IPSEC

- Objetivo: proporcionar a IP (IPv4, IPv6) mecanismos de seguridad

- Servicios de Seguridad
  - Integridad sin conexión
  - Control de Acceso
  - Autenticación
  - Mecanismos anti-replay
  - Confidencialidad de datos
  - Confidencialidad de flujo de tráfico limitada

IPSEC

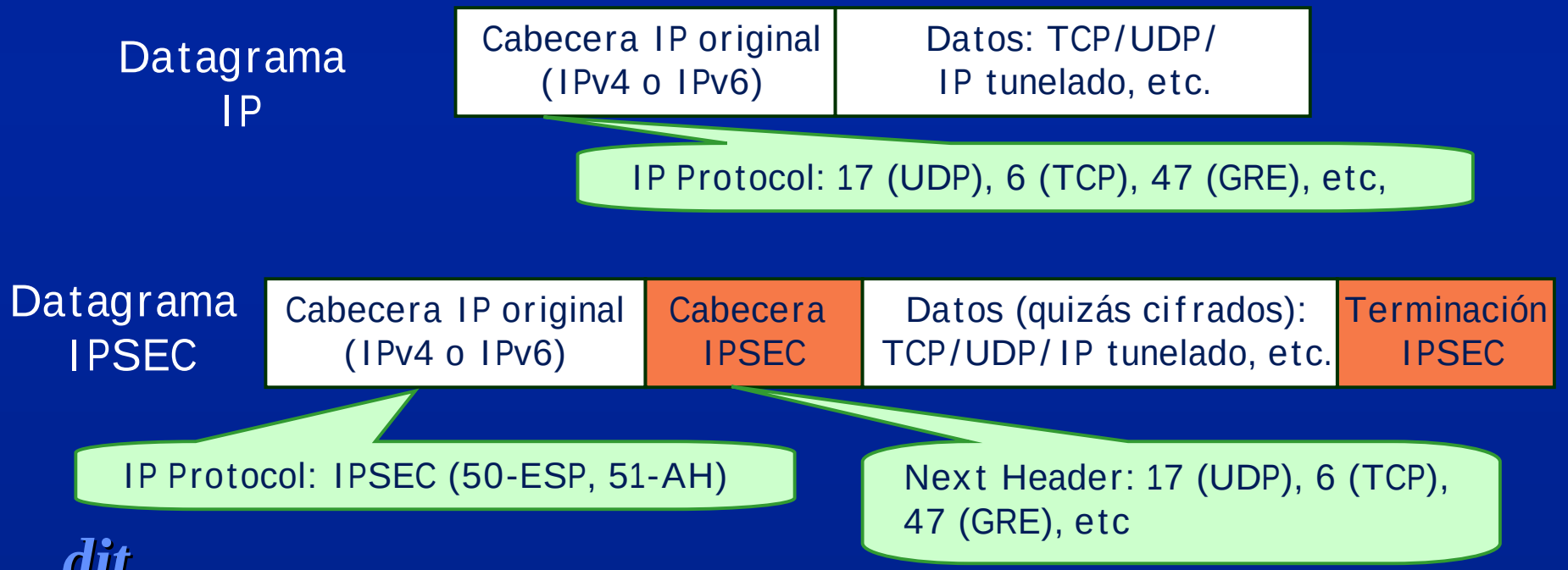
- Modos de utilización de IPSEC
  - Modo Transporte
    - ✓Directamente entre sistemas remotos
    - ✓Los sistemas remotos deben implantar IPSEC
  - Modo Túnel
    - ✓Entre sistemas intermedios
    - ✓Se establece un túnel seguro para encapsular los datagramas IP inseguros

Ámbito de IPSEC

- IPSEC ofrece tres funcionalidades principales:
  - Sólo autenticación
    - ✓Conocida como Authentication Header (AH)
  - Cifrado + Autenticación
    - ✓Conocida como Encapsulating Security Payload (ESP)
  - Una función de gestión de claves
    - ✓IKE (ISAKMP / Oakley)
- IPSEC no define los algoritmos de seguridad que se usan.
  - Marco para poder utilizar múltiples algoritmos a elección de los sistemas participantes.

