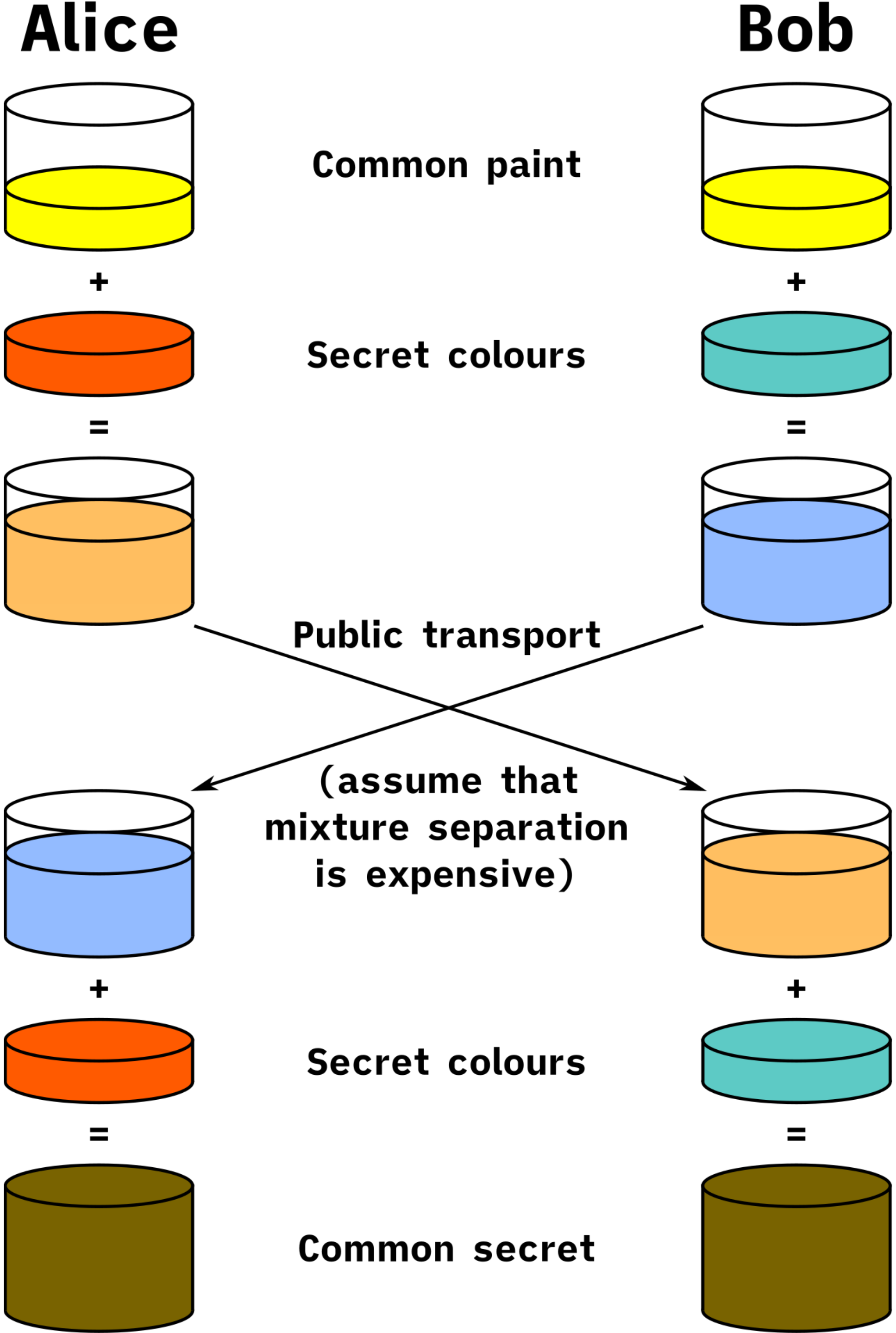
March 22, 2021
Tunneling

- Tunneling
  - Secure Shell
  - VPN
- Assignments
  - Project
    - Outline: Due Monday, Mar 29
  - Lab 2
    - Due Monday, Apr 5

