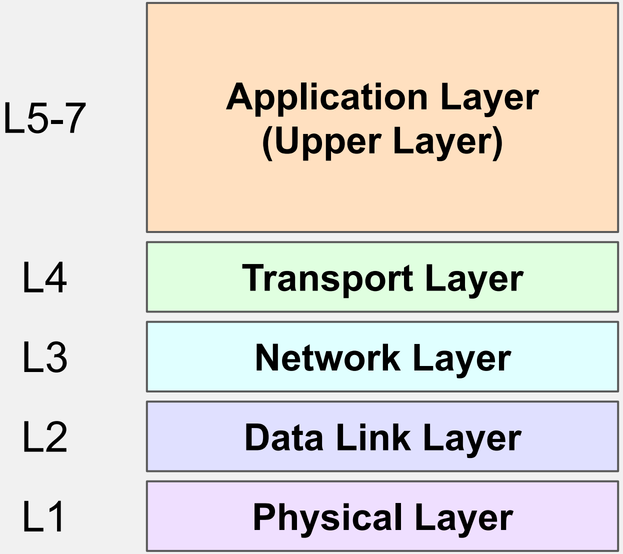
Network Security

Have you heard of VPNs?

This lecture is sponsored by [insert VPN provider].

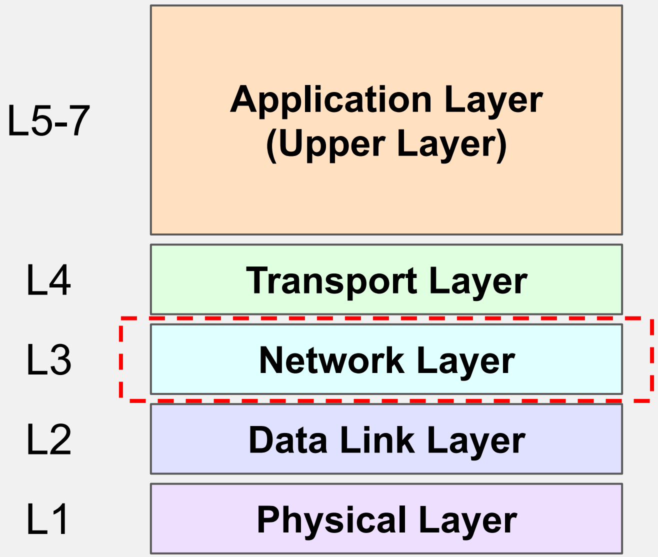
Gwendal Patat
Univ Rennes, CNRS, IRISA
2025/2026

Recall TCP/IP Model



TCP/IP Model

Today's Topic: Back to the Network Layer



TCP/IP Model

Remember IP

Internet Protocol (IP):

- Provide a best effort: no guarantee of packet delivery.
- Connectionless: no established connection between devices.
    - Remember: this is why TCP exists on the transport layer.

IP has no security by default:

- IP addresses can be spoofed.
- Packets can be sniffed.
- Packets can be modified.
- Packets can be replayed.

Security Issues with IP

When you receive an IP packet, you have **no guarantee** about:

- **Its origin.**
  - Can you be sure that the source address is the right one?
- **Its destination.**
  - Can you be sure that this packet was intended to you?
- **Its integrity.**
  - Can you be sure that nothing was modified during transit?
- **Its confidentiality.**
  - Can you be sure no one looked at the content of the packet?

Virtual Private Network (VPN)

Private Networks

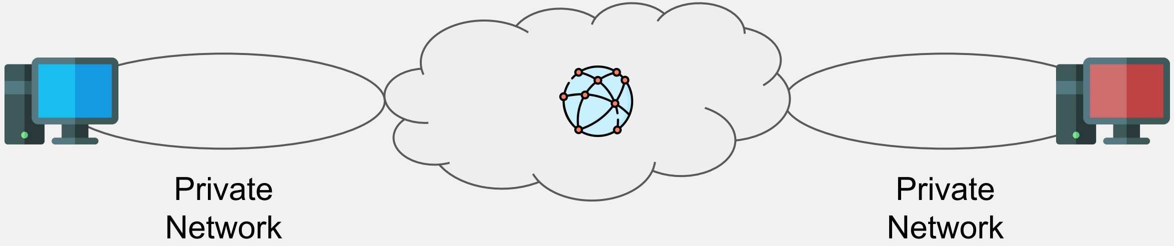
- Private networks offer notable security benefits:
  - Router on one end knows with confidence the identity of devices.
  - Router on the other end has good reason to believe no attackers were in the middle of the exchange.

- Problems:
  - A private network requires a lot of cables (imagine a private WAN)
  - Lack scalability and reliability

Virtual Private Network (VPN)

VPNs:

- Designed to provide a logical private network.
- Low cost, scalable, and reliable.
- Functions:
  - *Confidentiality*: no one in the middle should be able to **read** the data.
  - *Data Integrity*: no one in the middle should be able to **change** the data.
  - *Authentication*: the sender can check that the data **comes from the legitimate sender.**
  - *Antireplay*: the packet **cannot be copied and resent** later to appear as legitimate.



Remote Access VPN

The one we talk about with [Nord|Ghost|Mullvad|...] VPN or the ISTIC VPN.

Requires:

- A Network Access Server (NAS).
- A VPN client software.

NAS:

- Used to identify the user.
- Connects the user to the internet

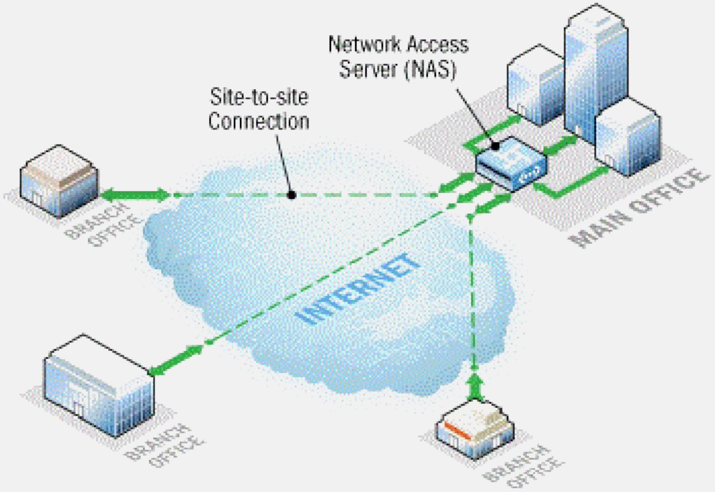
VPN client software:

- Used by the host to create a tunnel between them and the NAS.

Site-to-Site VPN

- Used to connect multiple locations together over the public network.
  - Useful for big organization.
  - Only need a VPN-aware router at each site.

- Advantages:
  - Transparent for hosts.
  - No need for a VPN client software,



Quick look at Cryptography

Security Goals

One of the pillars of security: **The CIA Triads**.

- **Confidentiality**
  - Information should be available only for the sender and the receiver.
- **Integrity**
  - For data: Information should not be tampered with.
  - For systems: The system inner workings have not been tampered with.
- **Availability**
  - Data or system should be available when needed.
    - e.g., resistant against Denial-of-Service (DoS).

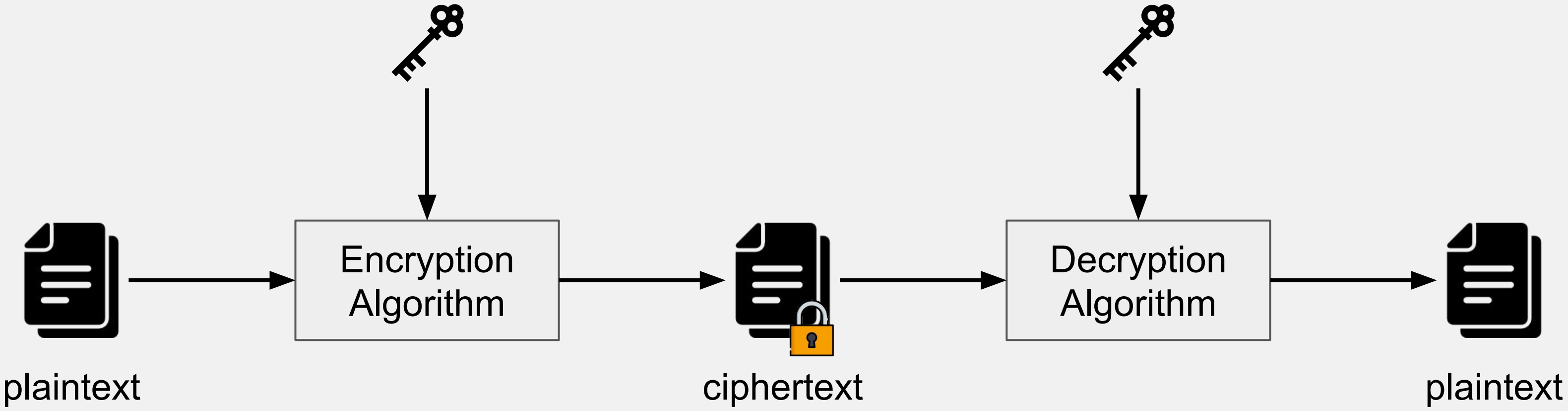
Additional Security Goals

- **Authentication**
  - User: Proven identity of communication partners.
  - Message: Information associated with its sender.
- **Accountability / Non-Repudiation**
  - Denial of communication not possible.

