T-79.4501
Cryptography and Data Security

Lecture 11:
Security systems using public keys
11.1 PGP
11.2 SSL/TLS
11.3 IPSEC
Stallings: Ch 16,17

Pretty Good Privacy

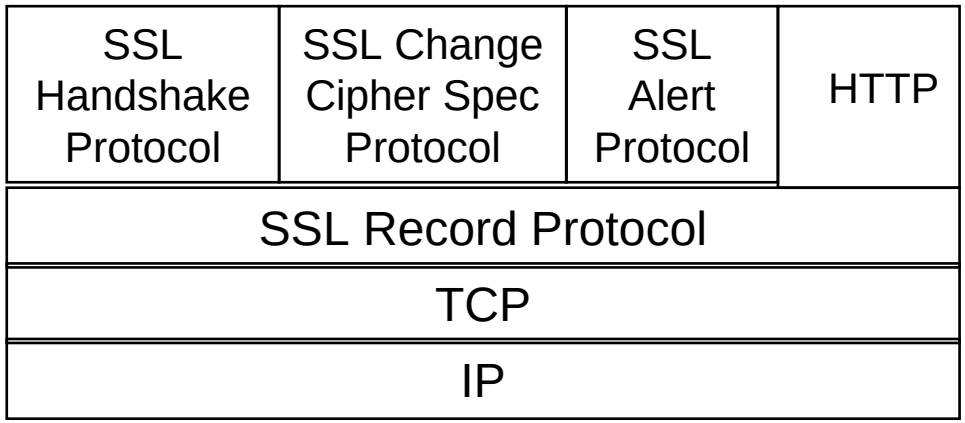
- Email encryption program
- Bottom–up approach to the distribution of trust
- Each user acts as his/her own CA and signs the public keys of other users
- User can accept authenticity of a public key based on recommendation by a third trusted user
- RSA public key encryption used for distribution of session keys *)
- Digital signatures produced by RSA or DSA signature algorithms
- Hash functions are MD5 and SHA-1
- Symmetric encryption performed using IDEA in CFB mode (self-synchronising stream cipher)
- Public keys held in ”Key-ring”
- Revocation of public keys is a problem

*) A data encryption protocol, where the data is encrypted using symmetric encryption, and the symmetric encryption key is encrypted using public key encryption, is called as ”hybrid encryption”

