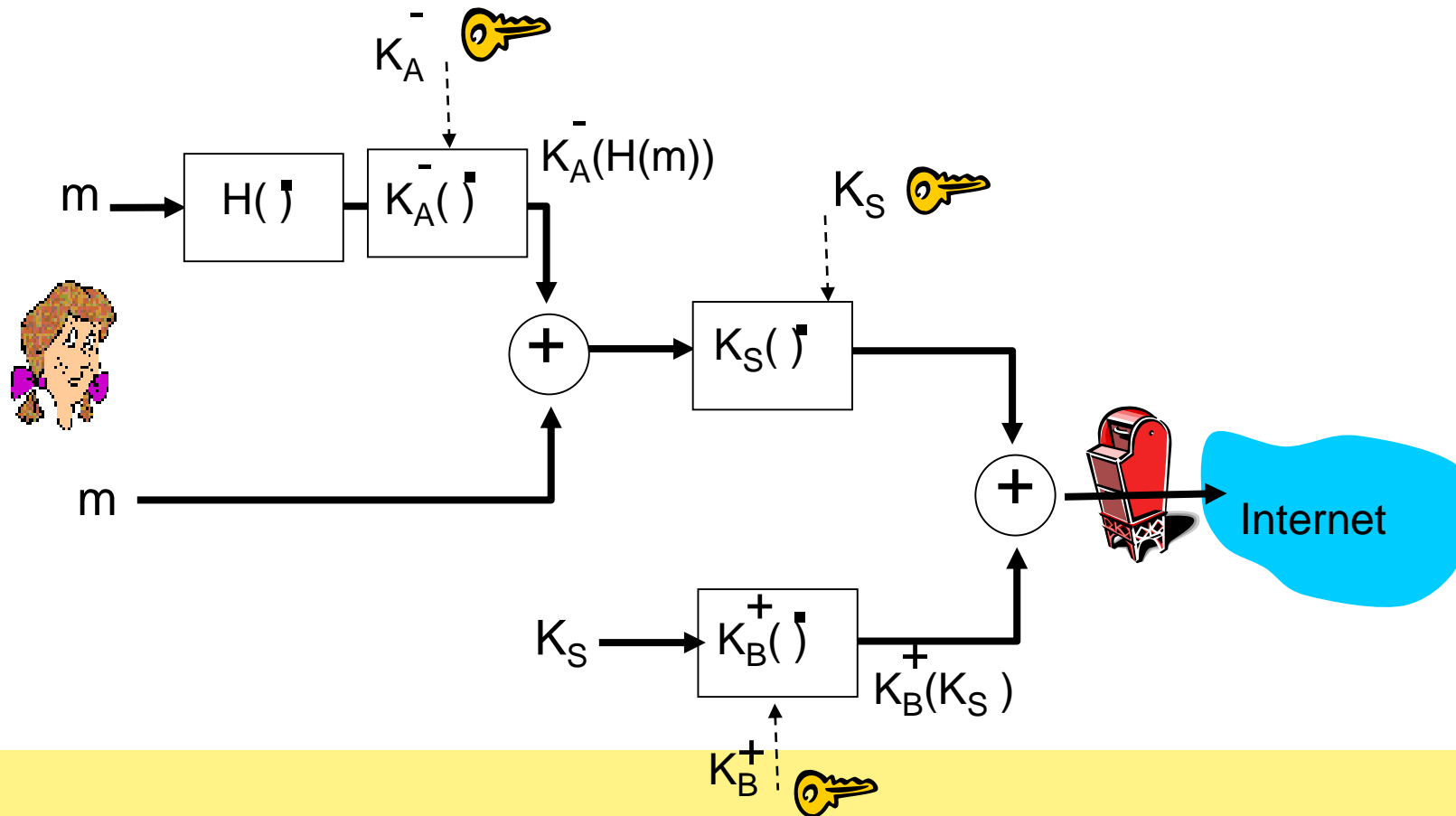
# Secure Application layer email - PGP (Pretty Good Privacy)