Cryptography

Encryption & key Exchange

Encryption



Encryption Algorithm
Decryption Algorithm
plaintext
ciphertext
plaintext

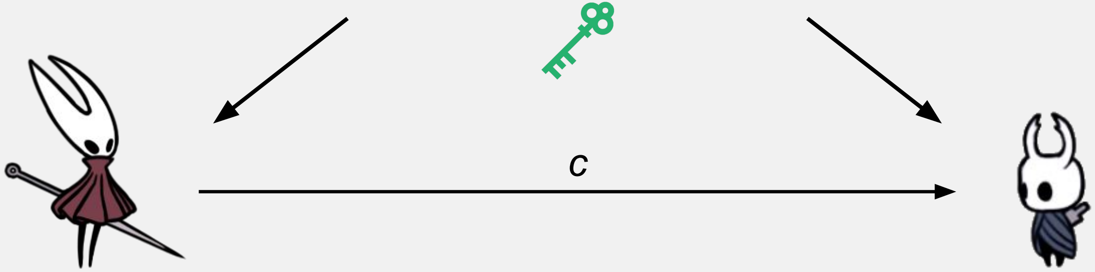
Symmetric Encryption

- Both Alice and Bob share the same ***secret key k***.
- This shared secret is used both for the **encryption** and **decryption** process.
- Ensure:
  - **Confidentiality.**

- **Example of algorithms:**
  - AES ➡ the go to since the mid 2000s.
    - Various modes: GCM, CBC
  - DES, 3DES ➡ Just don’t.
  - RC4 ➡ No really, just don’t.

Symmetric Encryption

Shared secret key ***k***



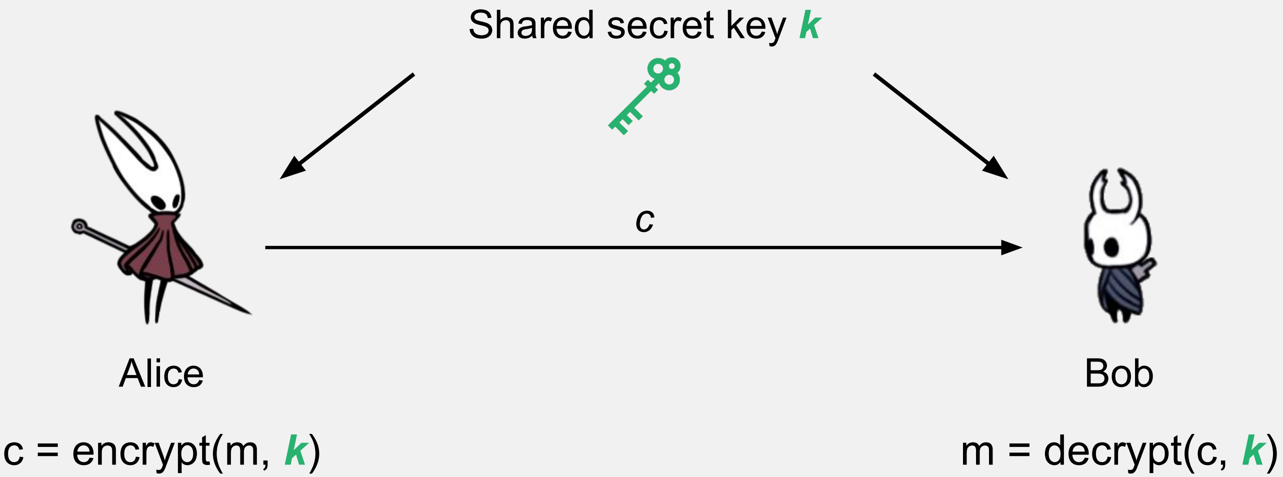
Alice

c = encrypt(m, ***k***)

Bob

m = decrypt(c, ***k***)

Symmetric Encryption



- Remaining problem: *How to share the secret key beforehand?*

Key Distribution Problem

Problem:

- Sender and receiver need to use encryption to create a secure channel.
- They need to share the same key.
- Therefore, they need a secure channel to share the secret key.
- Need a secure channel to create a secure channel?

Naive Key Distribution

Pre-Shared Key (PSK):

- The sender and receiver agree on a shared key before being apart.
- This PSK will probably never change.
    - This is a problem if an attacker managed to steal it: all past, present, and future communication will be vulnerable.

Key Exchange

Principle:

- The two parties agree on a shared secret key over an untrusted channel.

Diffie-Hellman (DH):

- Solves the key distribution problem using public keys.
- Two parties create a common symmetric key by exchanging public keys.

Hybrid Approach:

- Asymmetric algorithm to generate a new symmetric key.
- Symmetric algorithm for confidentiality.

Diffie-Hellman Key Exchange (DH-Key Exchange)

Alice

Public Channel

Alice and Bob agree on public parameters ***p*** *and* ***g***

Bob

Generate number a

$A = g^a \bmod p$

$s = B^a \bmod p$

Generate number b

$B = g^b \bmod p$

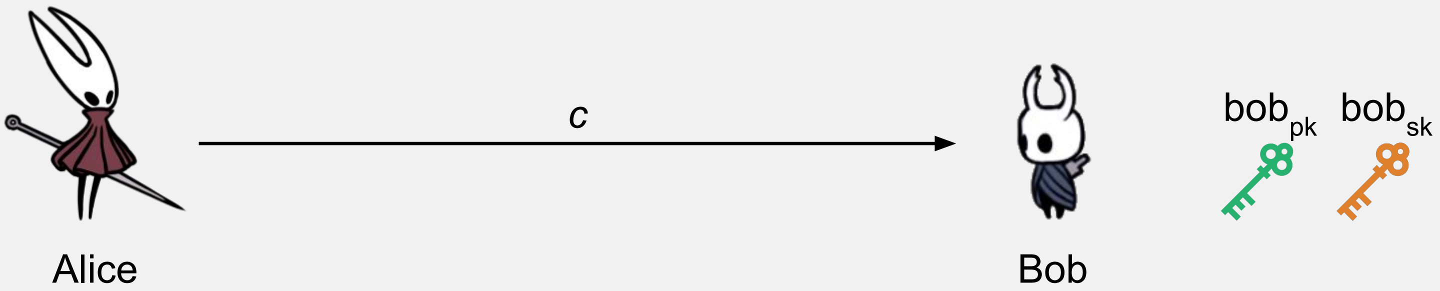
$s = A^b \bmod p$

Asymmetric Encryption

- Uses ***asymmetric cryptography***, also known as ***public-key cryptography***.
- Alice and Bob do not share the same secret.
- Each of them have both a public and a private key.
  - A ***public key*** (***pk)*** for others to send them messages.
  - A ***private key*** (***sk***) to decrypt received messages.
- Ensure:
  - **Confidentiality**.

- **Example of algorithms:**
  - RSA.
  - ElGamal.
  - Elliptic-curve cryptography (ECC).

Asymmetric Encryption



$c = \text{encrypt}(m, \text{bob}_{pk})$

$m = \text{decrypt}(c, \text{bob}_{sk})$

Cryptography
Signatures

Symmetric Signature

- **Message Authentication Codes (MACs)**
  - A MAC ensures integrity and authenticity of a message.
  - Both Alice and Bob share the same ***secret key k***.
  - Alice computes a tag ***t = MAC_k(m)*** and sends ***(m, t)*** to Bob.
  - Bob recomputes *MAC_k(m)* with the same key and checks if it matches t.
- **HMAC (Hash-based MAC)**
  - Practical implementation of a MAC using a hash function (e.g. SHA-256).

