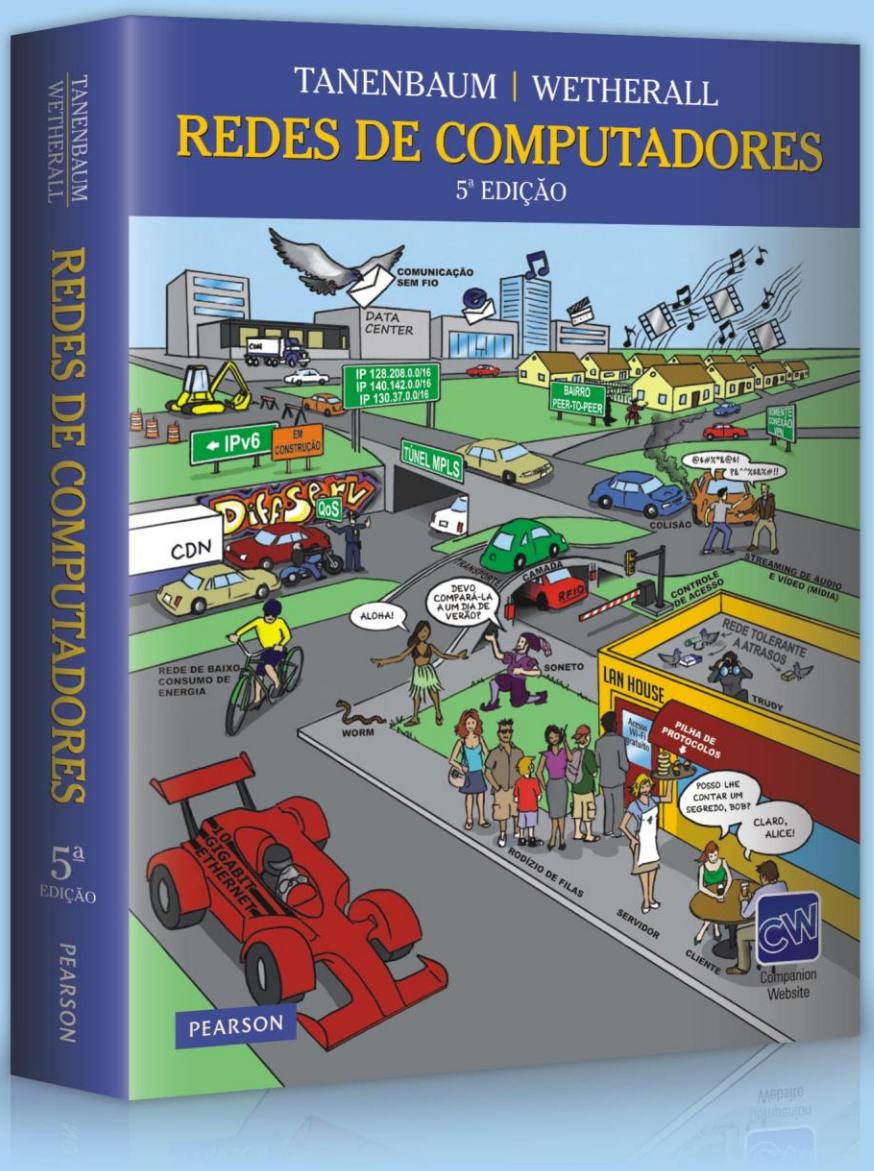
Capítulo 8

Segurança de redes



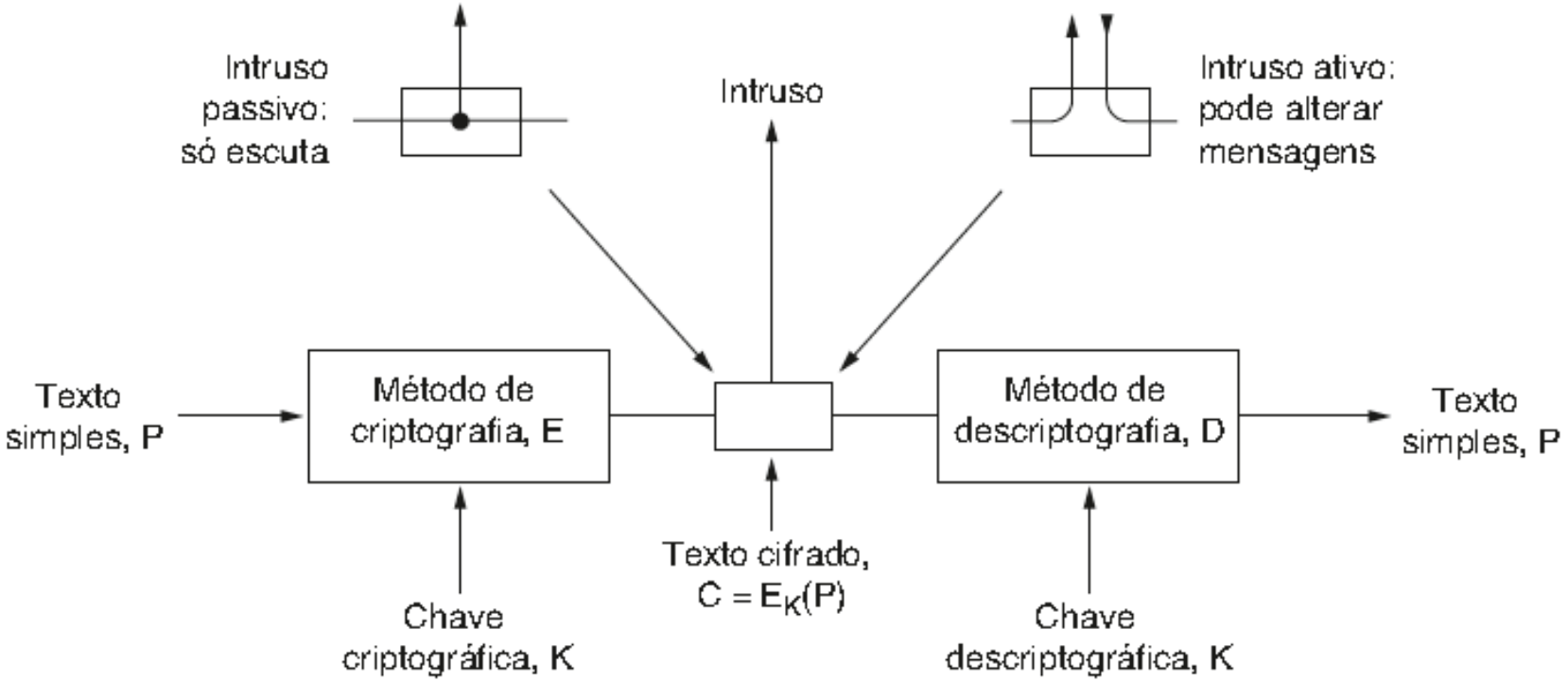
Segurança de redes

Adversário	Objetivo
Estudante	Divertir-se bisbilhotando as mensagens de correio eletrônico de outras pessoas
Cracker	Testar o sistema de segurança de alguém; roubar dados
Representante de vendas	Tentar representar toda a Europa e não apenas Andorra
Executivo	Descobrir a estratégia de marketing do concorrente
Ex-funcionário	Vingar-se por ter sido demitido
Contador	Desviar dinheiro de uma empresa
Corretor de valores	Negar uma promessa feita a um cliente por meio de uma mensagem de correio eletrônico
Vigarista	Roubar números de cartão de crédito e vendê-los
Espião	Descobrir segredos militares ou industriais de um inimigo
Terrorista	Roubar segredos de armas bacteriológicas

Criptografia

- Introdução
- Cifras de substituição
- Cifras de transposição
- Chave única
- Princípios fundamentais da criptografia

Introdução



O modelo de criptografia (cifra de chave simétrica).

