



NETWORK LAYER: IP SECURITY

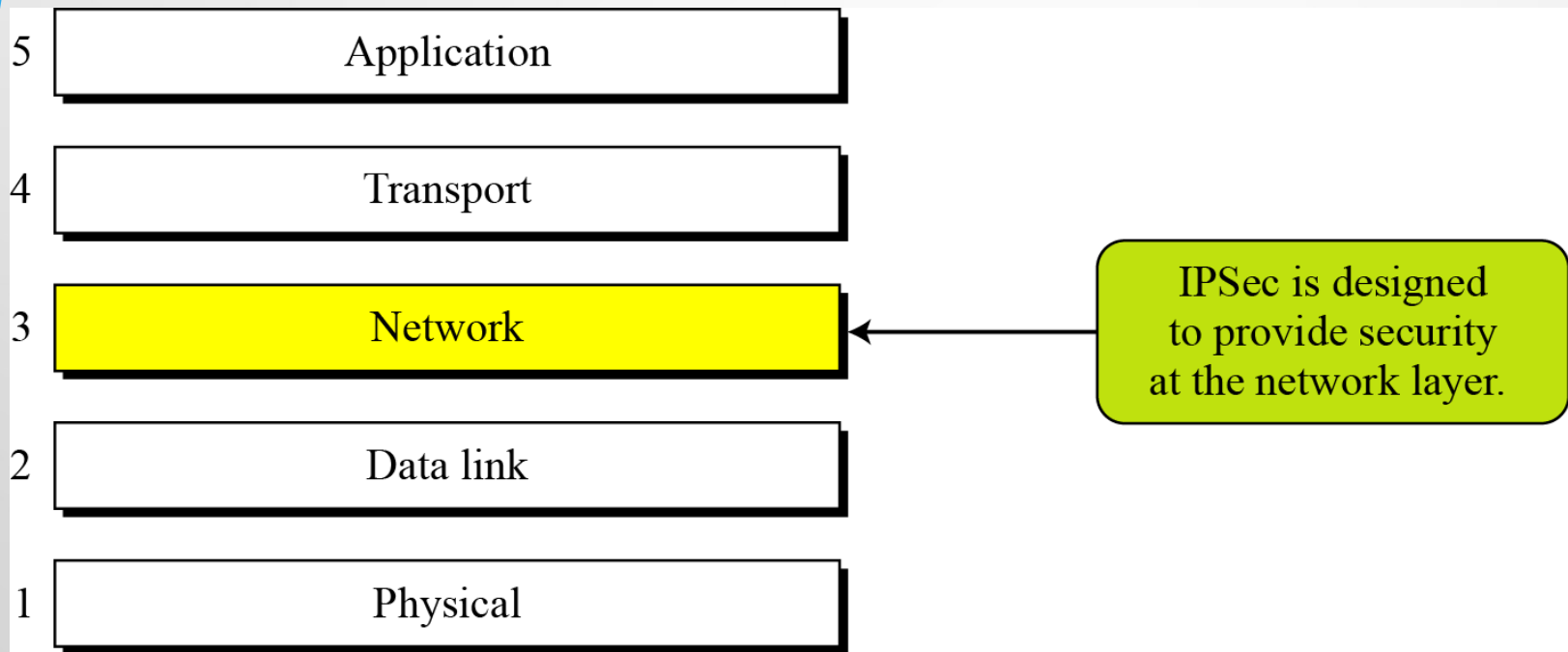
School of Electrical Engineering
Telkom University

Kerangka

- Arsitektur IPSec
- Mode transport dan tunnel
- Authentication header
- Encapsulating Security Payload
- Internet Key Exchange

IPSec (IP Security)

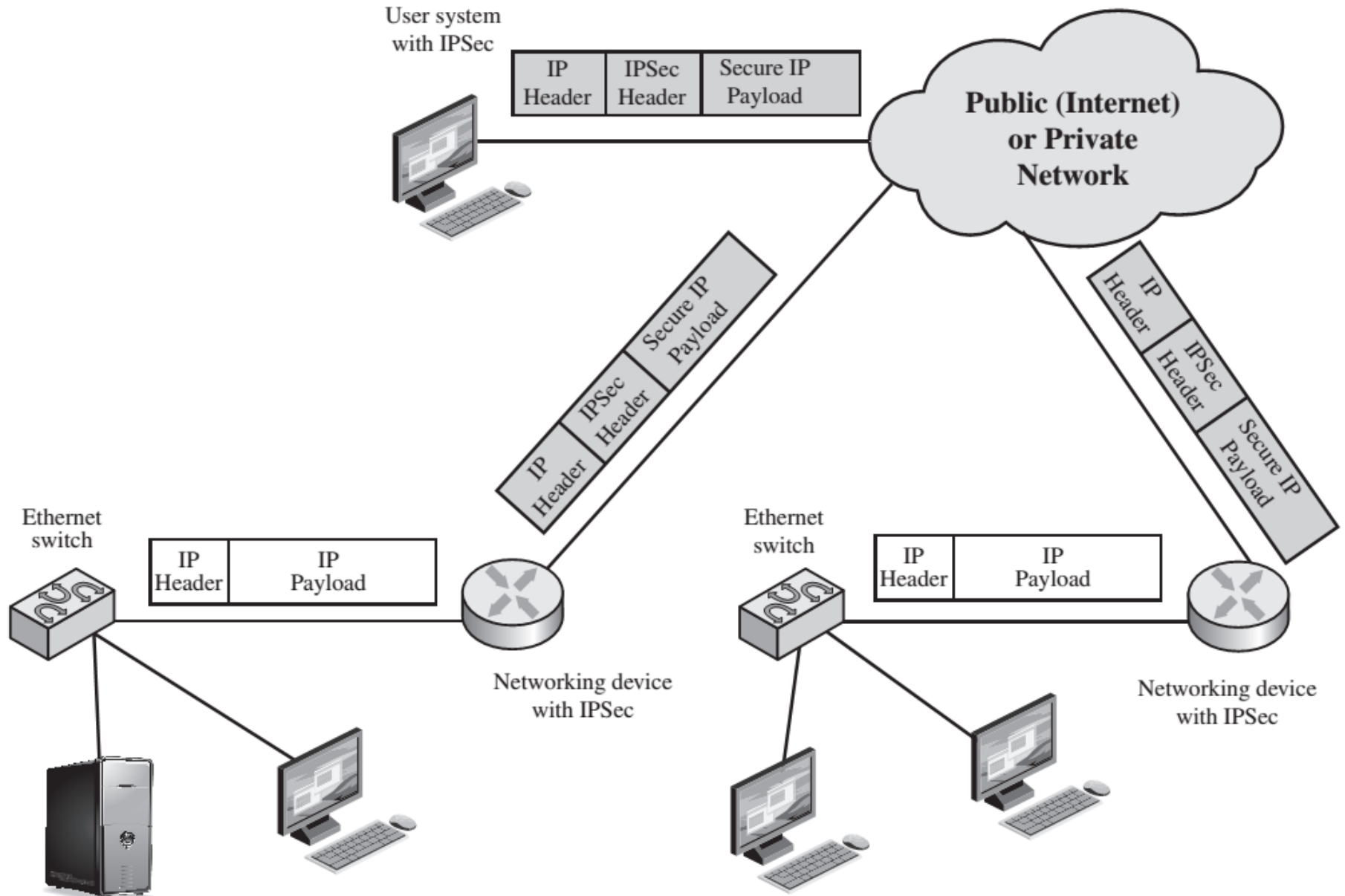
Figure 18.1 *TCP/IP Protocol Suite and IPSec*



IPSec

- A collection of protocols used to create VPNs
- A network layer security protocol providing cryptographic security services that can support various combinations of authentication, integrity, access control, and confidentiality
- Allows creation of an encrypted tunnel between two private networks
- Supports authentication of the two ends of the tunnel
- Cannot directly encrypt non-IP traffic
- Comprises of IKE, ESP, and AH