Secure Shell

- Encryption
- Authentication
- Use Cases



Alice

Bob

Common paint

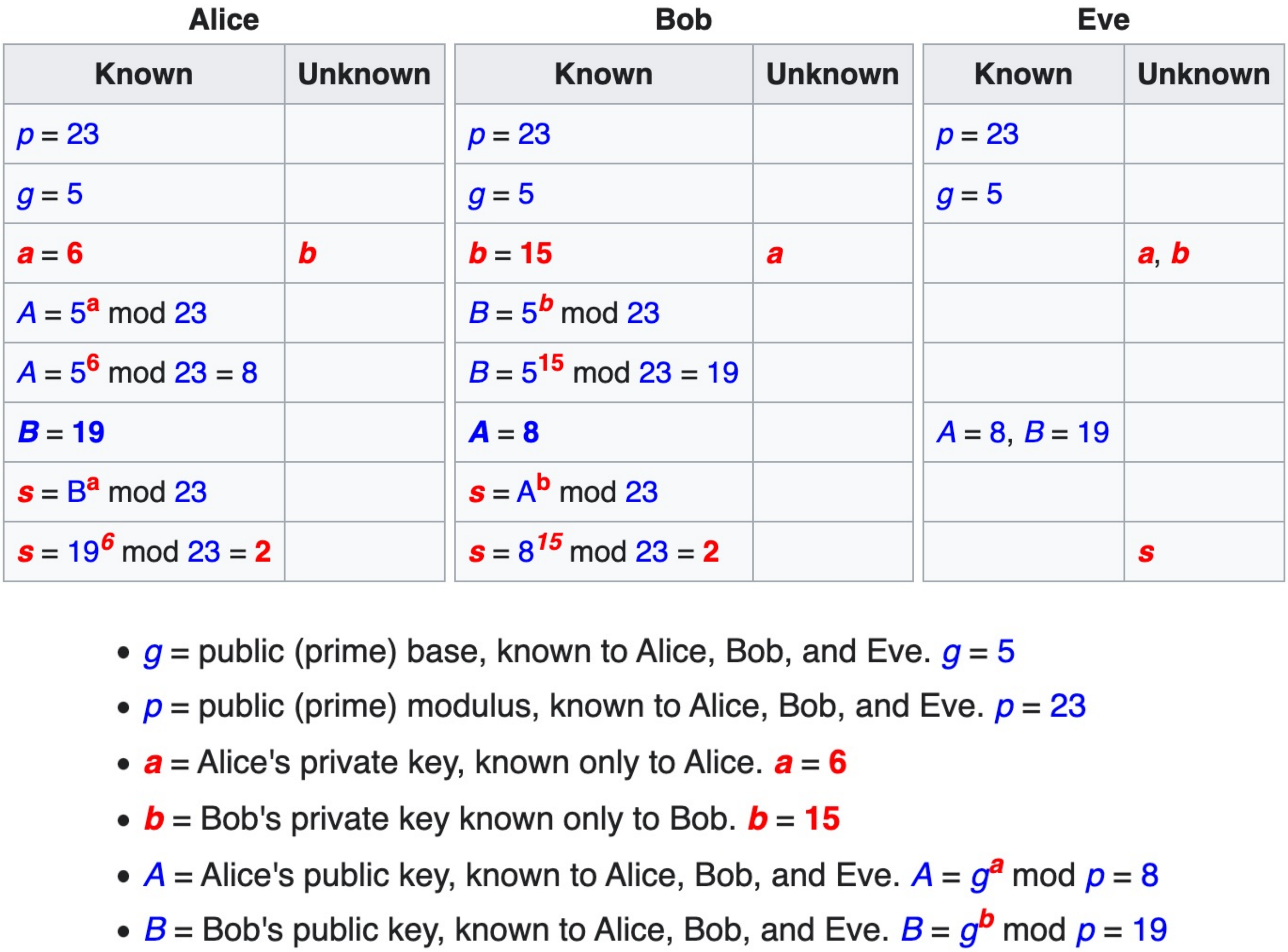
Secret colours

Public transport

(assume that mixture separation is expensive)

