

CS 547: Foundation of Computer Security

S. Tripathy
IIT Patna

Previous Classes

- Security in Networks
 - Threats in Networks & Security Controls
 - Threats in Layer 1 & Layer 2
 - Threats in Layer Network (IP) Layer
 - Threats in Transport Layer
- Network Security Controls
 - Link Encryption & End to End Encryption
 - IP-Sec

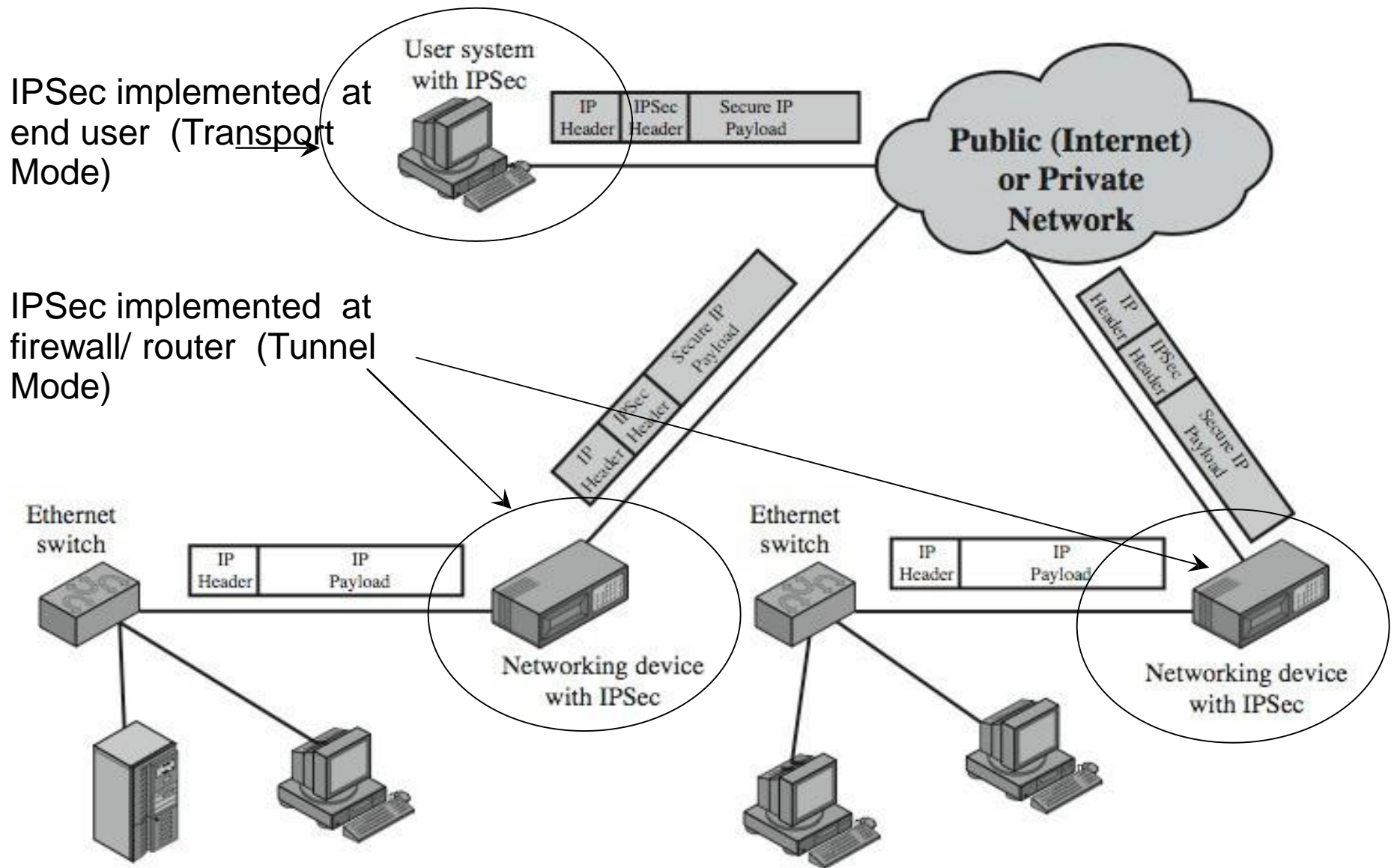
Present class

- Security in Networks
 - Network Security Controls
 - IPSec
 - IKE
 - VPN
 - TLS

Goals of IPSec

- to verify sources of IP packets
 - *authentication*
- to prevent replaying of old packets
- to protect integrity and/or confidentiality of packets
 - *data Integrity/Data Encryption*

Typical IPSec Scenario



Source: Figure 19.1 from William Stallings – Cryptography and Network Security, 5th Edition

IPSec

- ⑩ Implemented at the IP layer, so it does not require any change to existing TCP, UDP and application layer protocols.
- ⑩ Designed to address the fundamental shortcomings of the IP layer such as being subjected to **spoofing, eavesdropping and session hijacking**.
- ⑩ The basis of IPSec is security association (SA)
 - ⑩ SA is basically the set of security parameters for a secured communication channel.
 - ⑩ Each host can have several SAs in effect for current communications with different remote hosts.
- ⑩ A SA is identified using a security parameter index (SPI)
 - ⑩ SPI is a 32-bit identifier used to identify SA
 - ⑩ The SPI and the partner IP address are used to index to the security association database (SADB) that has information about the other characteristics of the different security associations
- ⑩ Two protocols have been developed to provide packet-level security for both IPv4 and IPv6:
 - ☞ **IP Authentication Header**, AH (Next Header protocol ID: 51) provides integrity, authentication and non-repudiation.
 - ☞ **IP Encapsulating Security Payload**, ESP provides confidentiality, along with authentication and integrity protection.

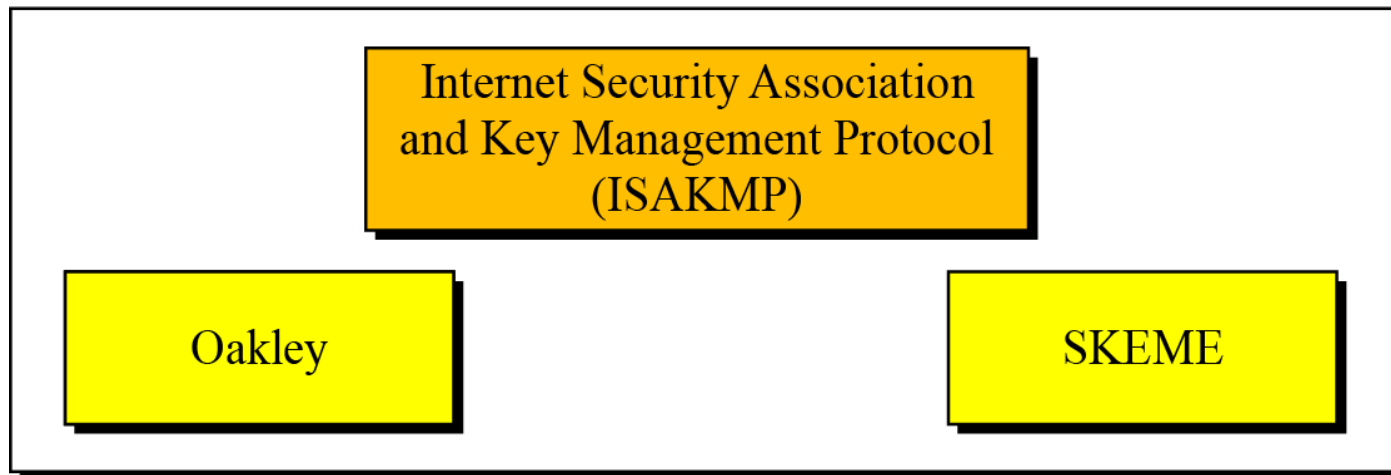
Internet Key Exchange (IKE)

- Exchange and negotiate security policies
- Establish security sessions
 - Identified as *Security Associations*
- Key exchange
- Key management

Key Management in IPSec

- The Internet Key Exchange (IKE) is a protocol designed to create both inbound and outbound Security Associations