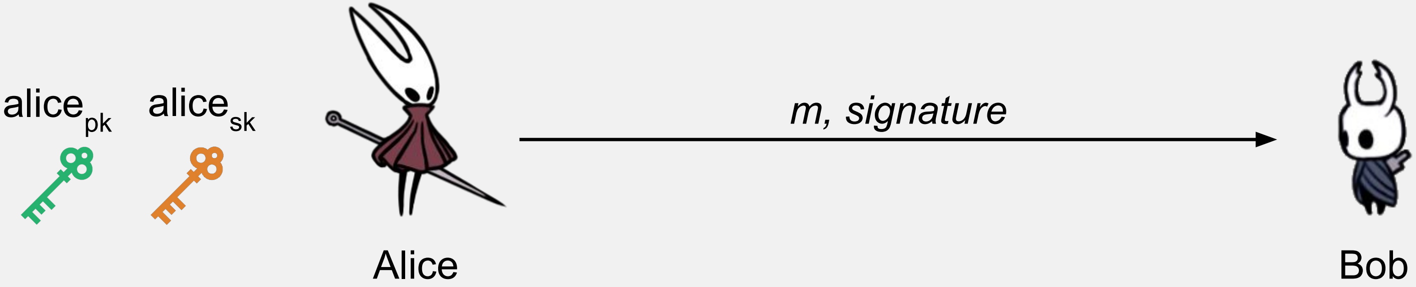
- Ensure **authenticity** and **integrity** but **no non-repudiation** since both share the same key.

Asymmetric Signature

- Also known as ***public-key signatures***.
- Alice uses her **private key (sk)** to **sign** a message.
- Anyone can use Alice's **public key (pk)** to **verify** the signature.
- Ensures:
  - **Authenticity** (message comes from Alice).
  - **Integrity** (message was not modified).
  - **Non-repudiation** (Alice cannot deny sending it).

- **Examples of algorithms:**
  - RSA signatures.
  - DSA (Digital Signature Algorithm).
  - ECDSA (Elliptic-curve DSA).

Asymmetric Signature



signature = sign(m, $alice_{sk}$)

verif(m, signature, $alice_{pk}$)

Symmetric VS Asymmetric

	Symmetric Key	Asymmetric Key
Encryption/Decryption	Same key used for both.	Different keys are used.
Speed of encryption/decryption	Fast.	Slower.
Size of ciphertext	~same as the message.	Bigger than the plaintext.
Key exchange	Problem to solve with, for instance, DH.	No problem.

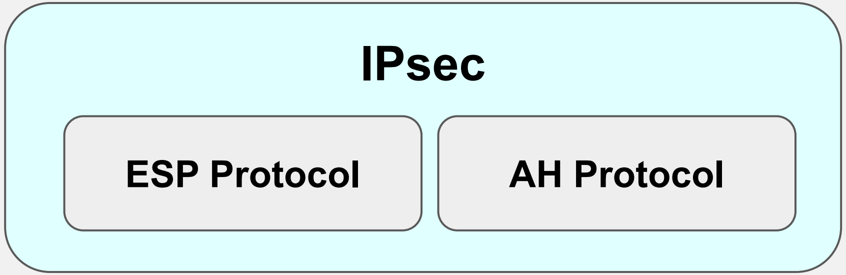
IPsec

IPsec Protocol Suite

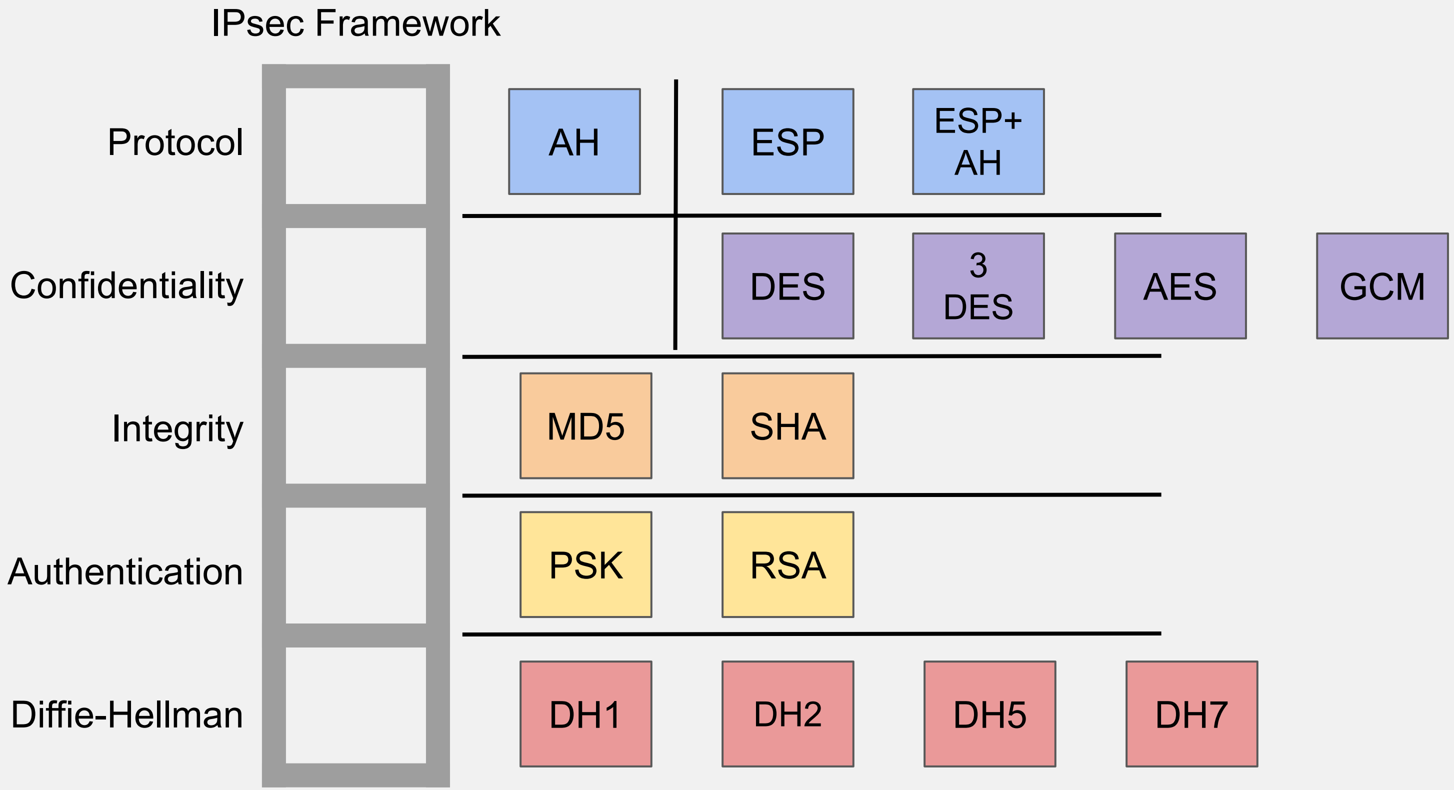
IPsec (Internet Protocol Security)

- Here to provide security to **layer 3**.
- One of the protocols used for VPNs.
- **Two protocols:**
  - *Authentication Header (AH)*
    - Integrity and authentication.
  - *Encapsulation Security Payload (ESP)*
    - Integrity, authentication, and confidentiality.
- **Two Modes:**
  - *Transport Mode*: end-to-end
  - *Tunnel Mode*: network-to-network