Secure Sockets Layer /Transport Layer Security

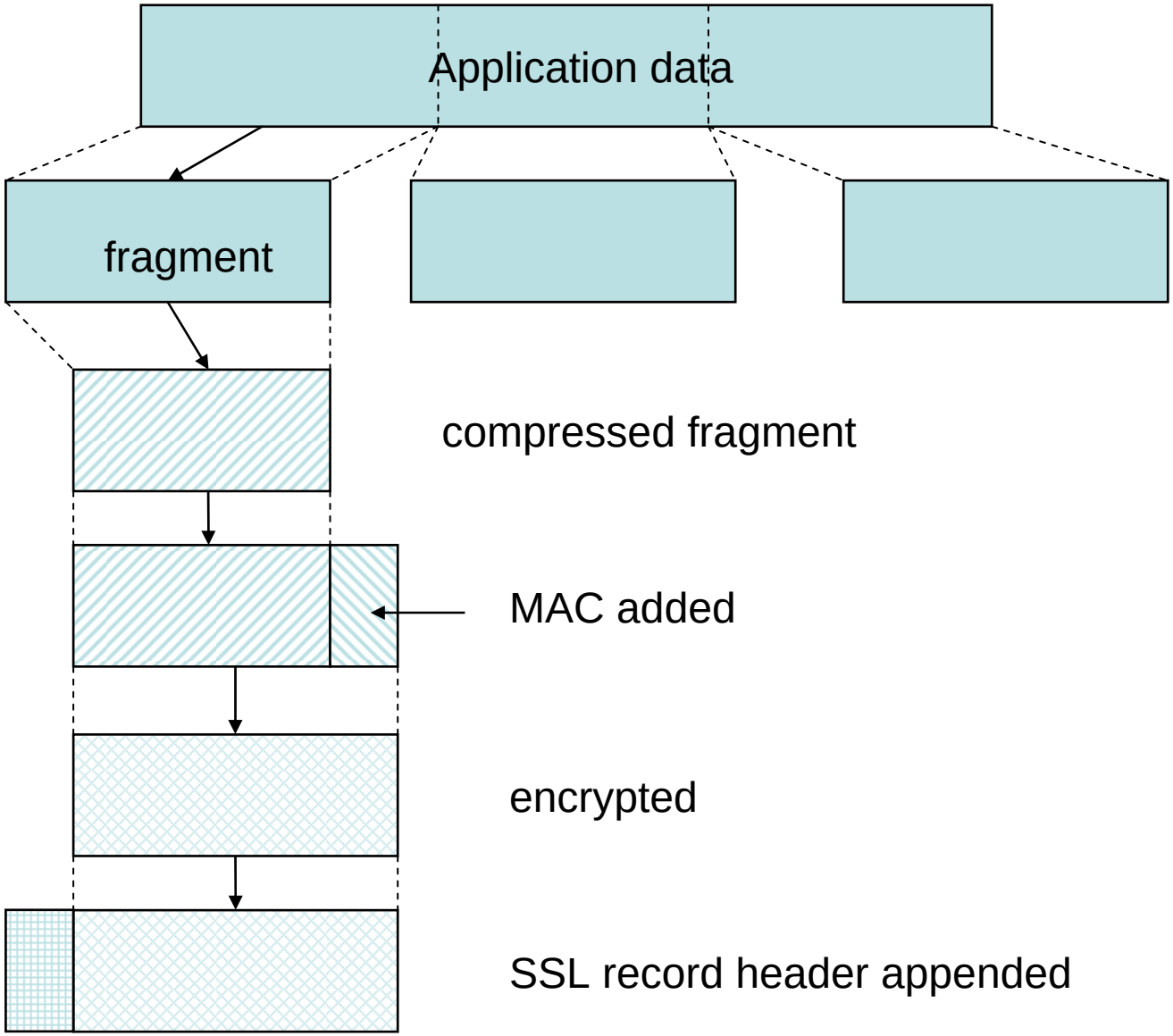
- SSL (by Netscape) adds security to the TCP level of the Internet Protocol stack
- Reliable end-to-end service.
- TLS developed by IETF is basically equivalent to SSL v 3.1

Structure:



- Hypertext Transfer Protocol (Web client/server interaction) can operate on top of SSL (https://...)

SSL Record Protocol



SSL Record Protocol Crypto

- The MAC is similar to HMAC (indeed, an early version of HMAC) with the difference that OPAD and IPAD fields are concatenated to the key data (not xored as in HMAC). MAC is based on MD5 or SHA-1
- Block Cipher Algorithms available (key size in bits):
  - IDEA (128)
  - RC2-40 (40)
  - DES-40 (40)
  - DES (56)
  - 3DES (112-168)
  - Fortezza (Skipjack) (80)
- Stream Cipher Algorithms available (key size)
  - RC4-40 (40)
  - RC4-128 (128)

FORTEZZA

- FORTEZZA is a registered trademark of the U.S. National Security Agency (NSA)
  - Defense Message System
  - Encrypted voice communications over secure telephones.
- FORTEZZA cards
  - cryptographic "co-processors"
  - provide authentication (DSA), data integrity (SHA-1), and confidentiality (KEA and Skipjack).
- FORTEZZA-enabled devices
  - PCMCIA-based crypto cards (see next slide)
  - serial port devices, Ethernet cards, and modems.
  - Cellular telephones, pagers, PDAs, and other mobile devices.
- Microsoft supports FORTEZZA in its products.