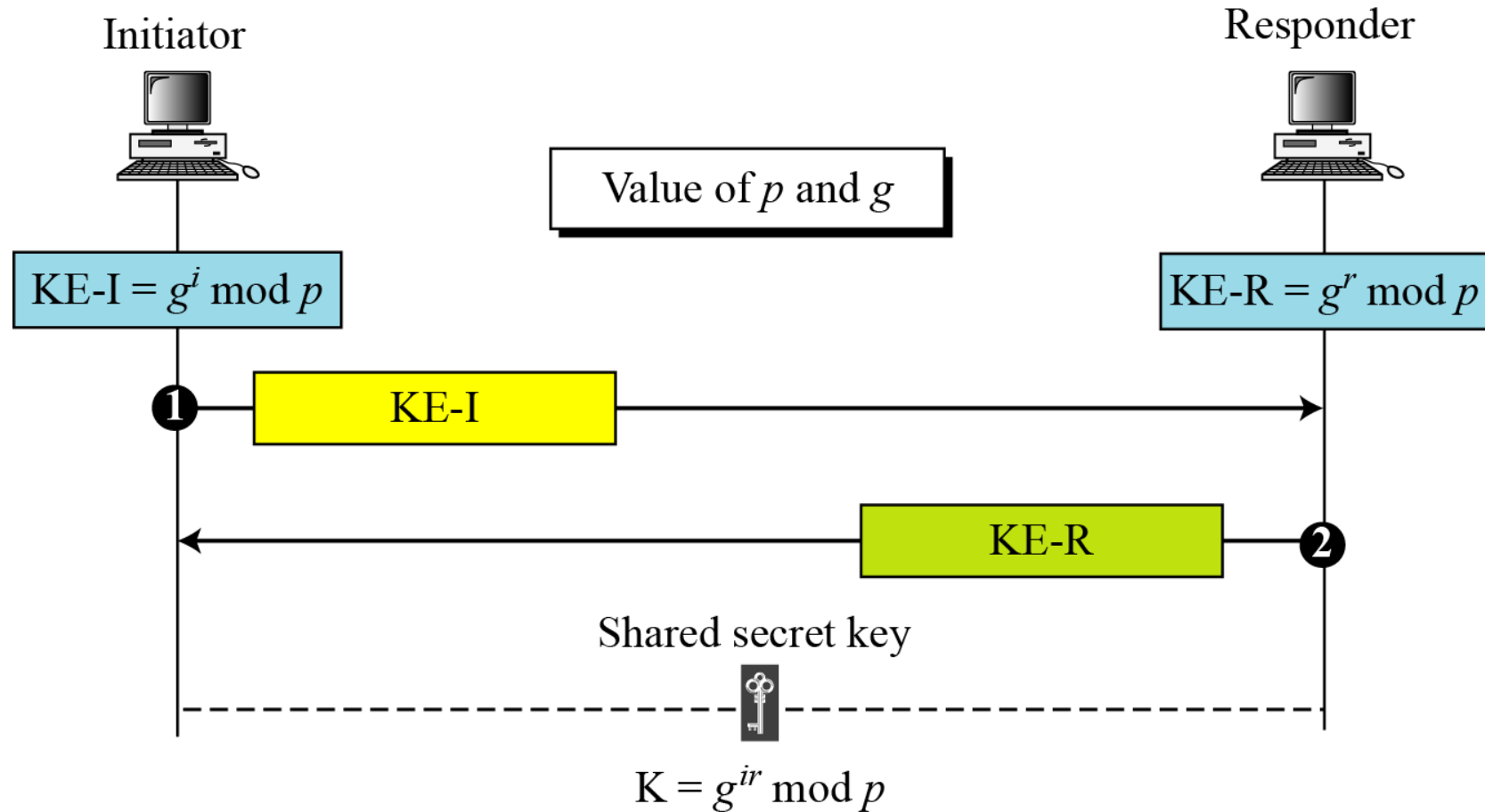
Internet Key Exchange (IKE)



the actual IKE protocol used in IPSec uses parts of Oakley and SKEME (Secure key exchange Mechanism for Internet) .
Uses ISAKMP messages to exchange authenticated keying material

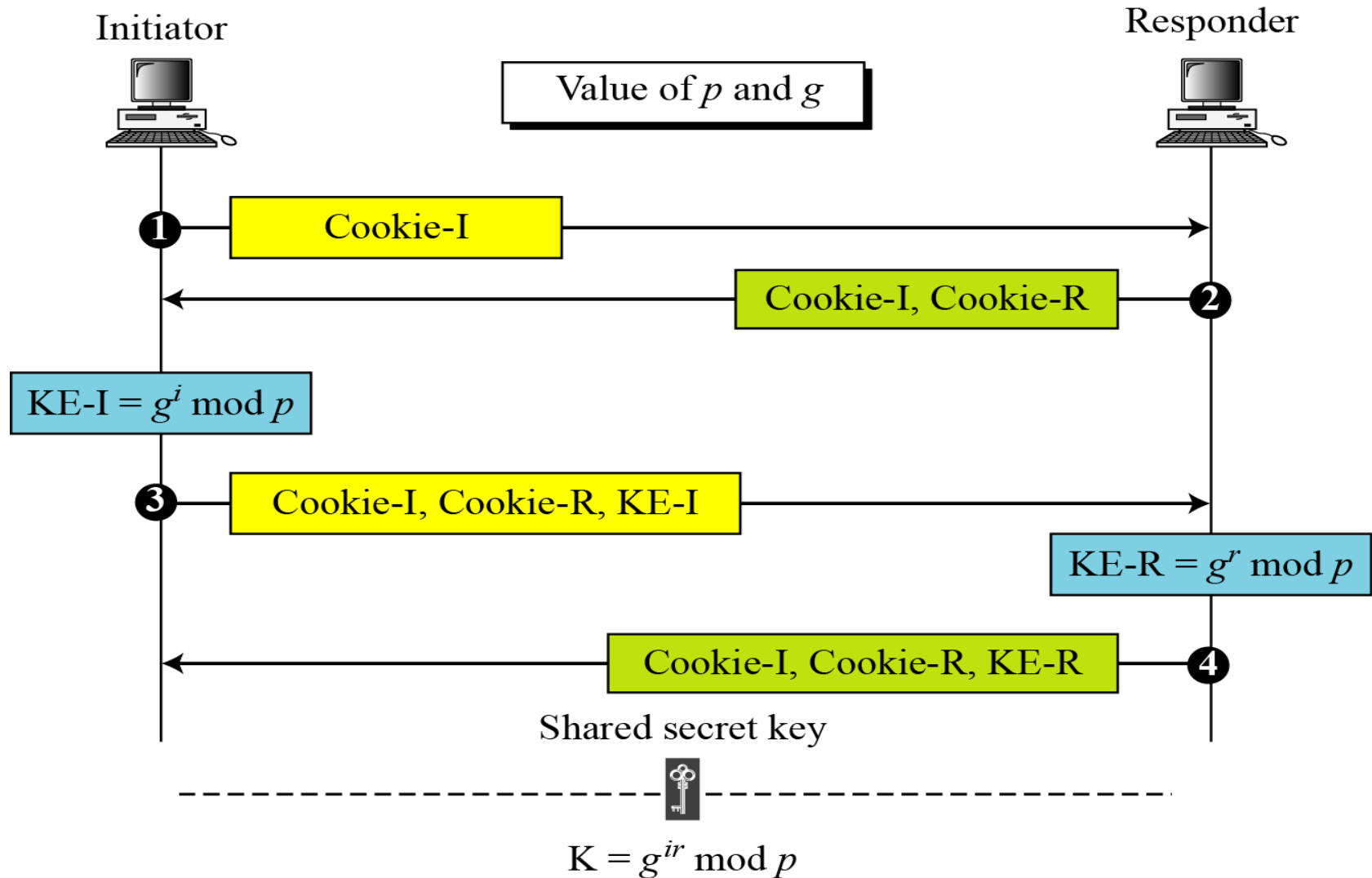
Basis of IKE:

Diffie-Hellman key exchange



Vulnerable!

