Escola Superior de Redes RNP

Teste de Invasão de Aplicações Web

Capítulo 1

Introdução e Revisão de Conceitos

Objetivos

- **Introduzir conceitos sobre desenvolvimento de software seguro e rever diversos tópicos relacionados à criptografia e aos protocolos HTTP e HTTPS.**

- **Ciclo de desenvolvimento de software seguro, arquiteturas e tecnologias de aplicações web, criptografia, protocolos HTTP e HTTPS.**

Tópicos abordados

- Introdução
- Ciclo de desenvolvimento de software seguro
- OWASP
- Arquiteturas e tecnologias de aplicações web
- Revisão de Criptografia
- Revisão dos protocolos HTTP e HTTPS
- Esquemas de codificação

Importante

NUNCA procure vulnerabilidades em sistemas, quaisquer que sejam, sem a devida AUTORIZAÇÃO!!!

Motivação

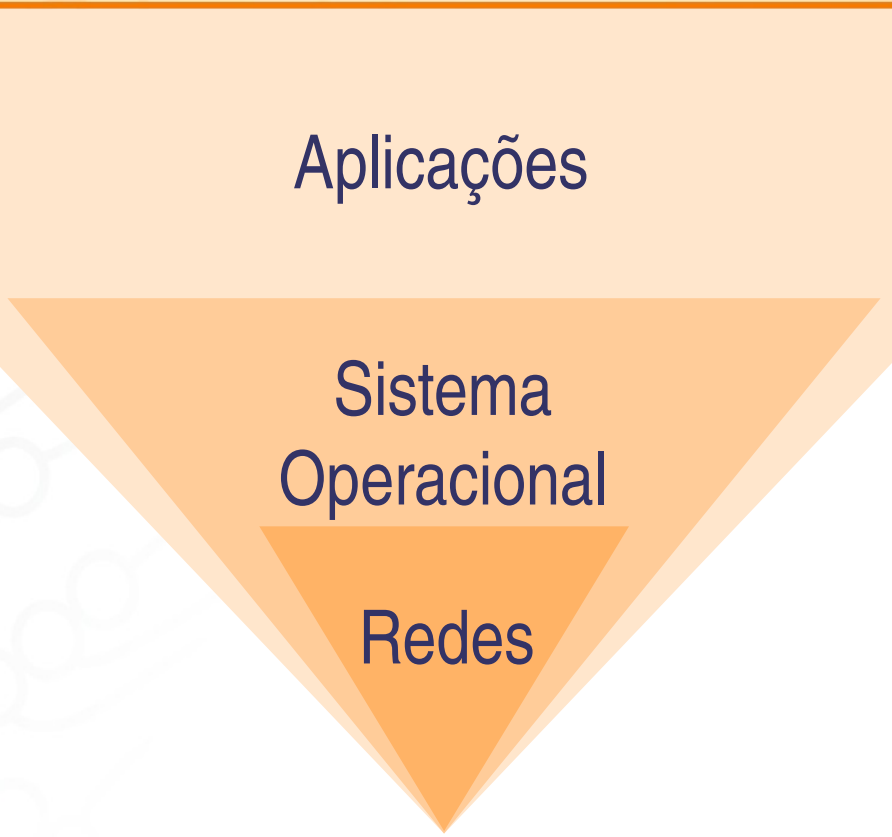
> *any program, no matter how innocuous it seems, can harbor security holes.*

Cheswick e Bellovin, 1994.

Cheswick

Bellovin

Distribuição de vulnerabilidades



Métodos para descobrir vulnerabilidades

Escola Superior de Redes RNP

Análise de documentos de requisitos, projeto e arquitetura

Análise de código-fonte

Teste de invasão

Ferramentas automatizadas

Exercício de Nivelamento 1

Desenvolvimento de software

- Sua organização adota um ciclo de desenvolvimento de software seguro?

Ciclo de desenvolvimento de software seguro

Escola Superior de Redes RNP

Um software seguro é aquele que satisfaz os requisitos implícitos e explícitos de segurança em condições normais de operação e em situações decorrentes de atividade maliciosa de usuários.

Embutir segurança quando o software já estiver pronto?

Segurança deve ser considerada em todo o ciclo de desenvolvimento de software!!