Ámbito de IPSEC

- ¿Cómo se transmite IPSEC?
  - Una nueva cabecera en el datagrama IP entre la cabecera original y los datos
  - Para ESP, los datos se cifran y se añade una terminación de datagrama



IPSEC Security Association (SA)

- Contexto de interoperabilidad usada en AH y ESP
- Relación uno a uno entre transmisor y receptor que define el conjunto de parámetros de seguridad utilizados
- Es necesario establecer una SA previamente a la comunicación: IKE
- Contenido de una SA:
  - Security Parameter Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier

Security Association (SA)

- Security Parameter Index (SPI)
  - Bitstring asignado a la SA con significado local sólo.
    - ✓Puntero a base de datos de SA (SPD: Security Policy Database).
  - Se transmite en las cabeceras de AH y ESP para seleccionar la SA que procesará dicho mensaje
- IP Destination Address
  - Solo se permiten direcciones unicast
- Security Protocol Identifier (SPI)
  - Identifica que tipo de seguridad se usa
    - ✓AH (solo autenticación)
    - ✓ESP (cifrado y posiblemente autenticación)

¿ Qué define una SA (I) ?

- *Sequence Number Counter*
  - Valor de 32 bits para generar el numero de secuencia transmitido en las cabeceras AH y ESP
- *Sequence Counter Overflow*
  - Indicador de acción ante un llenado del nº de secuencia
- *Anti-Replay Window*
  - Ventana para limitar la aceptación de datagramas válidos
- *AH Information*
  - Algoritmos de autenticación, claves, tiempos de vida, etc. usados en AH

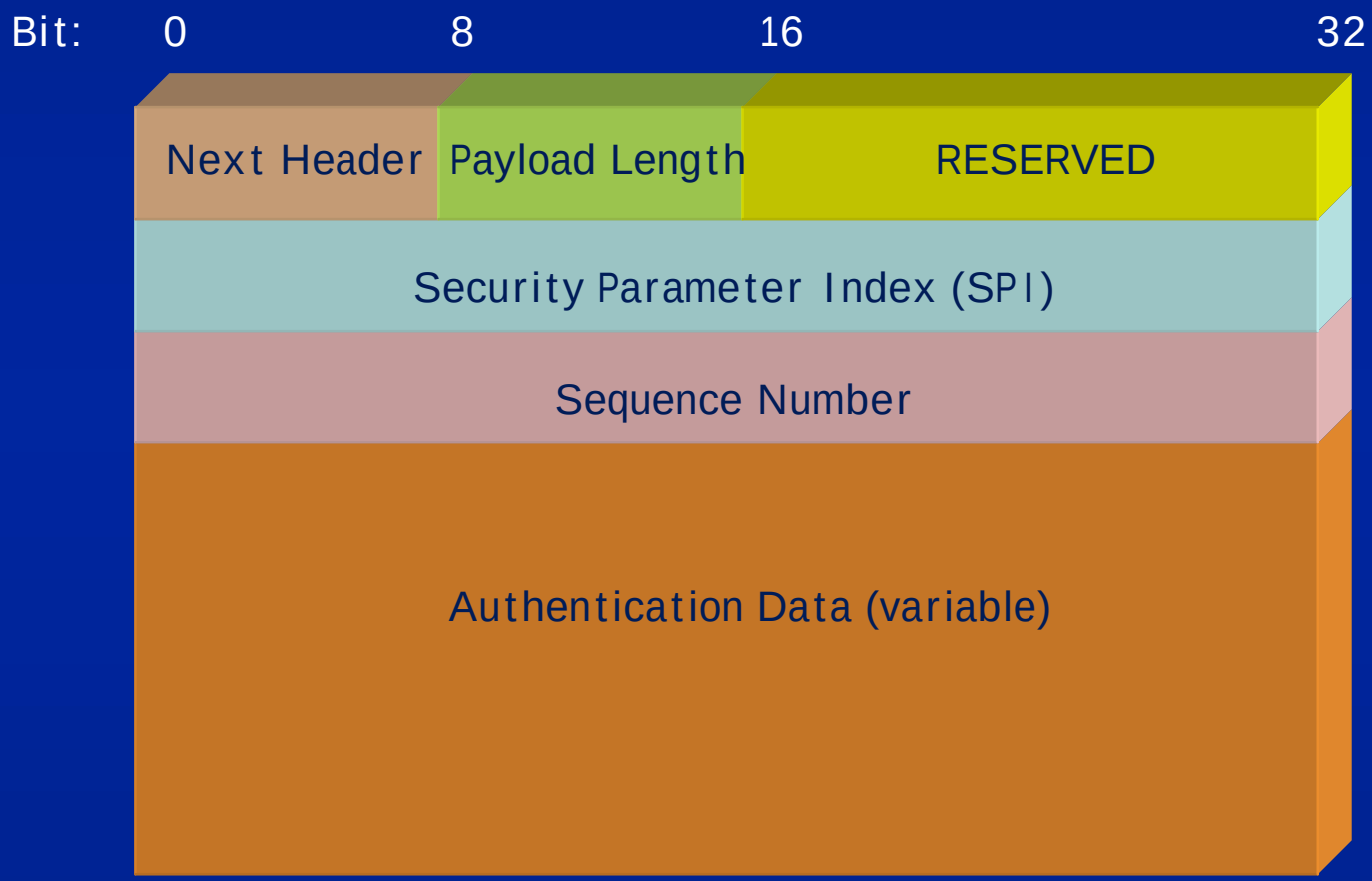
¿ Qué define una SA (II) ?