Secret colours

Common secret



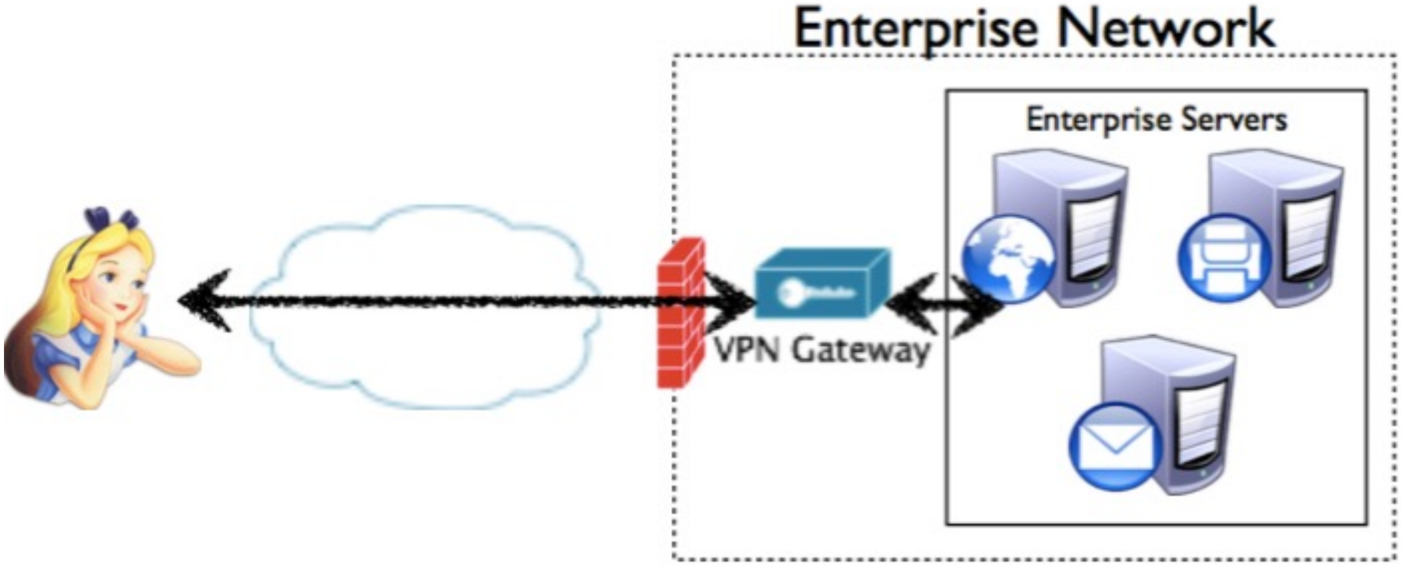
Alice		Bob		Eve	
Known	Unknown	Known	Unknown	Known	Unknown
$p = 23$		$p = 23$		$p = 23$	
$g = 5$		$g = 5$		$g = 5$	
$\boldsymbol{a = 6}$	$\boldsymbol{b}$	$\boldsymbol{b = 15}$	$\boldsymbol{a}$		$\boldsymbol{a}$, $\boldsymbol{b}$
$A = 5^{a} \bmod 23$		$B = 5^{b} \bmod 23$			
$A = 5^{6} \bmod 23 = 8$		$B = 5^{15} \bmod 23 = 19$			
$\boldsymbol{B = 19}$		$\boldsymbol{A = 8}$		$A = 8$, $B = 19$	
$s = B^{a} \bmod 23$		$s = A^{b} \bmod 23$			
$s = 19^{6} \bmod 23 = 2$		$s = 8^{15} \bmod 23 = 2$			s

- g = public (prime) base, known to Alice, Bob, and Eve. $g = 5$
- p = public (prime) modulus, known to Alice, Bob, and Eve. $p = 23$
- $\boldsymbol{a}$ = Alice's private key, known only to Alice. $\boldsymbol{a = 6}$
- $\boldsymbol{b}$ = Bob's private key known only to Bob. $\boldsymbol{b = 15}$
- A = Alice's public key, known to Alice, Bob, and Eve. $A = g^{a} \bmod p = 8$
- B = Bob's public key, known to Alice, Bob, and Eve. $B = g^{b} \bmod p = 19$