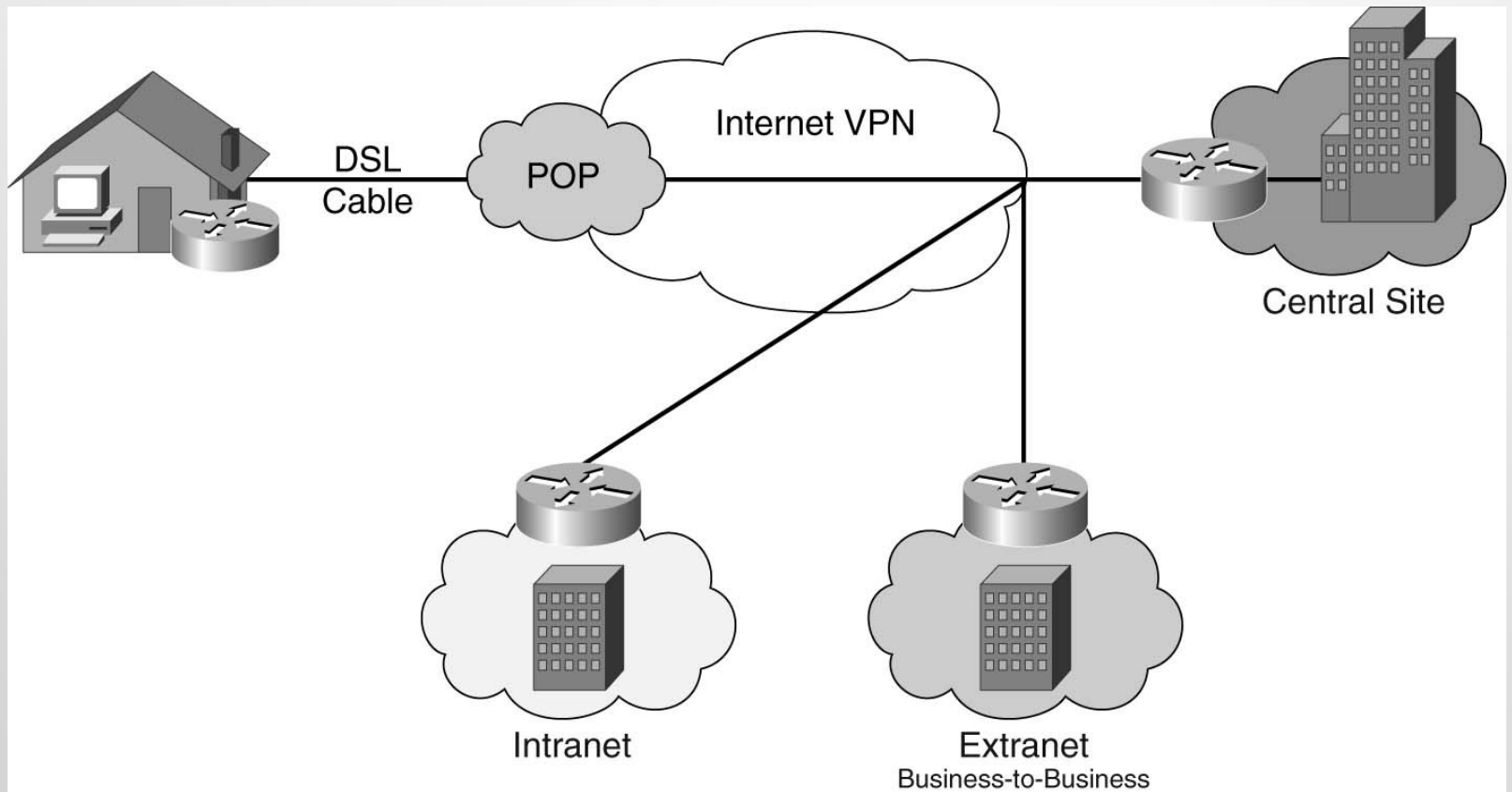
Skenario Keamanan IP



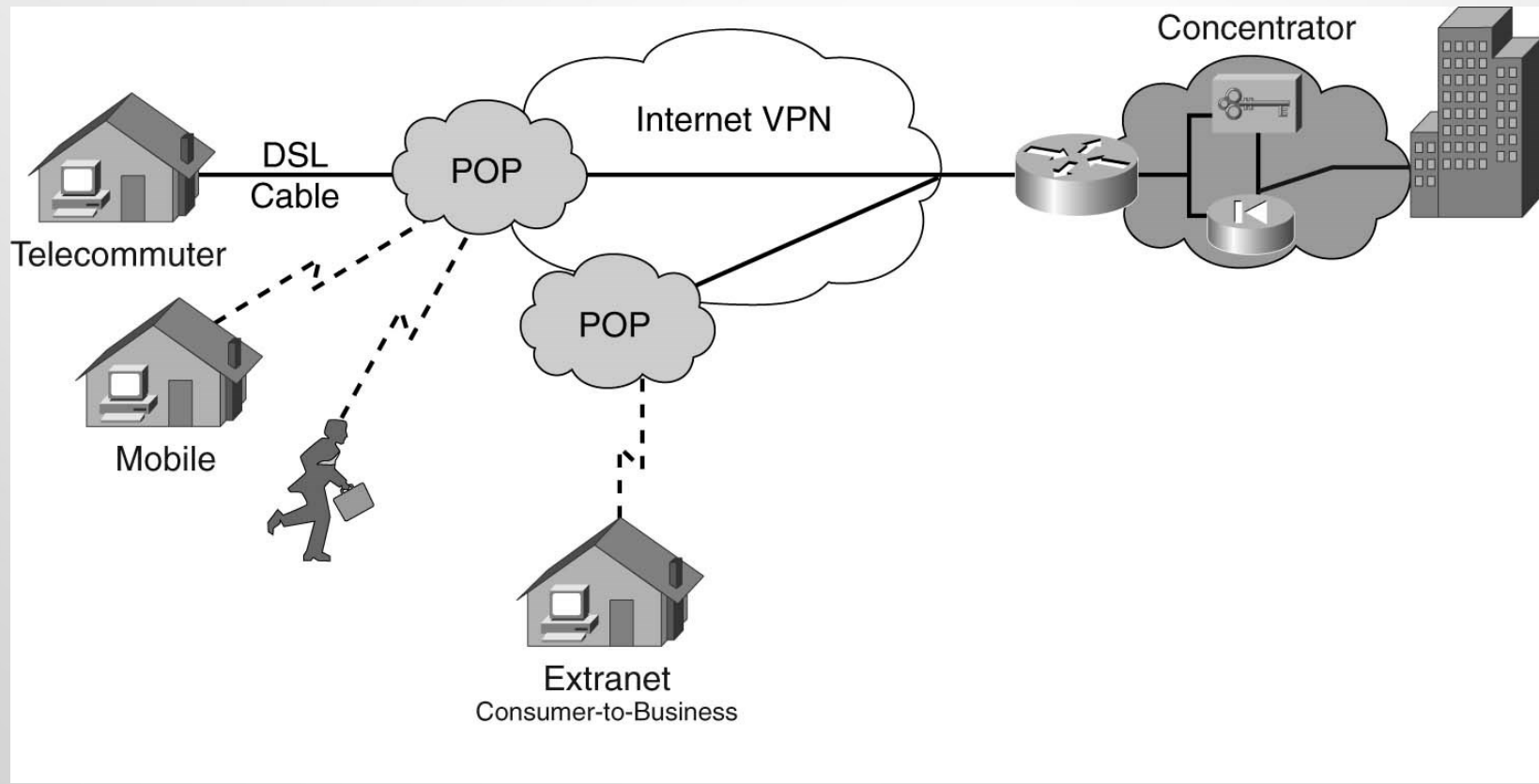
Tipe IPsec VPN

- LAN-to-LAN or site-to-site
 - Used to connect two private networks to form one combined virtual private network
- Remote-access client IPsec
 - Used to allow road warriors to be part of the trusted network

LAN-to-LAN atau Site-to-Site



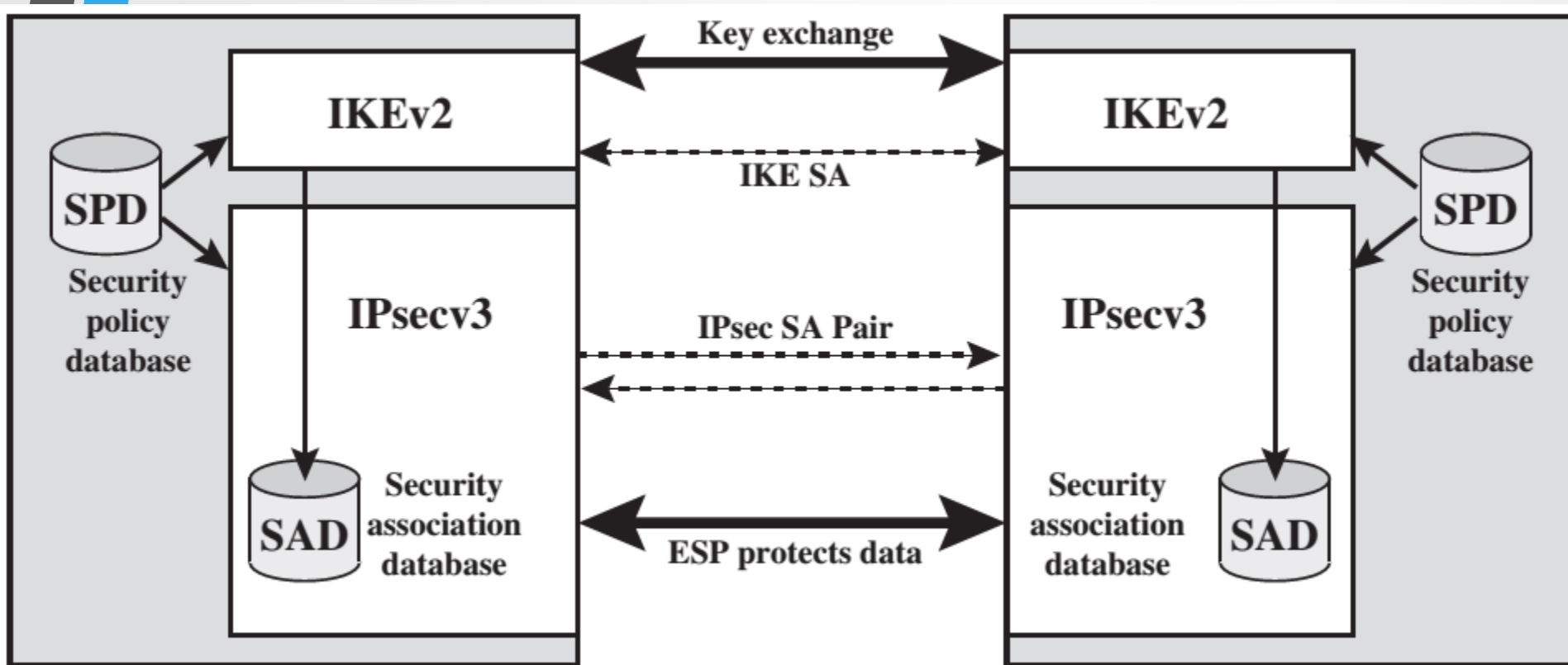
Remote-Access IPsec



Susunan Protokol IPsec


- Internet Key Exchange (IKE) protocol
 - For negotiating security parameters and establishing authenticated keys
 - Uses UDP port 500 for ISAKMP
- Encapsulating Security Payload (ESP) protocol
 - For encrypting, authenticating, and securing data
 - IP protocol 50
- Authentication Header (AH) protocol
 - For authenticating and securing data
 - IP protocol 51

Arsitektur IPSec



Definisi Security Association

- SA is uniquely identified by 3 parameters
- Security parameters index (SPI)
 - 32-bit unsigned integer assigned to this SA,
 - Enable the receiving system to select the SA under which a received packet will be processed
- IP destination address
 - Address of the destination endpoint of the SA
 - An end-user system or a network system
- Security protocol identifier
 - Indicates whether the association is an AH or ESP SA

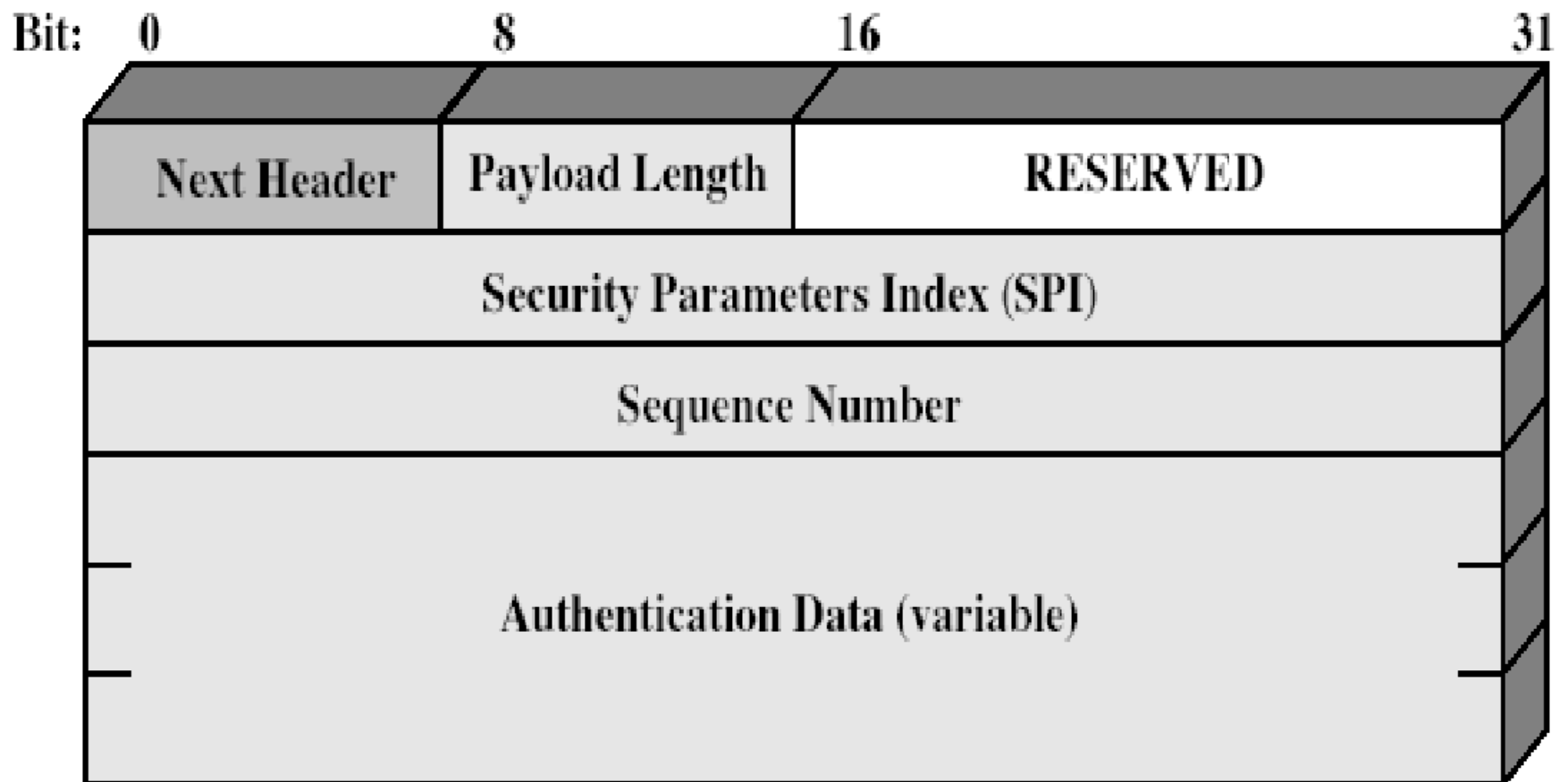


AH dan ESP

Authentication Header (AH)

