UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia e Certificação Digital
Sexta Aula

Prof. Frederico Sauer, D.Sc.

Segurança em Correio Eletrônico

- Aplicação mais usada no mundo
- Altamente vulnerável
- Serviços necessários:
  - Confidencialidade
  - Autenticação
  - Integridade
  - Não-repudiação

PGP - OpenPGP

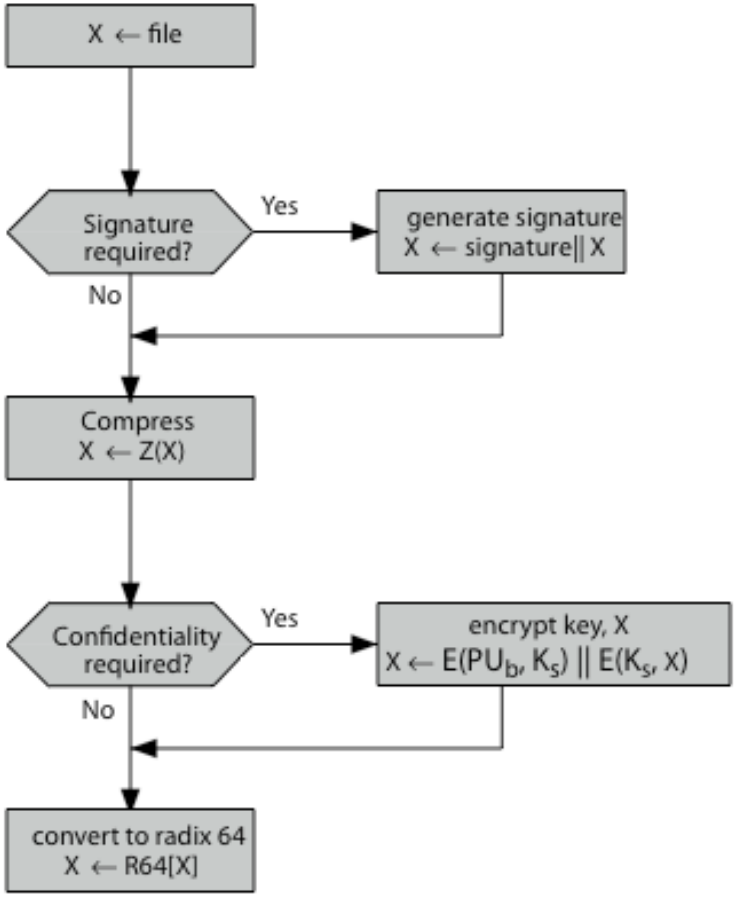
- Mecanismos:
  - Autenticação
    1. Emissor cria a mensagem
    2. É criado um hash com o SHA-1 (160 bits)
    3. O hash é assinato com a chave privada do emissor
    4. O receptor usa a chave pública do emissor para decifrar o hash
    5. O receptor compara o hash recebido com o calculado
  - Confidencialidade
    1. O emissor gera uma chave de sessão de acordo com o algoritmo
    2. Cifra a mensagem com o CAST-128 / IDEA / 3DES no CBC mode com a chave de sessão
    3. Cifra a chave de sessão com a chave pública do receptor e a concatena (criptografada) à mensagem
    4. O receptor usa sua chave privada para decifrar a chave de sessão
    5. O receptor usa a chave de sessão para decifrar a mensagem

PGP - OpenPGP

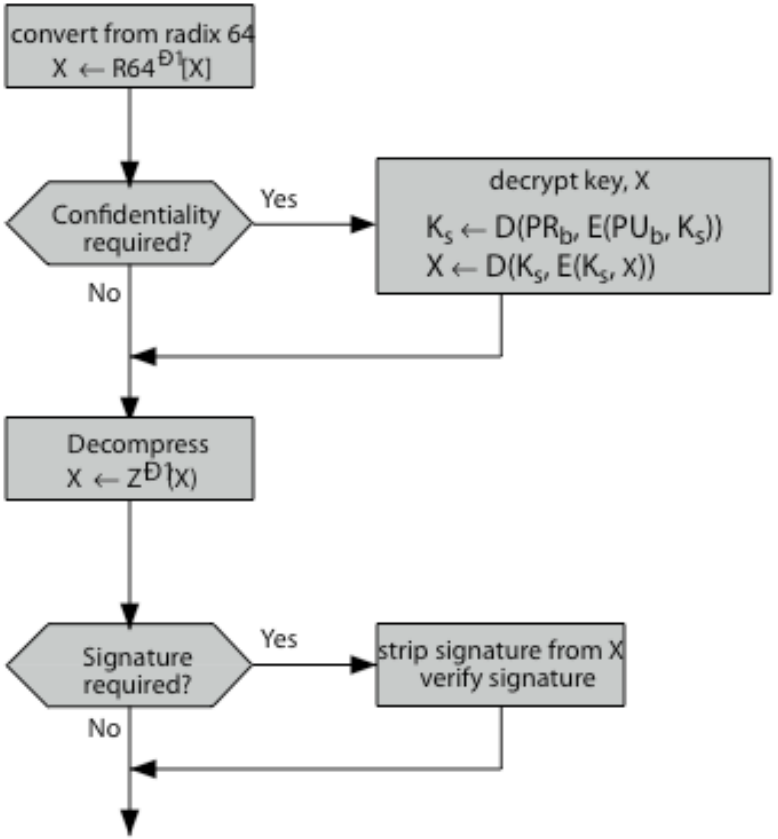
- Compressão
  - Por default, o PGP “zipa” a mensagem depois de assinar e antes de cifrar
  - As mensagens e hashes assinados são armazenados localmente descomprimidos
- Transmissão
  - Para compatibilidade com servidores de email (texto) os bits do criptograma são convertidos para caracteres ASCII (Radix-64 → 3 bytes = 4 caracteres)
  - Mensagens grandes são segmentadas na origem e remontadas no receptor