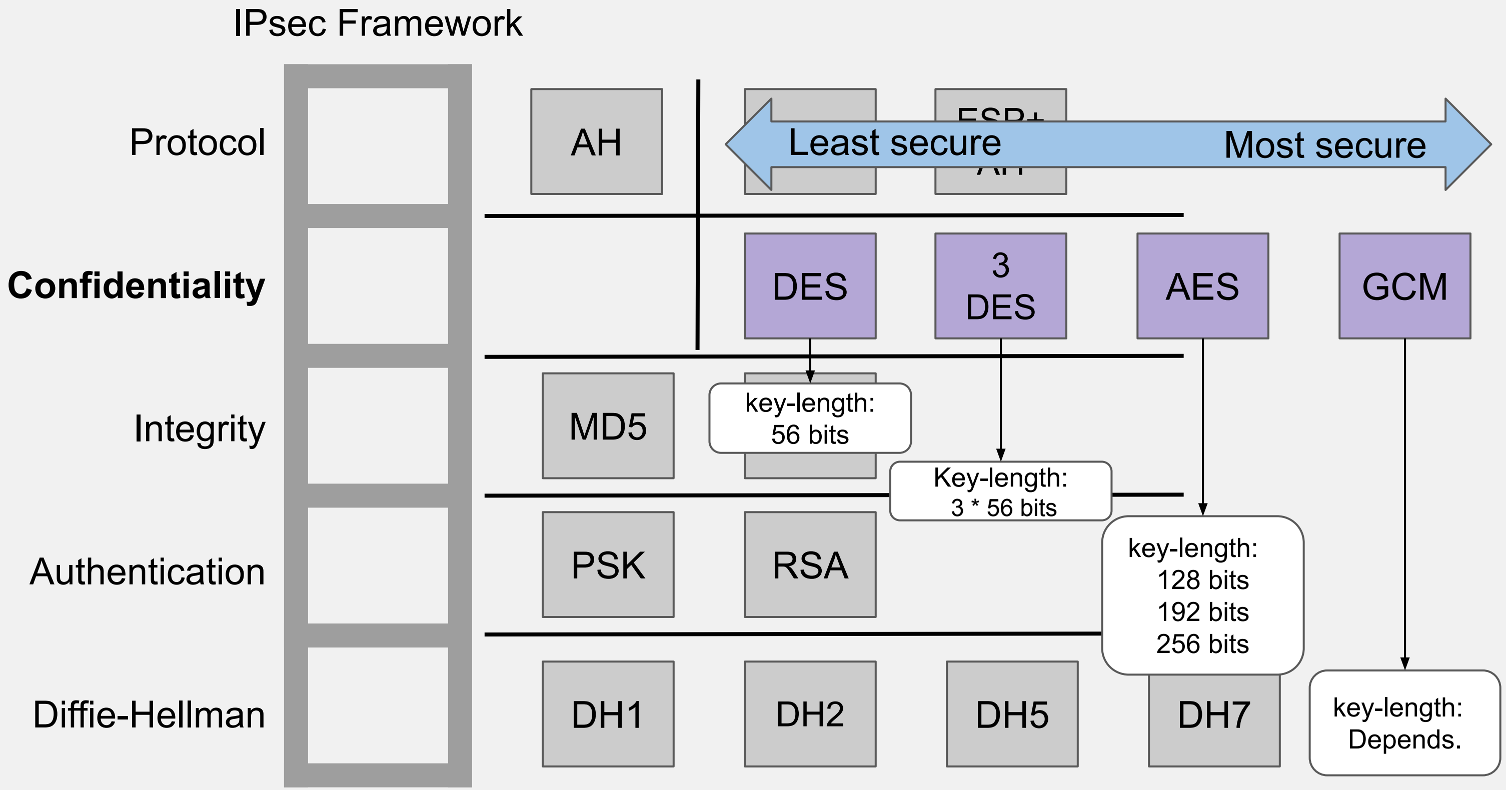
IPsec is highly configurable.