- *ESP Information*
  - Algoritmos de cifrado y autenticación, claves, valores de inicio, tiempos de vida, etc. usados en ESP
- *IPSEC Protocol Mode*
  - Modo transporte, túnel o wildcard
- *SA Lifetime*
  - Intervalo de tiempo o bytes después del cual hay que sustituirla por una nueva SA
- *Path MTU*
  - Máximo tamaño de paquetes transmitidos sin fragmentación

Modo de Autenticación: AH

- AH: Authentication Header
- Proporciona soporte para la autenticación e integridad de datagramas IP
  - Los cambios en el contenido son detectados
  - Los destinatarios pueden autenticar al origen
  - Previene los ataques de IP-spoofing
  - Protege el ataque de retransmisión

IPSEC Authentication Header (AH)



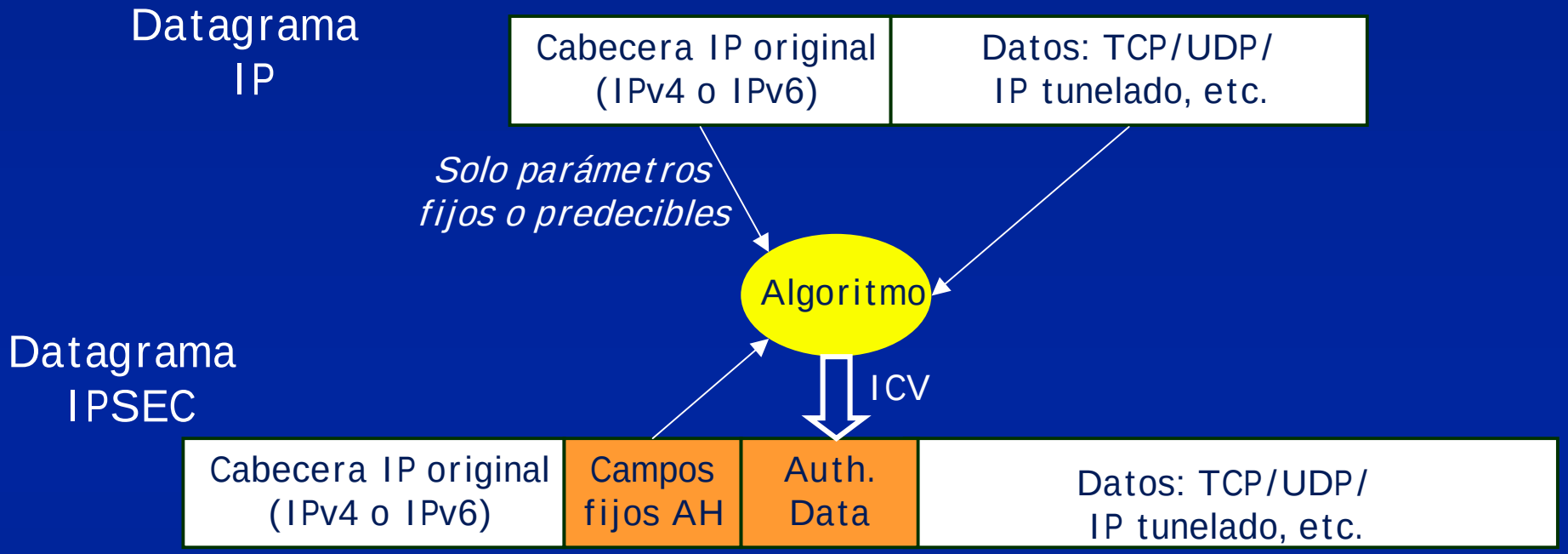
IPSEC Authentication Header

- Next Header: tipo de protocolo de datos que se transmite dentro de IP (p.e. TCP, UDP, GRE, etc.)
- Payload Length: Longitud de la cabecera AH
- Security Parameter Index (SPI): identificación de la SA de este datagrama.
- Sequence Number: contador que se incrementa monotónicamente con cada paquete
- Authentication Data: contiene el Integrity Check Value (ICV)

Authentication Header (AH)

- La autenticación se basa en el uso de un *Integrity Check Value* con un algoritmo especificado en la SA.
- Entrada: porción del mensaje y clave secreta
- Salida: ICV que se transmite en el campo Authentication Data de AH
- Se hace el calculo sobre:
  - Todo el contenido del datagrama
  - Los campos de la cabecera IP que no cambian en tránsito o son predecibles
  - La cabecera AH expecto el campo Authentication Data
- Algoritmos: para interoperabilidad, al menos MD5 y SHA-1

Calculo de Authentication Data



Campos mutables de cabecera IPv4

- TOS
- Flags
- Fragment Offset
- TTL
- Header Checksum

Campos predecibles de cabecera IPv4

- Destination Address

Anti-Replay

- Ataque: retransmitir paquete válido
- Defensa: número de secuencia en cabecera AH
  - Al establecer una SA, se inicializa a 0
  - Con cada paquete, se incrementa en 1 y se envía.
  - Si se llega a 2^{32}-1, se termina la SA y se negocia otra
- Pero IP no asegura la entrega ni el orden
  - El receptor tiene ventana deslizante de tamaño 64
  - Especifica los números de secuencia intermedios que el receptor es capaz de aceptar