- provides support for data integrity & authentication of IP packets
 - end system/router can authenticate user/app
 - prevents address spoofing attacks by tracking sequence numbers
- based on use of a *MAC*
 - HMAC-MD5-96 or HMAC-SHA-1-96
- parties must share a secret key

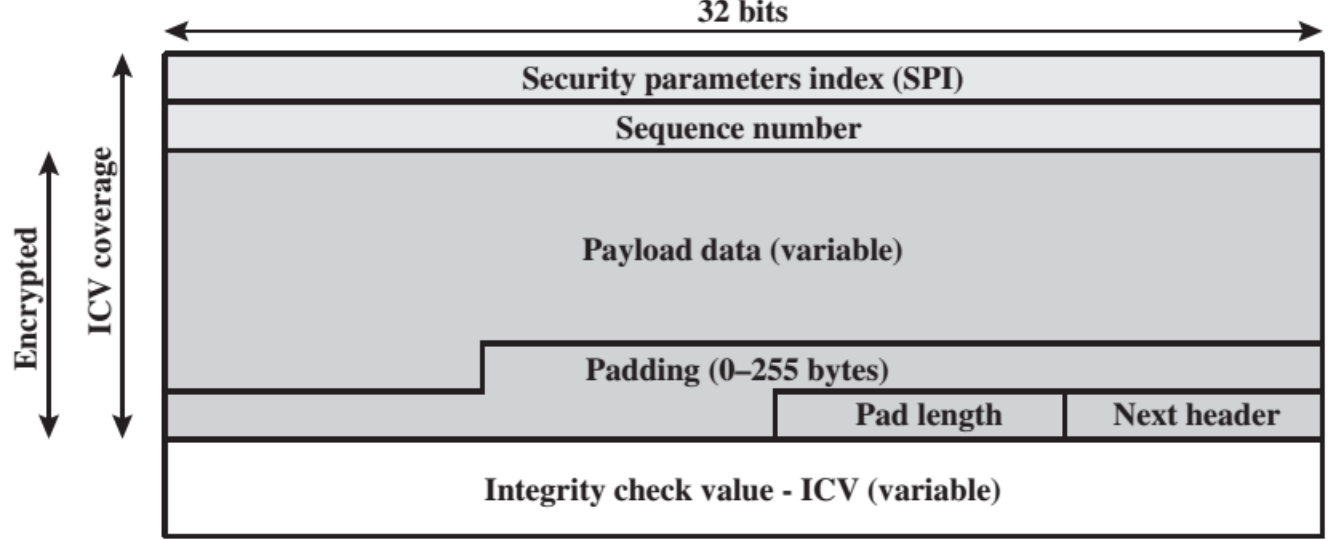
Authentication Header



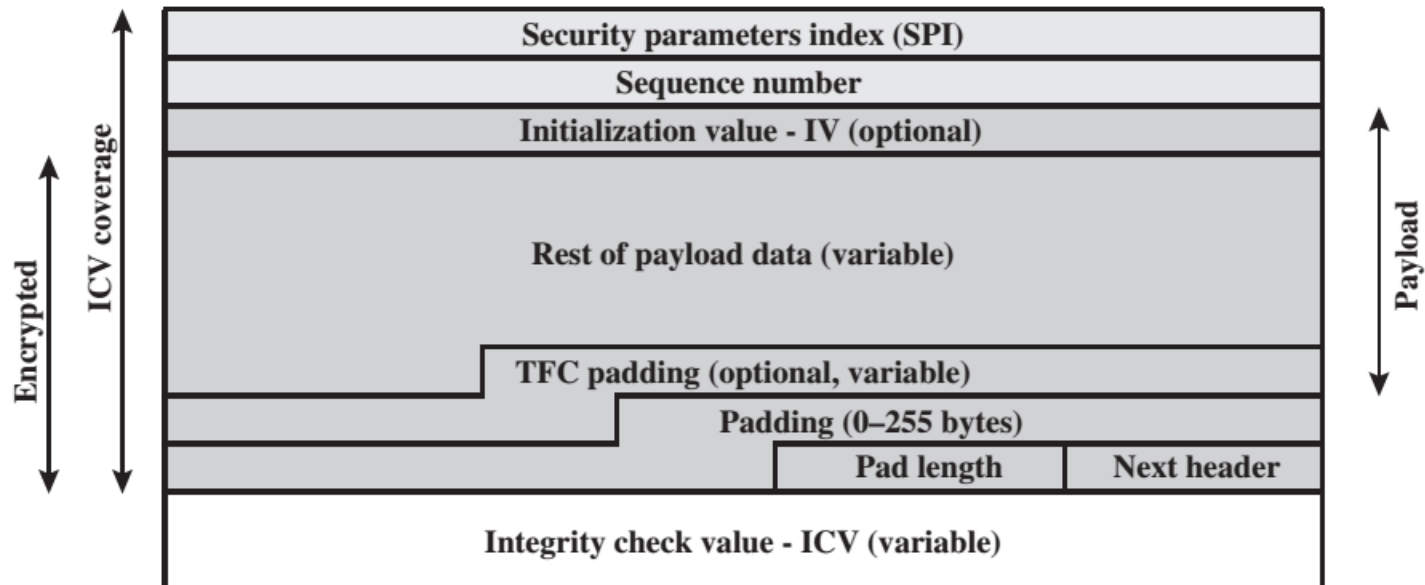
Encapsulating Security Payload (ESP)

- provides message content confidentiality & limited traffic flow confidentiality
- can optionally provide the same authentication services as AH
- supports range of ciphers, modes, padding
 - incl. DES, Triple-DES, RC5, IDEA, CAST etc
 - CBC most common
 - pad to meet blocksize, for traffic flow

Format Packet ESP



(a) Top-level format of an ESP Packet

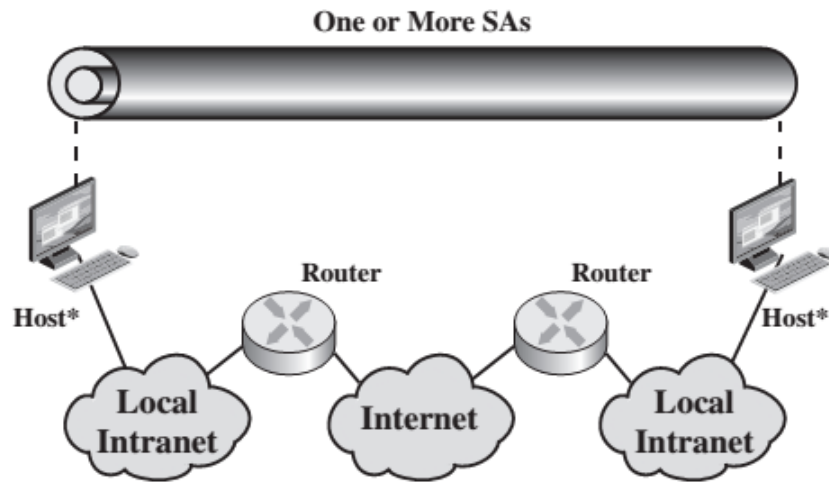


(b) Substructure of payload data

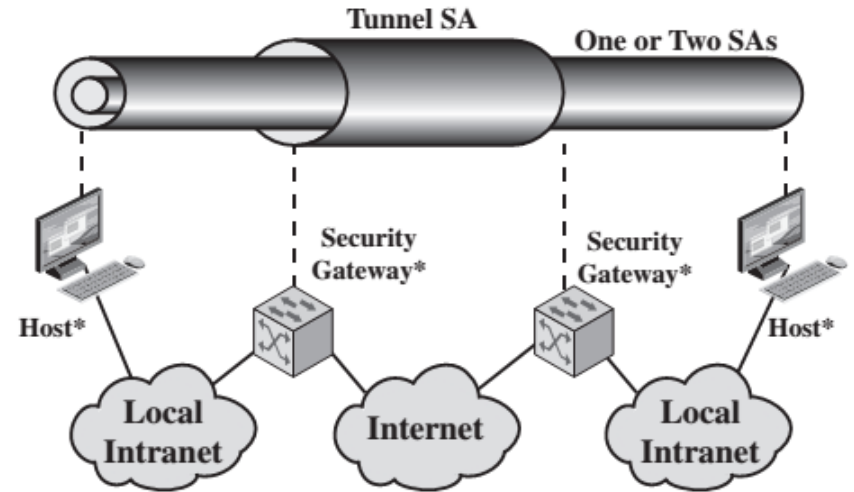
Penggabungan Security Association

- SA's can implement either AH or ESP
- to implement both need to combine SA's
 - form a security bundle
- have 4 cases (see next)

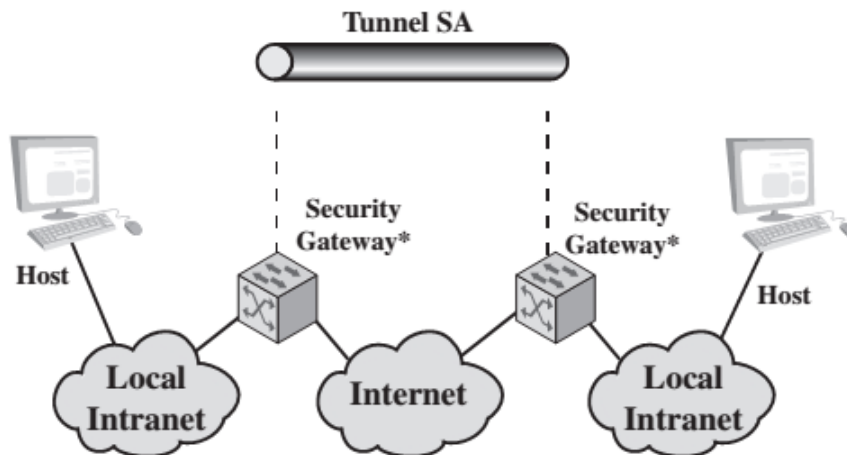
Kombinasi Dasar SA



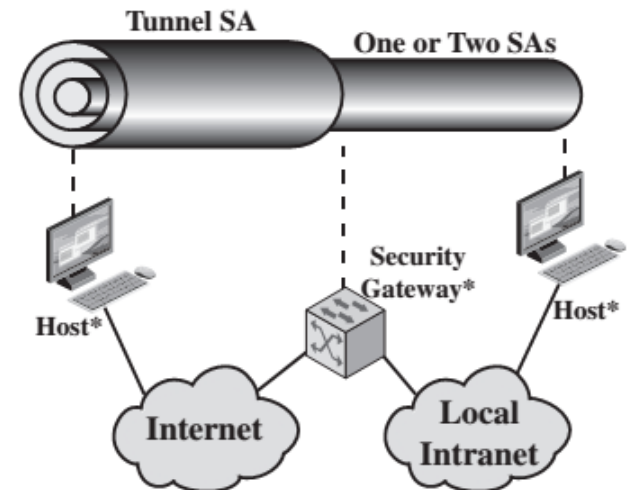
(a) Case 1



(c) Case 3



(b) Case 2



(d) Case 4



Mode Transpor vs Tunnel

Mode Transport

In transport mode, IPSec protects what is delivered from the transport layer to the network layer.

IPSec in transport mode does not protect
the IP header;
it only protects the information
coming from the transport layer.

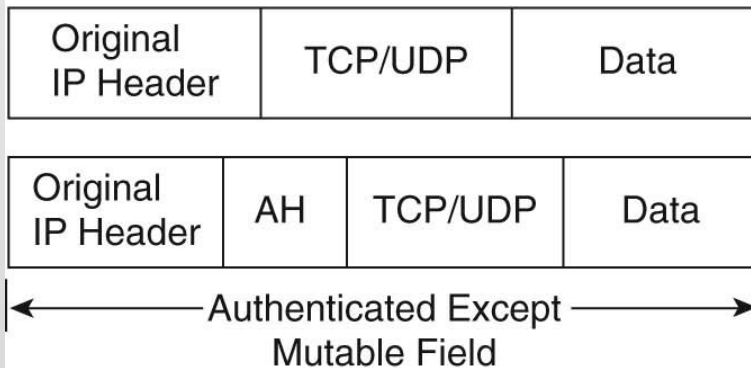
Mode Tunnel

In tunnel mode, IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header.