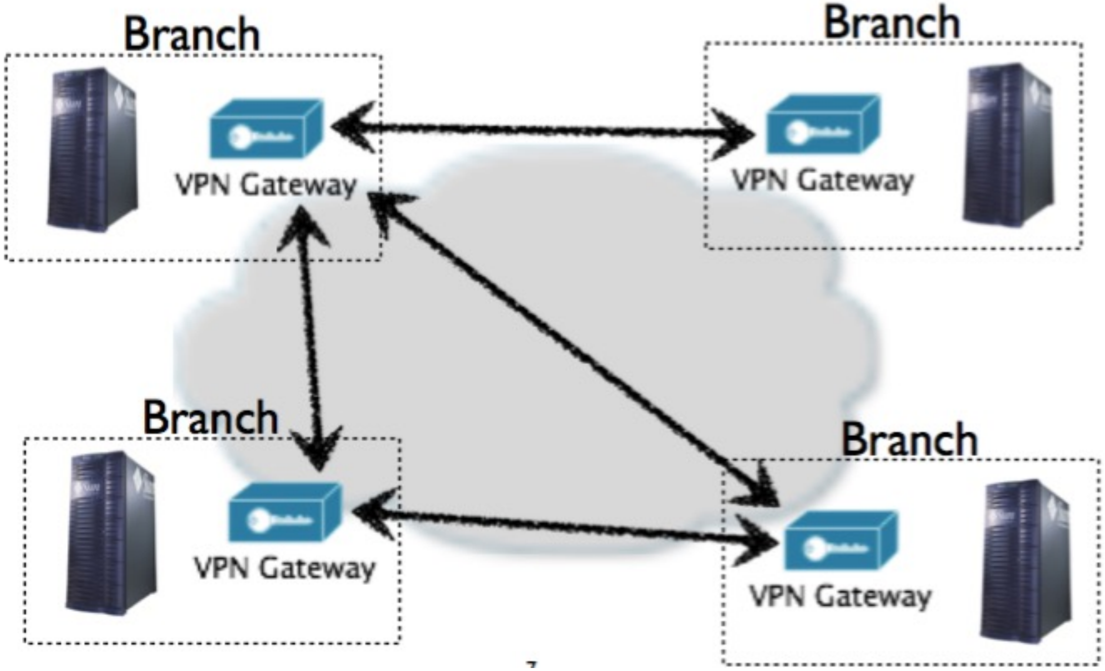
Virtual Private Networks

- PPTP
- OpenVPN
- IPSEC
    - L2TP

Telecommuter VPNs: Client-to-Gateway



Gateway-to-Gateway VPNs



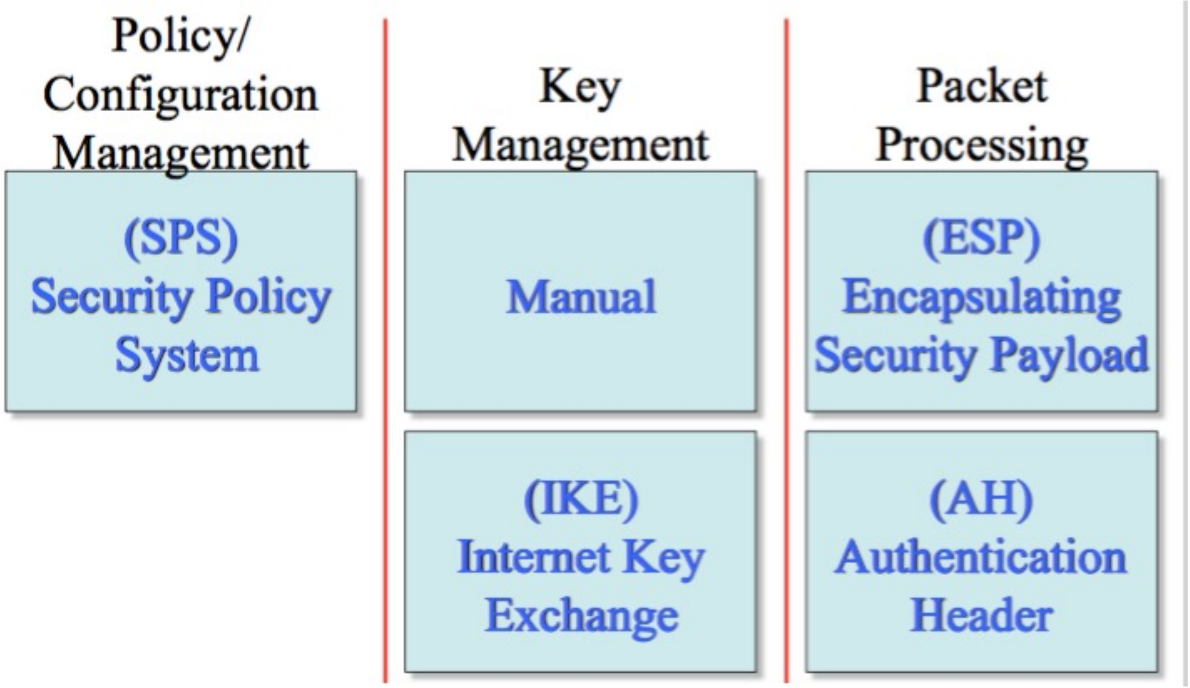
IPsec VPN

- IPsec is another technology which is more deeply integrated in the packets
- IPsec VPN more efficient than SSL VPN
- IPsec must be managed quite deep within the operating system network code
- SSL-based VPN only needs some way to hijack incoming and outgoing traffic; the rest can be down in user-level software.

IPsec

- Host level protection service
  - IP-layer security (below TCP/UDP)
  - De-facto standard for host level security
  - Developed by the IETF (over many years)
- Available in most operating systems/devices
  - E.g., Windows, OS X, Linux, BSD*, ...
- Not a single protocol; IPsec is a protocol suite
  - Implements a wide range of protocols and cryptographic algorithms
- ***Selectively*** provides ....
  - Confidentiality, integrity, authenticity, replay protection, DoS protection