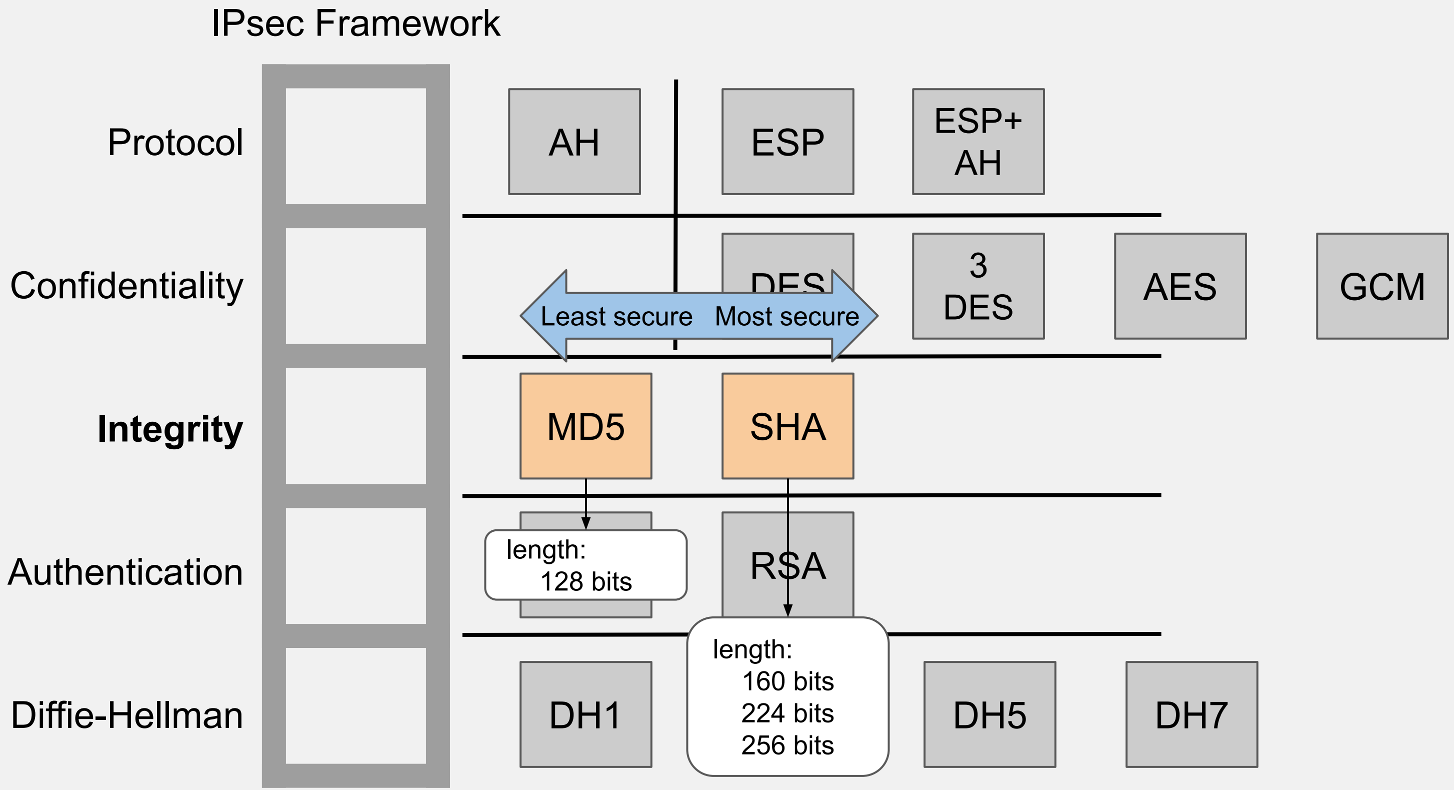
IPsec Protocol Framework



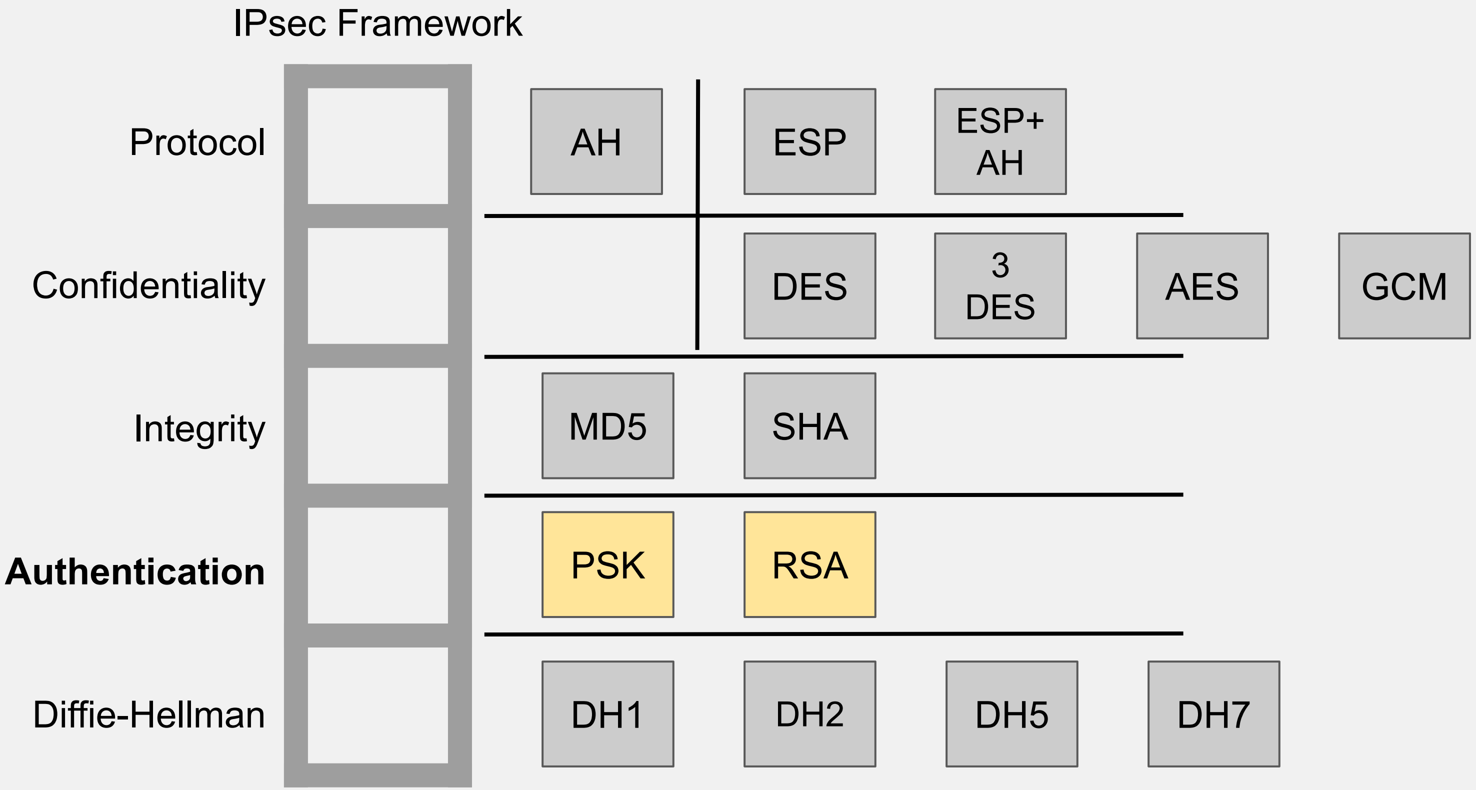
Confidentiality



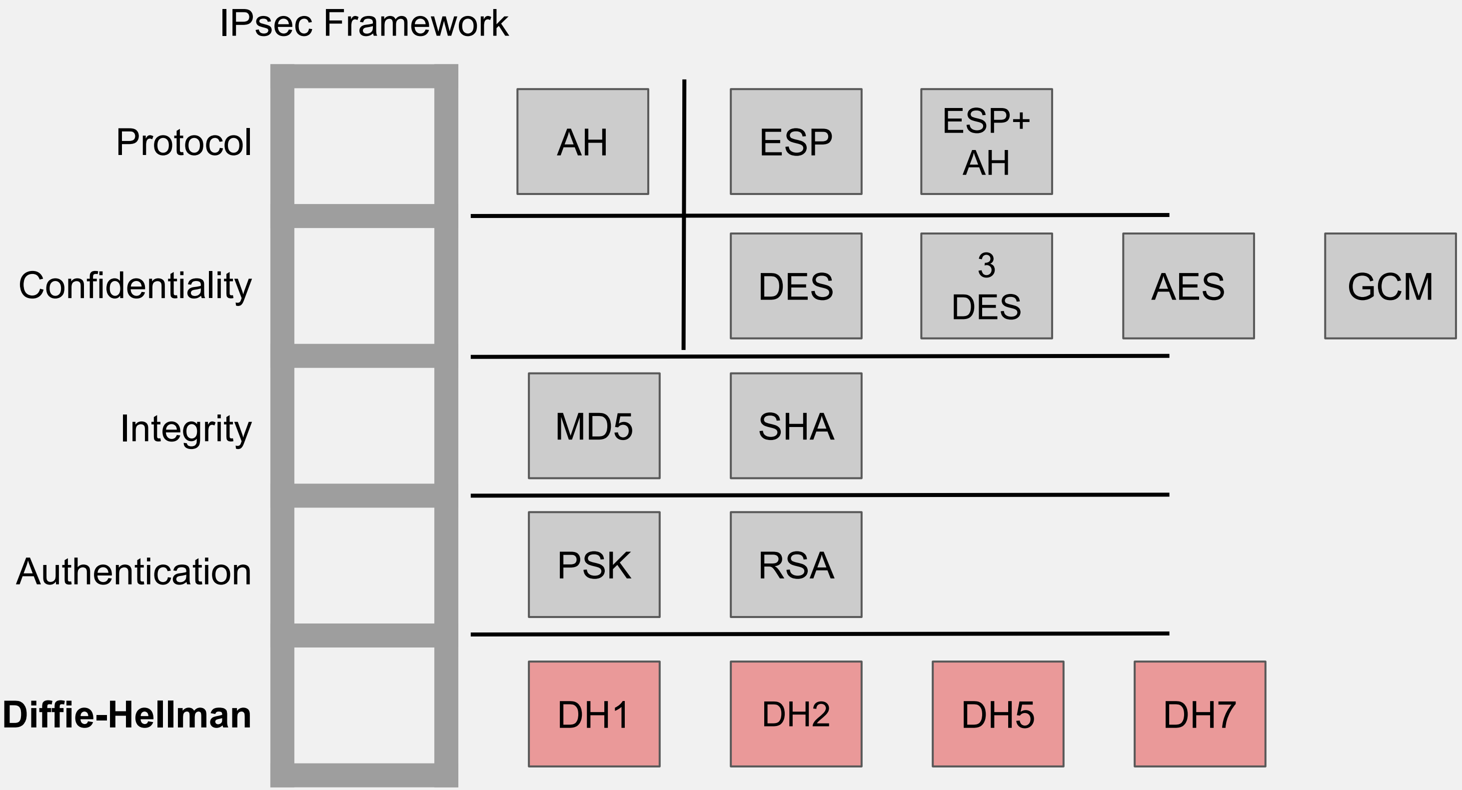
Integrity


IPsec Framework
Protocol
Confidentiality
Integrity
Authentication
Diffie-Hellman
AH
ESP
ESP+
AH
DES
3
DES
AES
GCM
Least secure
Most secure
MD5
SHA
length:
128 bits
RSA
length:
160 bits
224 bits
256 bits
DH1
DH5
DH7

Authentication



Diffie-Hellman



IPsec Modes

IPsec modes of Operation

Two modes:

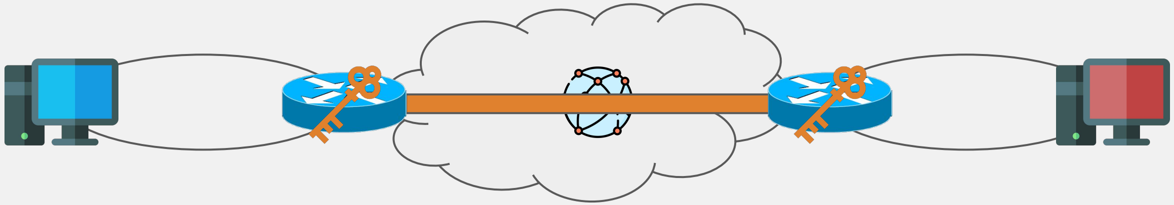
- Tunnel Mode
- Transport Mode

Modes:

- Defines how IP packets are encapsulated with IPsec.
- IPsec headers change depending on the mode of operation.
- IPsec modes is linked to the VPN types (site-to-site, remote-access).

Tunnel Mode

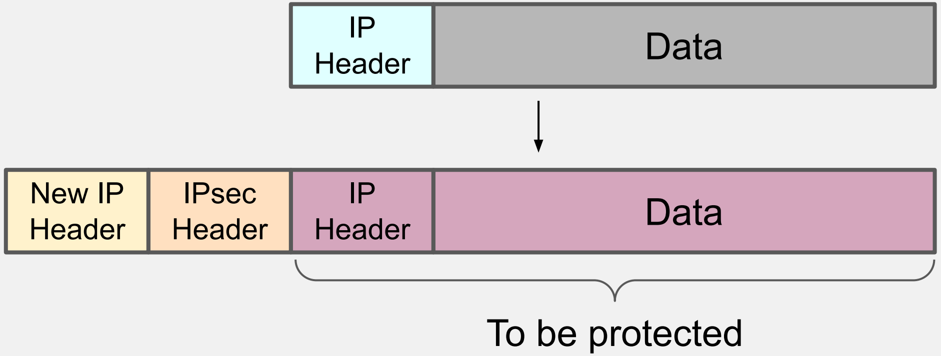
- IPsec server on each network.
- Security over the outside networks.
- Transparent for hosts.
- No security within the site network.



Tunnel Mode Encapsulation

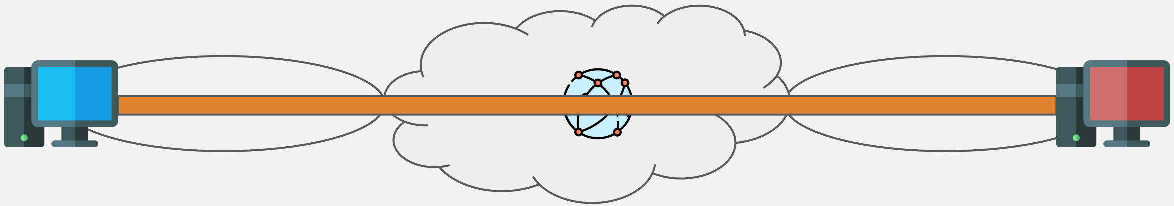
Encapsulate the whole packet and protect it:

- Original IP header could then be encrypted, we need a **new IP Header.**
- If the IPsec protocol encrypt the payload, the original src and dst IPs are hidden.