Diffie-Hellman with cookies

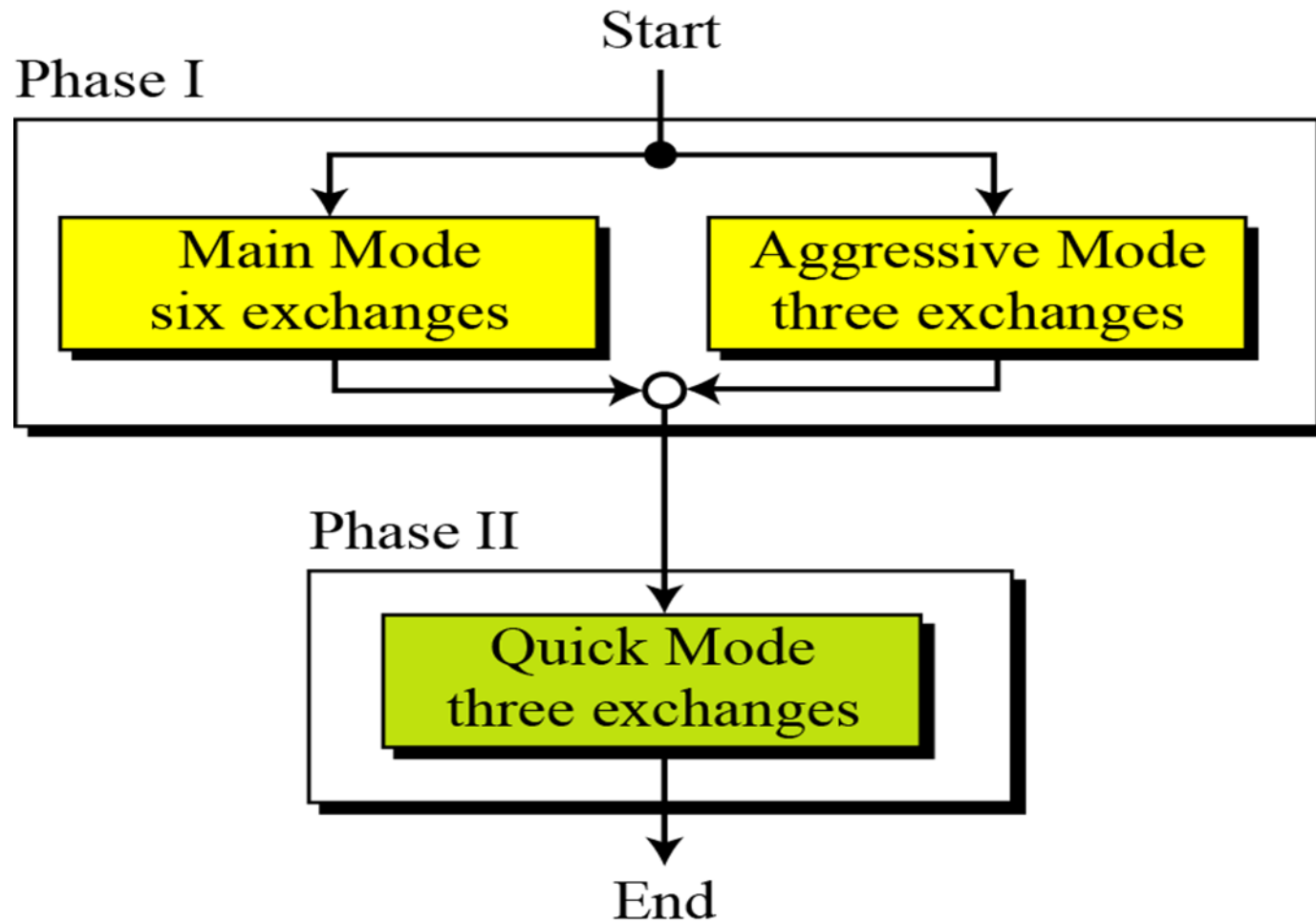


Cookie = hash((Ip, port, protocol), Secret random number known to the party who generated and a time stamp)

IKE:

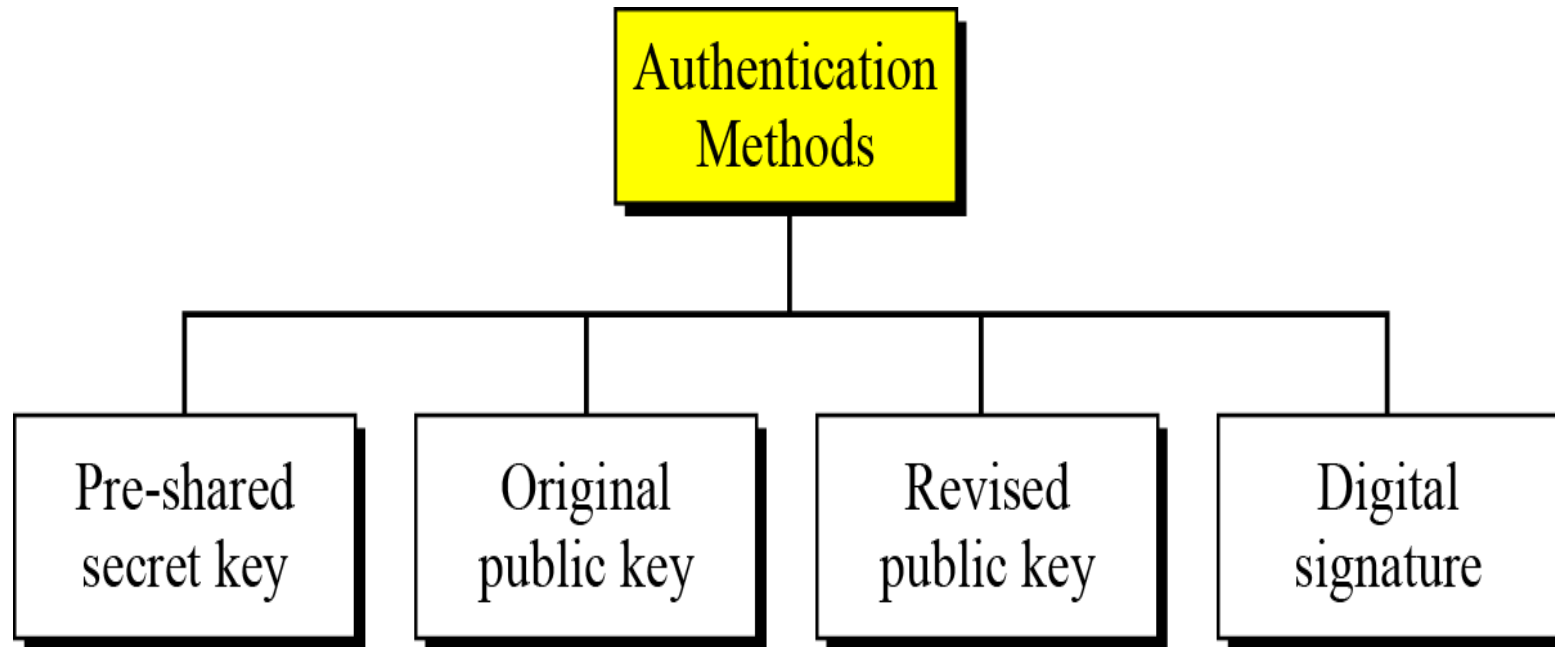
- To protect against a **clogging attack**, IKE uses **cookies**.
- To protect against a **replay attack**, IKE uses **nonces**.
- To protect against **man-in-the-middle attack**, IKE requires that each party shows that it **possesses a secret**.
- IKE is divided into two phases: (phase I and II)
- Phase I creates SAs for phase II;
- Phase II creates SAs for a data exchange protocol such as IPSec..