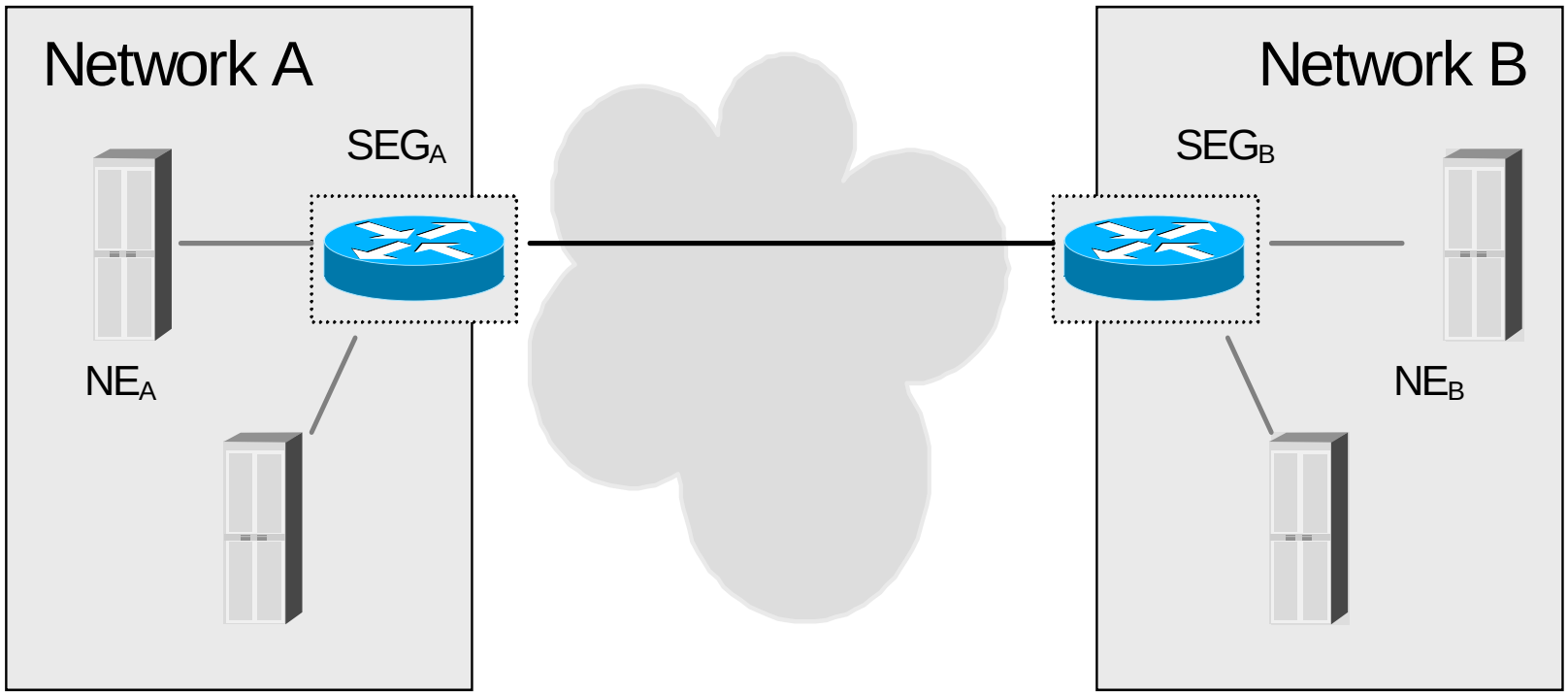
PCMCIA PC Card

SSL Handshake Protocol

- Phase 1: Establishing Security Capabilities
  - Nonces
  - Session ID
  - Cipher Suite
    1. Key Exchange method: RSA, Fixed, ephemeral, or anonymous Diffie-Hellman, Fortezza
    2. Cipher Algorithm: Any of the ones mentioned above; Cipher type: Stream or Block; Exportability: Yes or No;
    3. Hash algorithm: MD5 or SHA-1; Hash size: 0, 16 (MD5), or 20 (SHA-1)
    4. Key Material (session key data) and IV size (for CBC mode)
  - Compression method
- Phase 2: Server Authentication and Key Exchange
- Phase 3: Client Authentication and Key Exchange
- Phase 4: Finish
  - Explicit verification that the authentication and key exchange was successful