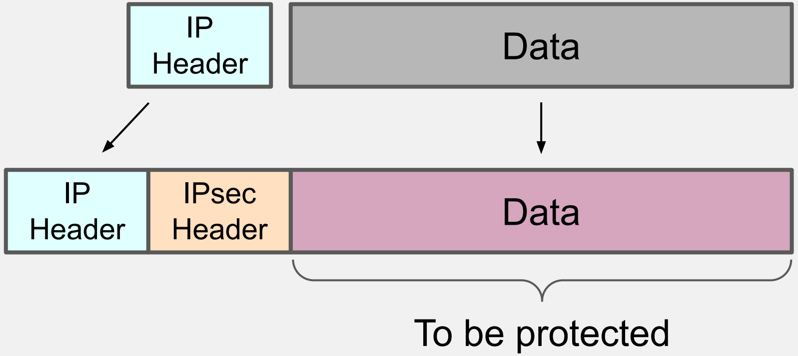
Transport Mode

- End-to-end security between hosts.
- Security within local site as well.
- IPsec on host.

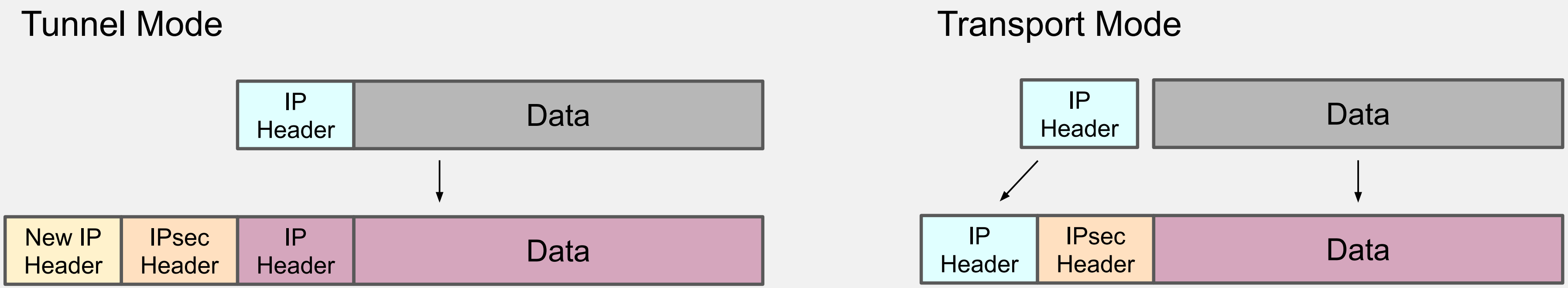


Transport Mode

- The IPsec header is inserted between the IP header and the data.
- Both addresses are visible on the public network.



IPsec Encapsulation



Tunnel Mode VS Transport Mode

- Tunnel Mode
  - Protect the original IP header.
  - Not vulnerable to traffic analysis attacks.
  - No on-site protection.
  - Add 20 bytes (new IP header) to the packet.
  - Good for VPN, gateway to gateway

- Transport Mode
  - Packets are protected from source to destination.
  - No additional byte.
  - Good with ESP.

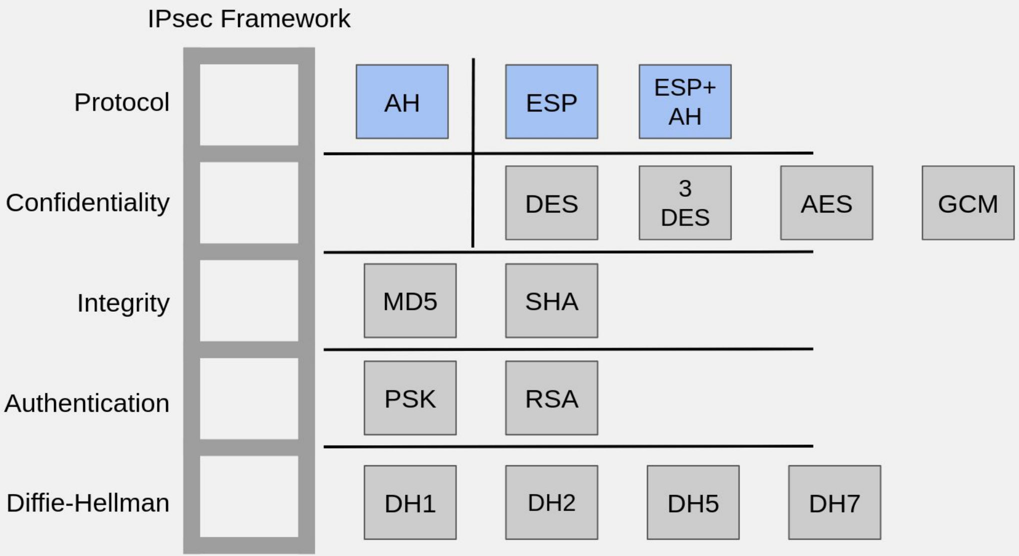
IPsec Protocols

IPsec Protocols

Main protocols:

- **AH:** Authentication Header
- **ESP:** Encapsulation Security Payload

Can be used together or separately.



Authentication Header (AH)

AH provides:

- *Integrity*: the data have not been tampered with.
- *Authentication*: the sender can be authenticated.

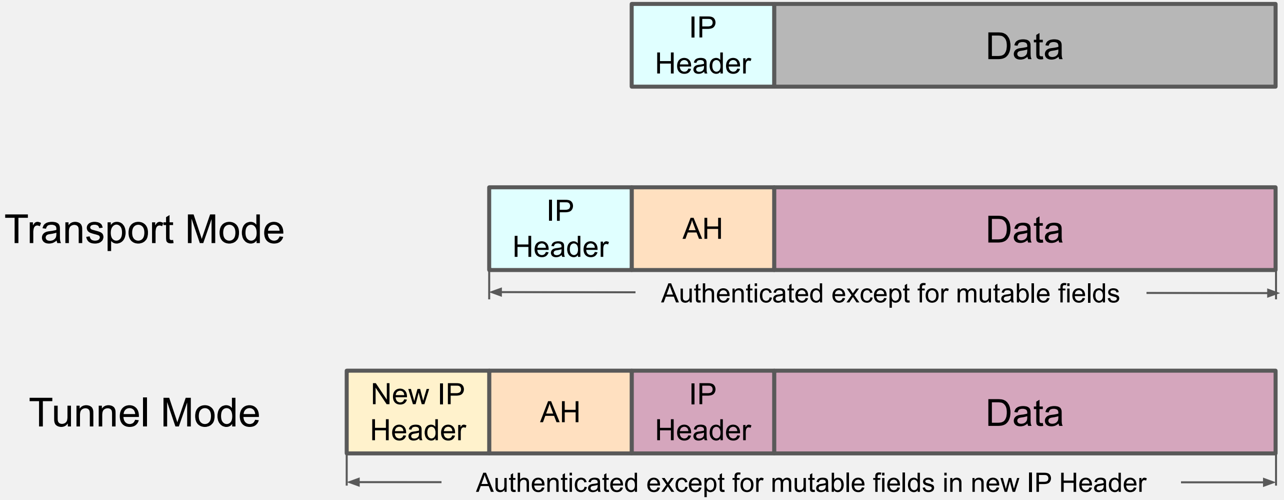
AH **does not** provide confidentiality.

- The data are not encrypted.

Relies on HMAC-MD5 and HMAC-SHA algorithms.

IPsec Modes with AH

Protect the whole IP packet, including the IPsec header and new IP header in tunnel mode.