IKE Phases



Main mode or aggressive mode

- Phase 1 uses one of the following authentication method



Main (pre-shared key) mode

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

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

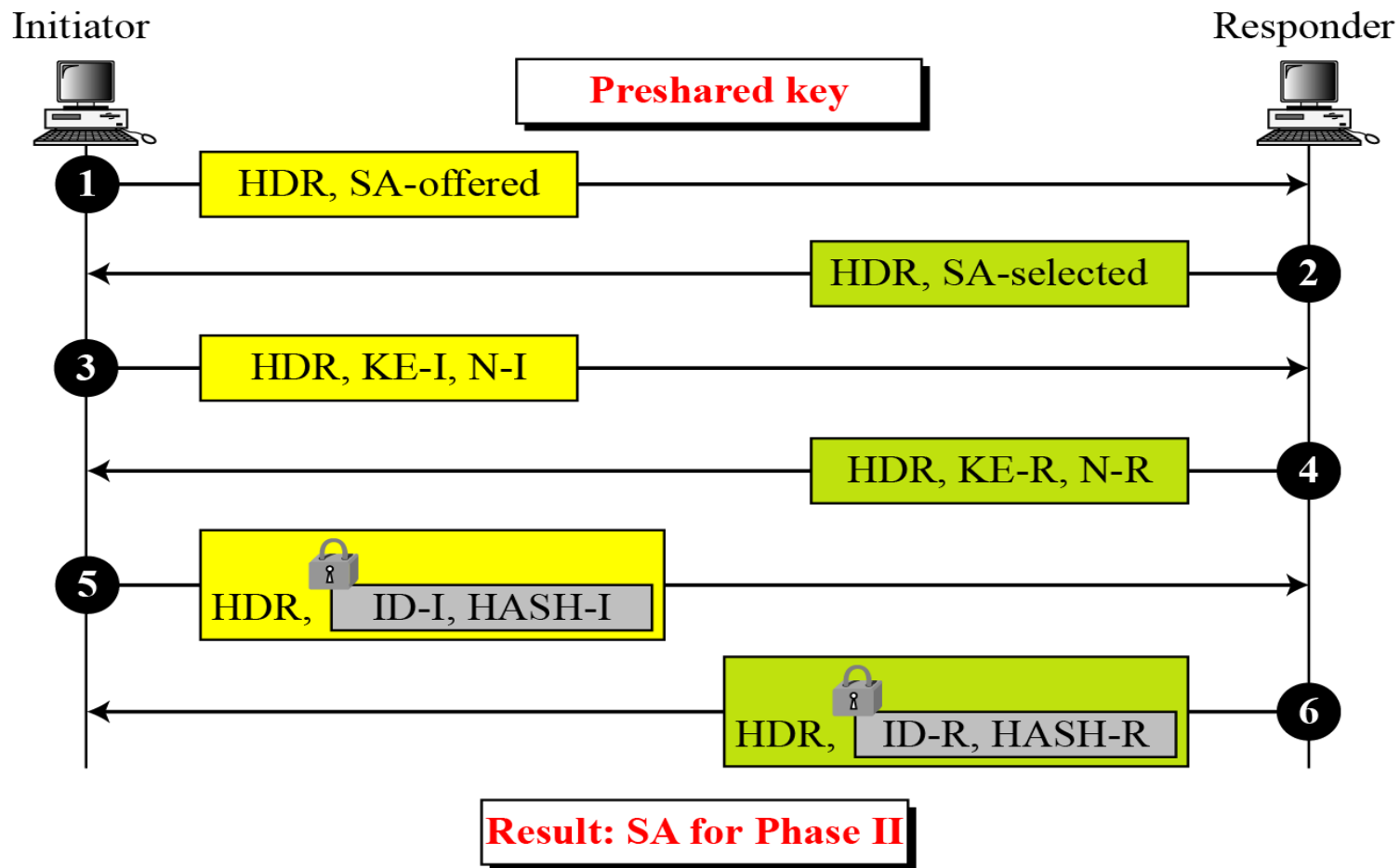
ID-I (ID-R): Initiator's (responder's) ID

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

HDR: General header including cookies



Encrypted with SKEYID_e



Pre-shared Key Method

$$\text{SKY ID} = \text{Prf}(\text{Pre-shared Key} \parallel \text{N-I} \parallel \text{N-R})$$

Public-Key Method

$$\text{SKY ID} = \text{Prf}(\text{N-I} \parallel \text{N-R} \parallel g^{ir})$$

Digital Sign Method

$$\text{SKY ID} = \text{Prf}(\text{hash}(\text{N-I} \parallel \text{N-R}), \text{cookie_I}, \text{cookie_R})$$

Other Common Secrets

(derived key)

$$\text{SKEY ID_d} = \text{Prf}(\text{SKY ID}, g^{ir} \parallel \text{cookie_I} \parallel \text{cookie_R})$$

(Authentication Key)

$$\text{SKEY ID_a} = \text{Prf}(\text{SKY ID}, \text{SKYID_d} \parallel g^{ir} \parallel \text{cookie_I} \parallel \text{cookie_R} \parallel 1)$$

(Encryption Key)

$$\text{SKEY ID_e} = \text{Prf}(\text{SKY ID}, \text{SKYID_a} \parallel g^{ir} \parallel \text{cookie_I} \parallel \text{cookie_R} \parallel 2)$$

$$\text{Hash_I} = \text{Prf}(\text{SKY ID}, \text{KE_I} \parallel \text{KE_R} \parallel \text{cookie_I} \parallel \text{cookie_R} \parallel \text{SA_I} \parallel \text{ID_I})$$

$$\text{Hash_R} = \text{Prf}(\text{SKY ID}, \text{KE_I} \parallel \text{KE_R} \parallel \text{cookie_I} \parallel \text{cookie_R} \parallel \text{SA_I} \parallel \text{ID_R})$$


Main (pre-shared key) mode (Aggressive)

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

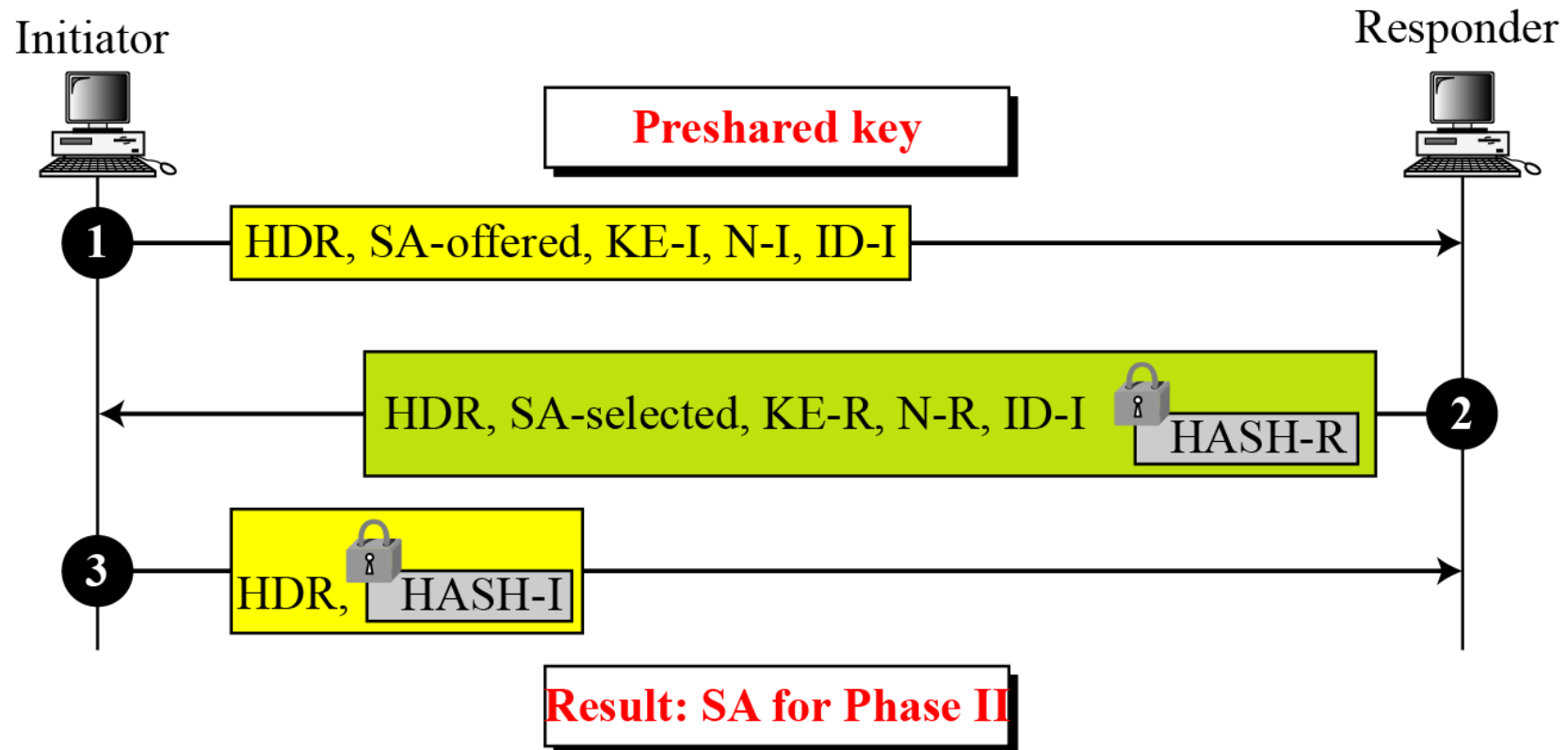
N-I (N-R): Initiator's (responder's) nonce

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

HDR: General header including cookies

 Encrypted with SKEYID_e

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



Main mode (Public-key)