IPsec Protocol Suite



Policy/ Configuration Management

(SPS) Security Policy System

Key Management

Manual

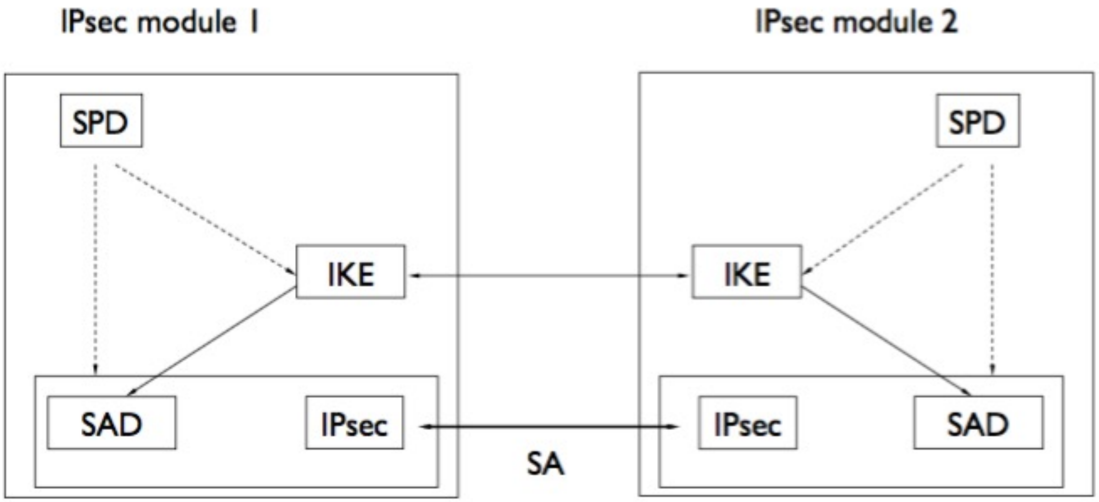
(IKE) Internet Key Exchange

Packet Processing

(ESP) Encapsulating Security Payload

(AH) Authentication Header

IPsec Architecture

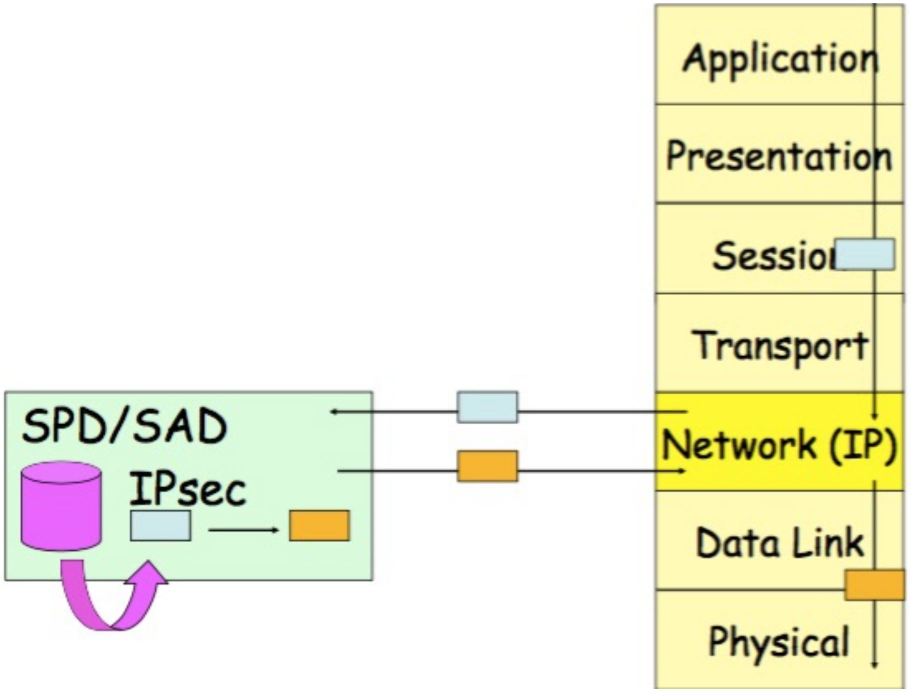


SPD: *Security Policy Database*; IKE: *Internet Key Exchange*;
SA: *Security Association*; SAD: *Security Association Database*.

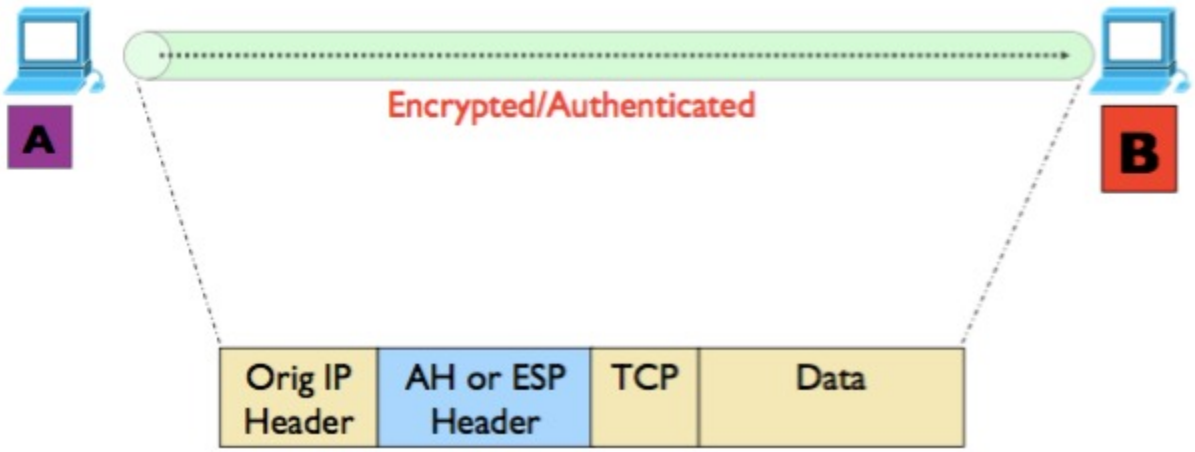
Internet Key Exchange (IKE)