Cifras de substituição

texto simples:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
texto cifrado:	Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

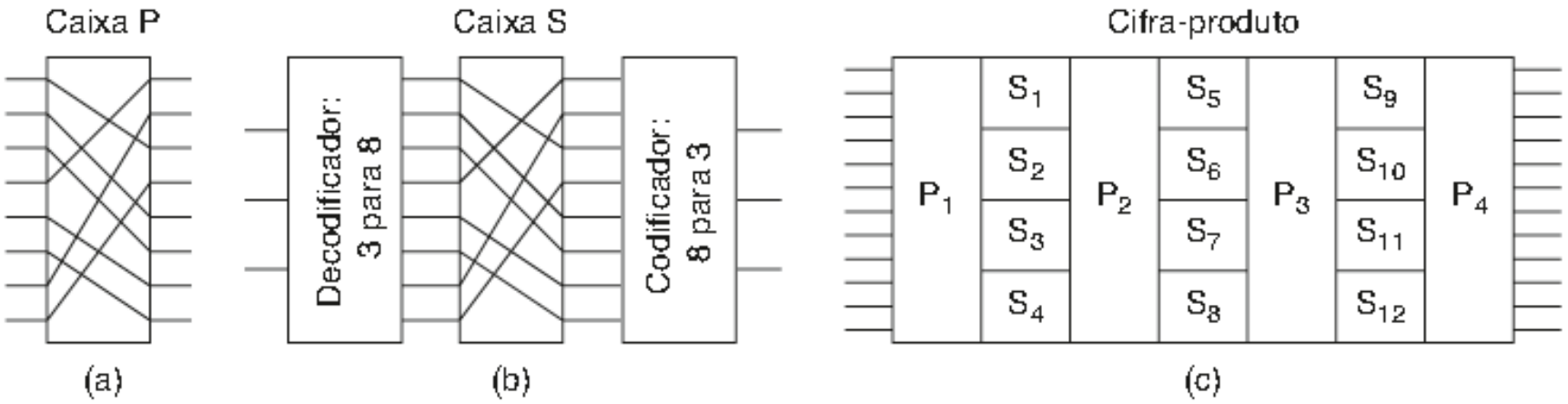
Substituição monoalfabética.

Chave única (1)

Mensagem 1:	1001001	0100000	1101100	1101111	1110110	1100101	0100000	1111001	1101111	1110101	0101110
Chave 1:	1010010	1001011	1110010	1010101	1010010	1100011	0001011	0101010	1010111	1100110	0101011
Texto cifrado:	0011011	1101011	0011110	0111010	0100100	0000110	0101011	1010011	0111000	0010011	0000101
Chave 2:	1011110	0000111	1101000	1010011	1010111	0100110	1000111	0111010	1001110	1110110	1110110
Texto simples 2:	1000101	1101100	1110110	1101001	1110011	0100000	1101100	1101001	1110110	1100101	1110011

O uso de criptografia de chave única e a possibilidade de se obter um texto simples a partir de um texto cifrado usando alguma outra chave.

Algoritmos de chave simétrica

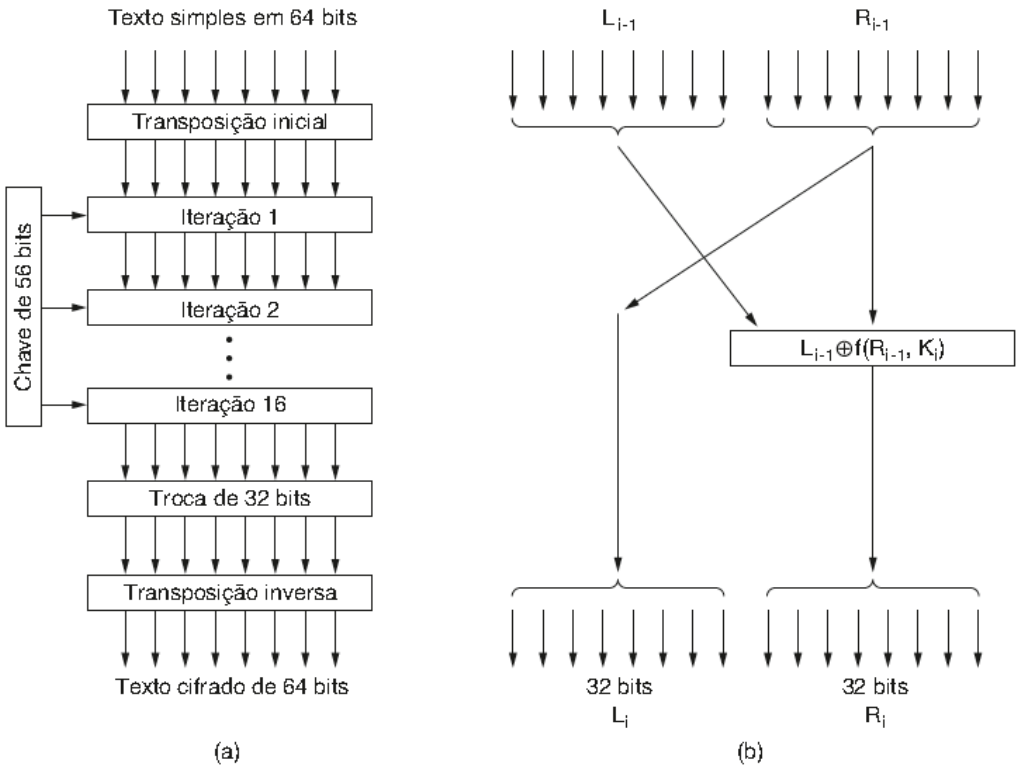


Elementos básicos das cifras-produto.
(a) Caixa P. (b) Caixa S. (c) Produto.