IPSec

- The toolbox for building Virtual Private Networks (VPN)
  - Secure “branch office” connectivity over Internet
  - Secure Remote Access over Internet
  - Extranet and Intranet connectivity with partners
  - Enhanced electronic commerce security
- Efficient protection if IPSec implemented in firewall
- IPSec is below transport layer and so is transparent to applications
- IPSec is typically also transparent to end users
- IPSec can be used to provide secure remote login for individual users.


Network A
SEG$_A$
NE$_A$
Network B
SEG$_B$
NE$_B$

IP Sec

New specifications December 2005:

RFC 4301 Security Architecture for the Internet Protocol (obsoletes2401)

RFC 4302 IP Authentication Header (obsoletes 2402)

RFC 4303 IP Encapsulating Security Payload (ESP) (obsoletes 2406)

RFC 4304 Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)

RFC 4305 Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) (obsoletes 2404, 2406)

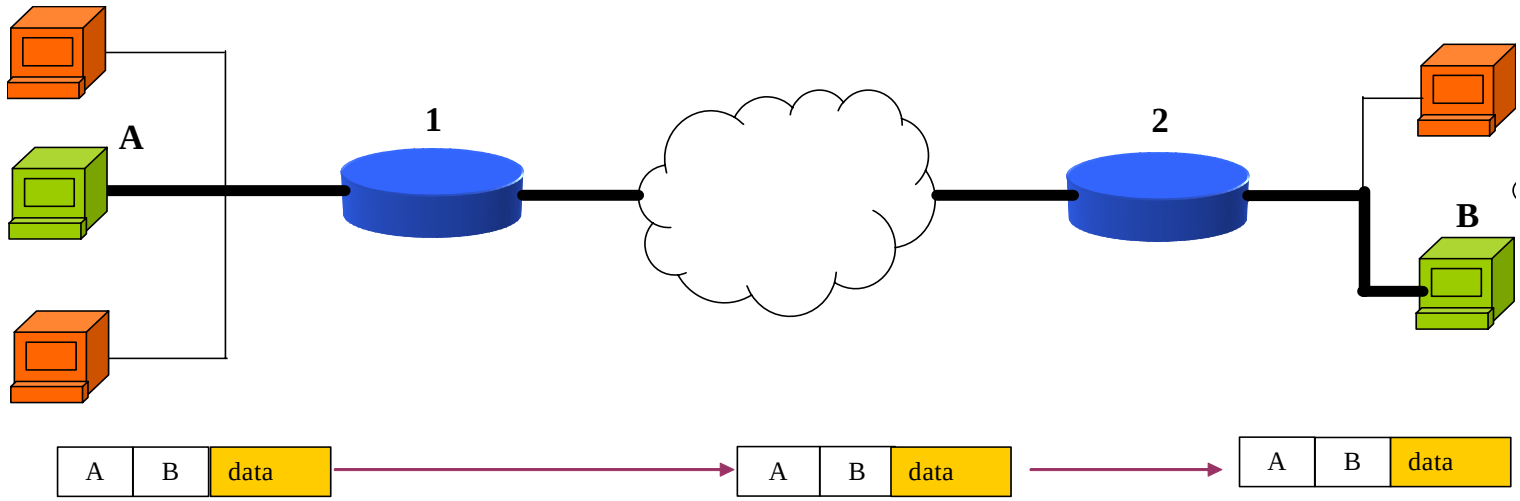
RFC 4306 Internet Key Exchange (IKEv2) Protocol (obsoletes 2407, 2408, 2409)