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Sumário de Operações



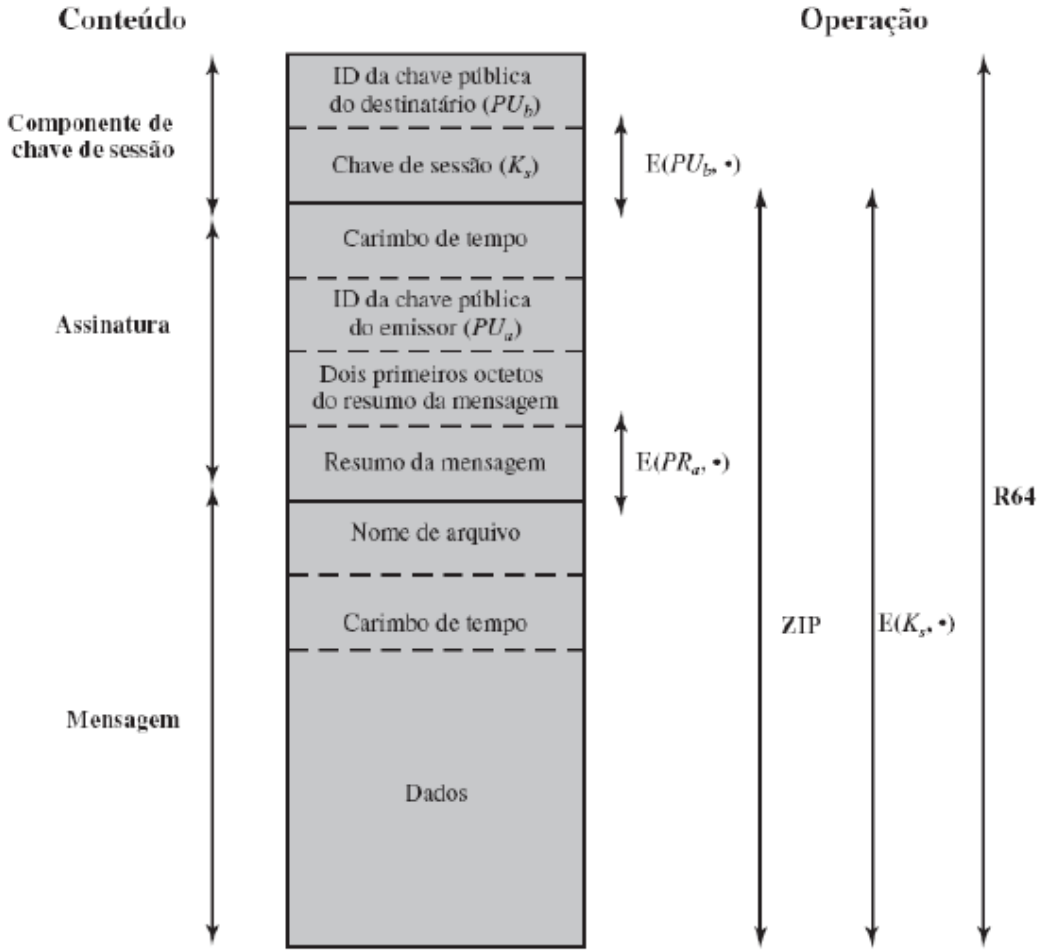
(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Formato da Mensagem PGP



Notação:

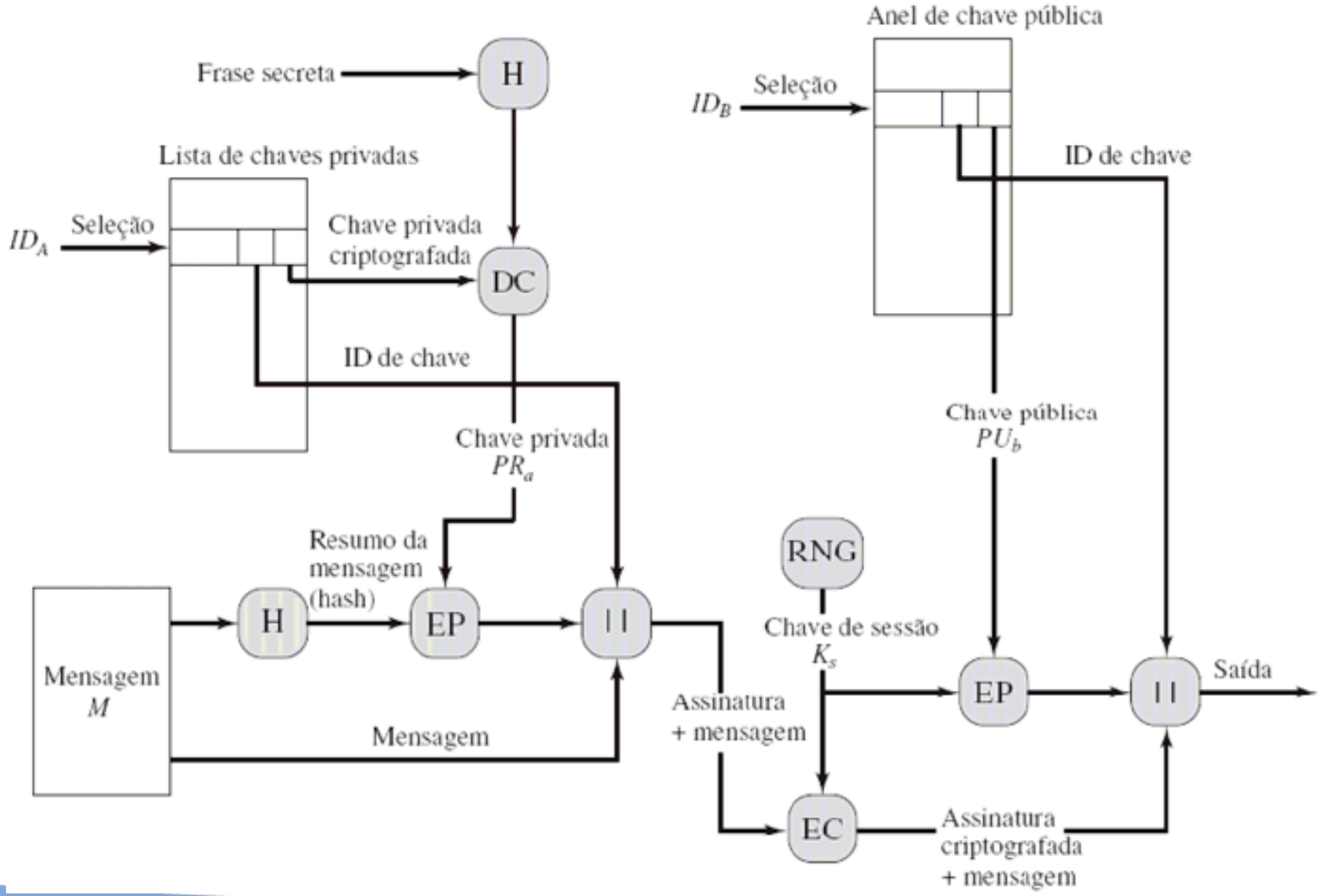
E(PU_b, •) = criptografia com a chave pública do usuário b
E(PR_a, •) = criptografia com a chave privada do usuário b
E(K_s, •) = criptografia com chave de sessão
ZIP = função de compressão Zip
R64 = função de conversão radix 64