Algoritmos de chave simétrica

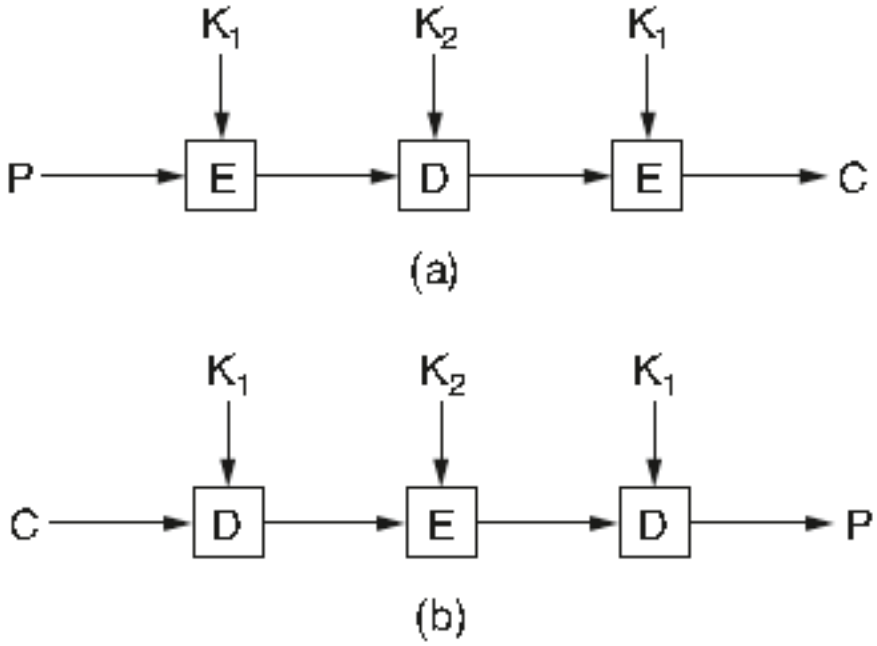
- DES – Data Encryption Standard
- AES – Advanced Encryption Standard
- Modos de cifra
- Cifras
- Criptoanálise

DES – Data Encryption Standard



O DES. (a) Visão geral. (b) Detalhamento de uma iteração. O sinal + dentro do círculo significa OU exclusivo (XOR).

DES – Data Encryption Standard

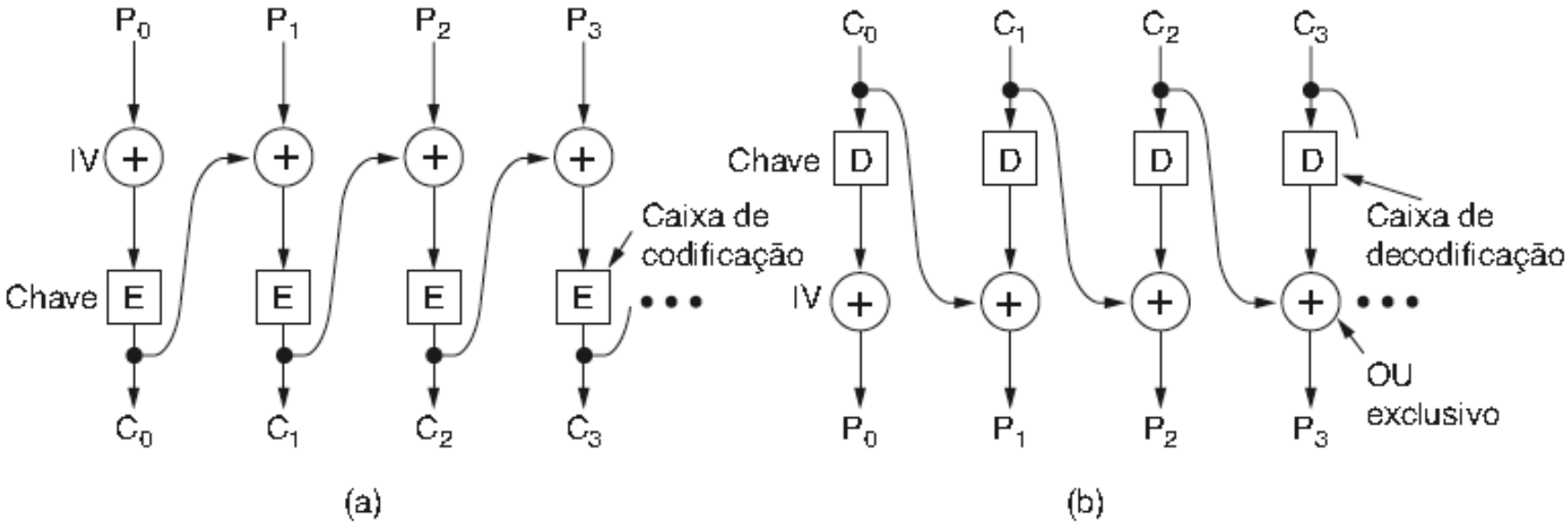


(a) Criptografia tripla com DES. (b) Descriptografia.

AES – Advanced Encryption Standard

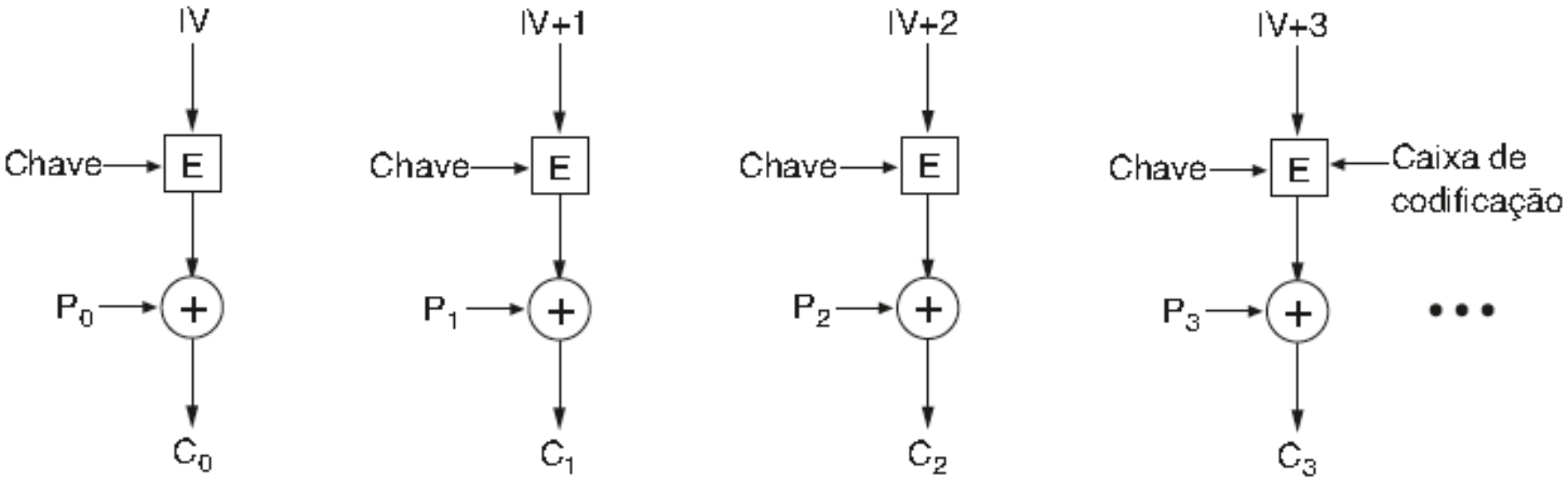
1. Algoritmo de cifra de bloco simétrica
2. Projeto completo de domínio público
3. Chaves com tamanho de 128, 192 e 256 bits
4. Implementações em software e hardware
5. Algoritmo de domínio público ou de licença não discriminatória

Modos de cifra



Encadeamento de blocos de cifra.
(a) Codificação. (b) Decodificação.