Custo de correção

Fase	Custo relativo para correção
Definição	1
Projeto alto nível	2
Projeto detalhado	5
Codificação	10
Teste de unidade	15
Teste de integração	22
Teste do sistema	50
Pós-entrega	100

Fonte: Wysopal *et al.* (2006)

Vulnerabilidades por fase do SDLC

Fase	Vulnerabilidade
Especificação	• Levantamento de requisitos de segurança • Análise dos funcionais se introduzem vulns • Ex: Microsoft Bob
Arquitetura e projeto	• Topologia de rede • Seleção de algoritmos criptográficos fracos
Codificação	• Extravasamento de buffer
Implantação	• Infra-estrutura subjacente vulnerável • Gerenciamento inadequado de chaves

Exercício de Fixação 1

Atividades de segurança

1. Que atividades de segurança podem ser incluídas em cada etapa de um ciclo de desenvolvimento de software seguro?

OWASP

Escola Superior de Redes RNP

Top Ten	Guia de desenvolvimento	Guia de testes
Guia de revisão de códigos	WebScarab	WebGoat

Arquiteturas e tecnologias de aplicações web

Escola Superior de Redes RNP

Nos primórdios da Internet, os servidores web forneciam, basicamente, conteúdo estático.

Modelo cliente-servidor.

Somente navegação por documentos referenciados por meio de hiperlinks.

Não é possível classificar tais provedores de conteúdo como aplicações web.