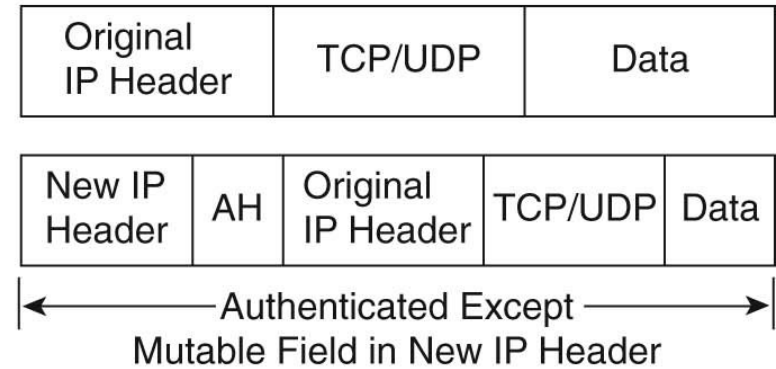
IPSec in tunnel mode protects the original IP header.

Format Paket Menggunakan AH pada Mode Tunnel dan Transpor

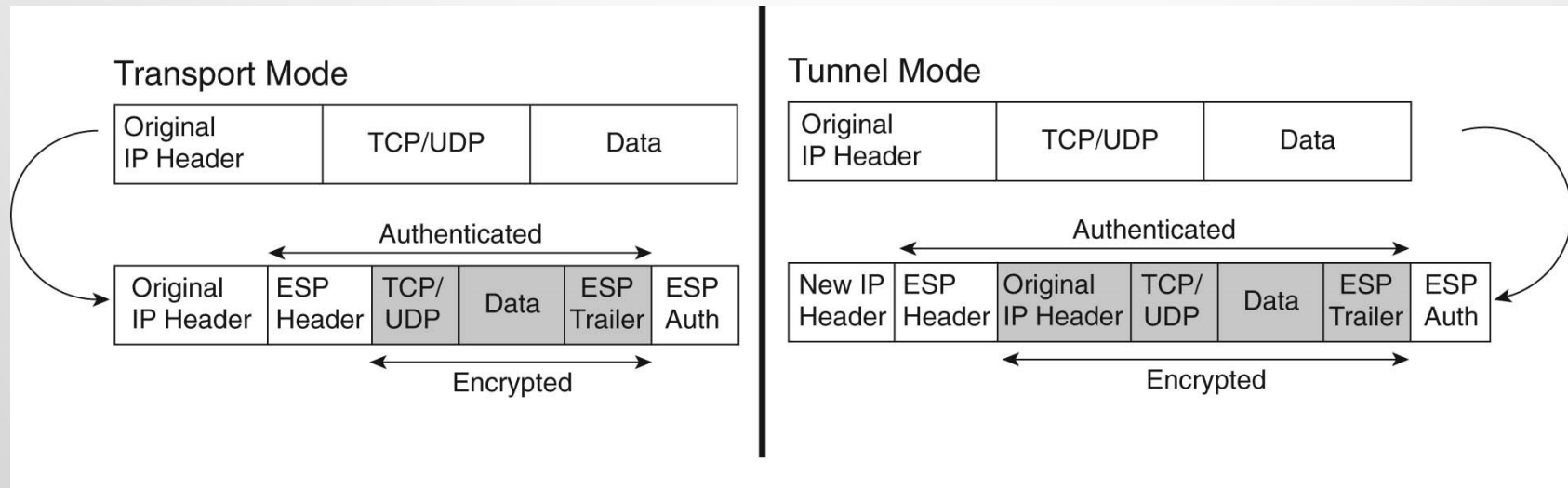
Transport Mode



Tunnel Mode



Format Paket Menggunakan ESP pada Mode Tunnel dan Transpor





Internet Key Exchange

IKE pada Protokol IPSec

- Negotiates IPsec tunnel characteristics between two IPsec peers
- Negotiates IPsec protocol parameters
- Exchanges public keys
- Authenticates both sides
- Manages keys after the exchange
- Automates entire key-exchange process

Komposisi IKE

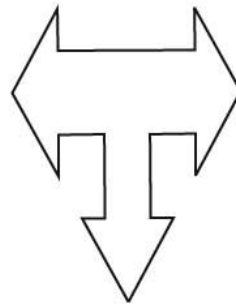
IKE (Internet Key Exchange) (RFC 2409)
Is a Hybrid Protocol

SKEME

Mechanism for Utilizing
Public Key Encryption for Authentication

Oakley

Modes Based Mechanism for
Arriving At an Encryption Key
Between Two Peers



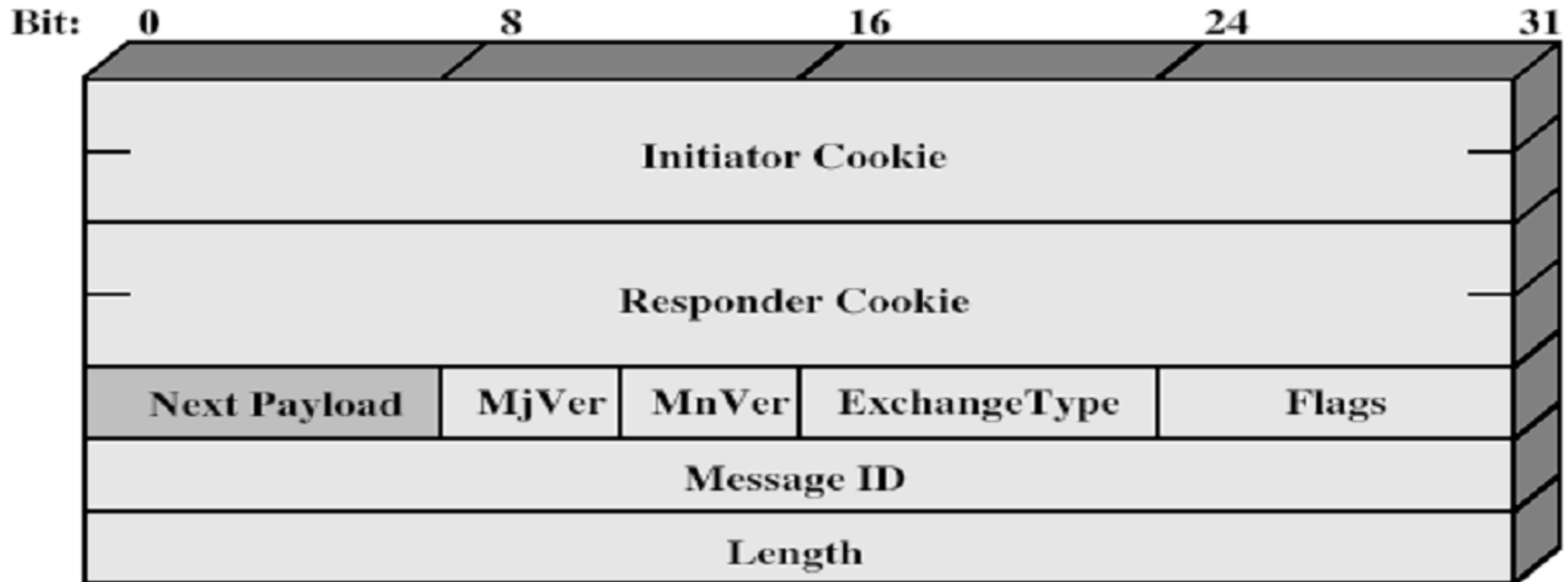
ISAKMP

Architecture for Message Exchange
Including Packet Formats
and State Transitions Between
Two Peers

ISAKMP

- Internet Security Association and Key Management Protocol
- provides framework for key management
- defines procedures and packet formats to establish, negotiate, modify, & delete SAs
- independent of key exchange protocol, encryption alg, & authentication method

ISAKMP



(a) ISAKMP Header



(b) Generic Payload Header

Algoritma Diffie-Hellman

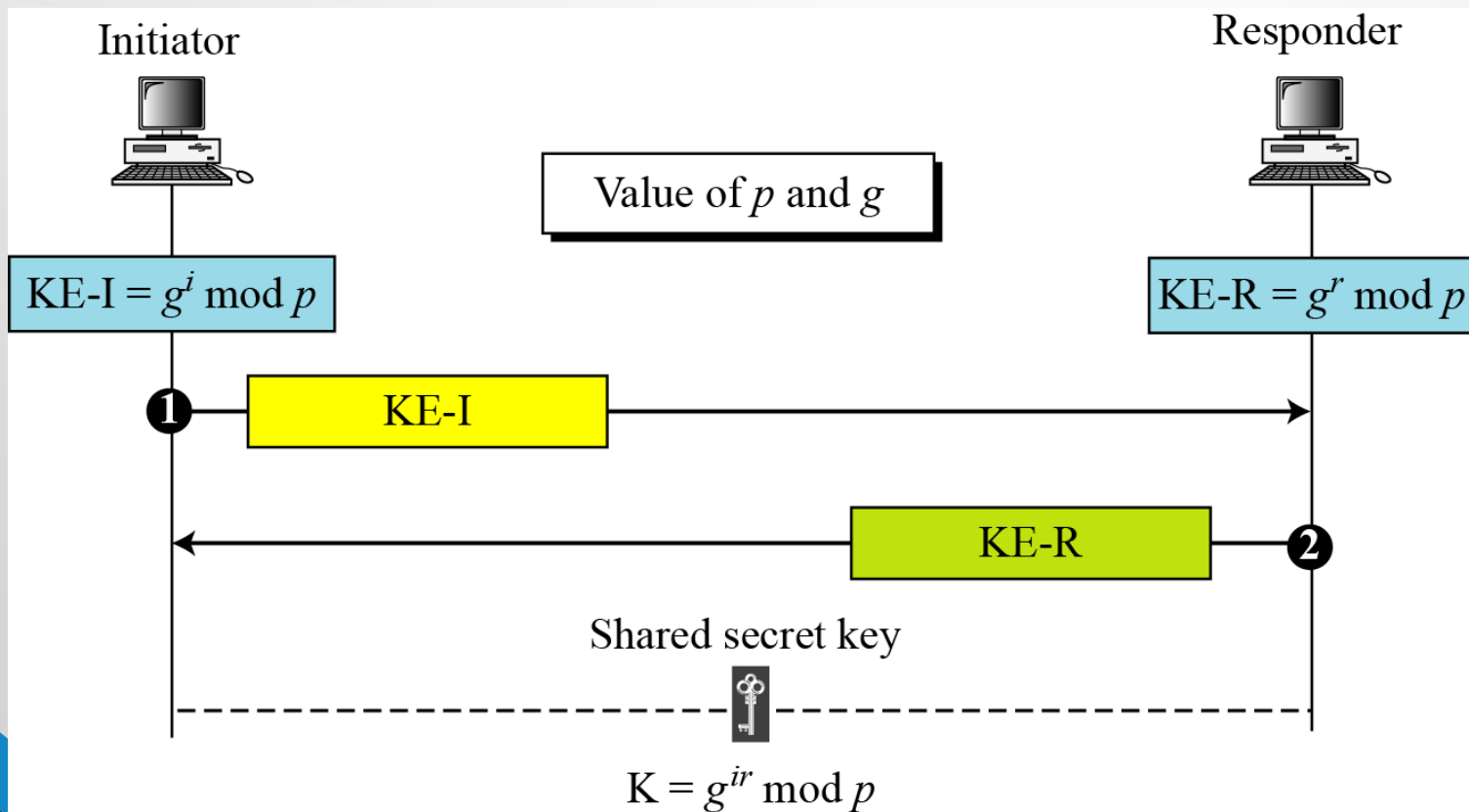
- Used in IKE by two peers to generate a shared DH secret and to generate keying material for later use
- DH secret also used with preshared secret to authenticate two peers to each other