Modos de cifra



Codificação usando o modo contador.

Cifras

Cifra	Autor	Comprimento da chave	Comentários
DES	IBM	56 bits	Muito fraco para usar agora
RC4	Ronald Rivest	1 a 2.048 bits	Atenção: algumas chaves são fracas
RC5	Ronald Rivest	128 a 256 bits	Bom, mas patenteado
AES (Rijndael)	Daemen e Rijmen	128 a 256 bits	Melhor escolha
Serpent	Anderson, Biham, Knudsen	128 a 256 bits	Muito forte
DES triplo	IBM	168 bits	Bom, mas está ficando ultrapassado
Twofish	Bruce Schneier	128 a 256 bits	Muito forte; amplamente utilizado

Alguns algoritmos criptográficos de chave simétrica comuns.

Algoritmos de chave pública

- Uma chave é pública e a outra é privada
- O que se criptografa com uma chave só se decriptografa com a outra
- RSA
  – Autores: Rivest, Shamir, Adleman
- Outros algoritmos de chave pública

RSA

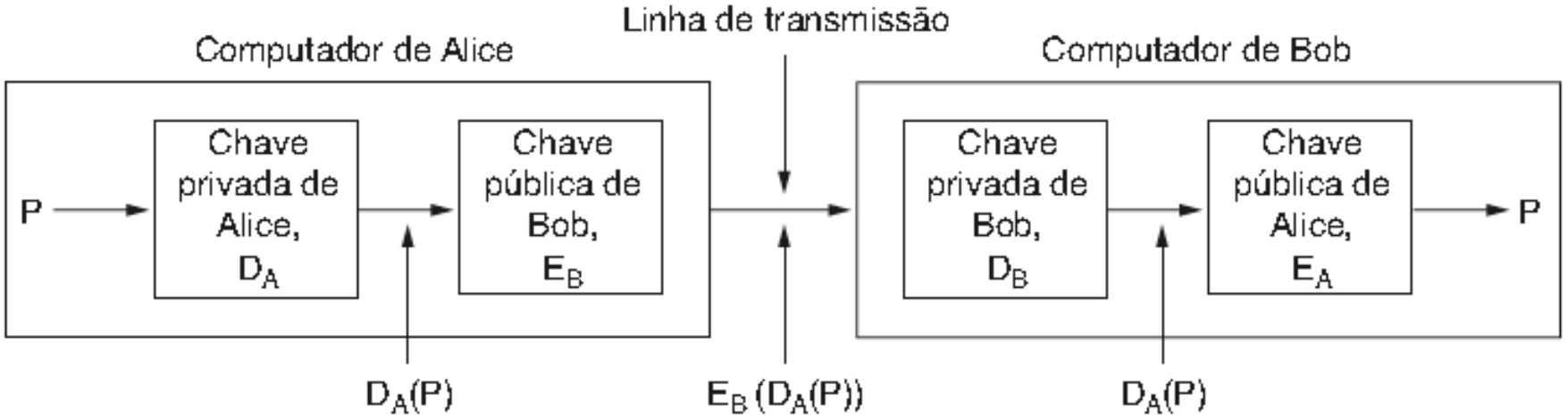
Resumo do método:

1. Escolha dois números primos grandes, p e q
2. Calcule
   $n = p \times q$ e $z = (p - 1) \times (q - 1)$
3. Escolha um número d de forma que z e d sejam primos entre si
4. Encontre e de forma que $e \times d = 1 \ mod \ z$

Assinaturas digitais

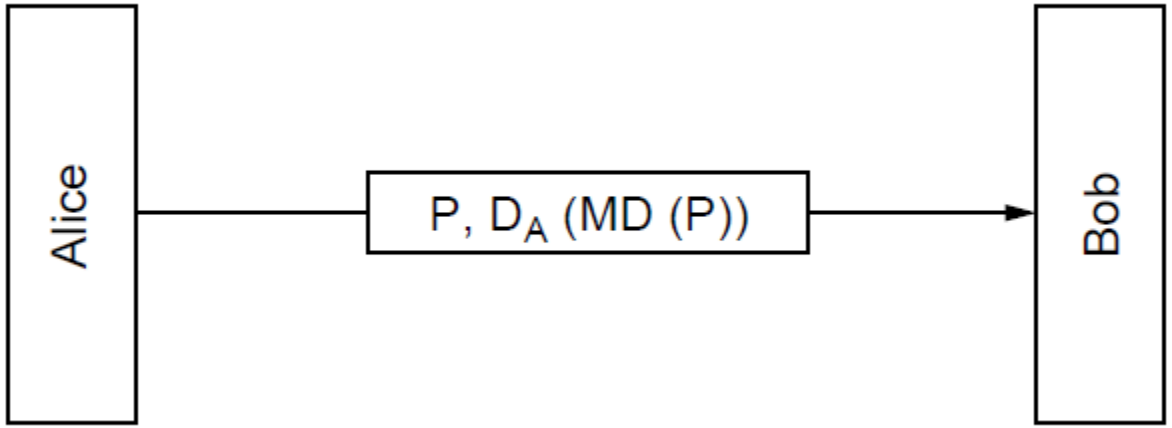
- Assinaturas de chave pública
- Sumário de mensagens
- O ataque do aniversário

Assinaturas de chave pública



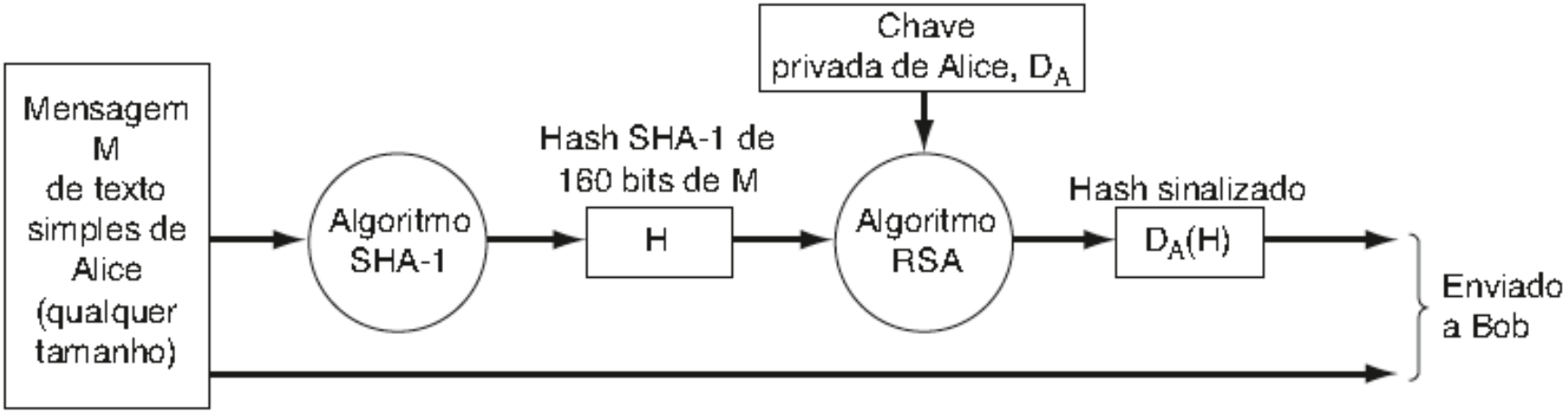
Assinaturas digitais usando criptografia de chave pública.