- Two phase protocol used to establish parameters and keys for session
  - **Phase 1**: authenticate peers, establish secure channel via Diffie- Hellman key exchange
  - **Phase 2:** negotiate parameters, establish a **security association (SA)**
- The SA defines algorithms, keys, and policy used to secure the session for a unidirectional traffic flow
  - Pairing requires two SAs -- one for each direction
  - SAs stored in host's Security Association Database (SAD)
    - Each gateway may define policies for each SA
    - Policies stored in the SAD

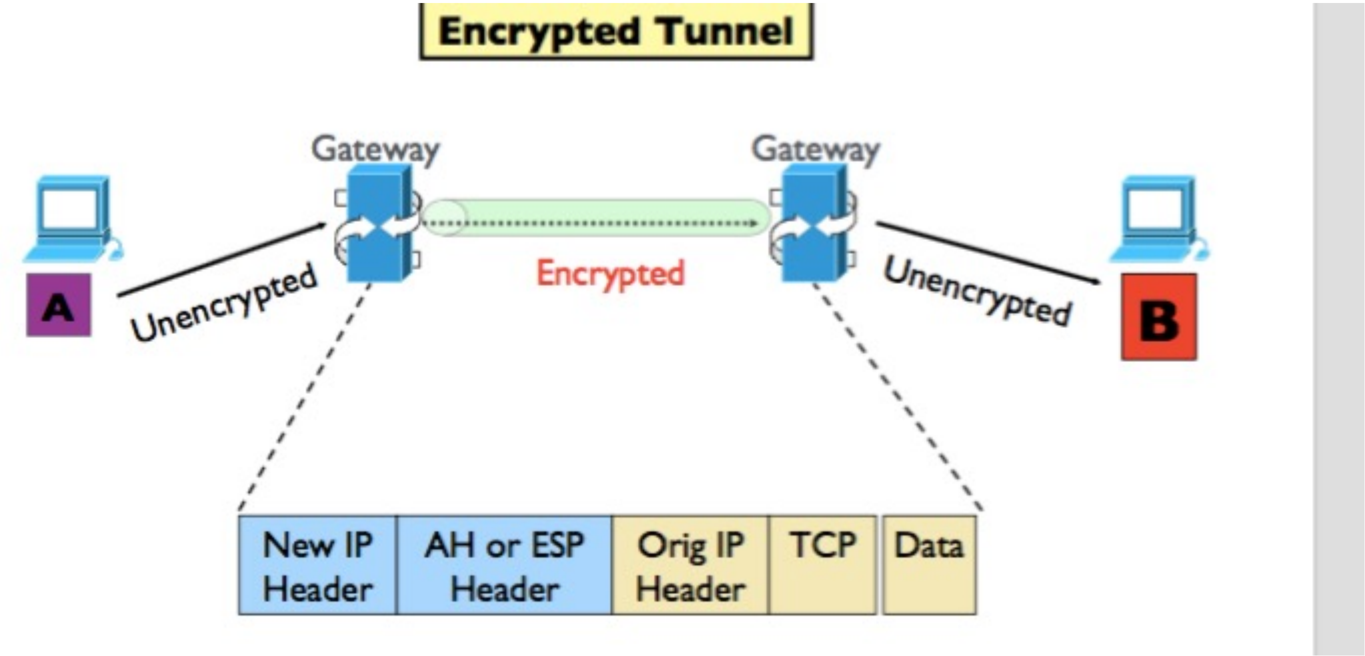
IPsec: Packet Handling



Transport Mode



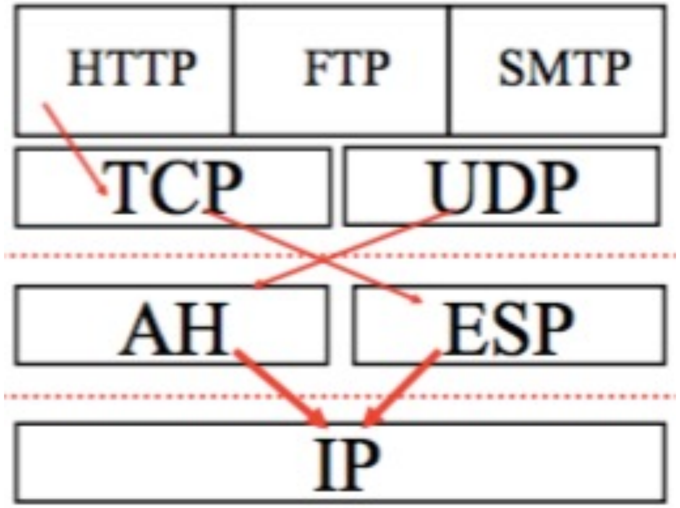
Tunnel Mode


Encrypted Tunnel
Gateway
Gateway
A
Unencrypted
Encrypted
Unencrypted
B
New IP Header
AH or ESP Header
Orig IP Header
TCP
Data