**Alice wants to provide  
sender authentication message integrity**



# Secure Application layer email - PGP (Pretty Good Privacy)

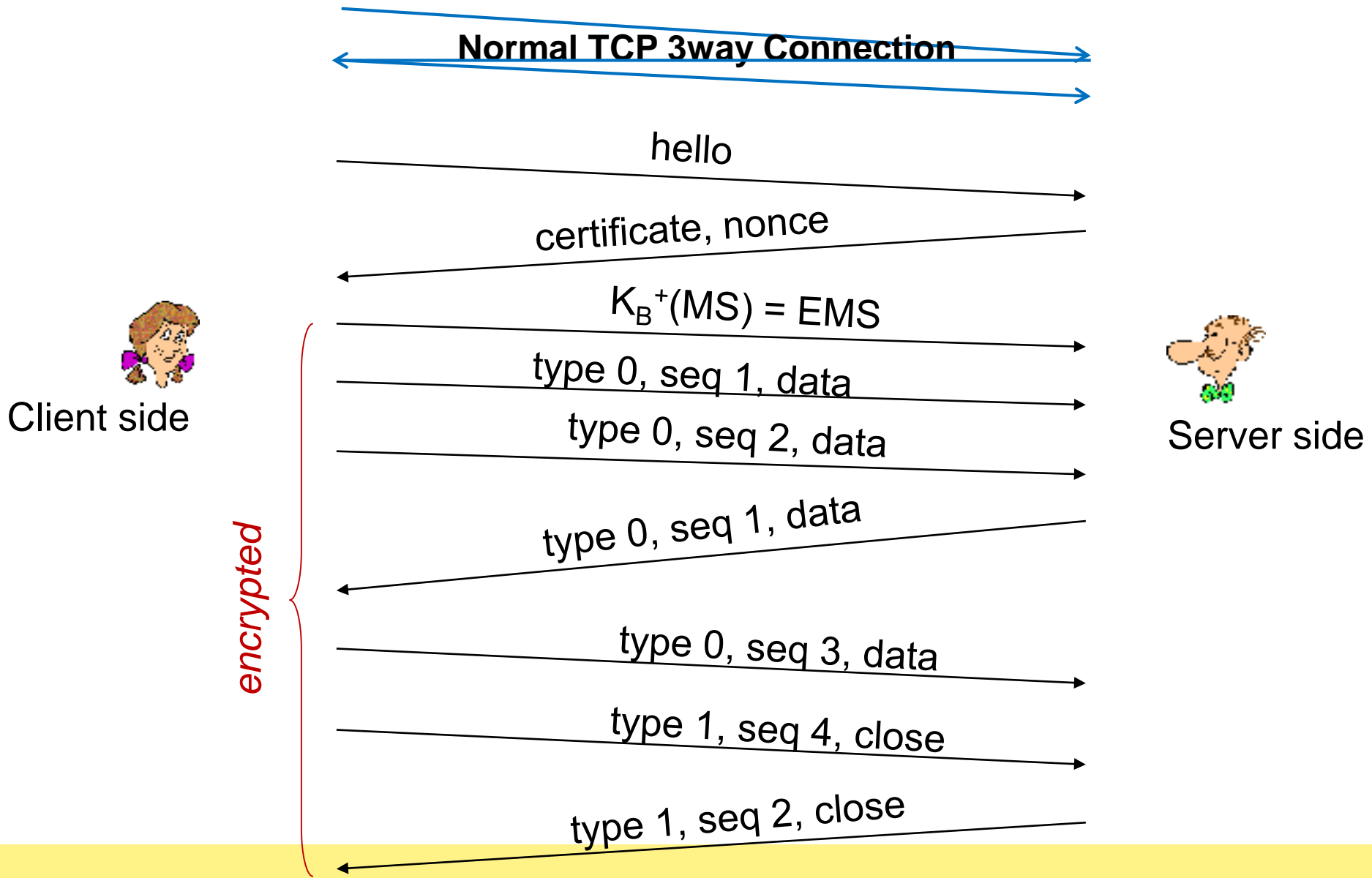
Alice wants to provide sender authentication message integrity and a confidential email