Sumário de mensagens



Assinaturas digitais usando sumário de mensagens.

Sumário de mensagens



Uso do SHA-1 e RSA na assinatura de mensagens não secretas.

Gerenciamento de chaves públicas

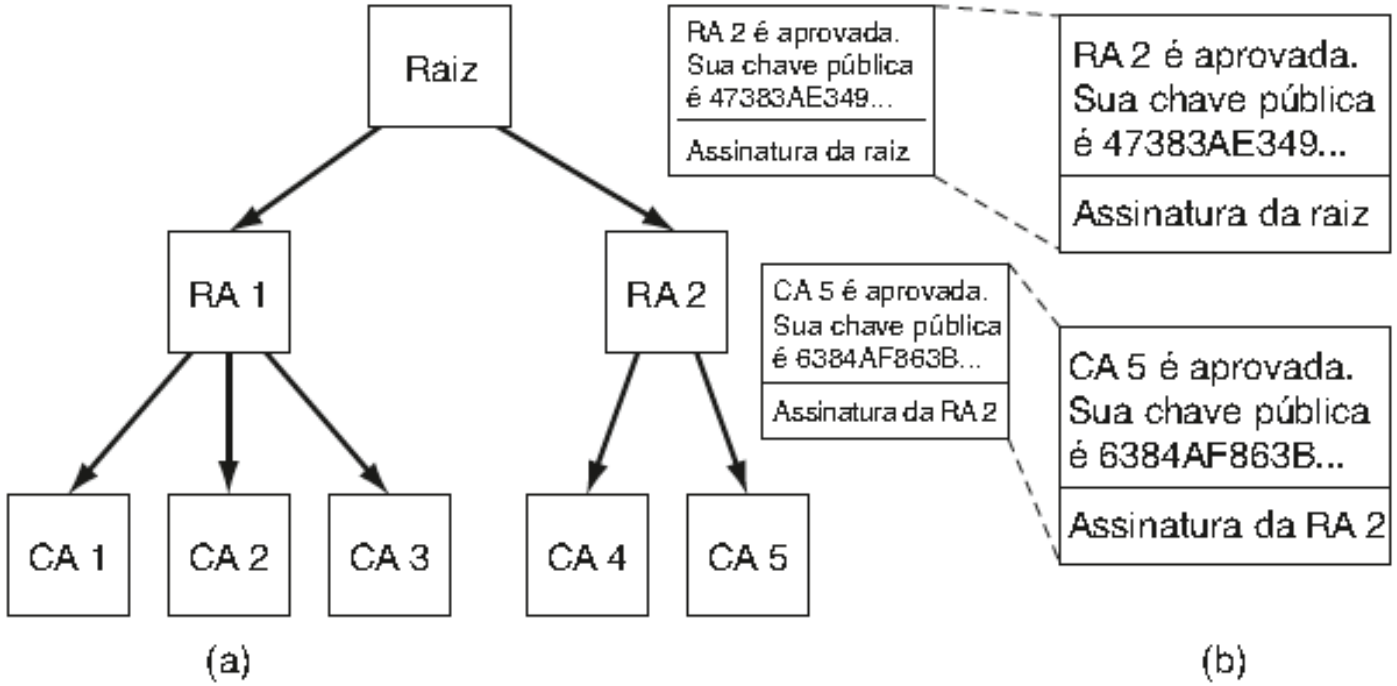
- Certificados
- X.509
- Infraestruturas de chave pública

X.509

Campo	Significado
Version	A versão do X.509
Serial number	Este número, somado ao nome da CA, identifica o certificado de forma exclusiva
Signature algorithm	O algoritmo usado para assinar o certificado
Issuer	Nome X.500 da CA
Validity period	Períodos inicial e final de validade
Subject name	A entidade cuja chave está sendo certificada
Public key	A chave pública da entidade certificada e a ID do algoritmo utilizado
Issuer ID	Uma ID opcional que identifica de forma exclusiva o emissor do certificado
Subject ID	Uma ID opcional que identifica de forma exclusiva a entidade certificada
Extensions	Muitas extensões foram definidas
Signature	A assinatura do certificado (assinado pela chave privada da CA)

Campos básicos de um certificado X.509.

Infraestruturas de chave pública

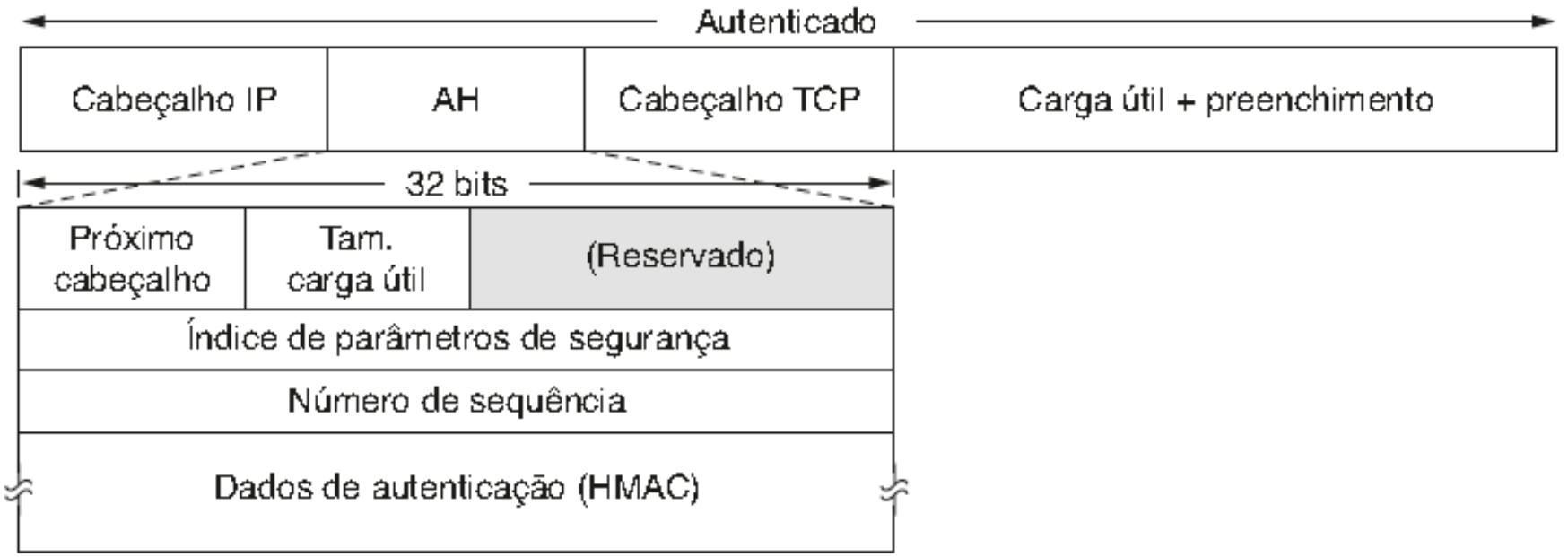


(a) Uma PKI hierárquica. (b) Cadeia de certificados.