Key Management

- Two options:
    - Manual: use preshared secrets;or
    - Internet Key Exchange (IKE)

IPsec and the IP protocol stack



Security Association (SA)

- An association between a sender and a receiver
  - Consists of a set of security related parameters
  - E.g., sequence number, encryption key
- One way relationship
- Determine IPsec processing for senders
- Determine IPsec decoding for destination
- SAs are not fixed! Generated and customized per traffic flows

Security Parameter Index (SPI)

- A bit string assigned to an SA.
- Carried in AH and ESP headers to enable the receiving system to select the SA under which the packet will be processed.
- 32 bits
    - SPI + Dest IP address + IPsec Protocol
- Uniquely identifies each SA in SA Database (SAD)

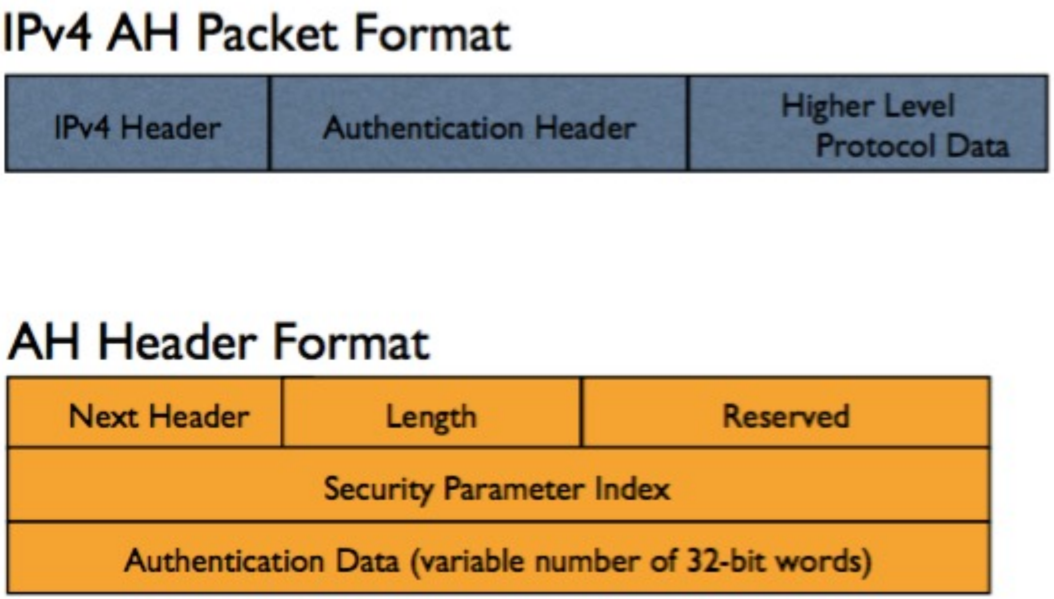
SA Database (SAD)

- Holds parameters for each SA
  - Sequence number counter
  - Lifetime of this SA
  - AH and ESP information
  - Tunnel or transport mode
- Every host or gateway participating in IPsec has their own SA database

Authentication Header (AH)

- Provides **authenticity** and **integrity**
  - via HMAC
  - over immutable IP headers and data
- Advantage: the authenticity of data and IP header information is protected
- Disadvantage: the set of immutable IP headers isn’t necessarily fixed
- Confidentiality of data is *not* preserved
- Replay protection via AH sequence numbers
  - note that this replicates some features of TCP

IPsec AH Packet Format



IPv4 AH Packet Format

IPv4 Header

Authentication Header

Higher Level Protocol Data

AH Header Format

Next Header

Length

Reserved

Security Parameter Index

Authentication Data (variable number of 32-bit words)