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

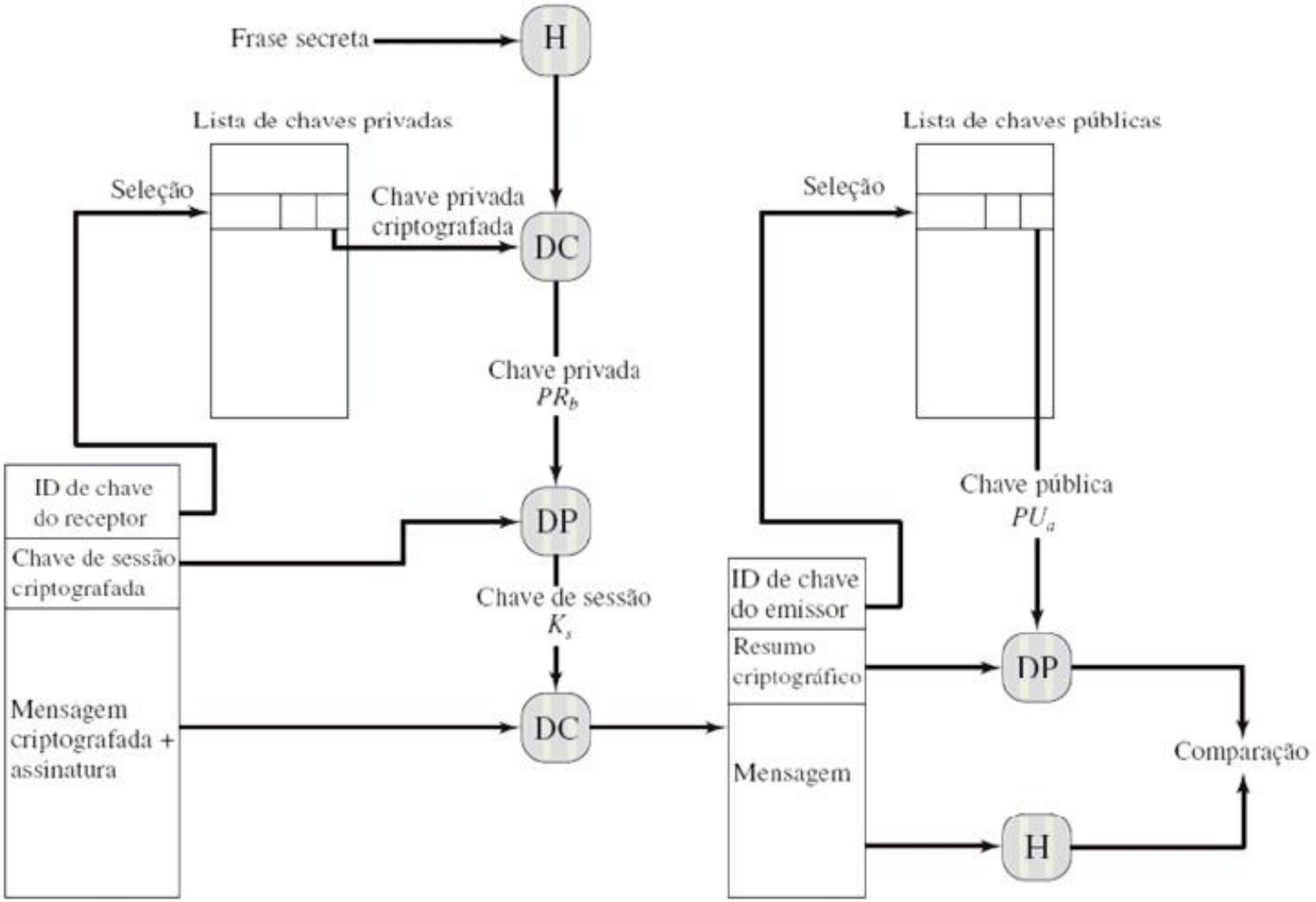
Gerenciamento de Chaves

- Key ID – últimos 64 bits da chave pública → usado para identificação do usuário
- Keyrings
  - Public Ring – Chaves públicas indexadas por key-ID
  - Private Ring – Chaves pública e privada do(s) usuário(s) local. A privada é encriptada com o hash de uma passphrase