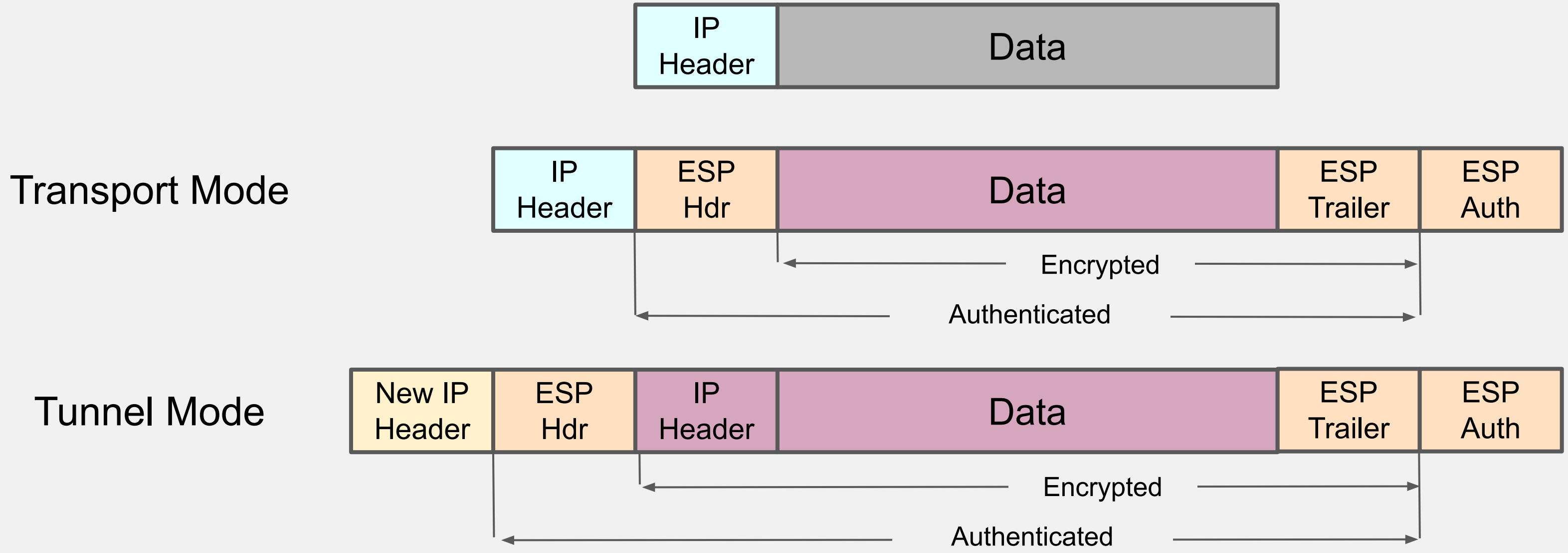


Encapsulation Security Payload (ESP)

- Can also be found under the name ***Encapsulation Security Protocol***.
- ESP provides ***confidentiality***, ***integrity***, and ***authentication.***
  - But **not for the whole packet**.
  - Uses HMAC for data integrity, anti-replay, MitM protection …
- ESP can also be used with confidentiality or authentication only.
  - When both are used: ***encrypt then authenticate***.
    - Less processing time if the packet needs to be discarded.

IPsec Modes with ESP

ESP does not protect IP headers, or encrypt the IPsec headers.



ESP vs AH

Property	ESP	AH
Authentication	Yes, partial	Yes
Integrity	Yes	Yes
Confidentiality	Yes	No
Antireplay	Yes	No

Why AH then?

- AH and ESP are designed by different groups.
    - AH designers were IPv6 supporters.
    - AH looks more like IPv6: uses extension headers instead of full encapsulation.
- Originally, ESP was only for encryption.
    - Integrity was added after to ESP.
- Routers and firewall can use layer 4 header for filtering.

IPsec vs NAT

Private Addressing

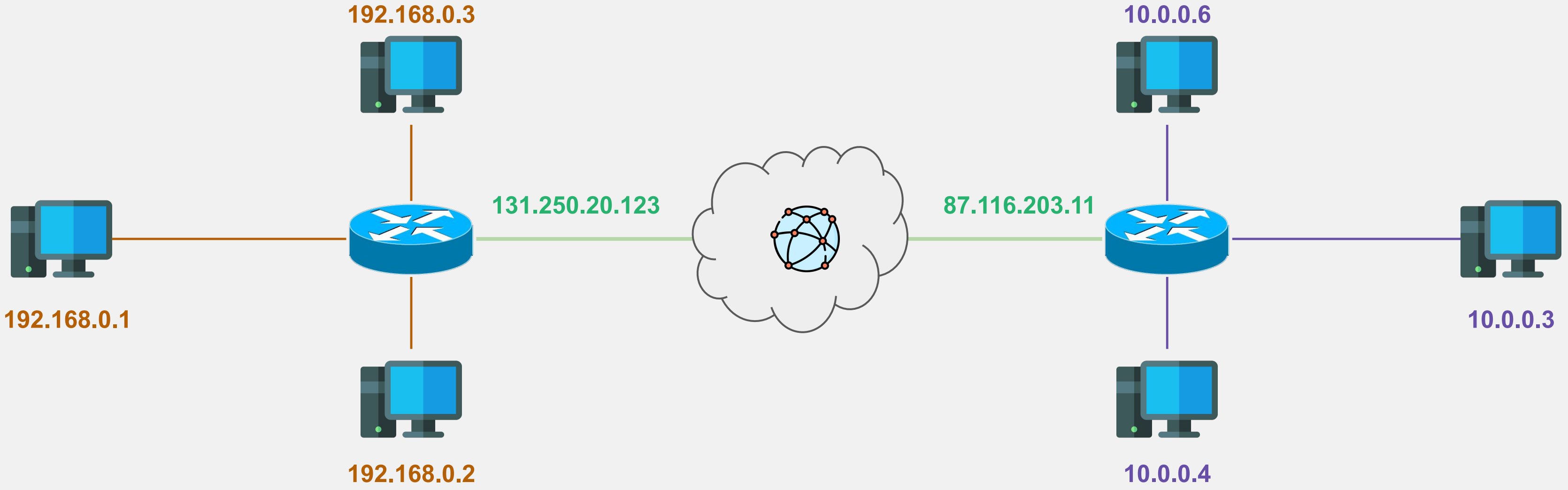
- Public vs Private IPs
  - Public: unique address over the Internet.
  - Private: unique within the LAN.
- The private IP ranges have been defined by the IANA and cannot be advertised over the internet:

CIDR	**Range**
10.0.0.0/8	10.0.0.0 – 10.255.255.255
172.16.0.0/12	172.16.0.0 – 172.31.255.255
192.168.0.0/16	192.168.0.0 – 192.168.255.255

Network Address Translation (NAT)

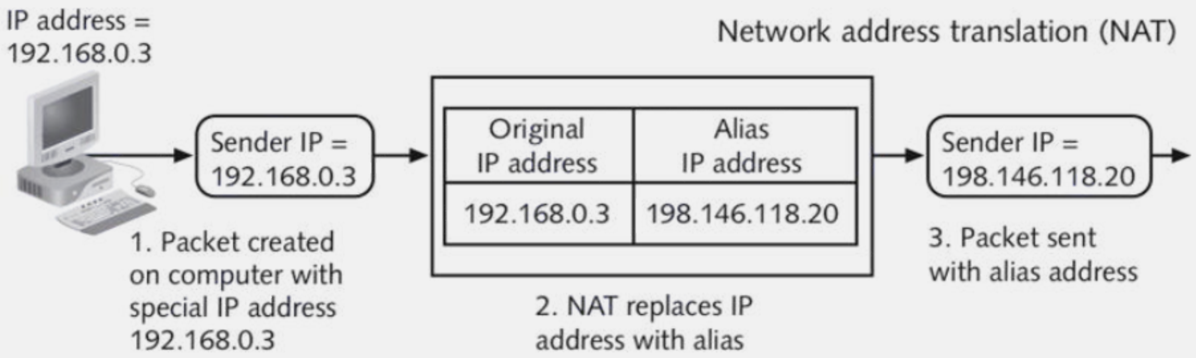
- The NAT protocol allows hosts with private IP addresses to access the Internet.
- NAT will translate IP addresses during:
  - **Outgoing traffic**: By replacing the src address with a public address.
  - **Incoming traffic**: By replacing the dst address with the corresponding private IP of the host.

Network Address Translation (NAT)

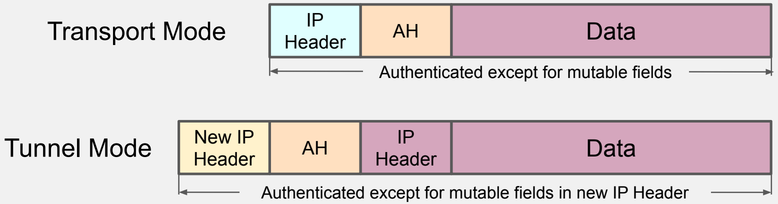


NAT

- NAT is run on routers that connect private networks to the Internet.
- NAT modifies the IP header of the packet.