Segurança da comunicação

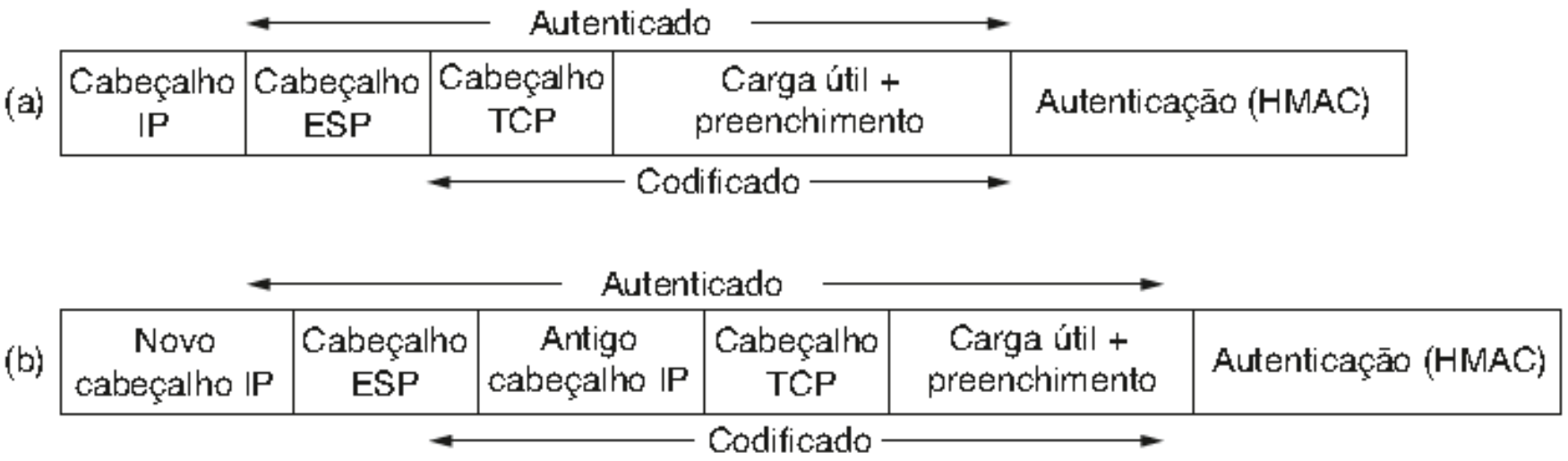
- IPsec
- Firewalls
- VPNs (Virtual Private Networks)
- Segurança em redes sem fio

IPsec



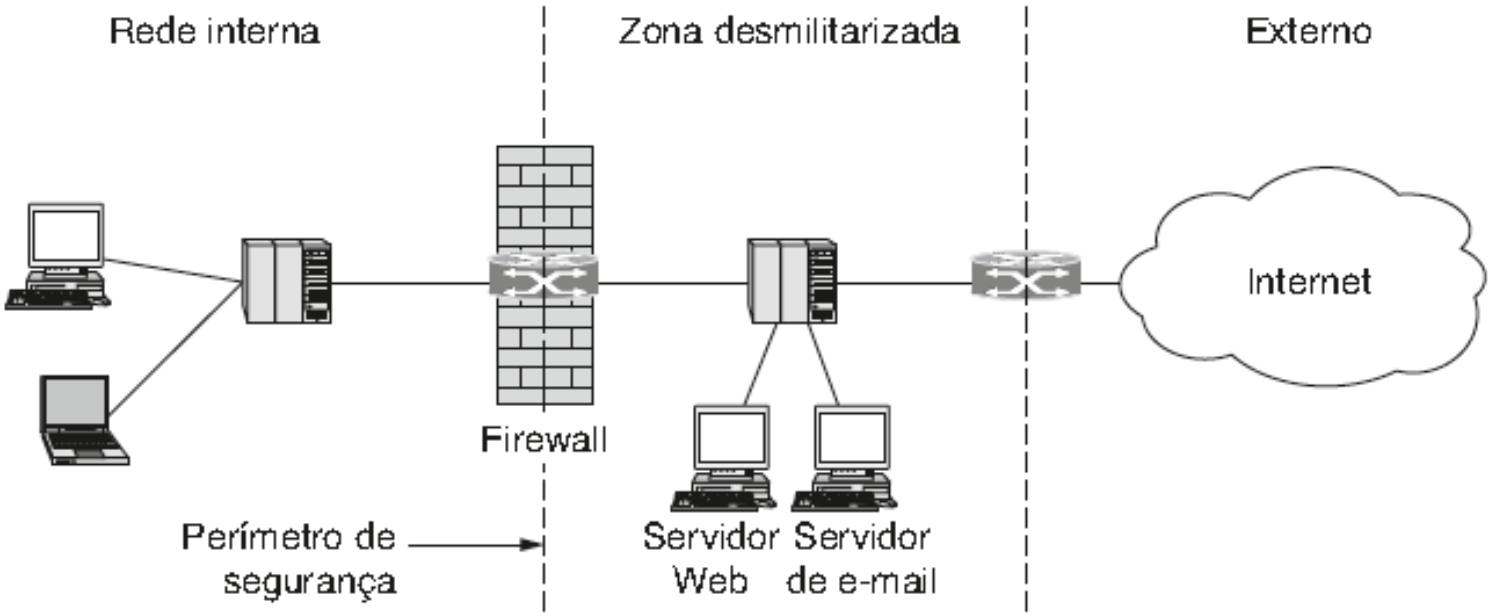
Cabeçalho de autenticação IPsec em modo de transporte para o IPv4.

IPsec



(a) ESP em modo de transporte. (b) ESP em modo túnel.