Geração de uma Mensagem PGP



Recepção de uma Mensagem PGP



Web of Trust

- Cada usuário é uma AC
- Níveis diferentes de confiança podem ser atribuídos às chaves

(a) Confiança atribuída ao proprietário da chave pública (aparece após o pacote de chave; definido pelo usuário)	(b) Confiança atribuída ao par chave pública/ID de usuário (aparece após o pacote de ID do usuário; calculada pelo PGP)	(c) Confiança atribuída à assinatura (aparece após o pacote de assinatura; cópia em cache de OWNERTRUST para esse assinante)
Campo OWNERTRUST – confiança indefinida – usuário desconhecido – normalmente não confiável para assinar outras chaves – normalmente confiável para assinar outras chaves – sempre confiável para assinar outras chaves – essa chave está presente na lista de chaves secretas (confiança máxima) Bit BUCKSTOP – marcado se essa chave aparecer na lista de chaves secretas	Campo KEYLEGIT – confiança desconhecida ou indefinida – proprietário da chave não confiável – confiança pequena no proprietário da chave – confiança completa no proprietário da chave Bit WARNONLY – marcado se o usuário só deseja ser avisado quando uma chave não totalmente validada for usada para criptografia	Campo SIGTRUST – confiança indefinida – usuário desconhecido – normalmente não confiável para assinar outras chaves – normalmente confiável para assinar outras chaves – sempre confiável para assinar outras chaves – essa chave está presente na lista de chaves secretas (confiança máxima) CONTIG – marcado se a assinatura levar um caminho de certificação confiável de volta ao proprietário da lista de chaves mais confiável.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

S-MIME

- Extensões para segurança em e-mail comercial e organizacional
- RFC 822 → msg = envelope + texto ASCII
- MIME → estende para objetos binários e “texto rico”
- Funções S-MIME:
  - Dados envelopados
    - Conteúdo criptografado e respectivas chaves
  - Dados assinados
    - Hash de mensagem assinado pelo emissor e concatenado à mensagem, que é codificada com Radix-64 (apenas vista por clientes compatíveis com S-MIME
  - Dados assinados e em texto claro
    - Hash da mensagem assinado pelo emissor, codificado pelo Radix-64 e concatenado à mensagem
  - Dados assinados e envelopados
    - Aninhamento de objetos assinados e criptografados

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Suporte ao S-MIME

Função	Requisito
Criar uma mensagem a ser usada na formação de uma assinatura digital Criptografar resumo da mensagem para formar assinatura digital.	DEVE admitir SHA-1. O recebedor DEVERIA oferecer suporte a MDS para compatibilidade com versões anteriores. Agentes de envio e recebimento DEVEM oferecer suporte à DSS. Agentes de recebimento DEVERIAM oferecer suporte à criptografia RSA. Agentes de recebimento DEVERIAM oferecer suporte à verificação de assinaturas RSA com tamanhos de chave de 512 bits a 1.024 bits.
Criptografar chave de sessão para transmissão com mensagem.	Agentes de envio e recebimento DEVERIAM oferecer suporte a Diffie-Hellman. Agentes de envio e recebimento DEVEM oferecer suporte à criptografia RSA com tamanhos de chave de 512 bits a 1.024 bits.
Criptografar mensagem para transmissão com chave de sessão de uso único.	Agentes de envio e recebimento DEVEM oferecer suporte à criptografia com 3DES. Agentes de envio DEVERIAM oferecer suporte à criptografia com AES. Agentes de envio DEVERIAM oferecer suporte à criptografia com RC2/40.
Criar um código de autenticação de mensagem.	Agentes de recebimento DEVEM oferecer suporte a HMAC com SHA-1. Agentes de recebimento DEVERIAM oferecer suporte a HMAC com SHA-1.