# Secure Transport layer - Secure Socket Layer (SSL)

- SSL support Confidential (HTTPS is based on SSL)
- SSL *can support Integrity*
- Four keys (part of EMS – Encrypted Master Secret):
  - $K_c$  = encryption key for data sent from client to server
  - $M_c$  = MAC key for data sent from client to server
  - $K_s$  = encryption key for data sent from server to client
  - $M_s$  = MAC key for data sent from server to client

# Secure Transport layer - Secure Socket Layer (SSL)



# Secure Network layer

## IPsec (Virtual Private Network - VPN)



- edge routers IPsec-aware (tunnel)
- ❖ hosts IPsec-aware



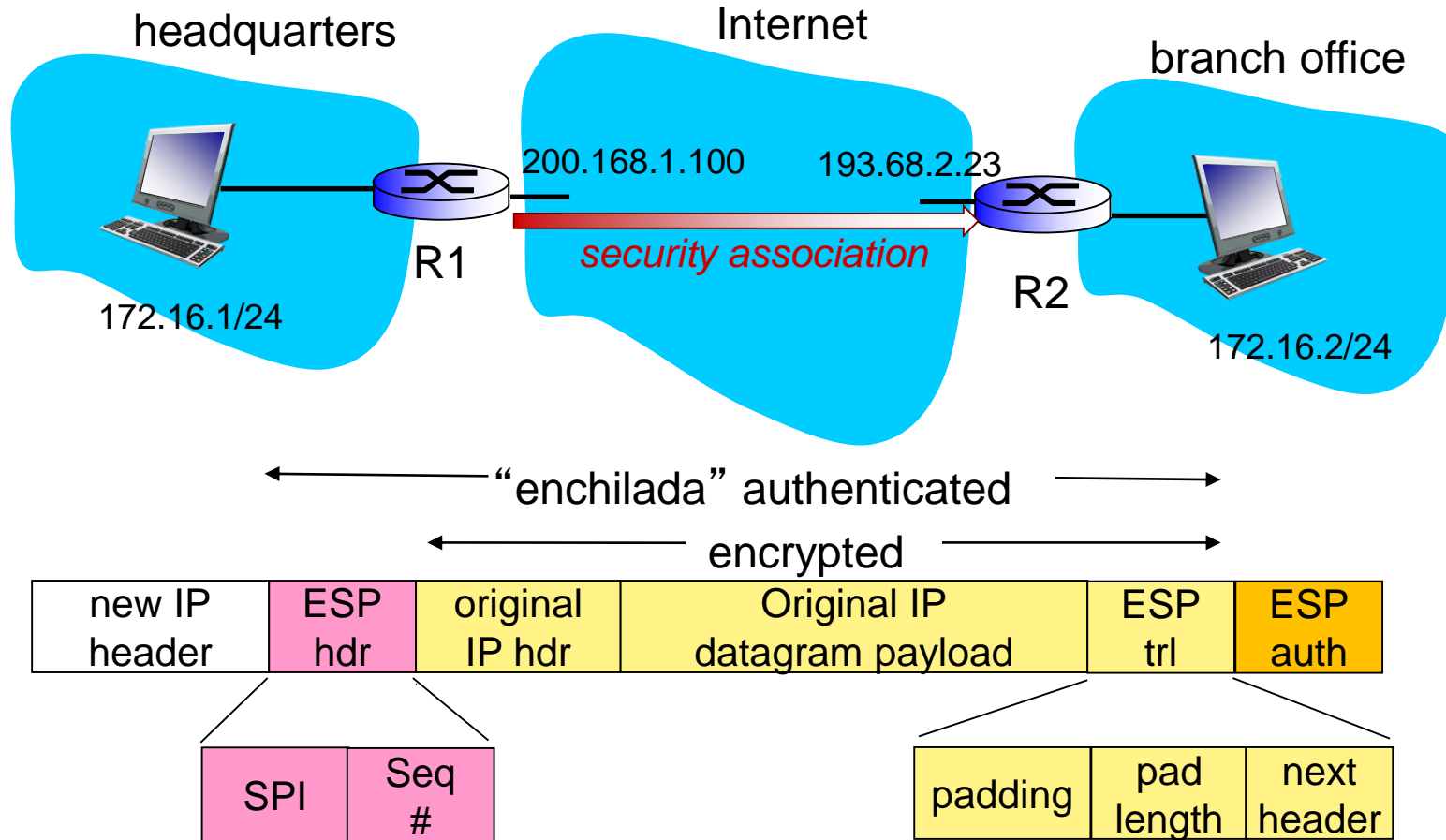
# Secure Network layer

## IPsec (Virtual Private Network - VPN)

- **Authentication Header (AH)** protocol
  - provides source authentication & data integrity but *not* confidentiality
- **Encapsulation Security Protocol (ESP)**
  - provides source authentication, data integrity, *and confidentiality*
  - more widely used than AH