IPsec



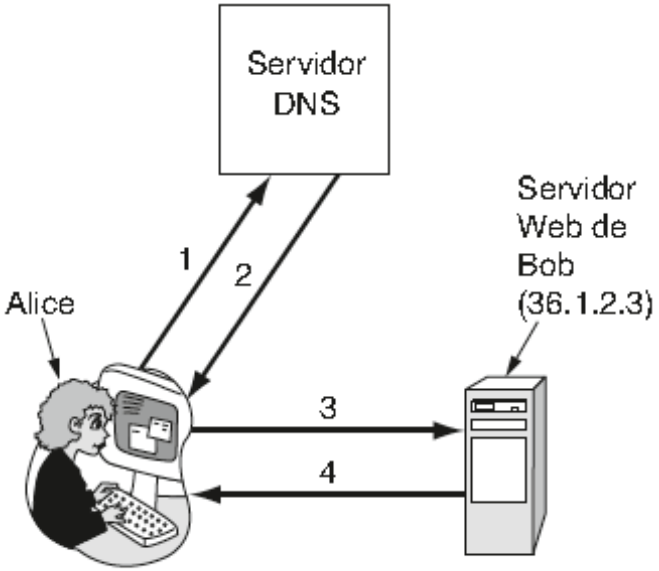
Um firewall protegendo uma rede interna.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Segurança na Web

- Ameaças
- Nomenclatura segura
- SSL – a camada de soquetes seguros
- Segurança em código móvel

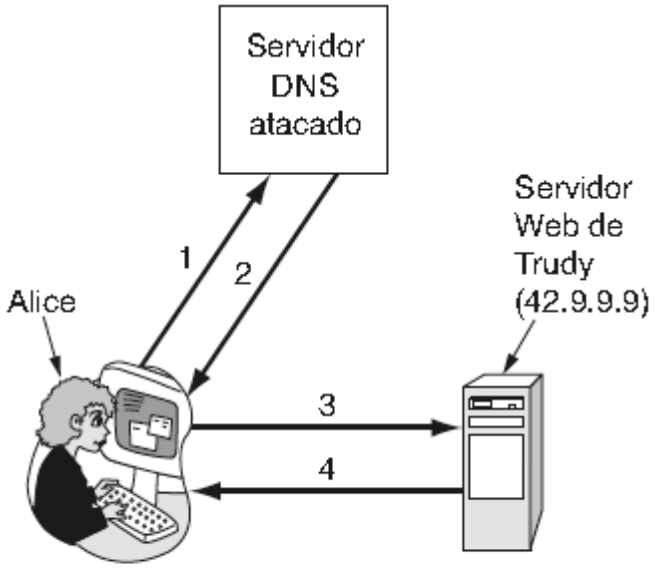
Nomenclatura segura



1. Dê-me o endereço IP de Bob
2. 36.1.2.3 (endereço IP de Bob)
3. GET index.html
4. Home page de Bob

Situação normal.

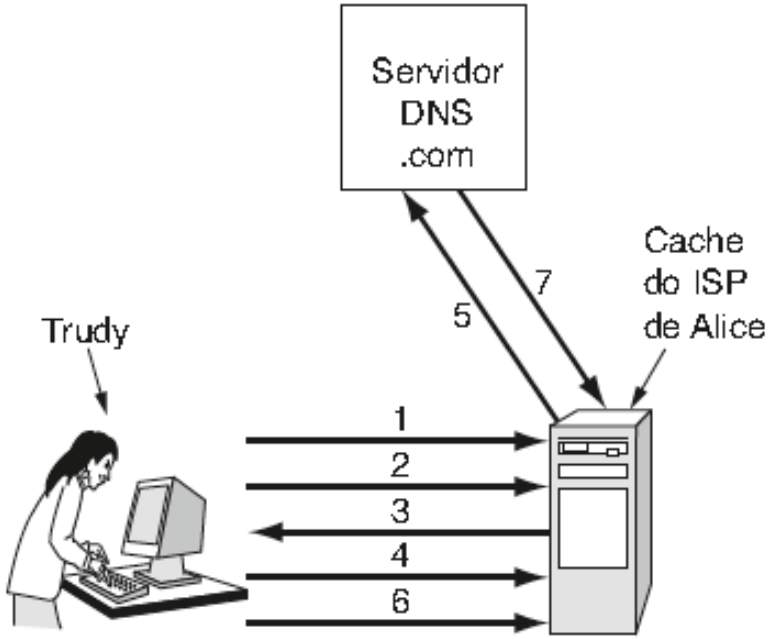
Nomenclatura segura



1. Dê-me o endereço IP de Bob
2. 42.9.9.9 (endereço IP de Trudy)
3. GET index.html
4. Home page de Bob modificada por Trudy

Ataque baseado na invasão do DNS e modificação do registro de Bob.

Nomenclatura segura



1. Procura foobar.trudy-the-intruder.com
   (para forçá-lo para o cache do ISP)
2. Procura www.trudy-the-intruder.com
   (para obter o próximo número de sequência do ISP)
3. Pedido para www.trudy-the-intruder.com
   (para forçar o ISP a consultar o servidor .com na etapa 5)
4. Rapidamente, procura bob.com
   (para forçar o ISP a consultar o servidos no passo 5)
5. Consulta legítima para bob.com com seq = n+1
6. Resposta forjada de Trudy: Bob é 42.9.9.9, seq = n+1
7. Resposta real (rejeitada; tarde demais)

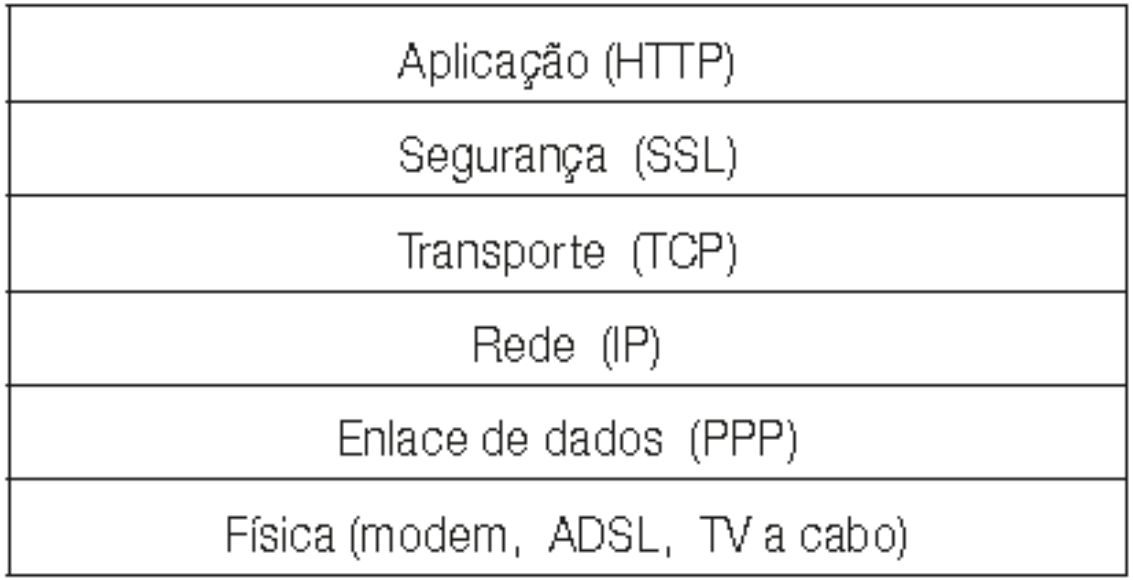
Como Trudy engana o ISP de Alice.