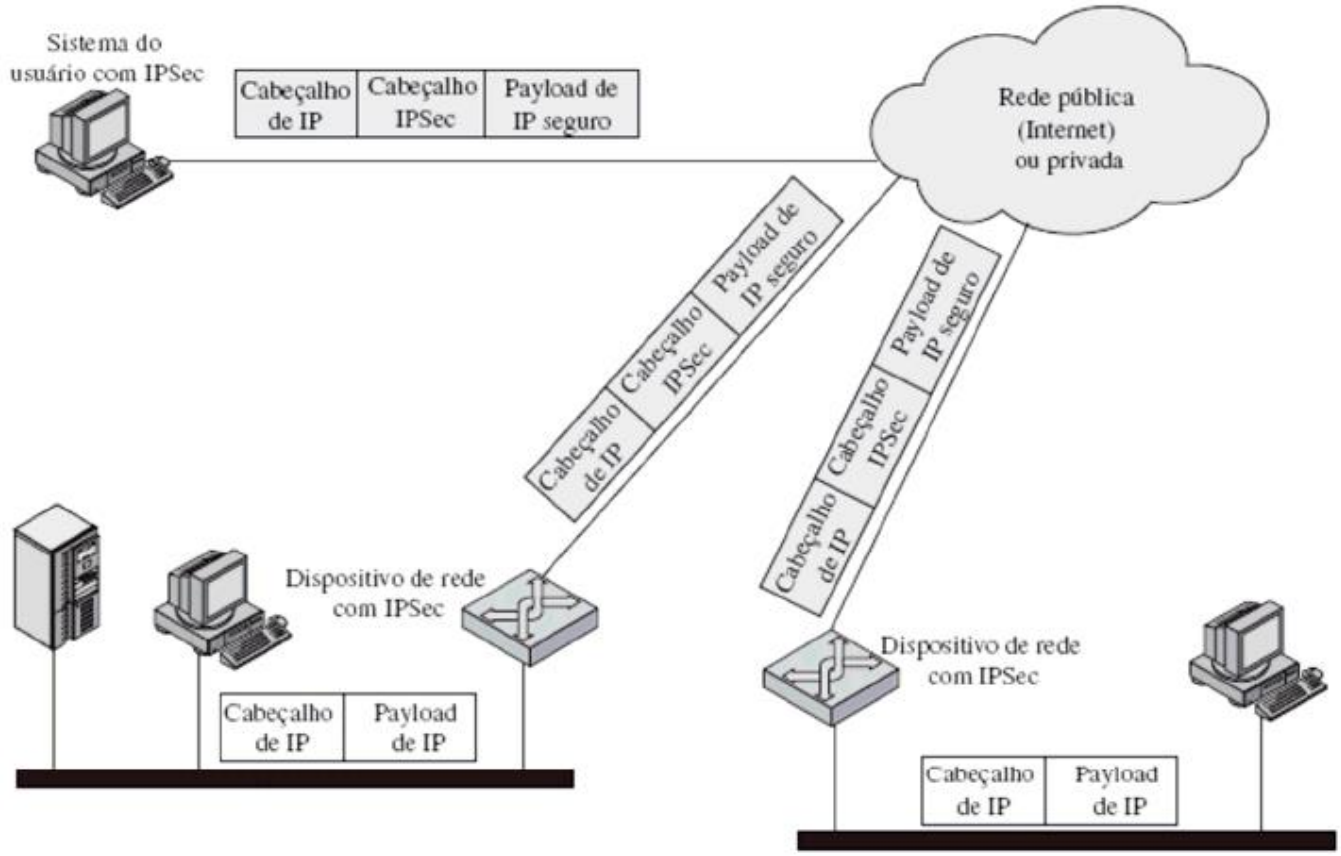
Chaves públicas para S-MIME

- Certificados X.509v3
- Híbrido da estrutura de certificados oficiais e "web of trust"
  - A manutenção dos certificados das AC e dos destinatários é local
  - A Verisign foi uma das pioneiras
- Classes de Certificados

Classe	**Verificação de ID**	**Uso típico**
1	Nome e email	web browsing/email pessoal
2	+ cadastro	email corp., troca senhas
3	+ documento de ID	e-banking/service access

IP Security

- Aplicações resolvem problemas específicos
- Segurança em camadas inferiores pode ser aplicável à qualquer aplicação



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Serviços IPSec

- Opcional no IPv4 e mandatório no IPv6

	AH	ESP (apenas criptografia)	ESP (criptografia mais autenticação)
Controle de acesso	✔	✔	✔
Integridade sem conexão	✔		✔
Autenticação da origem de dados	✔		✔
Rejeição de pacotes repetidos	✔	✔	✔
Confidencialidade		✔	✔
Confidencialidade limitada do fluxo de tráfego		✔	✔

Security Associations

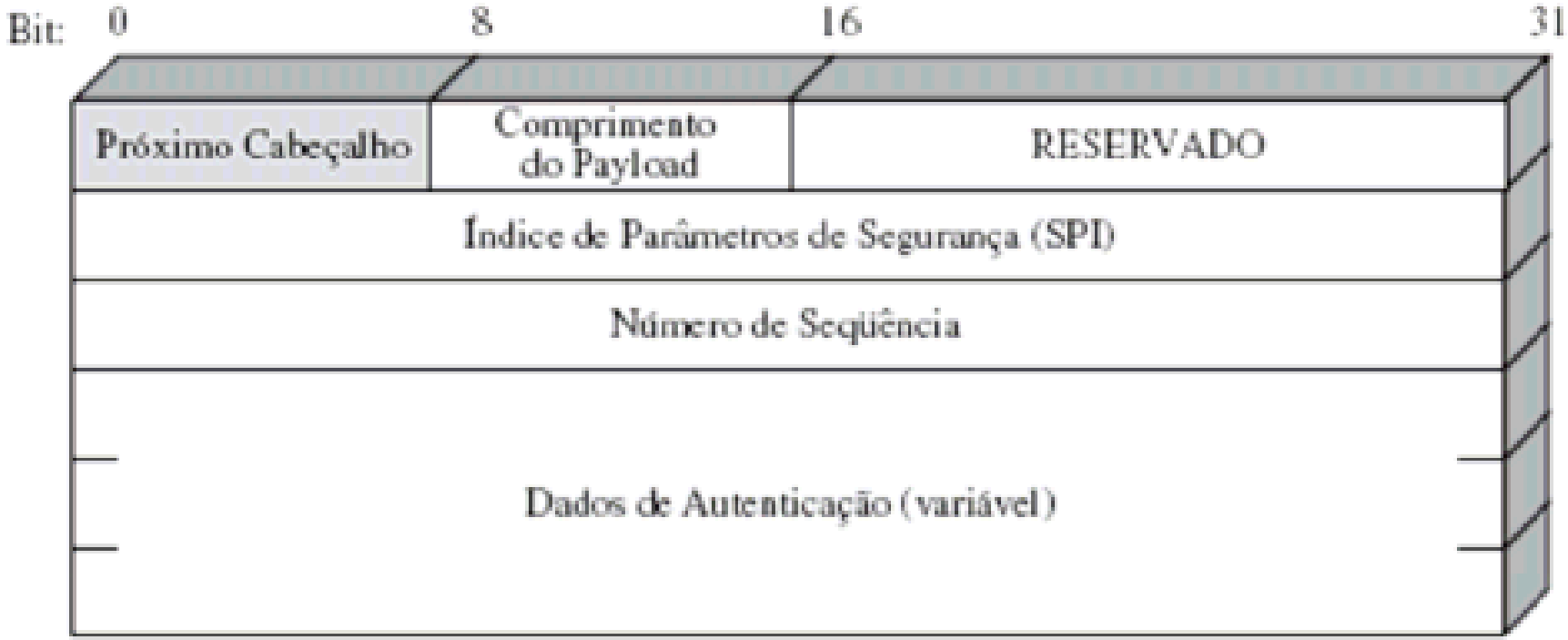
- Relacionamento de sessão em em um único sentido entre emissor e receptor
- Definido por 3 parâmetros principais:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier
- Outros parâmetros
  - Nº sequência, AH & EH info, lifetime etc
- As SA são armazenadas em uma base