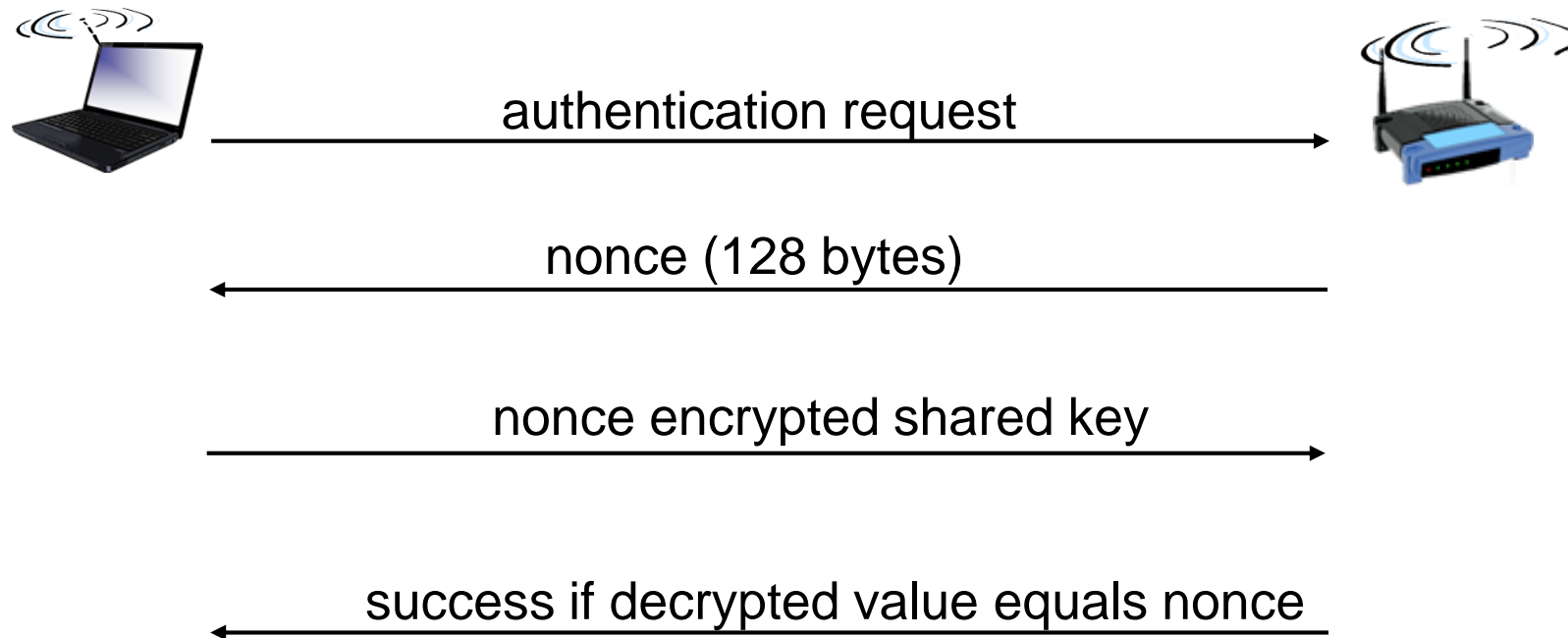
# IPsec (Virtual Private Network - VPN)

SA – or VPN as tunnel - the most often used security at Network layer



# Secure DataLink layer

## WEP - Wired Equivalent Privacy



Not very secure ! – use WPA/WPA2 -- Wifi Protected Access

# Secure DataLink layer

## EAP- Extensible Authentication Protocol