NAT and AH



AH protect the integrity of the **whole IP packet.**

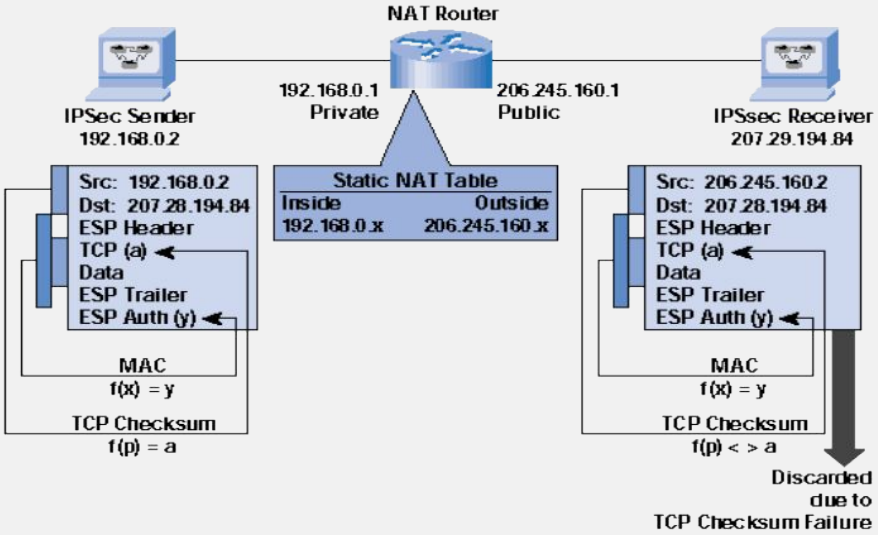
If any field of the original header is modified (private/public IPs), the authentication will fail.

AH + NAT cannot work.

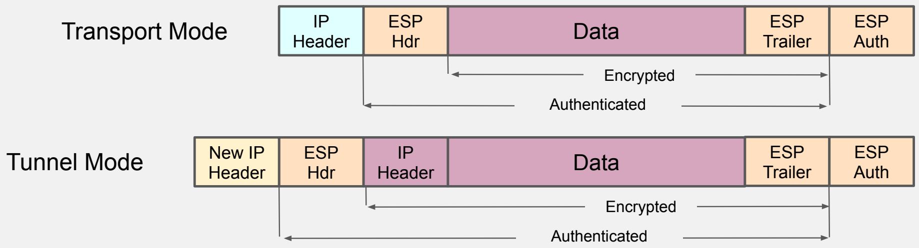
NAT and ESP

NAT modifies the **IP header.**

- NAT must also modify the **L4 checksum**.
  - Yes, in real life implementations the TCP/UDP checksum uses IPs…



NAT and ESP



With NAT, a router associate a private IP address with a public one.

- Meaning the **IP is modified** which **influence the L4 checksums**.

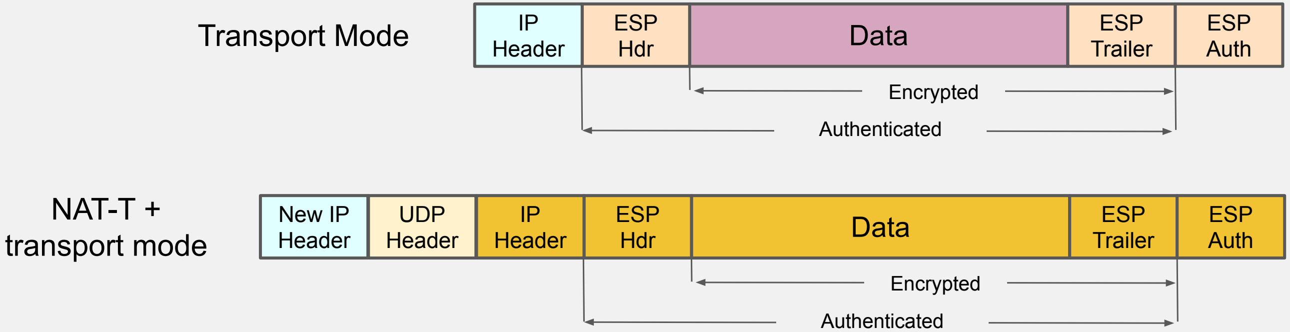
In transport mode, NAT need to modify the layer 4 header.

- If NAT updates the L4 checksum, ESP auth will fail.
- If it does not, due to encryption for instance, L4 verification will fail.

ESP + NAT can work in tunnel mode, or in transport mode with L4 checksums disabled or ignored, or using NAT-T.

NAT-T and ESP

To go around the problem, NAT-T can be setup on router to encapsulate the IPsec packet in a new UDP packet with new IP header.



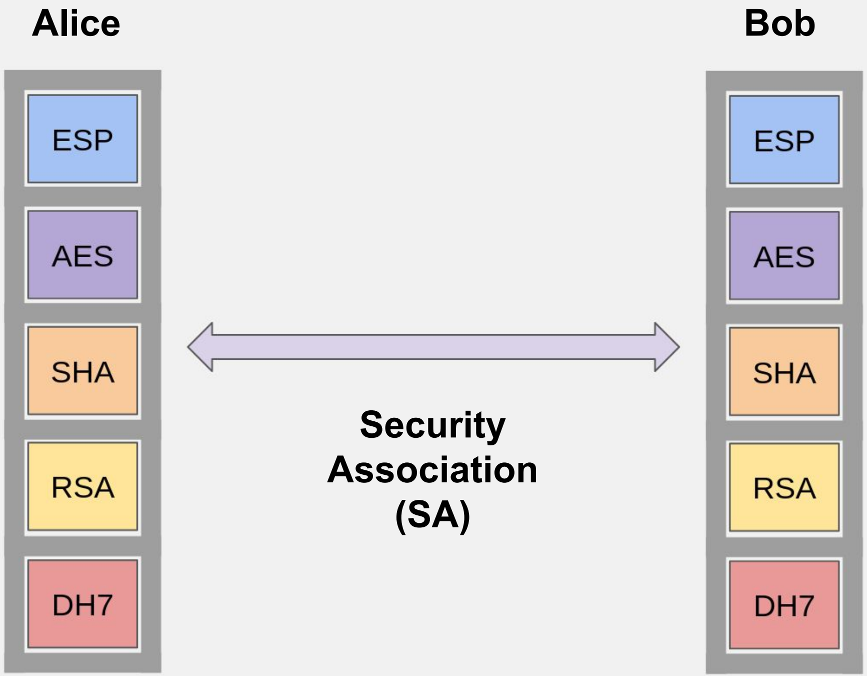
Internet Key Exchange (IKE)

IKE/IPsec Protocols

IPsec and IKE protocols are used to setup secure channels.

IKE Protocol:

- Exchange and negotiate security policies.
- Establish security session
  - Security Associations (SA)
- Key exchange
- Key Management



IKE

IKE operates in two phases.

Phase 1: Negotiate and establish a end-to-end secure channel.

- Used by phase 2.
- Established once between two endpoints.

Phase 2: Negotiate and establish custom secure channels.

- Can occur multiple times.

Both phases will use DH key exchange to share keys.

IKE Phase 1

The goal of phase 1 is to establish a secure channel between two hosts to allow phase 2 to be protected.

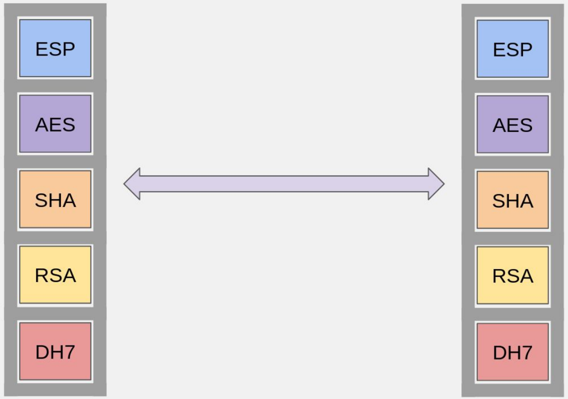
It provides:

- Source authentication
- Data integrity and confidentiality.
- Antireplay.

Uses standard parameters:

- Encryption = DES, hash=MD5/SHA1, authentication: Pre-shared key, Exchange: DH

IKE Phase 2



Use secure channel established in phase 1.

Goal: negotiate the ESP/AH parameters.

- 1er message: Authentication and parameters proposition [DH].
- 2nd message: Authentication and proposition acceptance [DH].
- 3rd message: Validation and acknowledgment.

Resources and Acknowledgements

- *Computer Networking: A Top-down Approach* by James F. Kurose, Keith W. Ross
- Previous materials from Prof. Mohamed Sabt, Univ Rennes, CNRS, IRISA.