HDR: General header including cookies


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


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

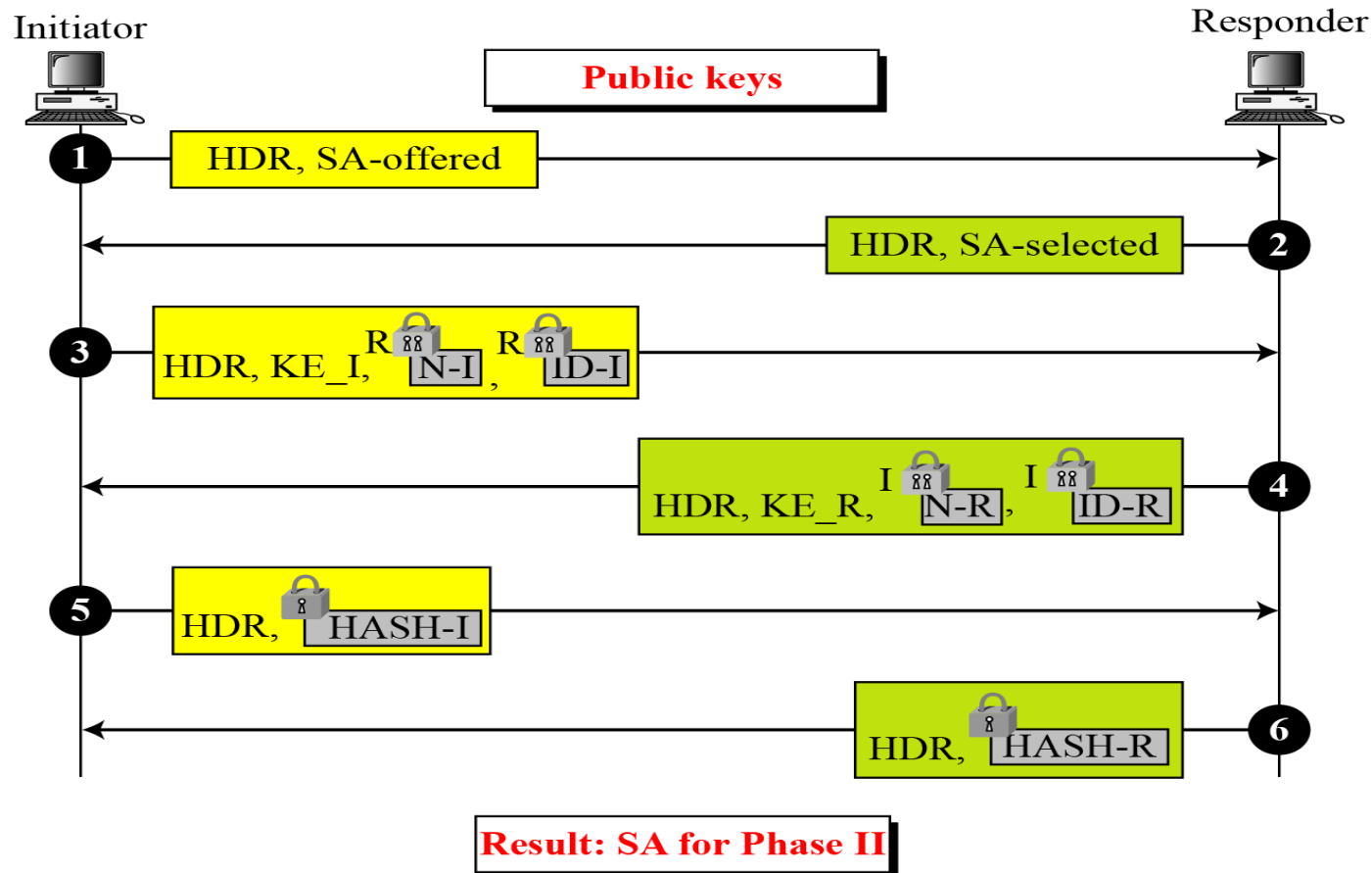
ID-I (ID-R): Initiator's (responder's) ID

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



Main mode (Public-key) Revised

HDR: General header including cookies






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

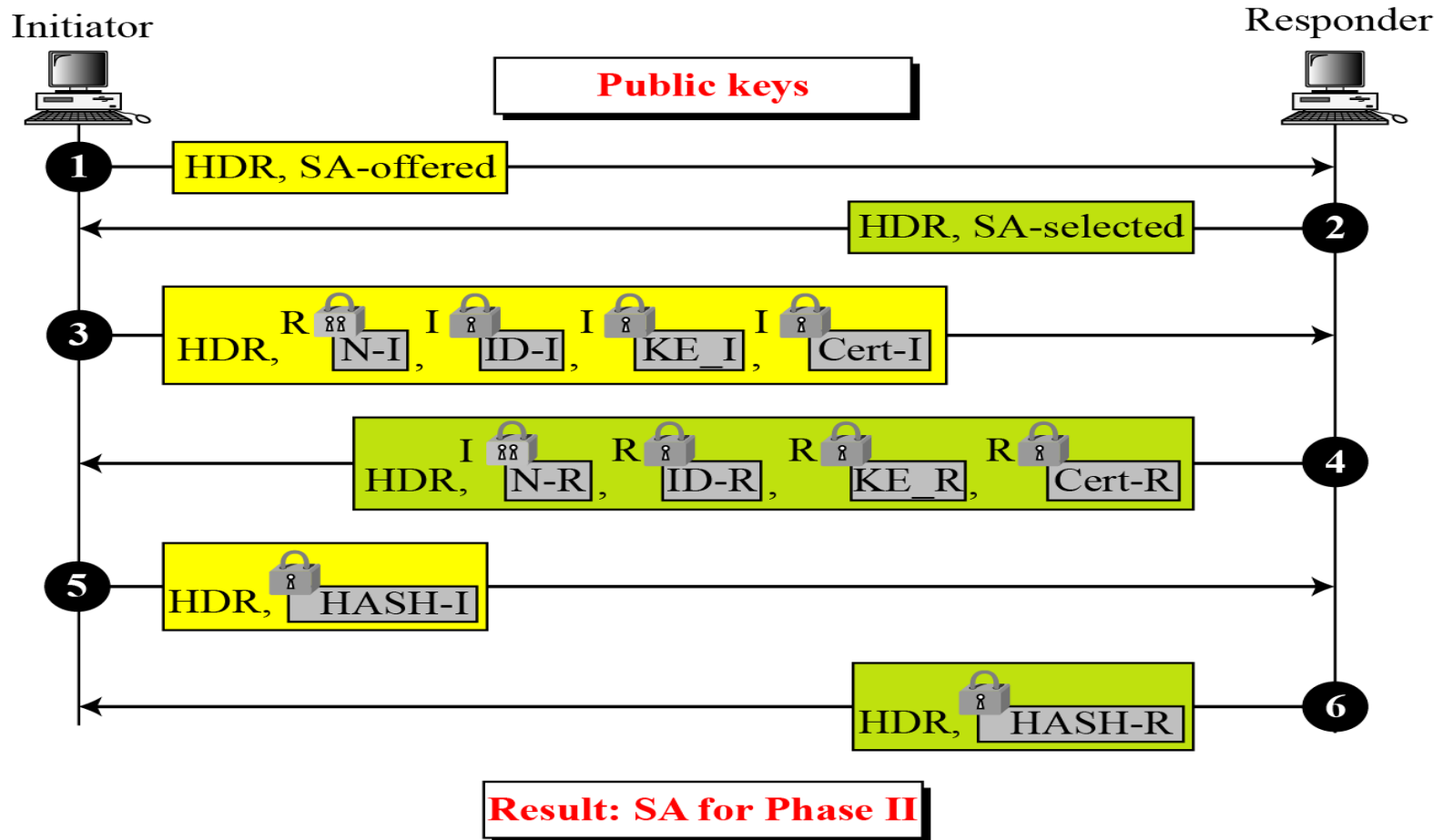
Cert-I (Cert-R): Initiator's (responder's) certificate

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



Main mode (Digital Signature)