RFC 4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

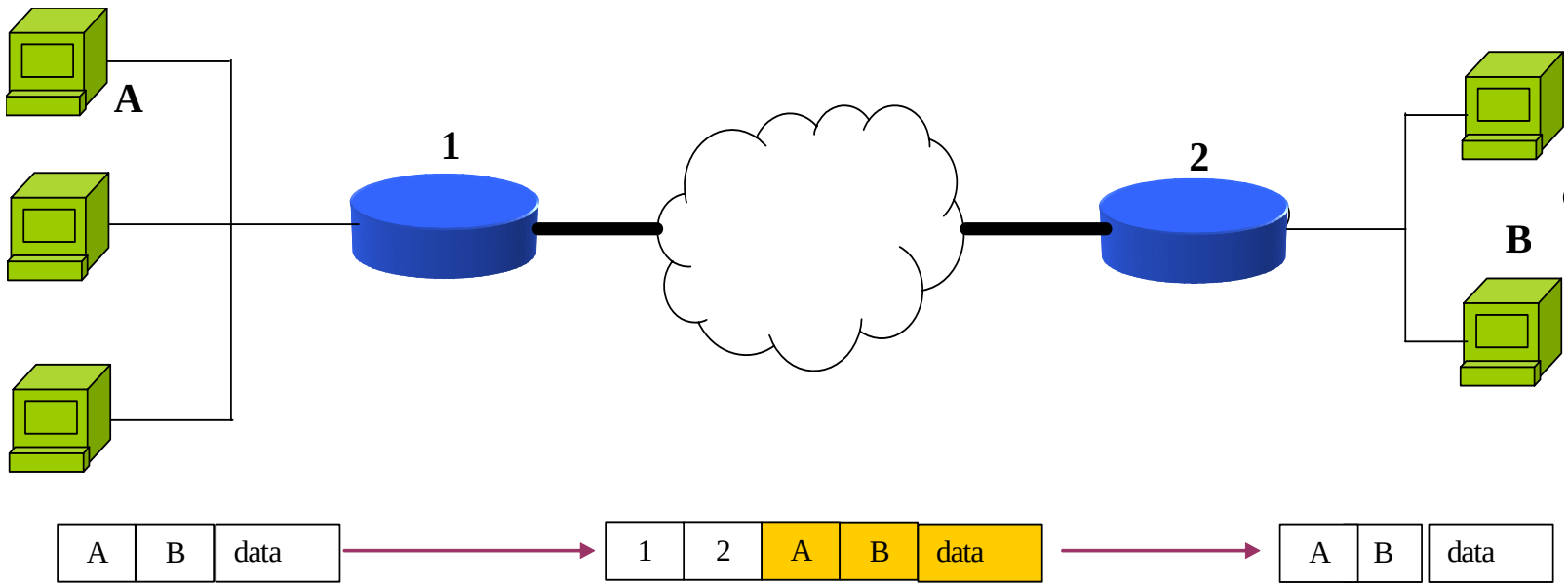
RFC 4308 Cryptographic Suites for IPsec

RFC 4309 Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)

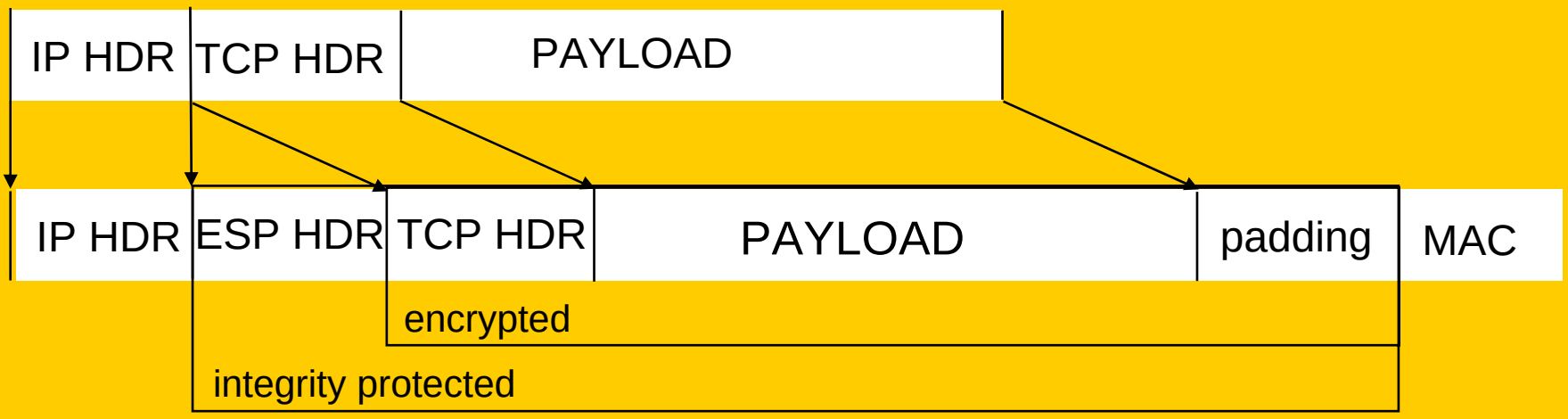
End-to-End Security (ESP in Transport Mode)