Algoritma Diffie-Hellman

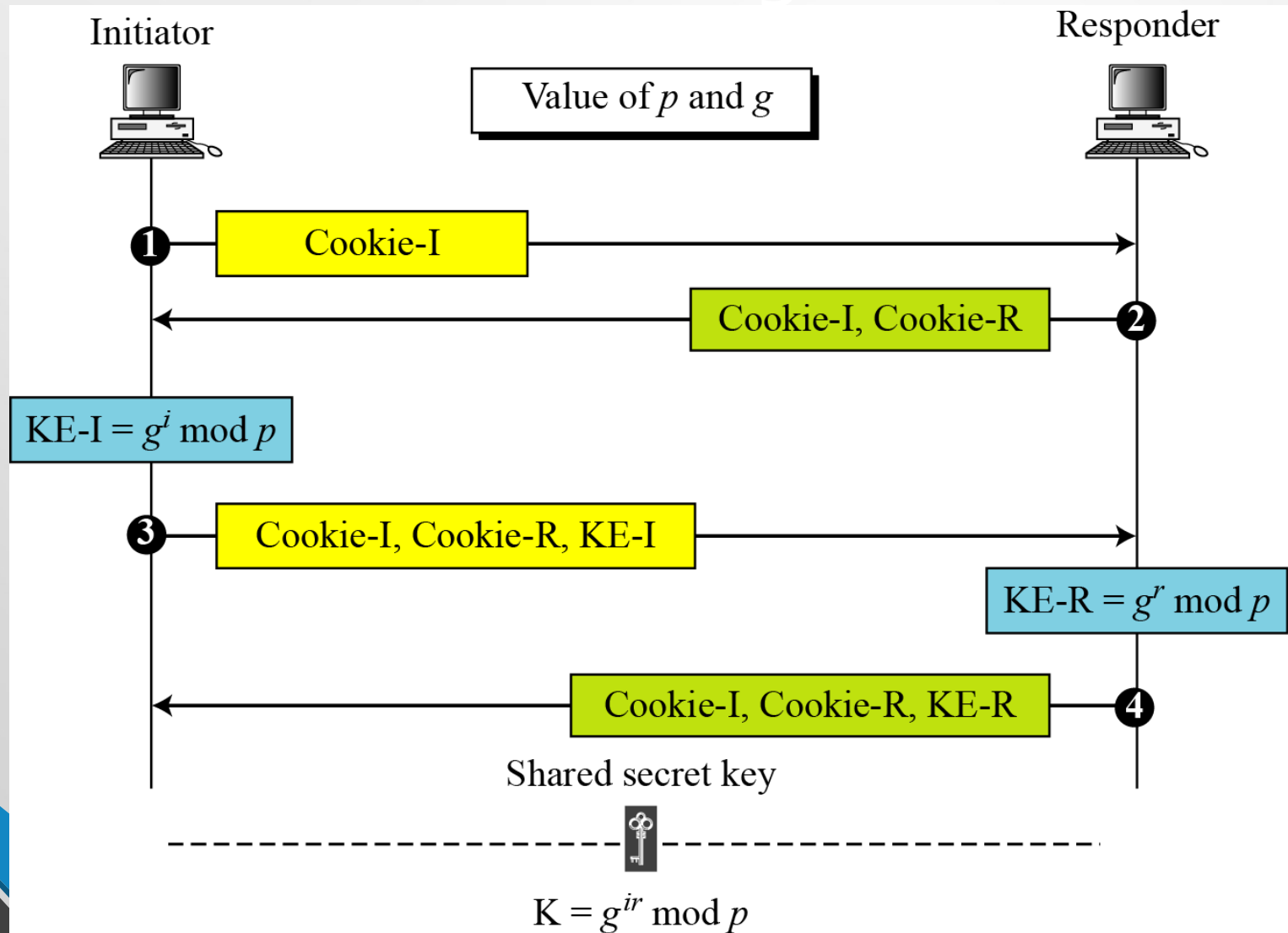
- There exists Y_a such that $Y_a = g^i \bmod p$ where g is the generator, p is a large prime number, and i is a private secret known only to the initiator
- There exists Y_b such that $Y_b = g^r \bmod p$ where g is the generator, p is a large prime number, and r is a private secret known only to the responder
- Initiator and responder can generate a shared secret known only to the two of them by exchanging the values Y_a and Y_b with each other
- Initiator secret = $(Y_b)^i \bmod p = (Y_a)^r \bmod p = \text{responder secret} = g^{ir}$

Algoritma Diffie-Hellman

Figure 18.16 *Diffie-Hellman key exchange*



Diffie-Hellman dengan Cookies



Perbaikan Diffie-Hellman

Note

To protect against a clogging attack, IKE uses cookies.

Note

To protect against a replay attack, IKE uses nonces.

Note

To protect against man-in-the-middle attack, IKE requires that each party shows that it possesses a secret.

Fasa dan Mode IKE

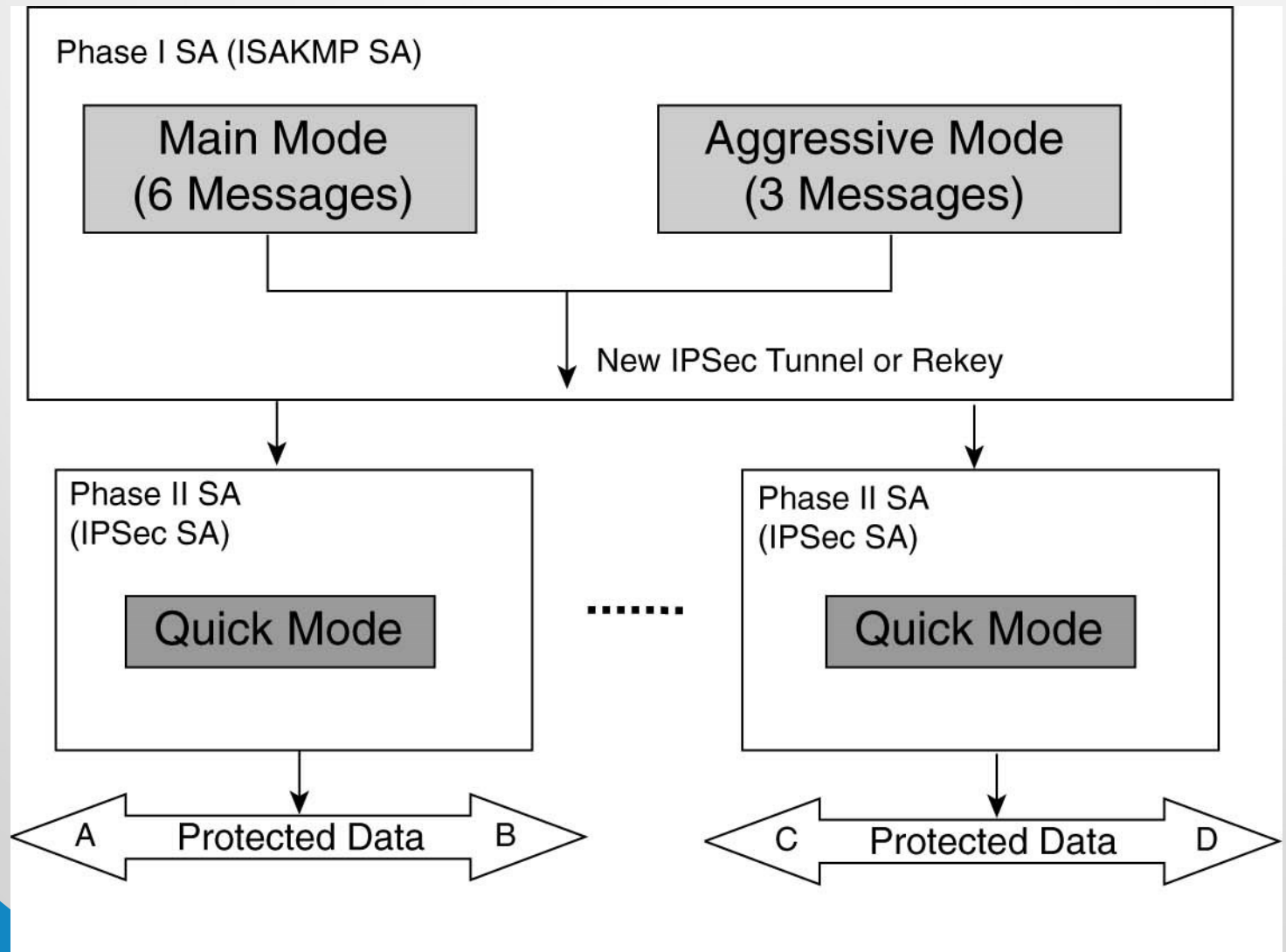
IKE has two phases:

- **IKE phase 1**
 - Uses *main* or *aggressive* mode exchange
 - Negotiates IKE SA
- **IKE phase 2**
 - Uses *quick* mode exchange
 - Negotiates IPsec SAs

Pembentukan IPsec Tunnel Menggunakan IKE

- Identify interesting traffic by an IPsec peer that has been configured to initiate an IPsec session for this traffic
- IPsec peers negotiate a secure authenticated communication channel using main mode or aggressive mode negotiation, resulting in creation of an IKE Security Association (SA) between the two IPsec peers (IKE phase I)
- Create two IPsec SAs between the two IPsec peers via IKE quick mode negotiation (IKE phase II)
- Send data over encrypted tunnel using ESP and/or AH encapsulation

IKE Mode Utama, Mode Agresif, dan Mode Cepat



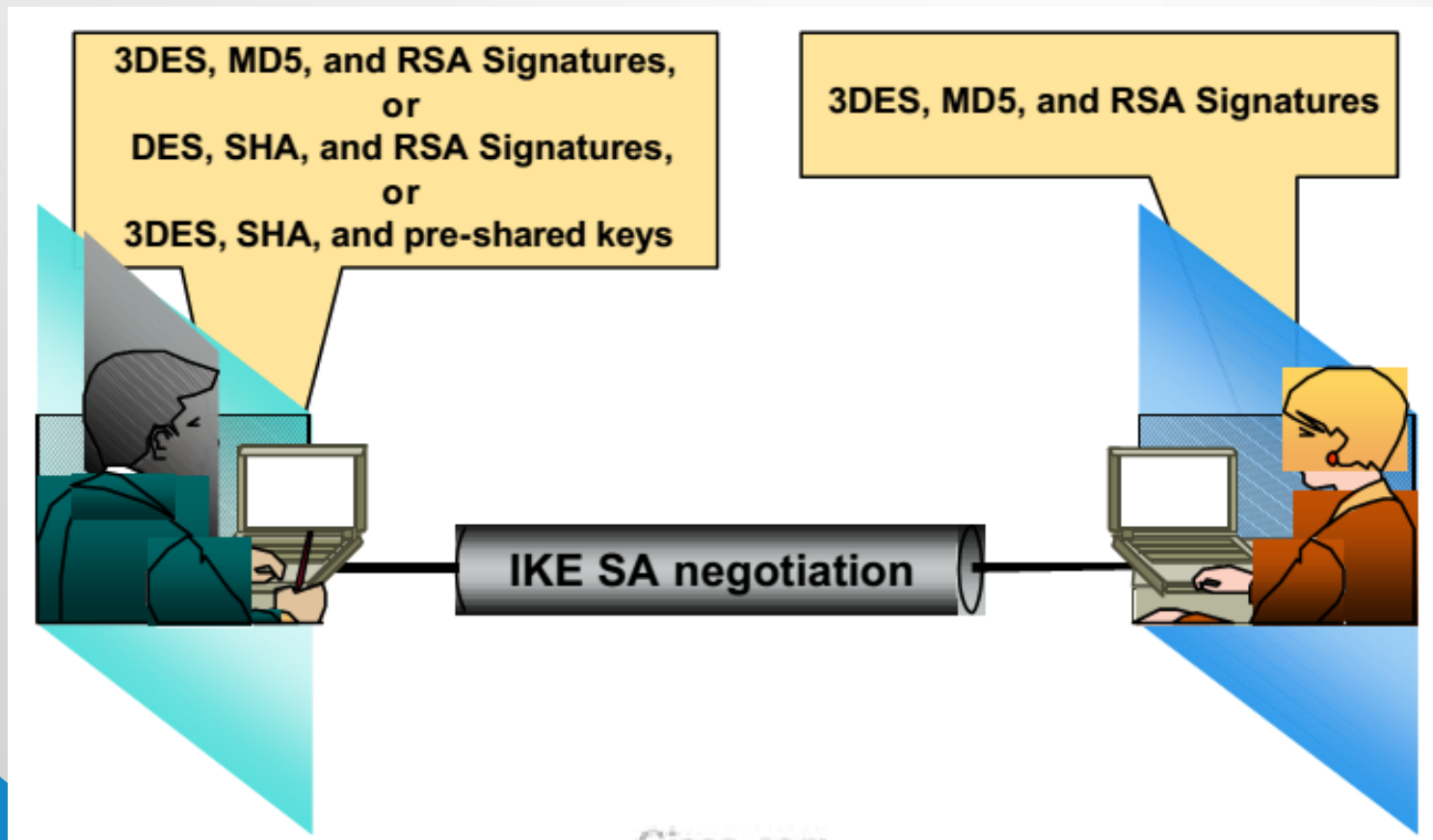


IKE Fasa I

Tujuan Mode Utama dan Mode Agresif

- Agreeing on a set of parameters that are to be used to authenticate the two peers
- Agreeing on parameters used to encrypt a portion of the main mode and all of the quick mode messages
- None of the aggressive mode messages are encrypted
- Authenticate the two peers to each other
- Generate keys used to generate keying material for subsequent encryption of data
- All of the parameters negotiated and the keys used to generate keys for encryption are stored as IKE or ISAKMP security association (SA)