SSL – camada de soquetes seguros

Conexão segura inclui:

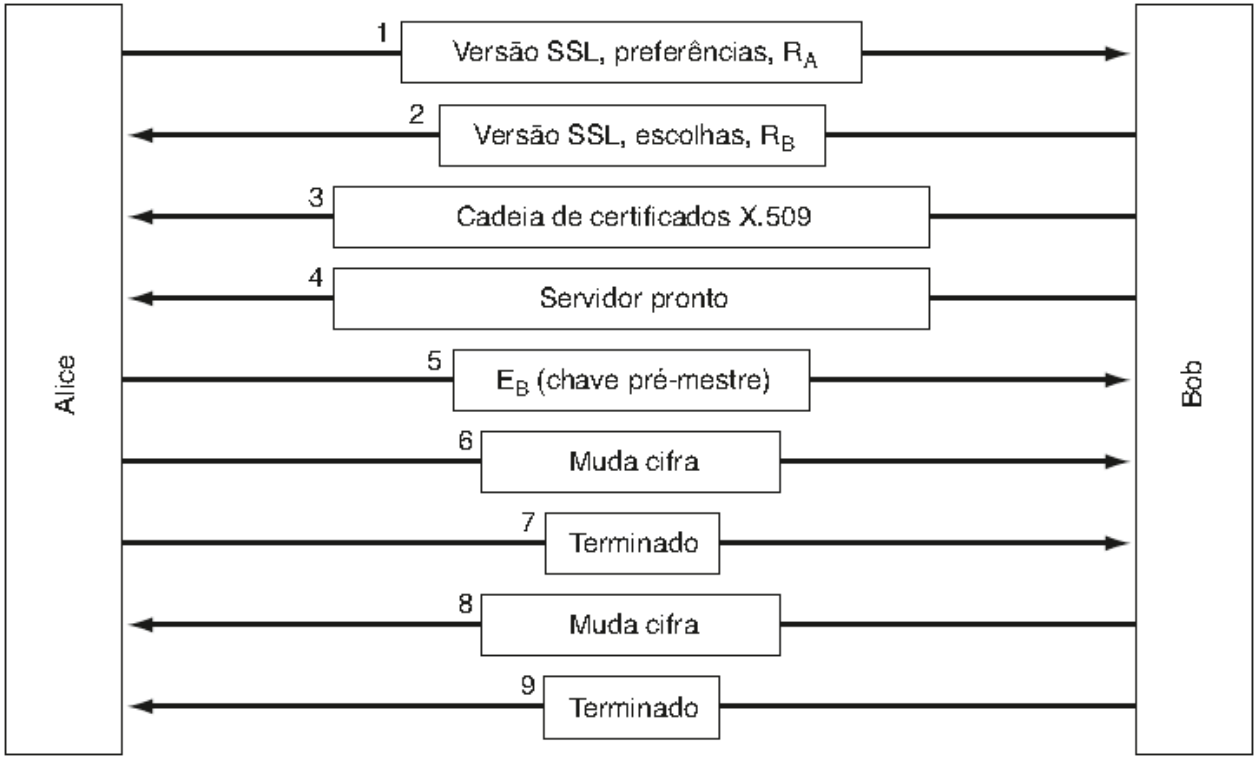
- Negociação de parâmetro entre cliente e servidor
- Autenticação do servidor pelo cliente
- Comunicação secreta
- Proteção da integridade dos dados

SSL – camada de soquetes seguros



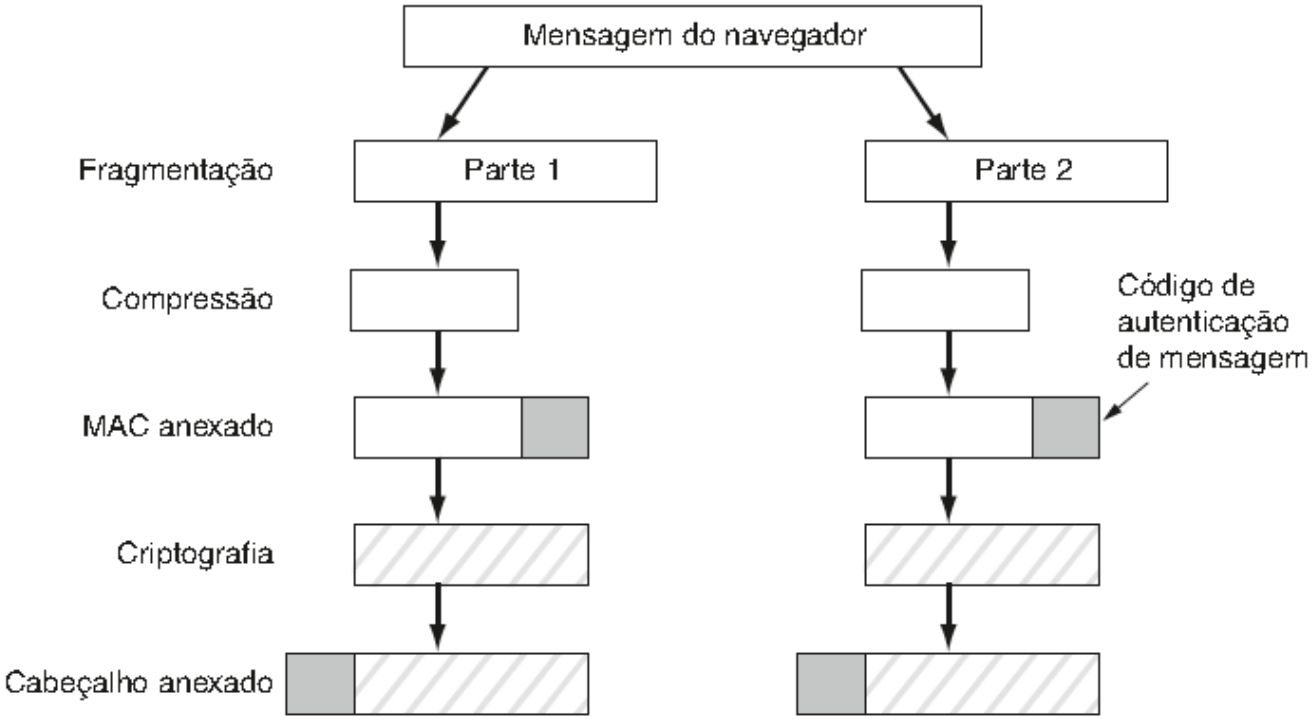
Camadas (e protocolos) para usuário doméstico navegando com SSL.

SSL – camada de soquetes seguros



Versão simplificada do subprotocolo de estabelecimento de conexões SSL.

SSL – camada de soquetes seguros



Transmissão de dados com SSL.