Modo de cifrado: ESP

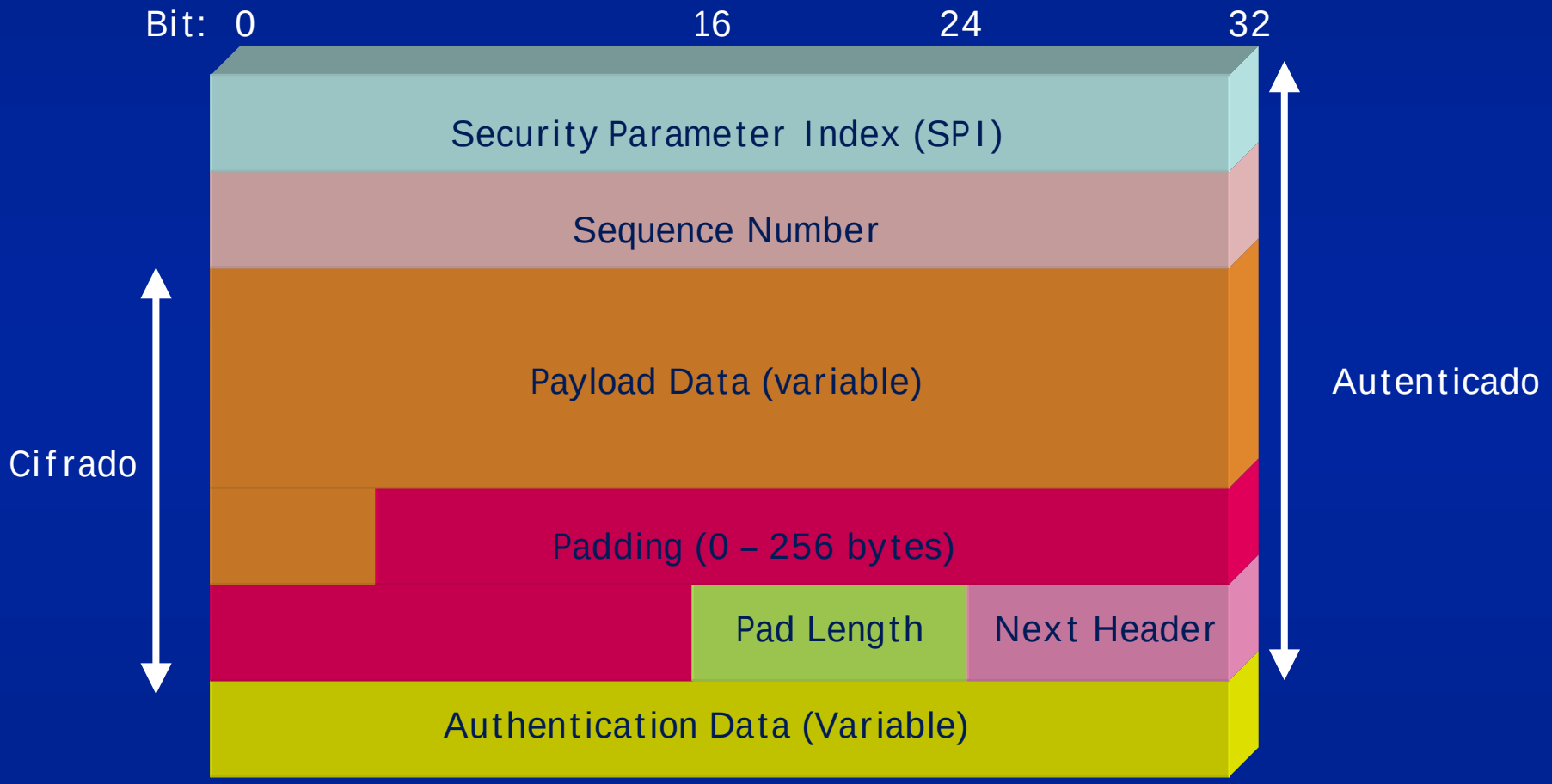
- ESP: Encapsulating Security Payload

- Proporciona:
  - Confidencialidad de contenidos
  - Confidencialidad limitada de flujo de tráfico
  - Opcionalmente, servicio de autenticación como AH