Negosiasi IKE Fasa I



Kunci Sesi yang Dibangkitkan oleh Inisiator

Calculation of Three Keys (Initiator)

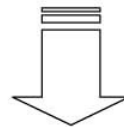
SKEYID_d — Used to Calculate Subsequent IPsec Keying Material

SKEYID_a — Used to Provide Data Integrity and Authentication to IKE Messages

SKEYID_e — Used to Encrypt IKE Messages

PRF = A Pseudo
Random Function Based
on the Negotiated Hash

$SKEYID = PRF(\text{Pre-shared Key}, N_i \parallel N_r)$



$SKEYID_d = PRF(SKEYID, g^{ab} \parallel CKY-I \parallel CKY-R \parallel 0)$

$SKEYID_a = PRF(SKEYID, SKEYID_d \parallel g^{ab} \parallel CKY-I \parallel CKY-R \parallel 1)$

$SKEYID_e = PRF(SKEYID, SKEYID_a \parallel g^{ab} \parallel CKY-I \parallel CKY-R \parallel 2)$

Kunci Sesi yang Dibangkitkan oleh Responder

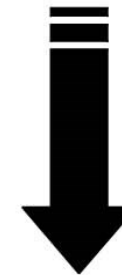
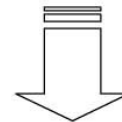
Calculation of Three Keys (Responder)

SKEYID_d — Used to Calculate Subsequent IPsec Keying Material

SKEYID_a — Used to Provide Data Integrity and Authentication to IKE Messages

SKEYID_e — Used to Encrypt IKE Messages

$$\text{SKEYID} = \text{PRF}(\text{Pre-shared Key}, N_i \parallel N_r)$$



$$\text{SKEYID}_d = \text{PRF}(\text{SKEYID}, g^{ab} \parallel \text{CKY-I} \parallel \text{CKY-R} \parallel 0)$$

$$\text{SKEYID}_a = \text{PRF}(\text{SKEYID}, \text{SKEYID}_d \parallel g^{ab} \parallel \text{CKY-I} \parallel \text{CKY-R} \parallel 1)$$

$$\text{SKEYID}_e = \text{PRF}(\text{SKEYID}, \text{SKEYID}_a \parallel g^{ab} \parallel \text{CKY-I} \parallel \text{CKY-R} \parallel 2)$$

Penyelesaian IKE Fasa I (Mode Utama) Menggunakan Kunci Preshared

- IKE SA established
- Main mode using preshared key authentication completed
- Quick mode will be used to negotiate parameters of IPsec SA

Fasa I: Mode Utama

Figure 18.20

*Main mode,
preshared secret-
key method
Metoda Enkripsi
IPSec*

- *Data
Encryption
Standard
(DES)*
- *Triple DES
(3DES)*


KE-I (KE-R): Initiator's (responder's) half-key

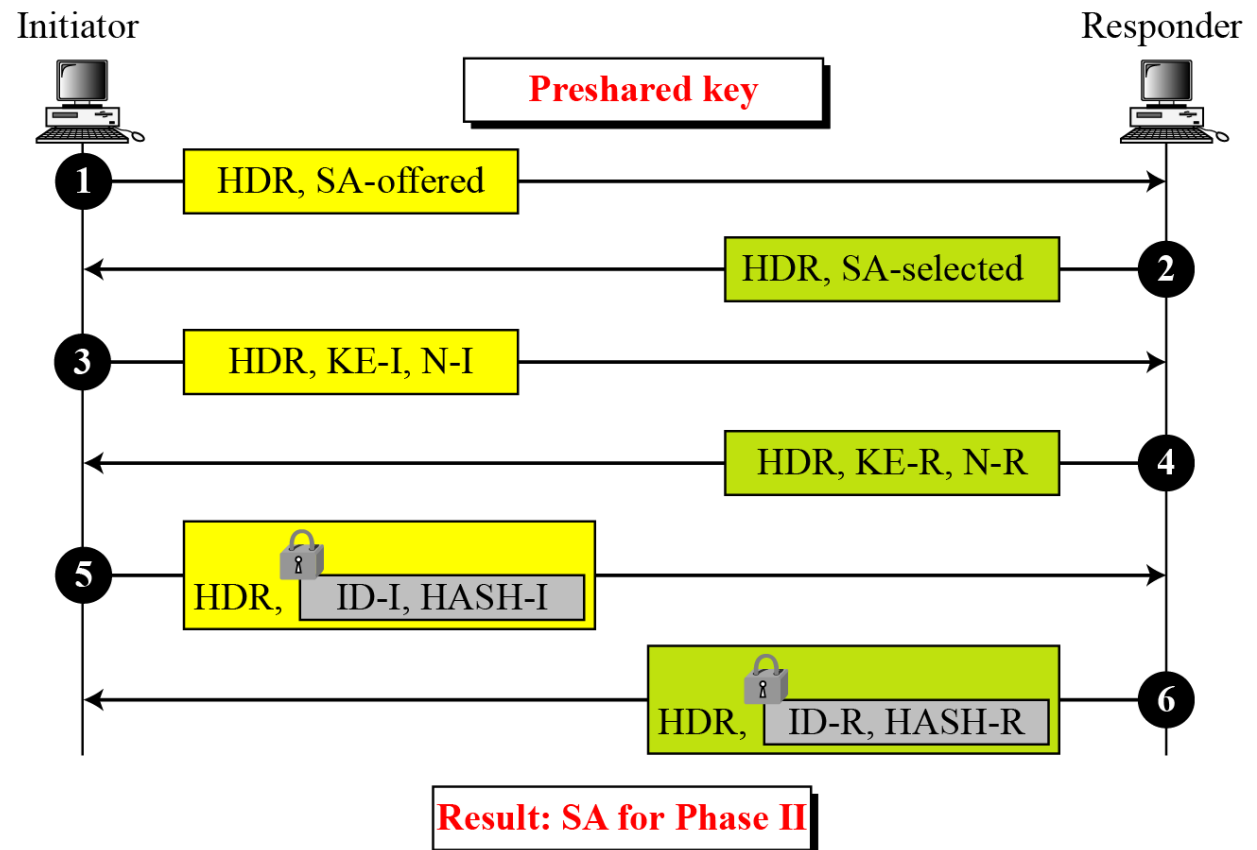
N-I (N-R): Initiator's (responder's) nonce

ID-I (ID-R): Initiator's (responder's) ID

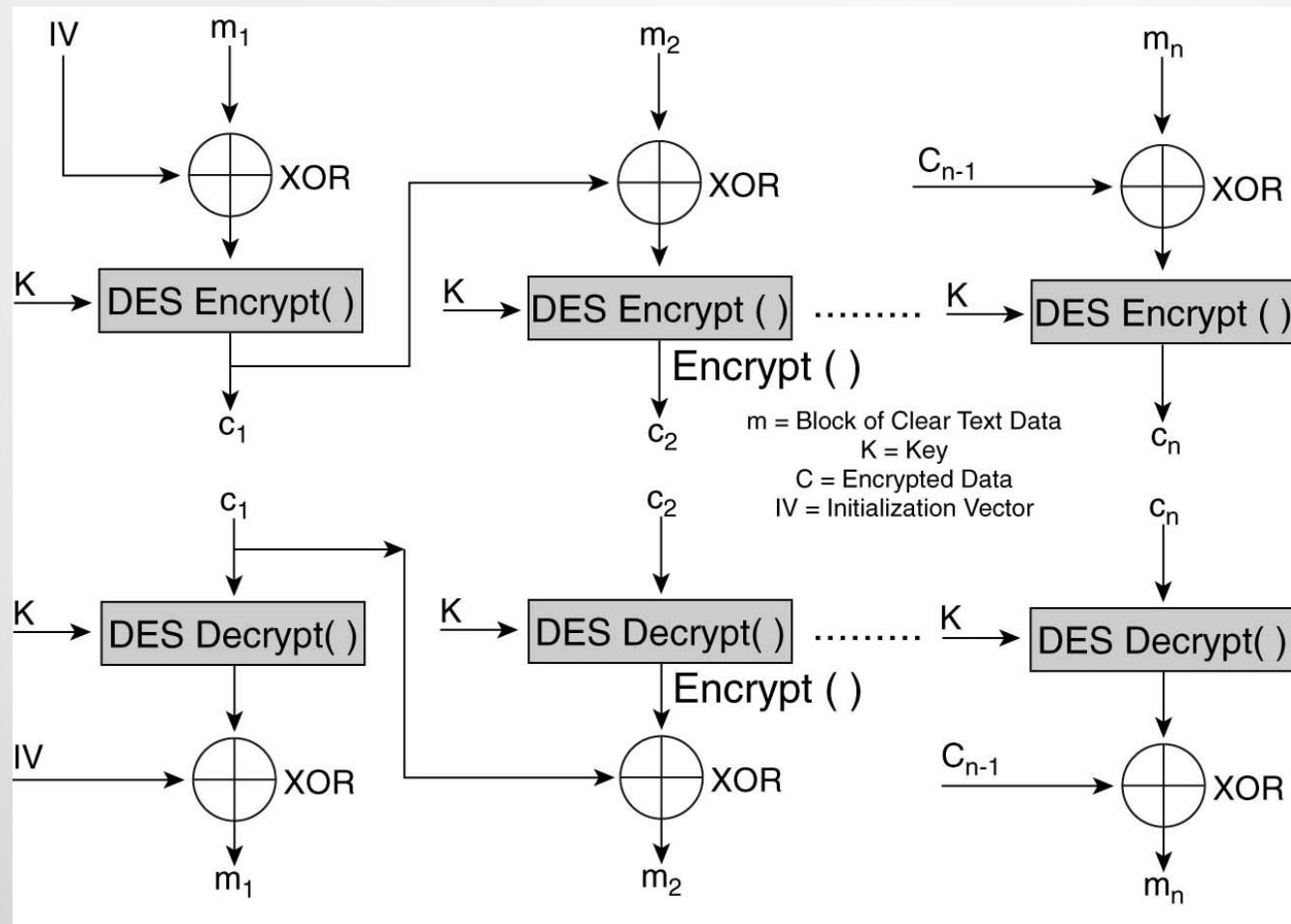
HASH-I (HASH-R): Initiator's (responder's) hash