Sítios web eram centrados nos documentos e não nos usuários

Fluxo de processamento

Escola Superior de Redes RNP

Recebimento da requisição do usuário

Interpretação da solicitação e subsequente encaminhamento

Controle do acesso

Fluxo de processamento

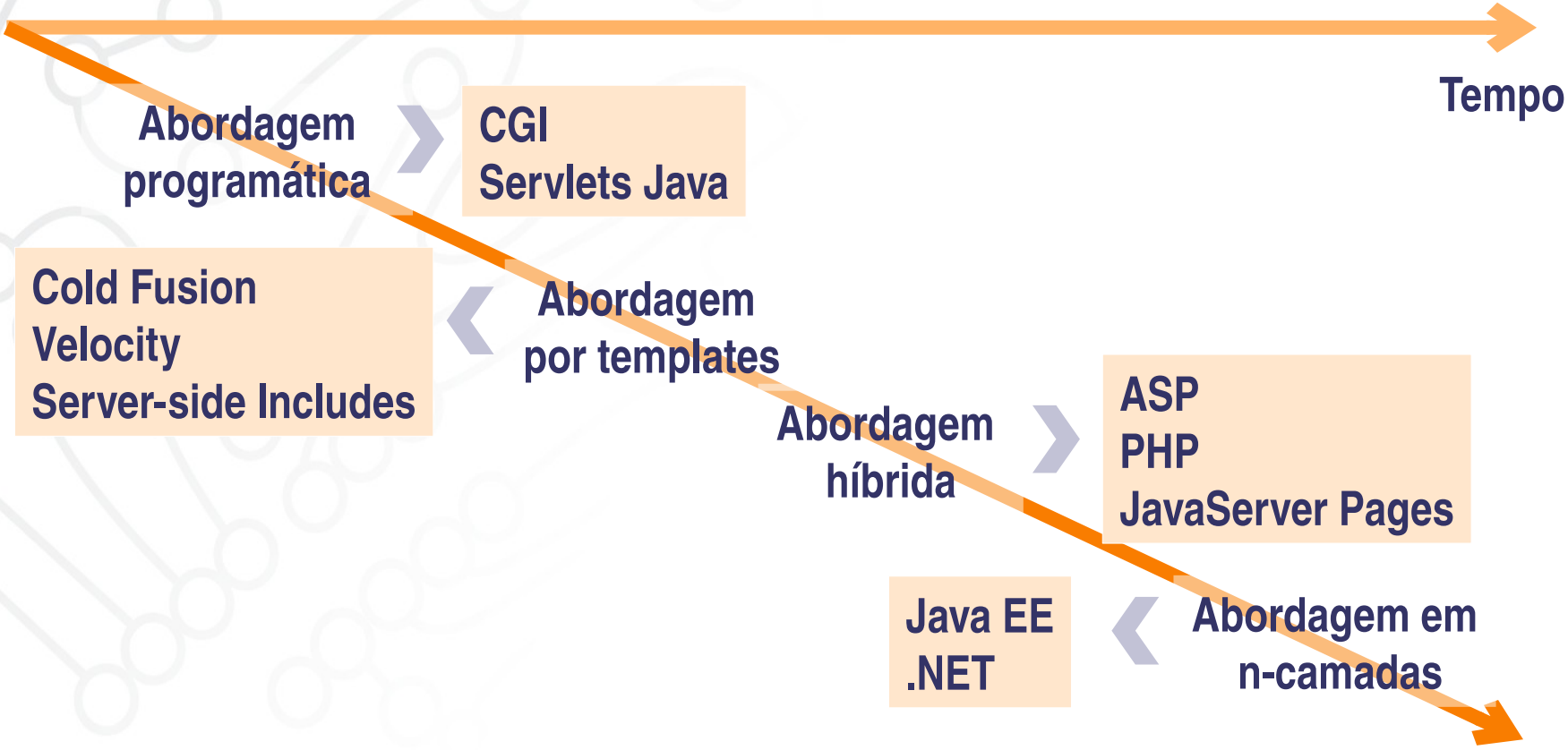
Escola Superior de Redes RNP

Acesso e atualização de dados

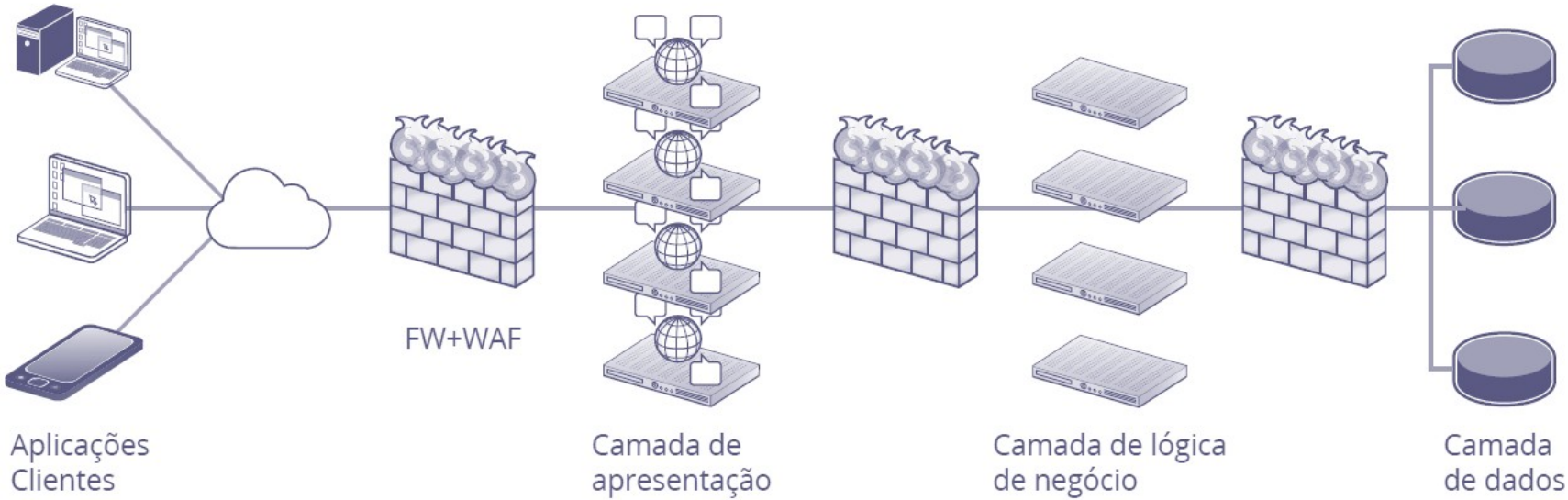
Personalização da resposta

Transmissão da resposta para apresentação ao usuário

Evolução


Tempo
Abordagem programática
CGI
Servlets Java
Cold Fusion
Velocity
Server-side Includes
Abordagem por templates
Abordagem híbrida
ASP
PHP
JavaServer Pages
Java EE
.NET
Abordagem em n-camadas

Topologia de aplicação em n-camadas



Fonte: Topologia de uma aplicação em n-camadas.

Exemplos de tecnologias

Componente	Exemplos
Camada de cliente	Navegadores web, aplicações Java, MS Office
Camada de apresentação	IIS, Apache, Tomcat, WebSphere, Jboss, Oracle GlassFish, Oracle WebLogic, Apache Geronimo.
Camada de negócio	WebSphere, Jboss, Oracle GlassFish, Oracle WebLogic, Apache Geronimo.
Camada de dados	Oracle database, MS SQL Server, MySQL.
Firewall de aplicação	Apache modSecurity, Imperva SecureSphere WAF, Cisco ACE WAF, Barracuda WAF.

Exercício de Nivelamento 2

Requisitos de segurança

- Que requisitos de segurança da informação podem ser atendidos por mecanismos criptográficos?