Authentication Header

- Autenticação e integridade de pacotes
  - Sistema final pode autenticar aplicação/user
  - Combate *spoofing* com *sequence numbers*
- Usa o MAC
  - HMAC-MD5-96 or HMAC-SHA-1-96
- Pares devem compartilhar uma cheve secreta

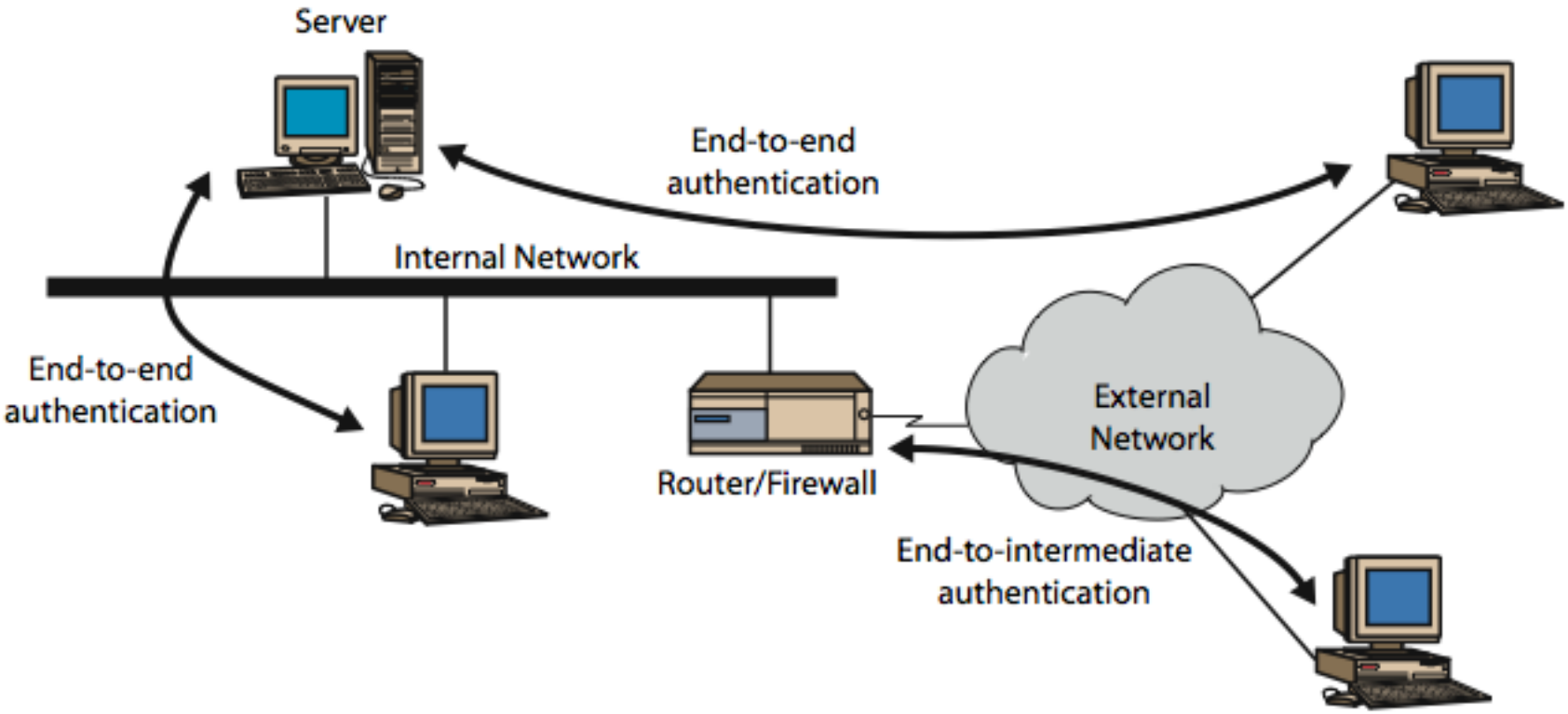
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Authentication Header