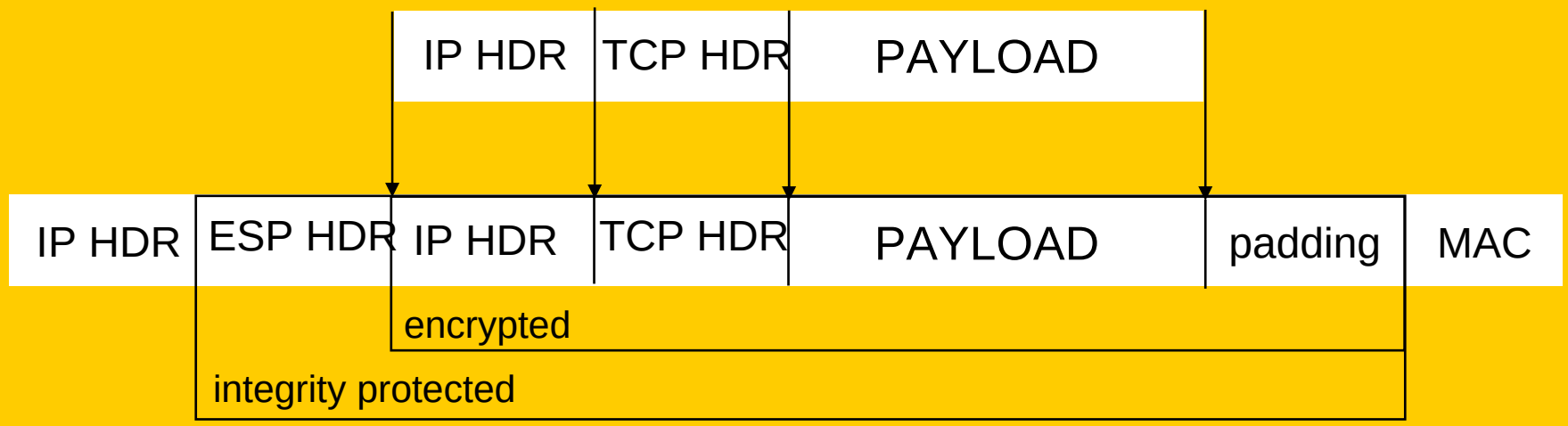
VPN Security
(ESP in Tunnel Mode)



Transport mode:

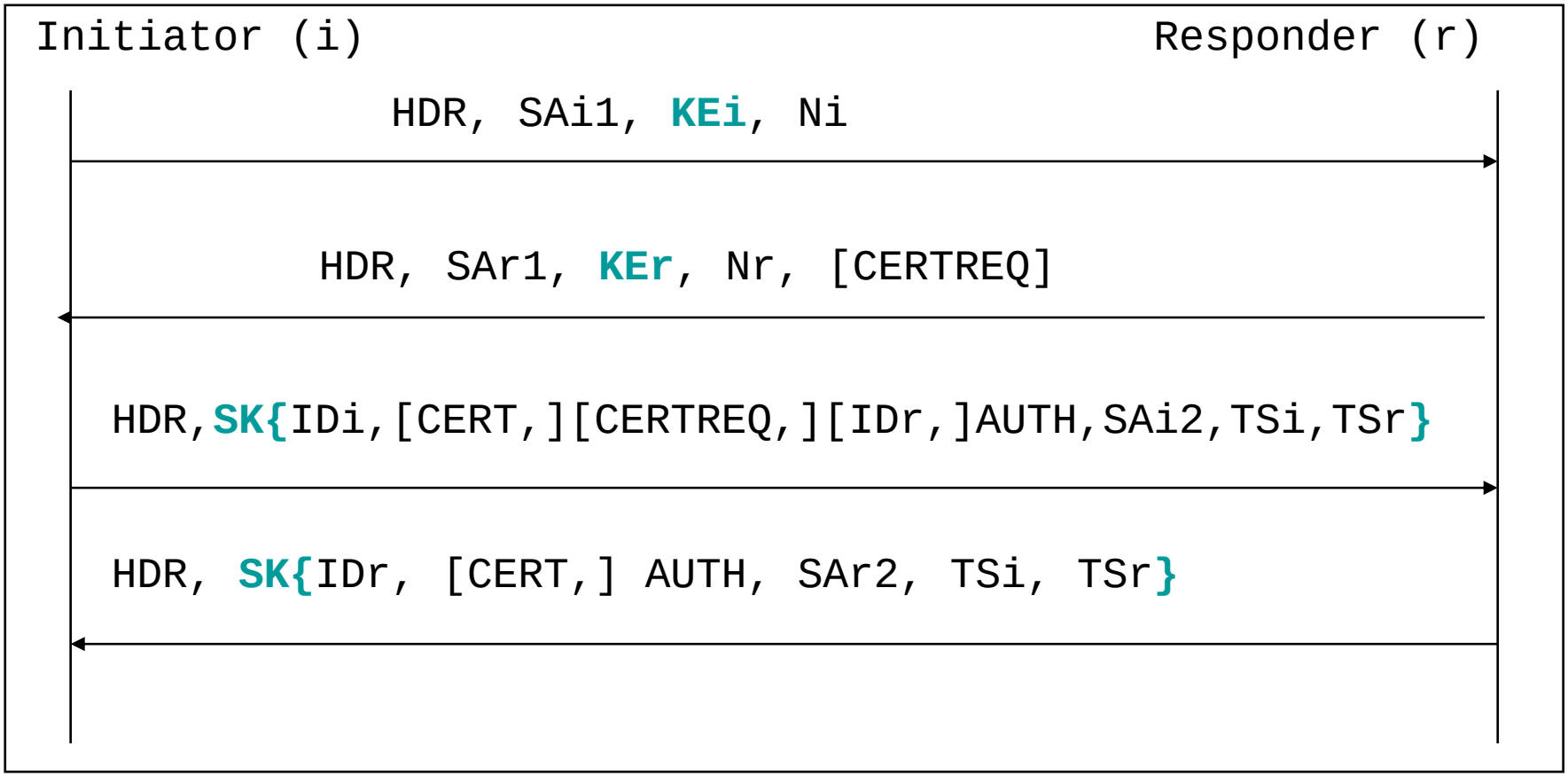


Tunnel mode:



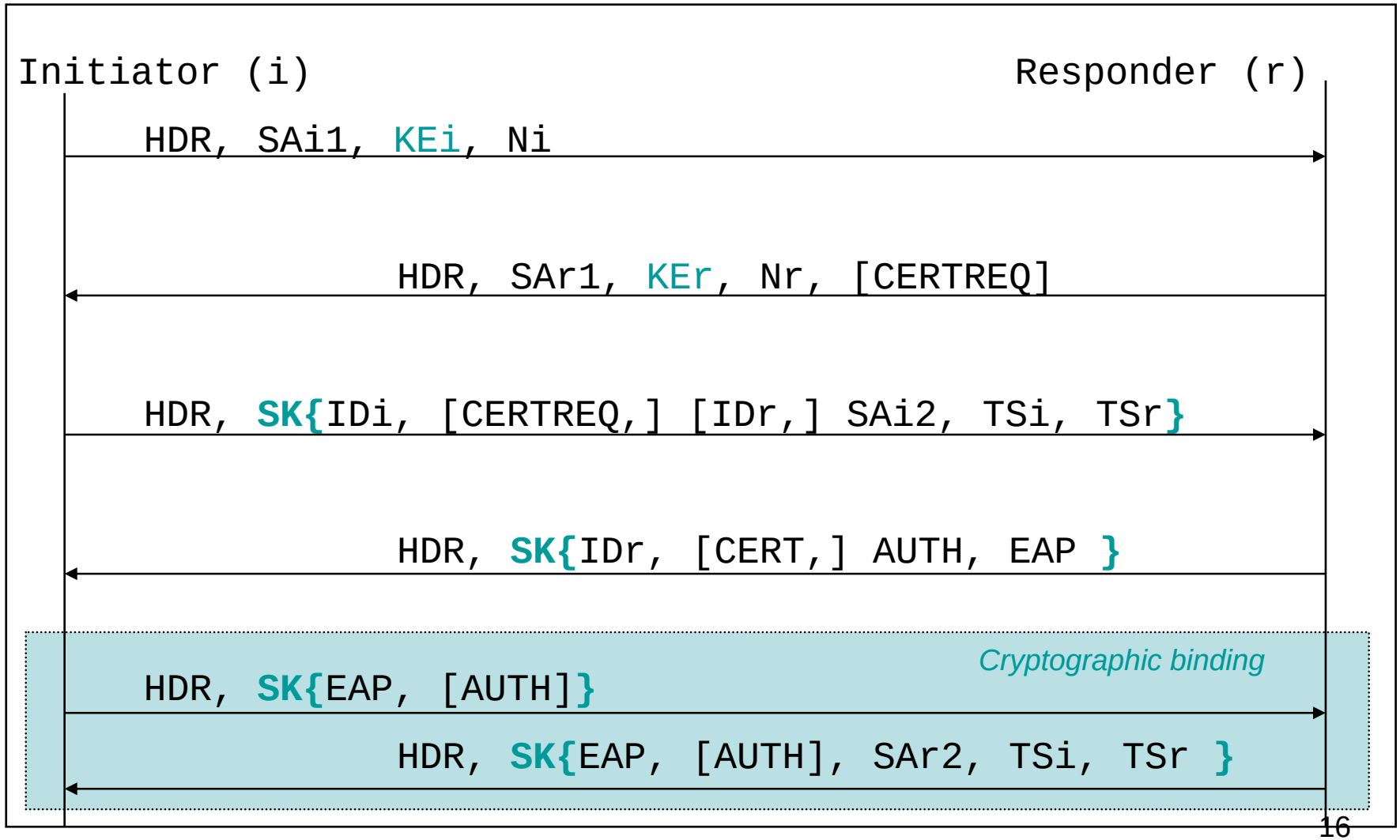
IKEv2

Based on Diffie-Hellman Key Exchange **KEi=g^a, KEr=g^b → SK=g^{ab}**



IKEv2

Secure Legacy Authentication (SLA)



Legacy Protocols and EAP

- IETF PPPEXT working group:

  RFC 2284 Extensible Authentication Protocol (EAP)
- EAP is not an authentication protocol in itself, but a standard way of encapsulating an authentication protocol.
- Composed of message pairs: EAP_Request - EAP_Response; final pair: EAP_Success/EAP_Failure
- EAP types have been standardised (”legacy” protocols):

  RFC2716: PPP EAP TLS Authentication Protocol

  – Internet Drafts:

  EAP SIM Authentication

  EAP AKA Authentication

  Protected EAP Protocol (PEAP)

  EAP-SKE authentication and key exchange protocol

  Microsoft EAP CHAP Extensions

  The EAP GPRS Protocol (EAP-GPRS)