Revisão de Criptografia

Escola Superior de Redes RNP

Criptografia clássica

está relacionada a métodos para prover sigilo da informação.

Criptografia moderna

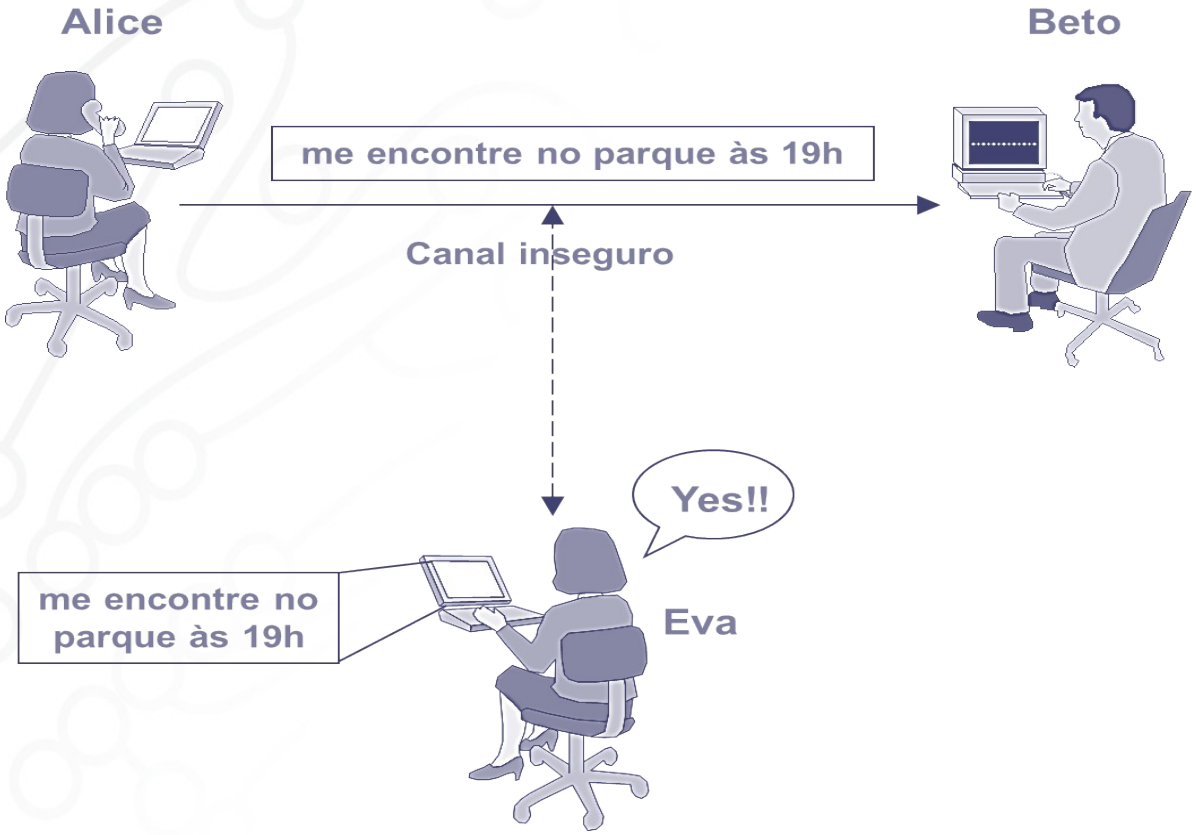
é um conjunto de técnicas matemáticas e computacionais para atender a diversos requisitos de segurança da informação.

Primitivas criptográficas

Escola Superior de Redes RNP

Primitiva criptográfica	Requisito de segurança
Cifra	Confidencialidade
Função de hash criptográfica	Integridade
Assinatura digital	Autenticidade da origem da mensagem Integridade Irretratabilidade
MAC	Autenticidade da origem da mensagem Integridade

Cifras - Motivação



Fonte:

Cifras

Escola Superior de Redes RNP

Mecanismo criptográfico utilizado para prover sigilo da informação.