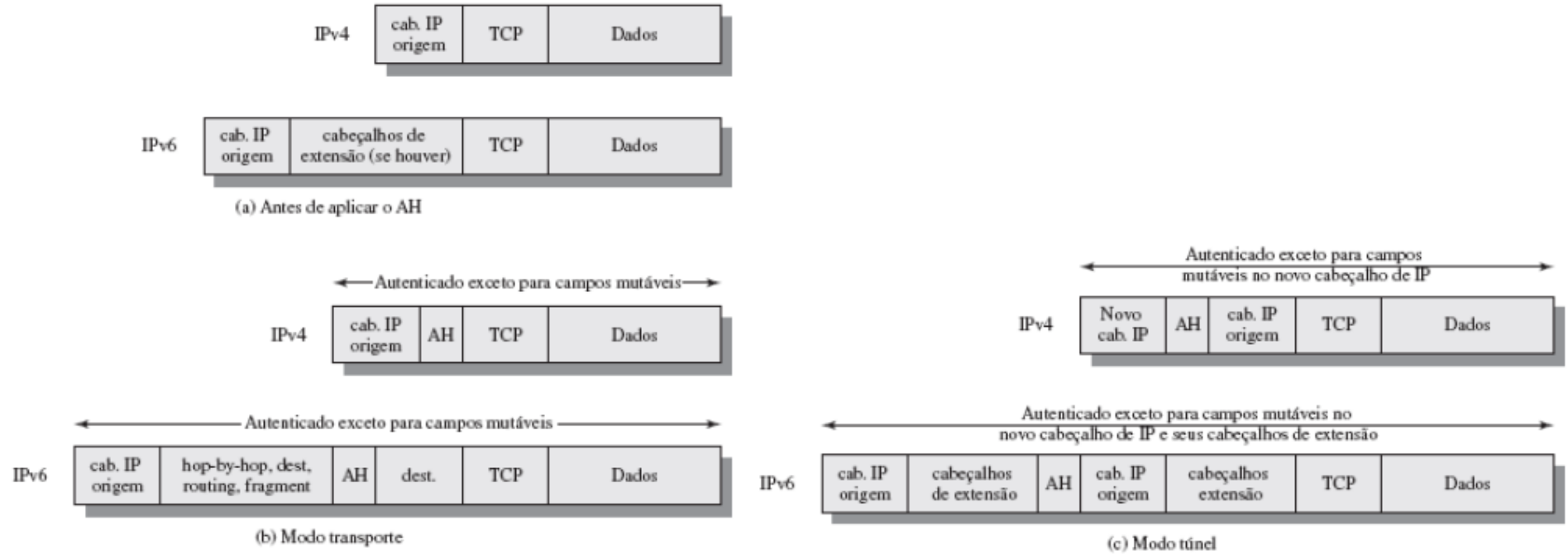


UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Modos Transporte e Túnel



AH

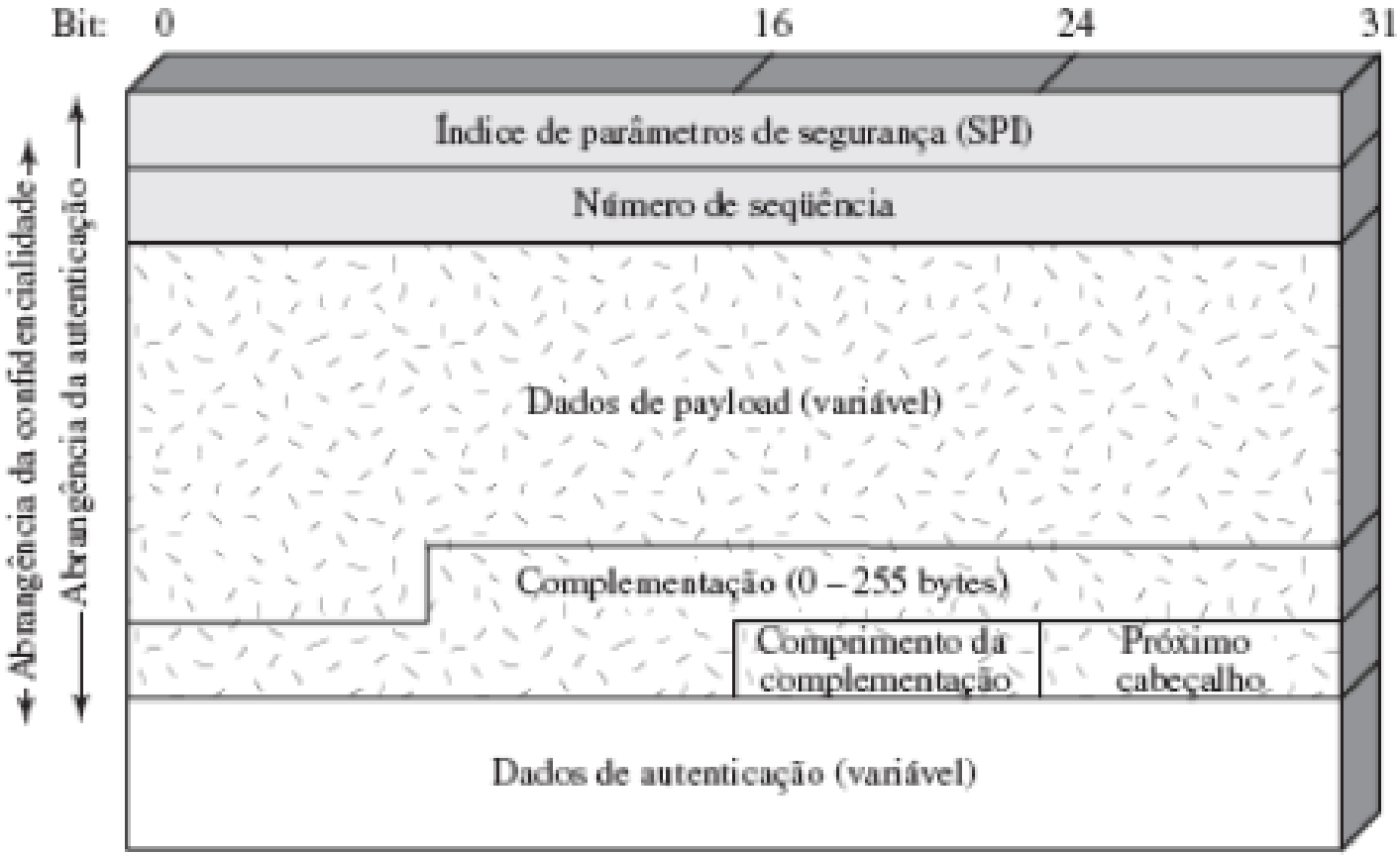

IPv4
cab. IP origem
TCP
Dados
IPv6
cab. IP origem
cabeçalhos de extensão (se houver)
TCP
Dados
(a) Antes de aplicar o AH
Autenticado exceto para campos mutáveis
IPv4
cab. IP origem
AH
TCP
Dados
Autenticado exceto para campos mutáveis
IPv6
cab. IP origem
hop-by-hop, dest, routing, fragment
AH
dest.
TCP
Dados
(b) Modo transporte
Autenticado exceto para campos mutáveis no novo cabeçalho de IP
IPv4
Novo cab. IP
AH
cab. IP origem
TCP
Dados
Autenticado exceto para campos mutáveis no novo cabeçalho de IP e seus cabeçalhos de extensão
IPv6
cab. IP origem
cabeçalhos de extensão
AH
cab. IP origem
cabeçalhos extensão
TCP