HDR: General header including cookies

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


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

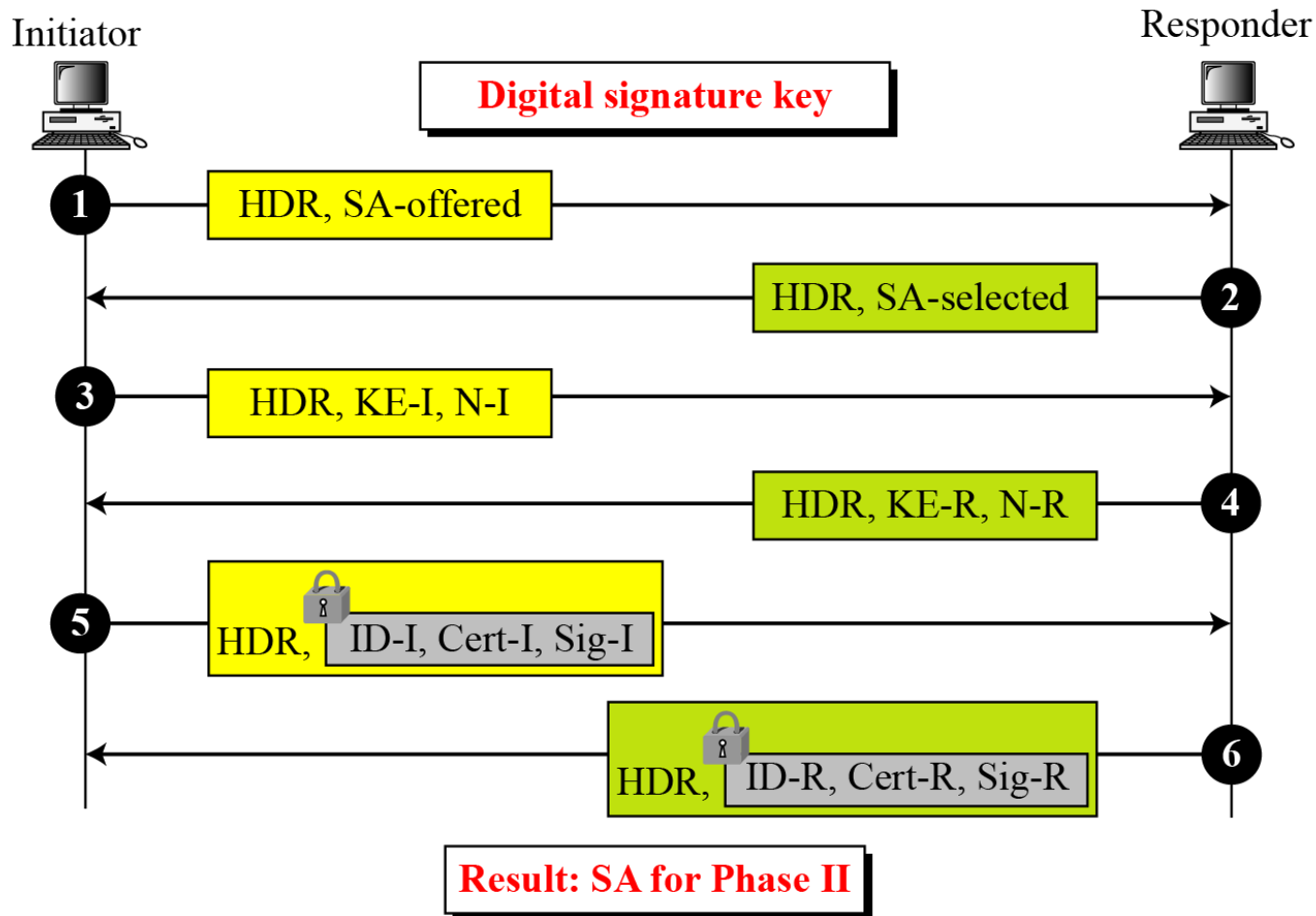
Cert-I (Cert-R): Initiator's (responder's) certificate

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



Aggressive mode (Digital Signature)



Encrypted with SKEYID_e

Sig-I (Sig-R): Initiator's (responder's) signature

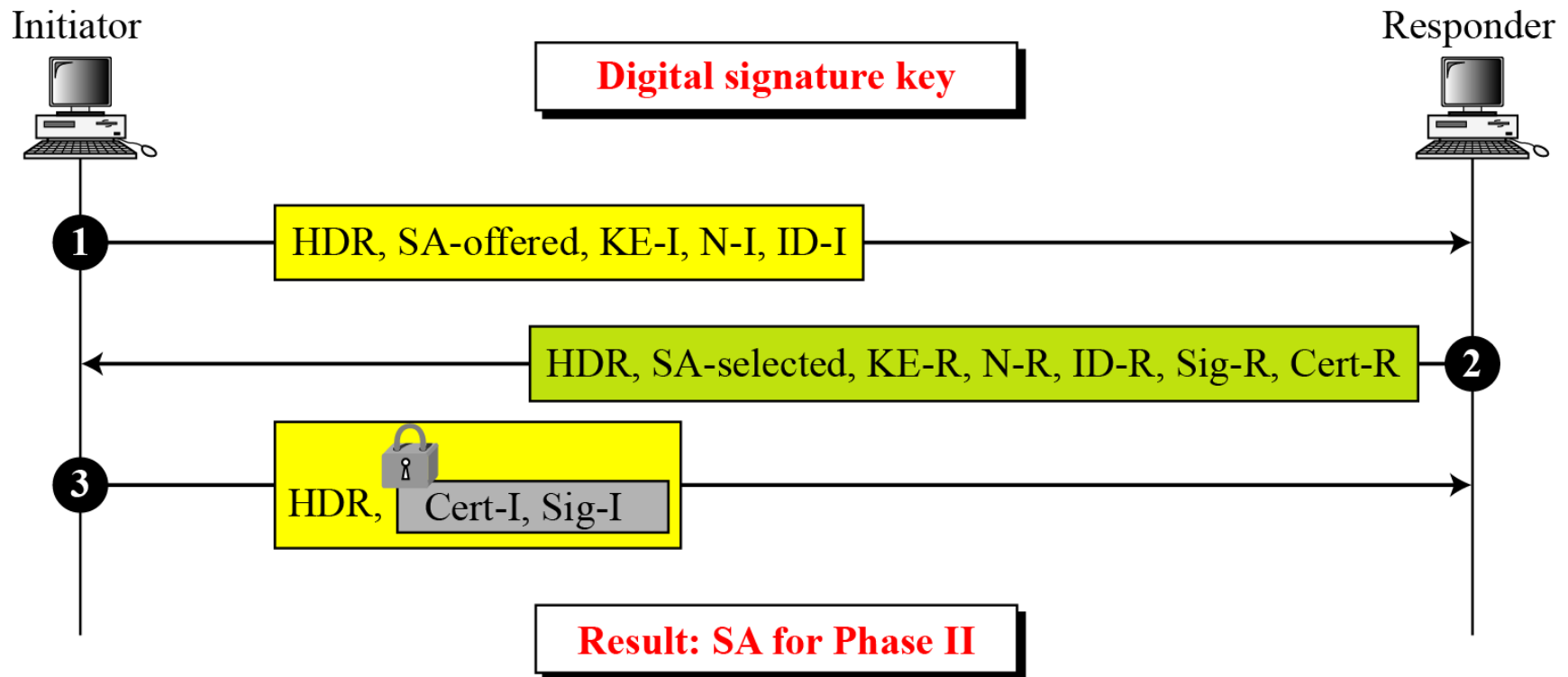
HDR: General header including cookies

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



IPSec (Phase 2)

- **Goal:** to establish custom secure channels between two end points
 - End points are identified by <IP, port>:
 - e.g. <www.mybank.com, 8000>
 - Or by packet:
 - e.g. All packets going to 128.124.100.0/24
 - Use the secure channel established in Phase 1 for communication
- **Only one mode:** Quick Mode
- Multiple quick mode exchanges can be multiplexed
- Generate SAs for two end points
- Can use secure channel established in phase 1


Phase-2 (Quick mode)