HDR: General header including cookies

 Encrypted with SKEYID_e

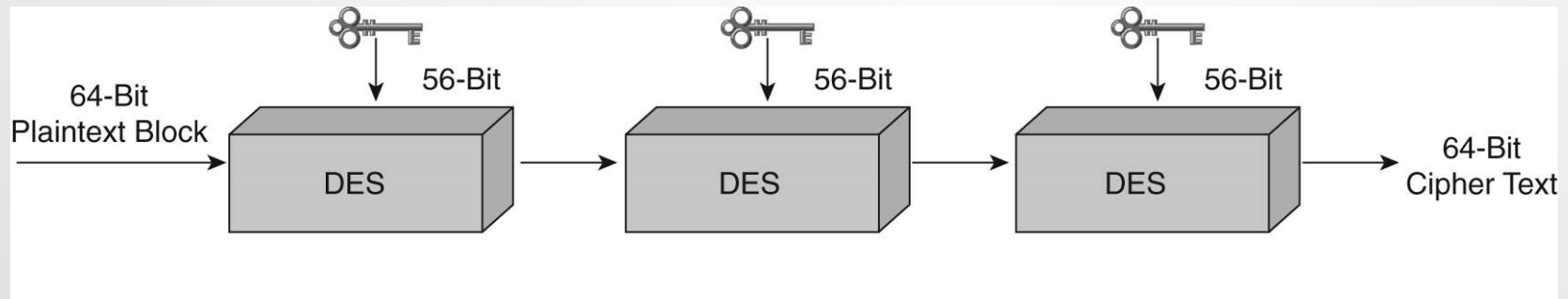


Enkripsi DES Menggunakan Perantaraan Blok Cipher (CBC)



- Cipher block: DES encryption algorithm converting fixed-length message into cipher text of same length
- block size of DES is 64 bits while key length is 56 bits
- Initialization vector is sent in ESP header

Enkripsi 3DES



Overall key length is 168 bits

Fasa I: Mode Utama

Figure 18.21 *Main mode, original public-key method*




HDR: General header including cookies

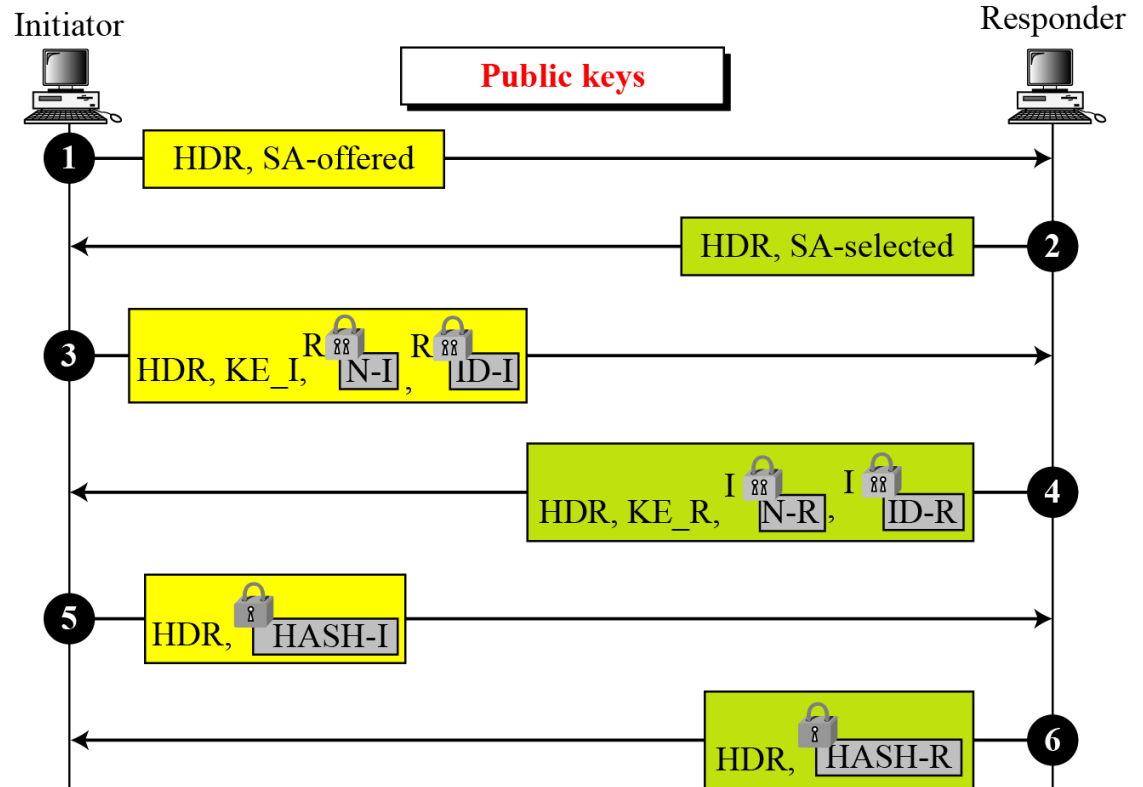
KE-I (KE-R): Initiator's (responder's) half-key

N-I (N-R): Initiator's (responder's) nonce

ID-I (ID-R): Initiator's (responder's) ID

HASH-I (HASH-R): Initiator's (responder's) hash

I  Encrypted with initiator's public key
R  Encrypted with responder's public key
 Encrypted with SKEYID_e



Result: SA for Phase II

Pembangkitan Kunci Sesi oleh Inisiator pada Metoda Tandatangan Digital

Calculation of Three Keys (Initiator)

SKEYID_d — Used to Calculate Subsequent IPsec Keying Material

SKEYID_a — Used to Provide Data Integrity and Authentication to IKE Messages

SKEYID_e — Used to Encrypt IKE Messages

PRF = A Pseudo
Random Function Based
on the Negotiated Hash

$\text{SKEYID} = \text{PRF}(\text{Pre-shared Key}, N_i \parallel N_r)$

$\text{SKEYID}_d = \text{PRF}(\text{SKEYID}, g^{ab} \parallel \text{CKY-I} \parallel \text{CKY-R} \parallel 0)$

$\text{SKEYID}_a =$
 $\text{PRF}(\text{SKEYID}, \text{SKEYID}_d \parallel g^{ab} \parallel \text{CKY-I} \parallel \text{CKY-R} \parallel 1)$

$\text{SKEYID}_e =$
 $\text{PRF}(\text{SKEYID}, \text{SKEYID}_a \parallel g^{ab} \parallel \text{CKY-I} \parallel \text{CKY-R} \parallel 2)$

Pembangkitan Kunci Sesi oleh Responder pada Metoda Tandatangan Digital

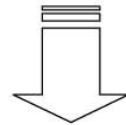
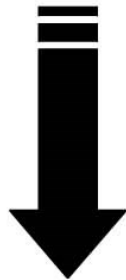
Calculation of Three Keys (Responder)

SKEYID_d — Used to Calculate Subsequent IPsec Keying Material

SKEYID_a — Used to Provide Data Integrity and Authentication to IKE Messages

SKEYID_e — Used to Encrypt IKE Messages

$$\text{SKEYID} = \text{PRF} (N_i \parallel N_r \parallel g^{ab})$$



$$\text{SKEYID}_d = \text{PRF} (\text{SKEYID}, g^{ab} \parallel \text{CKY-I} \parallel \text{CKY-R} \parallel 0)$$

$$\text{SKEYID}_a = \text{PRF} (\text{SKEYID}, \text{SKEYID}_d \parallel g^{ab} \parallel \text{CKY-I} \parallel \text{CKY-R} \parallel 1)$$

$$\text{SKEYID}_e = \text{PRF} (\text{SKEYID}, \text{SKEYID}_a \parallel g^{ab} \parallel \text{CKY-I} \parallel \text{CKY-R} \parallel 2)$$

Fasa I: Mode Utama

Figure 18.23 *Main mode, digital signature method*

HDR: General header including cookies

Sig-I: Initiator's signature on messages 1-4


Sig-R: Initiator's signature on messages 1-5

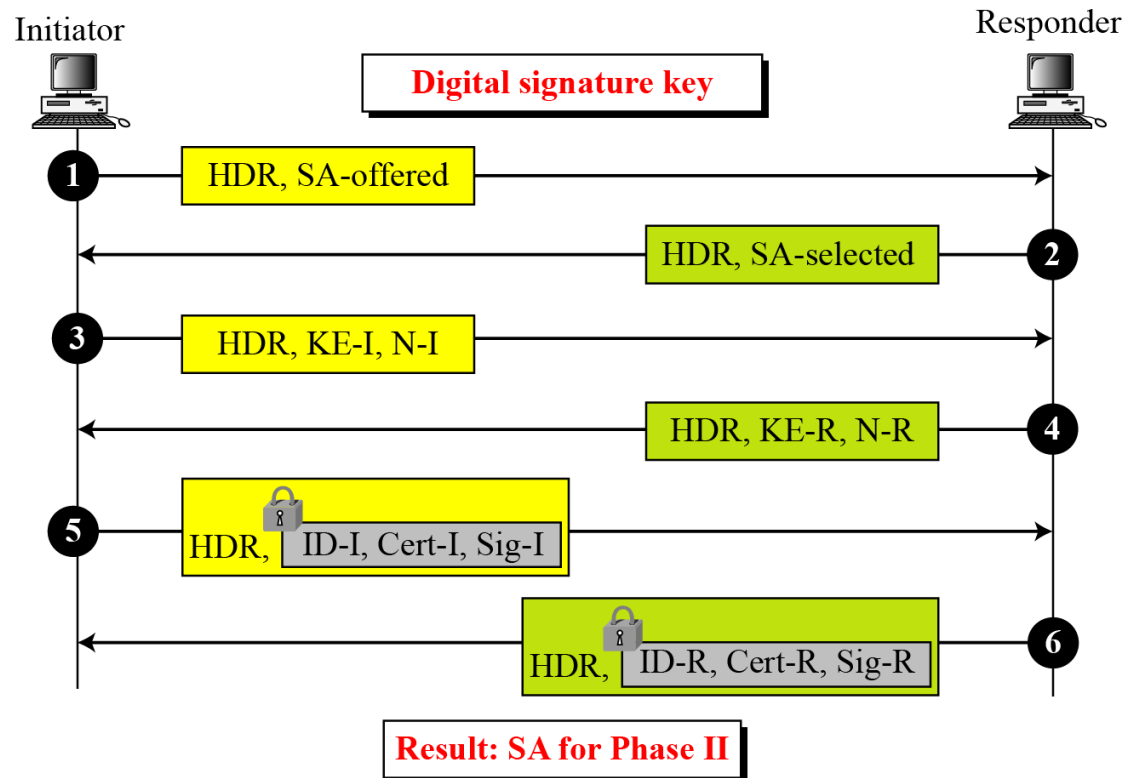
Cert-I (Cert-R): Initiator's (responder's) certificate