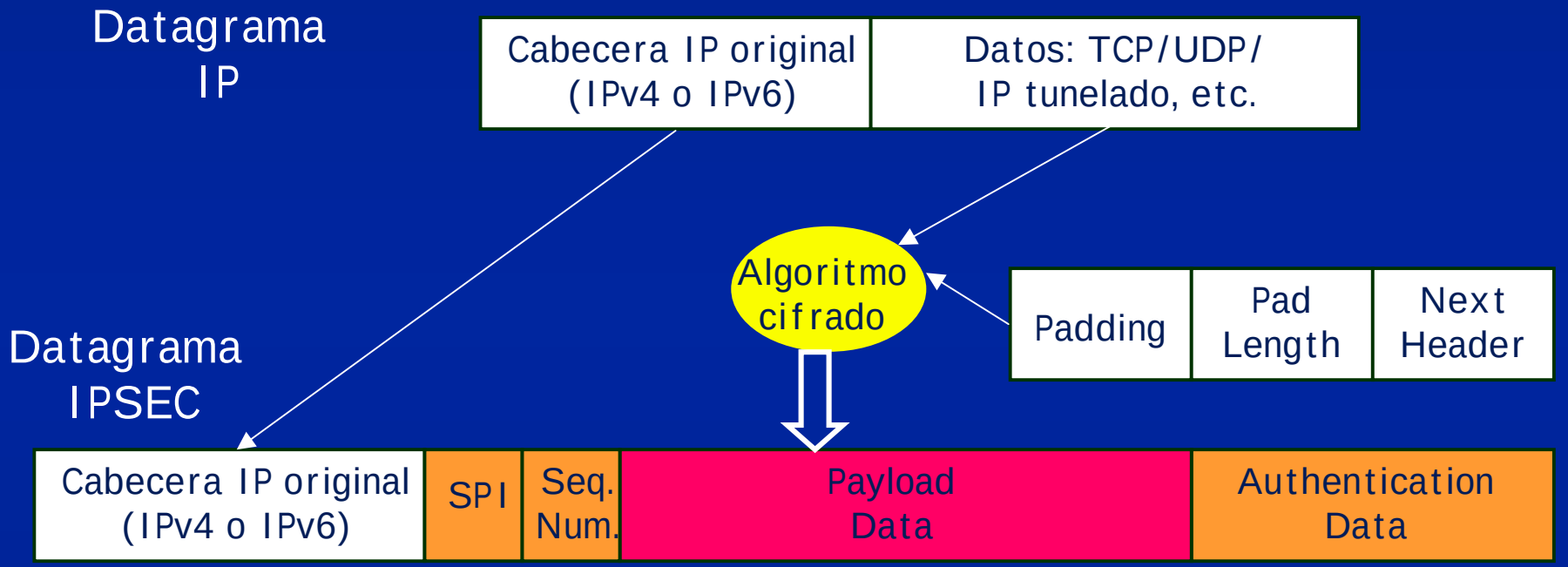
Campos de ESP

- Security Parameter Index (SPI): identificación de la SA de este datagrama.
- Sequence Number: contador que se incrementa monotónicamente con cada paquete
- Payload Data: Datos cifrados del protocolo IP
- Padding: bytes extra necesarios si el algoritmo de cifrado requiere bloques completos de texto
- Pad Length: Numero de bytes de pad en padding
- Next Header: tipo de protocolo de datos en el payload data.
- Authentication Data: ICV calculado sobre todo el datagrama (menos el campo Authentication Data)