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

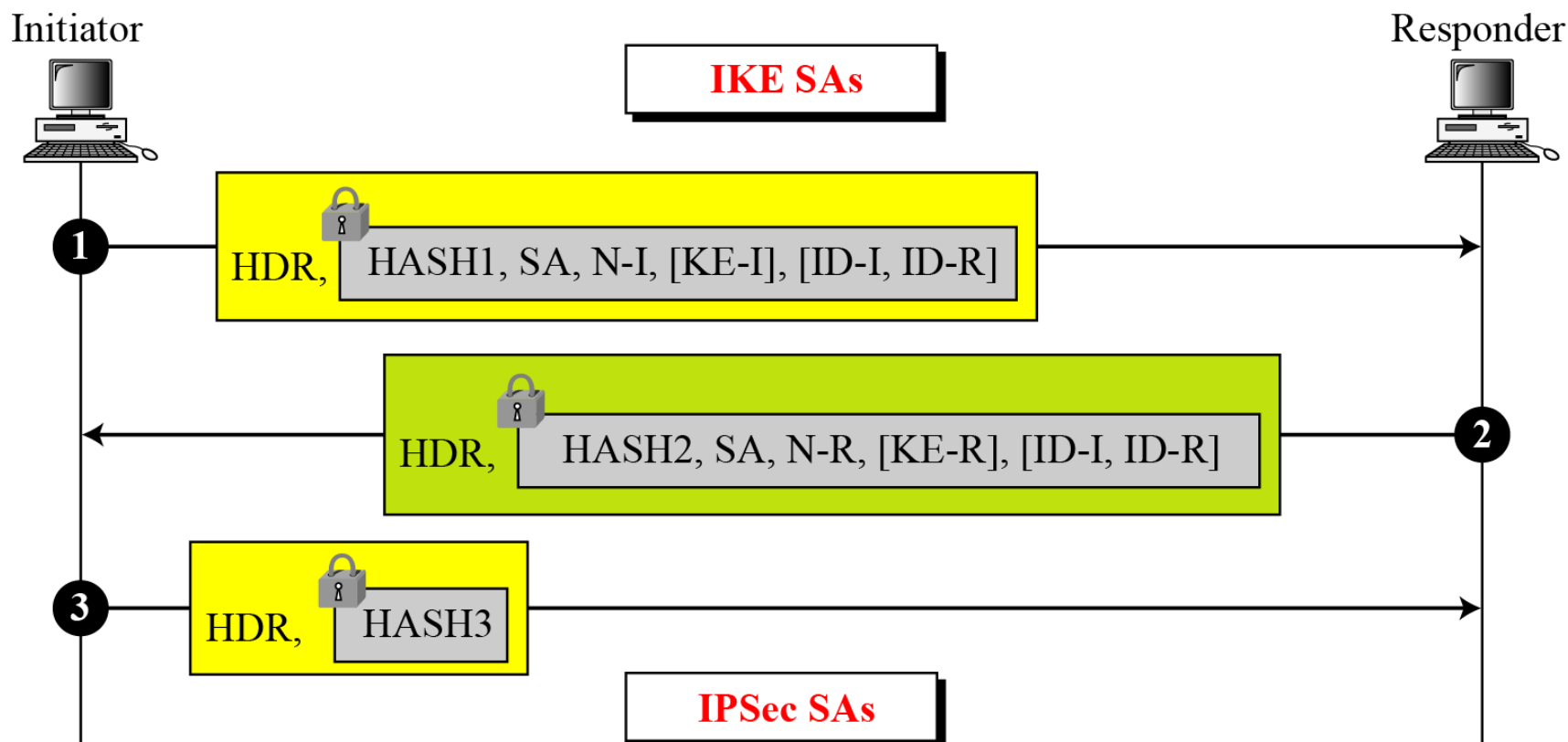
N-I (N-R): Initiator's (responder's) nonce

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

HDR: General header including cookies

 Encrypted with SKEYID_e

SA: Security association



$\text{HASH1} = \text{prf}(\text{SKEYID_d}, \text{MsgID} | \text{SA} | \text{N-I})$

$\text{HASH2} = \text{prf}(\text{SKEYID_d}, \text{MsgID} | \text{SA} | \text{N-R})$

$\text{HASH3} = \text{prf}(\text{SKEYID_d}, 0 | \text{MsgID} | \text{SA} | \text{N-I} | \text{N-R})$

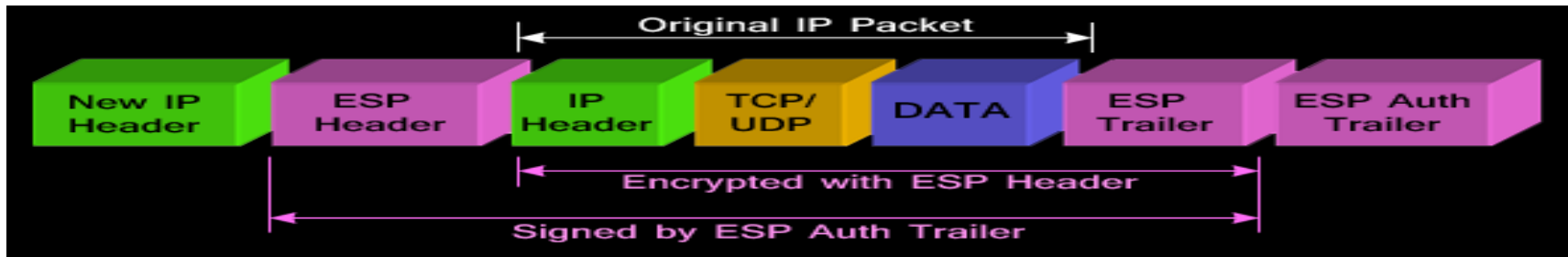
Combining Security Associations

- SA's can implement either AH or ESP
- To implement both, need to combine SA's
 - form a security association bundle
- A possible case: End-to-end Authentication + Confidentiality
 - Solution1: use ESP with authentication option on
 - Solution2: apply ESP SA (no auth.) first, then apply AH SA
 - Solution3: Apply AH SA first, then ESP SA
 - encryption is after the authentication

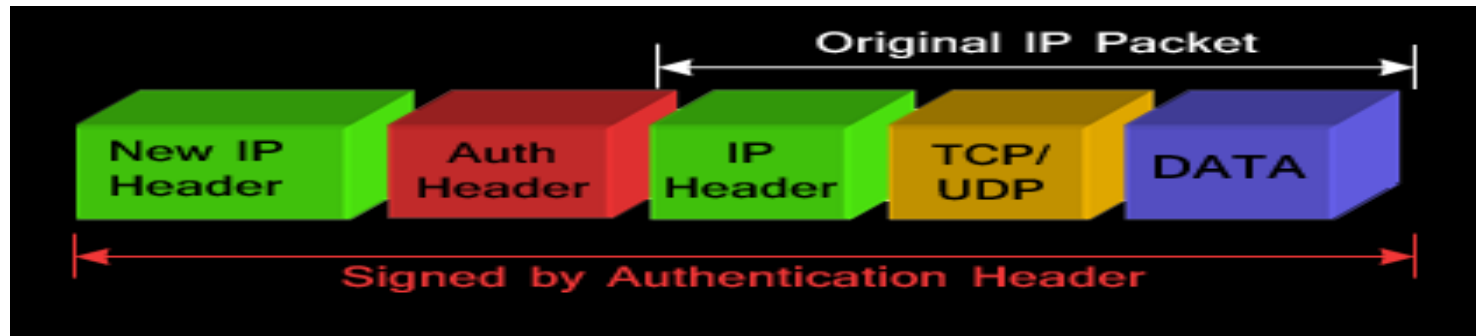
IP Payload Compression

- Used for compression
- Can be specified as part of the IPSec policy
- Will not cover!

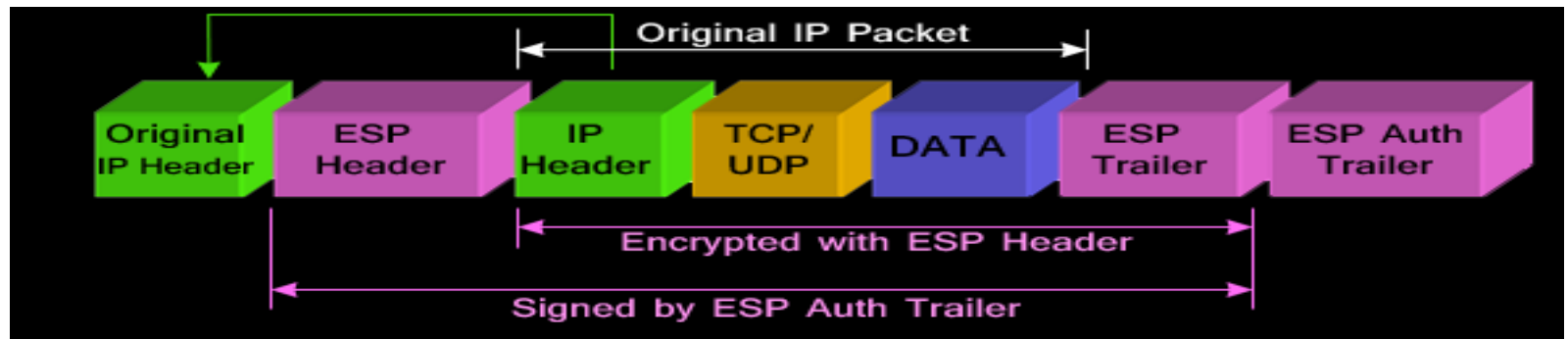
IPSec Tunnel mode with ESP header:



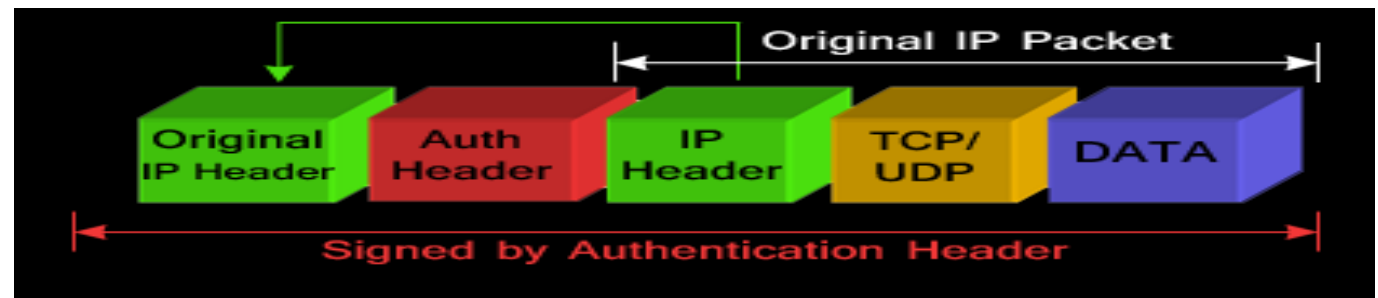
IPSec Tunnel mode with AH header:



IPSec Transport mode with ESP header



IPSec Transport mode with AH header



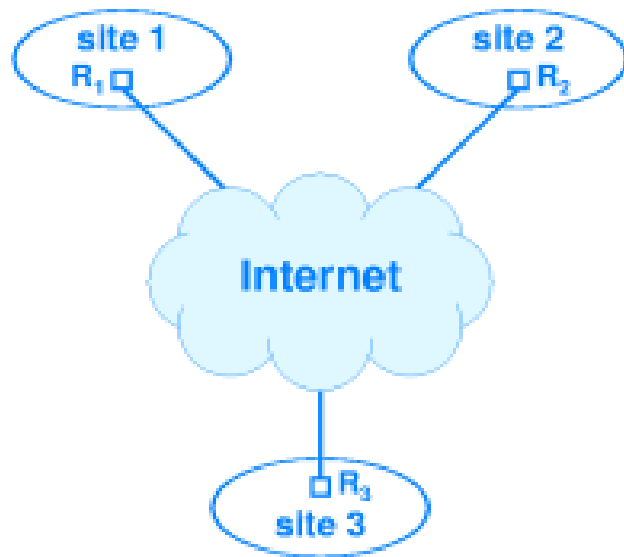
Virtual Private Networks (VPNs)

- Virtual: Not physical
- Private
 - Tunnels are encrypted to provide confidentiality
- CS dept might have a VPN
 - One can be on this VPN while traveling

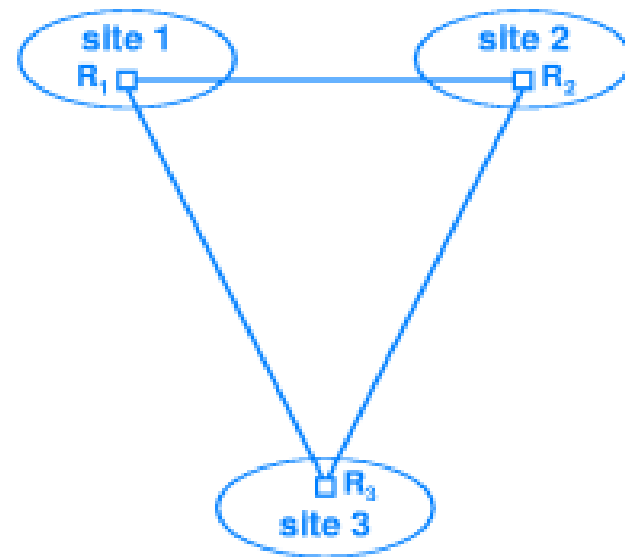
Virtual Private Network (VPN)

- ⑩ An organization with multiple geographically distributed sites can take either of the following two approaches to interconnect the sites:
 - **Private network connections:**
 - ☞ Lease serial lines (possibly from telephone companies) to connect the sites. A router at a site is directly connected to a router at another site using a leased line and data directly passes from one site to another.
 - **Public Internet connections:**
 - ☞ Each site signs up with a local ISP for Internet service and data is passed from site to another across the global Internet.
- ⑩ Although the serial lines are more costly than subscribing to a local ISP, they guarantee confidentiality of data, which is not possible when data is passed across the global Internet.
- ⑩ VPN is the technology used to build an organization's intranet that provides confidentiality and at the same time is economical as encrypted data is tunneled from one site to another site across the global Internet.

Virtual Private Network (VPN)



Physical interconnection between
routers at three sites
of an organization



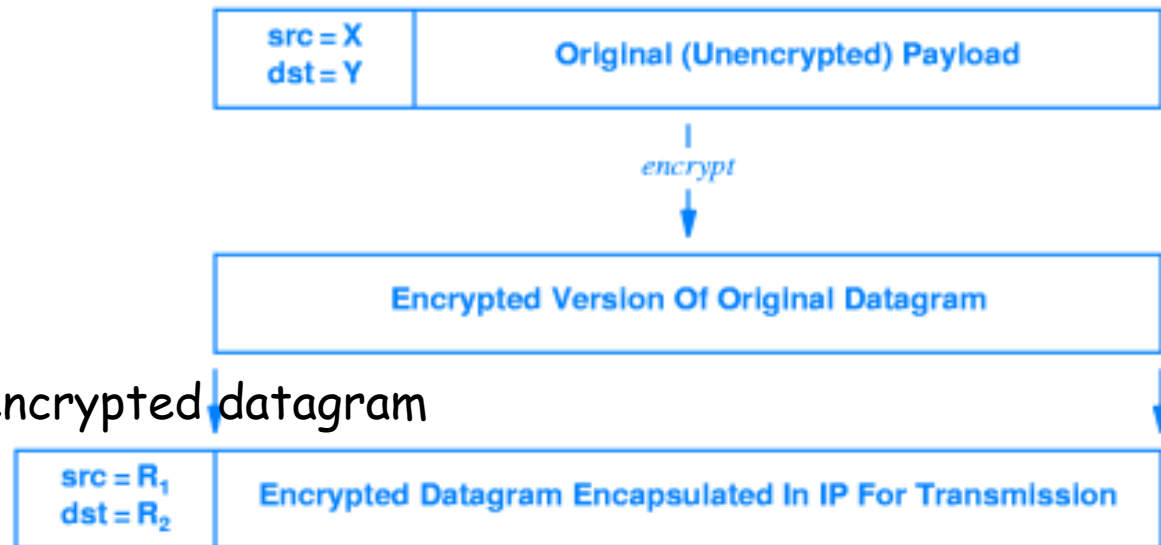
The equivalent logical
connections created by
VPN software
running on the routers

Virtual Private Network (VPN)

- ⑩ The VPN software installed at each of the routers R1, R2 and R3, does the following three functions:
 - ⌘ Make sure the next hop for each outgoing datagram is a router at another site of the organization and nothing else.
 - ⌘ Encrypt the IP datagram arriving from the host before forwarding to another site and decrypt the IP datagram received from another site before forwarding to the local host.
 - ⌘ Perform IP-in-IP tunneling to facilitate the encryption of the actual source and destination IP addresses in the IP datagram by encapsulating it into another IP datagram whose source and destination addresses are that of the routers at the two participating sites.

X at site 1 is
the original source of
the unencrypted datagram

Y at site 2 is the
target destination of the unencrypted datagram



Resources

- IP, IPsec and related RFCs:
 - <http://www.ietf.org/html.charters/ipsec-charter.html>
 - IPsec: RFC 2401, IKE: RFC 2409
 - www.freeswan.org
 - StrongSwan in Ubuntu

- Thanks