Dados
(c) Modo túnel

Encapsulating Security Payload (ESP)

- Provê confidencialidade e opcionalmente autenticação
- Suporta uma ampla gama de mecanismos
  - Incl. DES, Triple-DES, RC5, IDEA, CAST etc
  - CBC & outros modos
  - *Padding* necessário para complemento do bloco

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

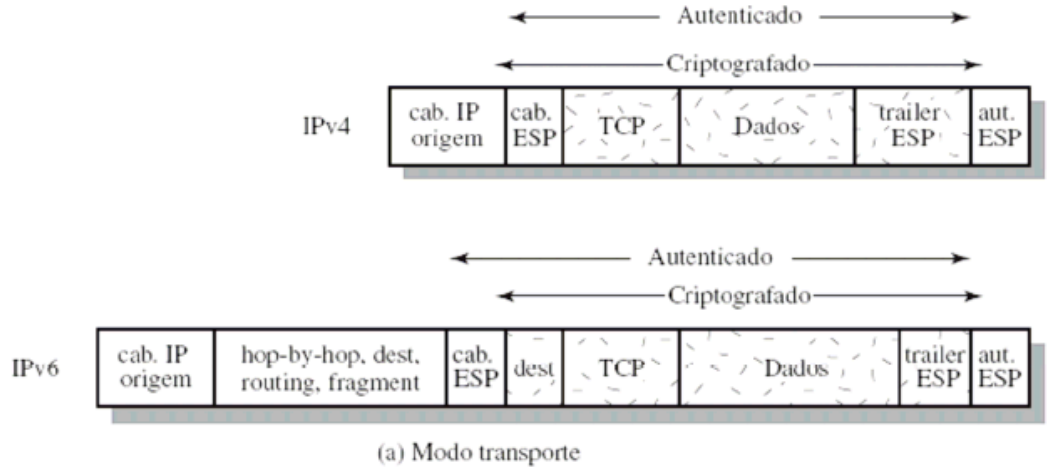
ESP



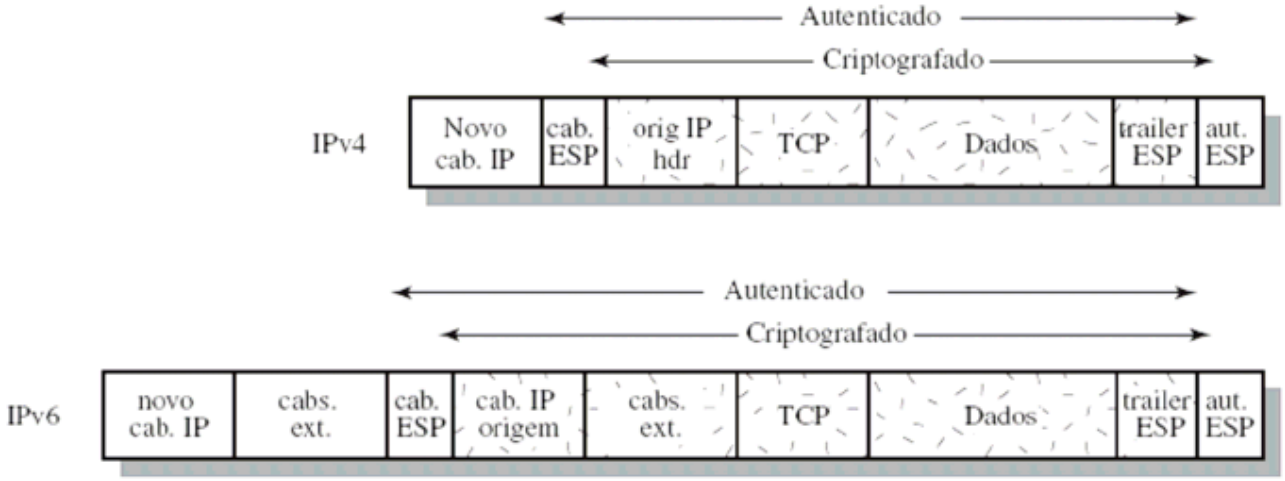
ESP Transporte e Túnel

- Modo Transporte usado para confidencialidade e opcionalmente autenticação
  - Dados protegidos e cabeçalho em claro
  - Permite análise de tráfego
  - Bom para tráfego fim-a-fim
- Modo Túnel encripta todo o datagrama
  - Adiciona um outro cabeçalho IP
  - Bom para VPNs, segurança *gateway-a-gateway*

ESP



(a) Modo transporte



(b) Modo túnel