Formato del datagrama ESP



Funcionamiento de ESP



Algoritmos criptográficos

- Se especifica en la SA
- Para cifrado, se deben usar algoritmos de cifrado simétrico
- Para interoperabilidad, al menos se deben soportar:
  - DES en modo CBC para cifrado
  - MD5 y SHA-1 para autenticación
- Se pueden usar muchos otros (con identificador):
  - Por ejemplo, triple DES, RC5, IDEA, CAST, Blowfish, etc.

Modo transporte y túnel

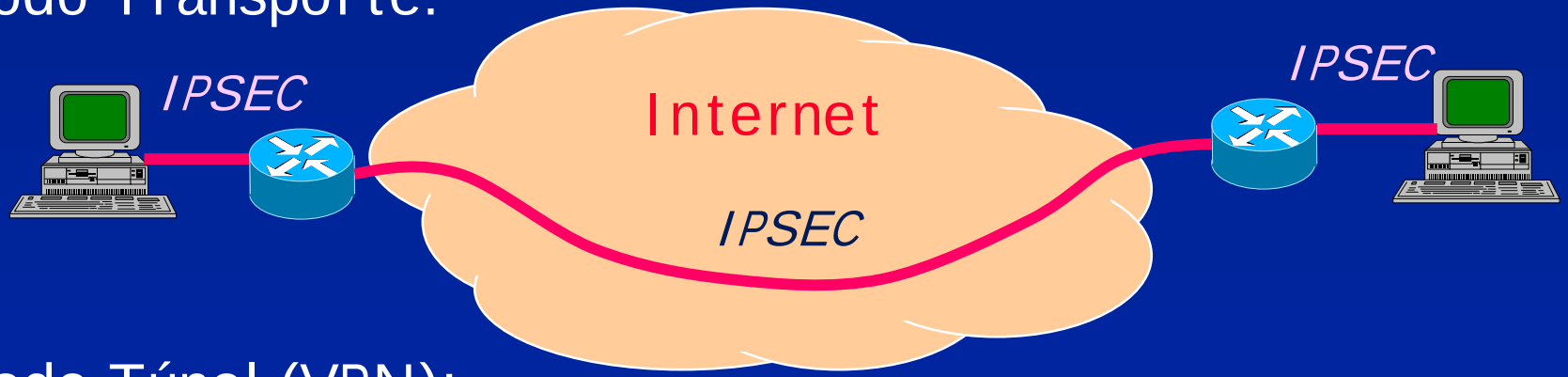
Datagrama IP

Datagrama IPSEC (modo transporte)