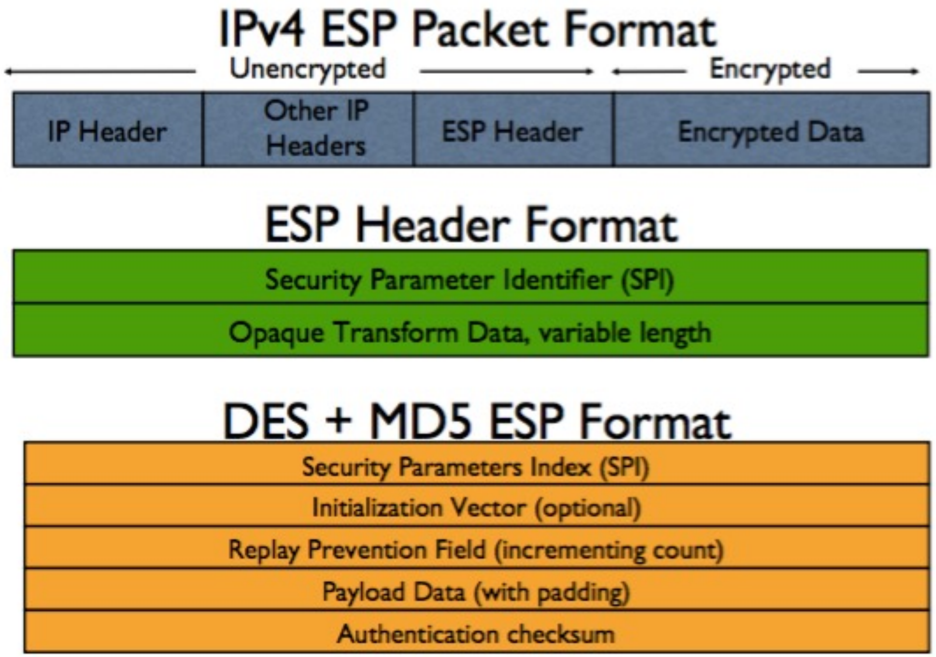
IPsec Authentication

- **SPI:** (spy) identifies the SA for this packet
  - Type of crypto checksum, how large it is, and how it is computed
  - Really, the policy for the packet
- Authentication data
  - Hash of packet contents include IP header as specified by SPI
  - Treat mutable fields (TTL, header checksum) as zero
  - Keyed MD5 Hash is default

Encapsulating Security Payload

- Confidentiality, authenticity, and integrity
  - via encryption and HMAC
  - over IP payload (data)
- Advantage: encapsulated packet is fully secured
- Use “null” encryption to get authenticity/integrity only
- Note that the TCP/UDP ports are hidden when encrypted
  - good: better security, less is known about traffic
  - bad: impossible for FW to filter/traffic based on port
- Cost: can require many more resources than AH

ESP Packet Format



IPv4 ESP Packet Format

← Unencrypted → ← Encrypted →

IP Header	Other IP Headers	ESP Header	Encrypted Data

ESP Header Format

Security Parameter Identifier (SPI)

Opaque Transform Data, variable length

DES + MD5 ESP Format

Security Parameters Index (SPI)

Initialization Vector (optional)

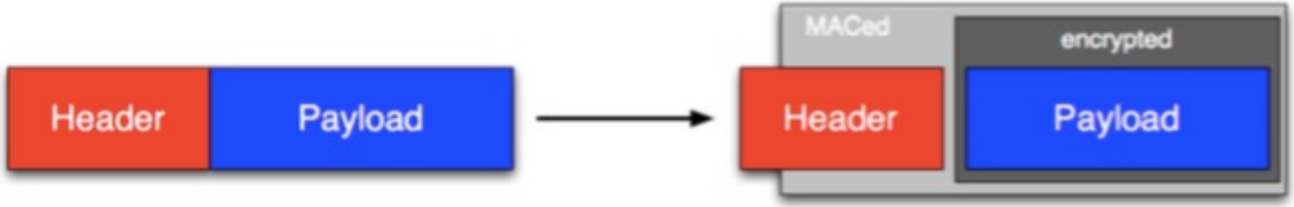
Replay Prevention Field (incrementing count)

Payload Data (with padding)

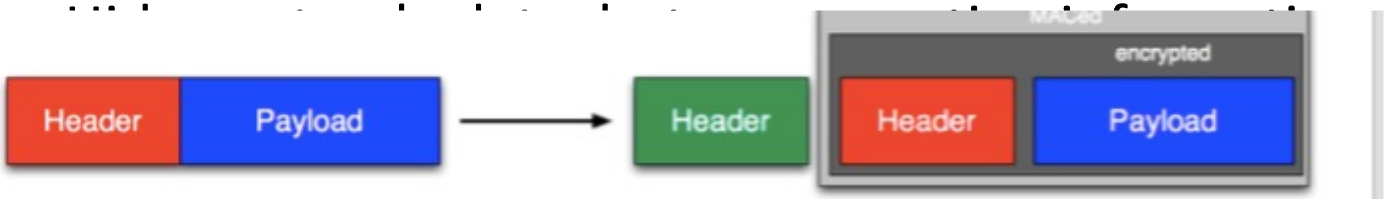
Authentication checksum

Modes of Operation

- **Transport**: the payload is (optionally) encrypted and the *non-mutable* fields are integrity verified (via MAC)



- **Tunnel**: each packet is completely encapsulated (and optionally encrypted) in an outer IP packet
  - [illegible]


Header
Payload
MACed
encrypted
Header
Header
Payload