N-I (N-R): Initiator's (responder's) nonce

KE-I (KE-R): Initiator's (responder's) half-key

ID-I (ID-R): Initiator's (responder's) ID

 Encrypted with SKEYID_e





IKE Fasa II

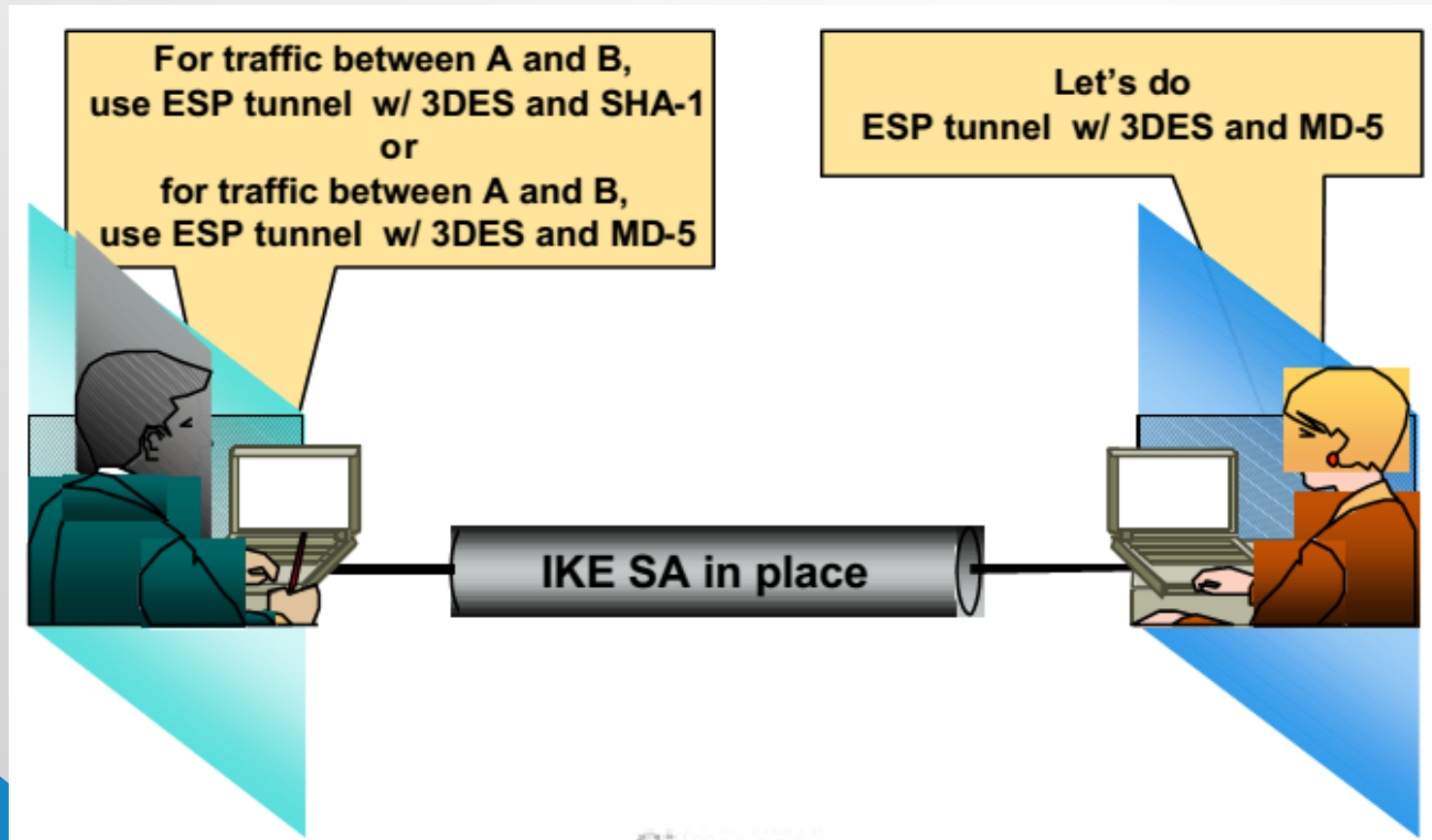
Fasa II IKE (Mode Cepat)

- Negotiate parameters of IPsec SA
- Perfect Forward Secrecy (PFS) may be used by initiator to request that a new DH secret be generated over an encrypted channel
 - New nonces generated: N_i' and N_r'
 - New DH public values:
 - $X_a' = g^a \text{ mod } p$
 - $X_b' = g^b \text{ mod } p$

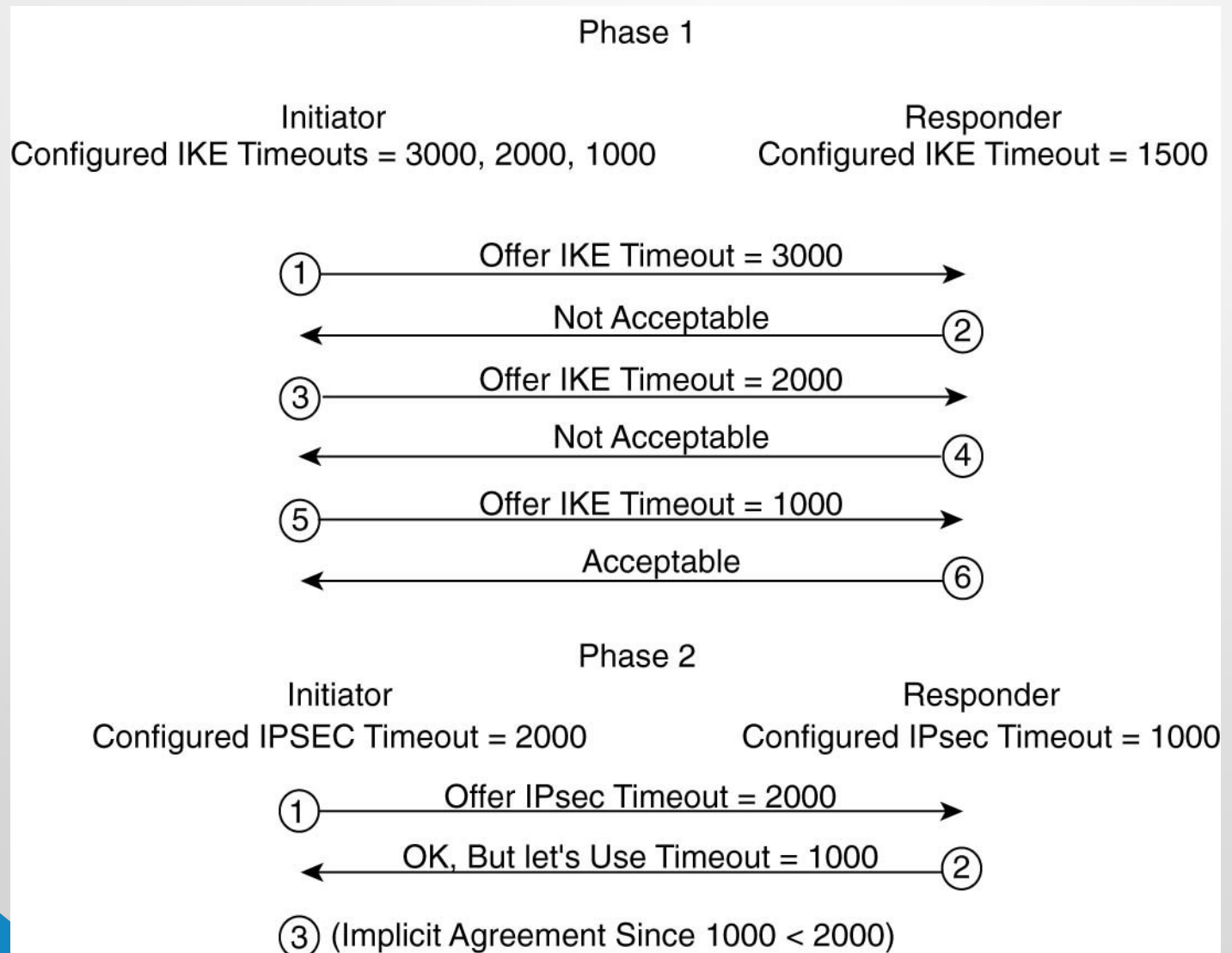
Tujuan Mode Cepat

- To have two peers agree on a set of attributes for creating the IPsec security associations that could be used by ESP to encrypt the data
- To redo Diffie-Hellman (DH) exchange so that new keying material can be used to generate IPsec encryption keys

Negosiasi IKE Fasa II



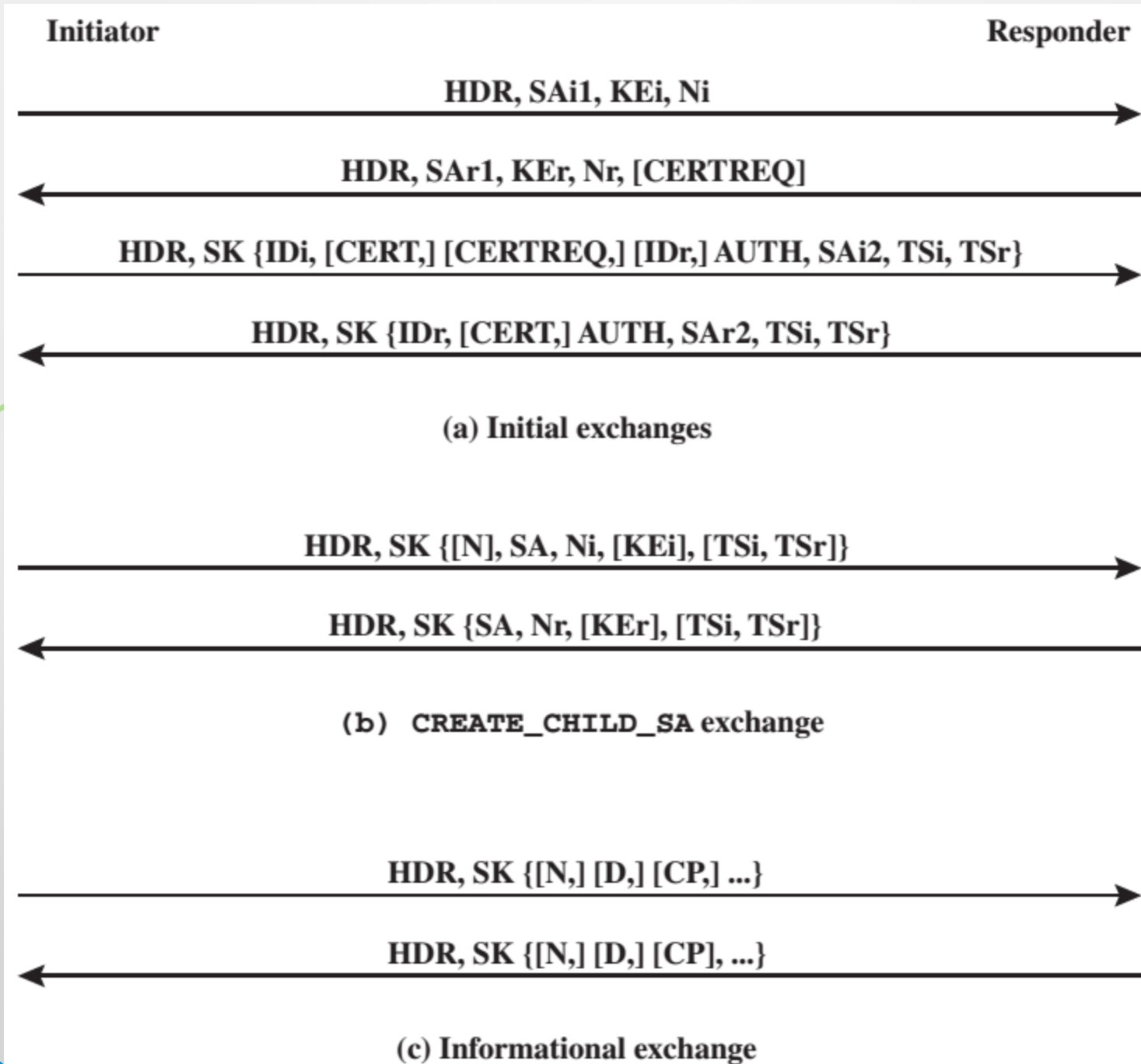
IKE dan Negosiasi Waktu Hidup IPsec





Pertukaran Pesan IKEv2

Pertukaran IKEv2



Pertukaran IKEv2

- HDR = IKE header
- SAg1 = offered & chosen algorithms, DH group
- KEg = Diffie Hellman public key
- Ng = nonce
- CERTREQ = certificate request
- IDg = identity
- CERT = certificate
- SK{...} = MAC & encrypt
- AUTH = authentication
- SAg2 = algorithms, parameters for IPSec SA
- TSg = traffic selectors for IPSec SA
- D = delete
- CP = configuration

References

- E. Gean, "Chapter 13 IPSec", California State University, 2015
- X.Y. Li, "IPSec", Illinois Institute of Technology, 2014
- W. Stallings, "Cryptography and Network Security: Principles and Practice", 7th ed., Pearson, 2016



TERIMA KASIH