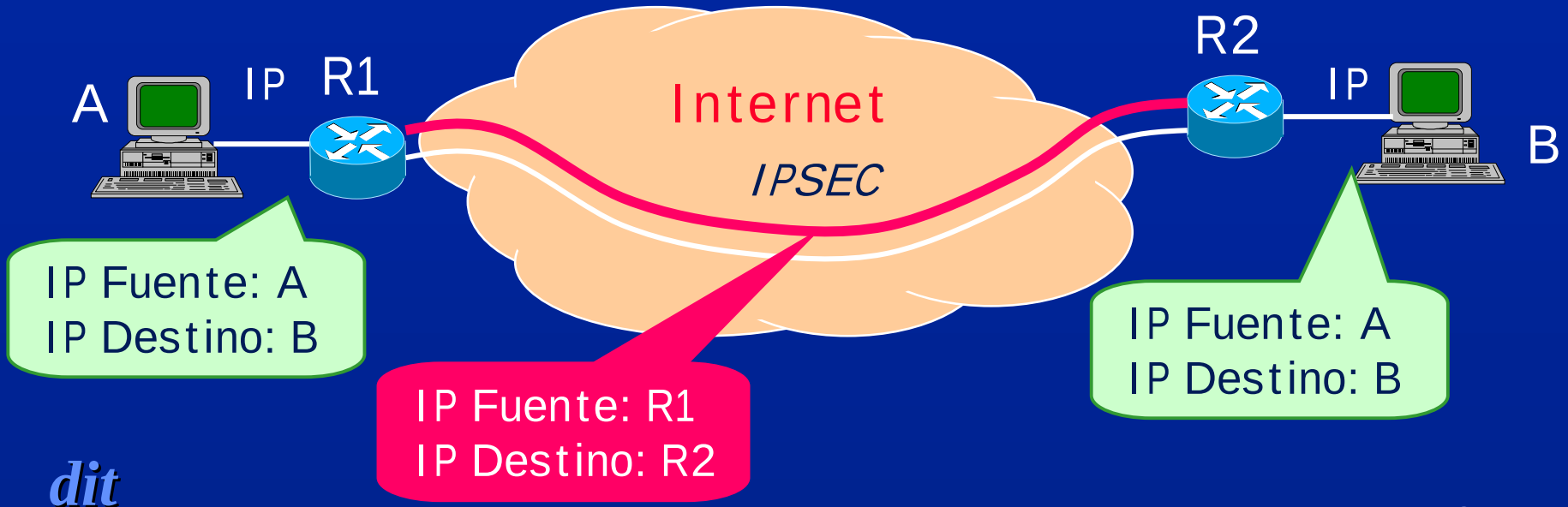
Datagrama IPSEC (modo túnel)

Modos de utilización

Modo Transporte:



Modo Túnel (VPN):



Gestión de claves

- Distribución manual
  - Se configura cada sistema con sus propias claves y con las claves del resto de sistemas
  - Solo utilizable en entornos pequeños y estáticos
- Distribución automática
  - Creación bajo demanda de claves para los SA
  - Es más flexible ....
  - Pero necesita más esfuerzo para configurar y más software

Gestión de claves

- Protocolo por defecto de gestión de claves para IPSEC: IKE (*Internet Key Exchange*)
- Método estándar para:
  - Autenticar dinámicamente extremos IPSEC
  - Negociar servicios de seguridad
  - Generar claves compartidas
- Tiene dos componentes:
  - ISAKMP: procedimientos y formatos de paquete para establecer, negociar, modificar y eliminar SA.
  - OAKLEY: protocolo de intercambio de claves.

OAKLEY

- Protocolo de determinación de claves.
- Objetivo principal: generar una clave de sesión compartida entre ambos extremos
- Método: algoritmo de Diffie-Hellman (modificado)
  - Acuerdo previo en dos factores
    - ✓Un número primo muy grande: q
    - ✓Una raiz primitiva de q: a (a mod q, a^2 mod q, .. a^{q-1} mod q son distintos)
  - A selecciona X_A (secreto) y transmite a B: $Y_A=a^{X_A}$
  - B selecciona X_B (secreto) y transmite a A: $Y_B=a^{X_B}$
  - Ambos calculan $K=(Y_B)^{X_A} \bmod q=(Y_A)^{X_B} \bmod q$
  - Se amplía para autenticar las partes y evitar el ataque de "*man-in-the-middle*".

ISAKMP

- Procedimientos y formatos para establecer, negociar, modificar y borrar SA.
- Tipos de intercambios ISAKMP:
  - Base: se transmite a la vez el intercambio de claves y la autenticación
  - Protección de Identidad: primero intercambio de claves y luego autenticación
  - Solo Autenticación: sin intercambio de claves
  - Agresivo: intercambio de claves y autenticación minimizando el número de transacciones
  - Informativo: para transmitir status o errores.