Escola Superior de Redes RNP

Composta por duas transformações:

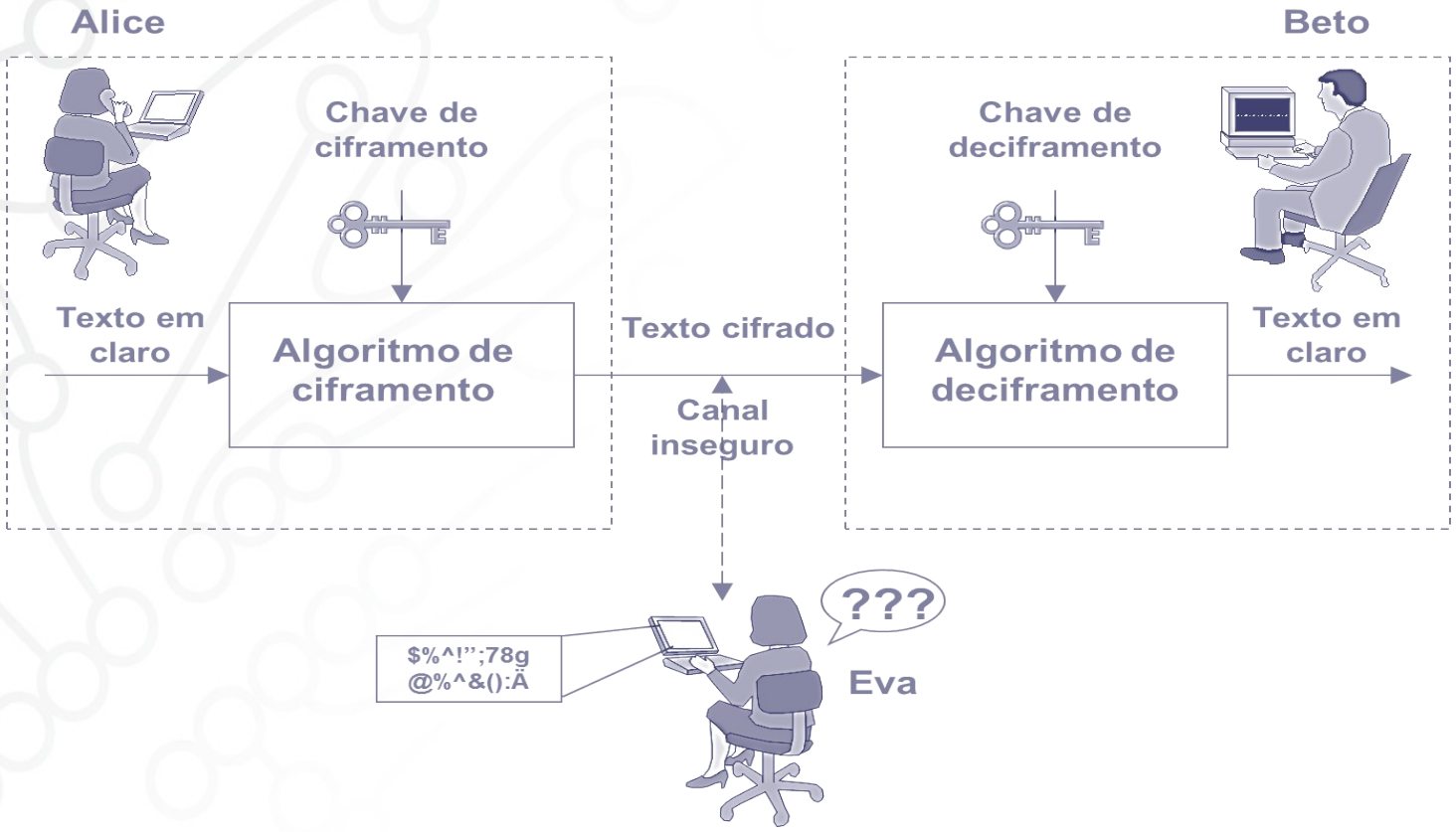
- Deciframento
- Ciframento

Escola Superior de Redes RNP

Termos importantes:

- Texto em claro
- Texto cifrado
- Chave

Cifras – Modelo geral



Fonte: Modelo geral para o uso de cifras.

Cifras simétricas

Escola Superior de Redes RNP

Na prática em muitas das cifras simétricas as chaves de ciframento e deciframento são iguais.

As partes que desejam se comunicar sigilosamente devem compartilhar uma chave simétrica.

Cifras simétricas

Escola Superior de Redes RNP

As chaves devem ser conhecidas apenas pelas partes que participam da comunicação.

Problema da distribuição de chaves – como chaves podem ser estabelecidas de maneira segura e eficiente?

Cifras simétricas - Classes

Escola Superior de Redes RNP

Cifra de bloco

é um esquema de ciframento que quebra a mensagem em blocos de tamanho fixo e cifra um bloco por vez.

Cifra de fluxo

é um esquema que cifra os caracteres individuais da mensagem, um por vez, empregando uma transformação variável.

Cifras assimétricas

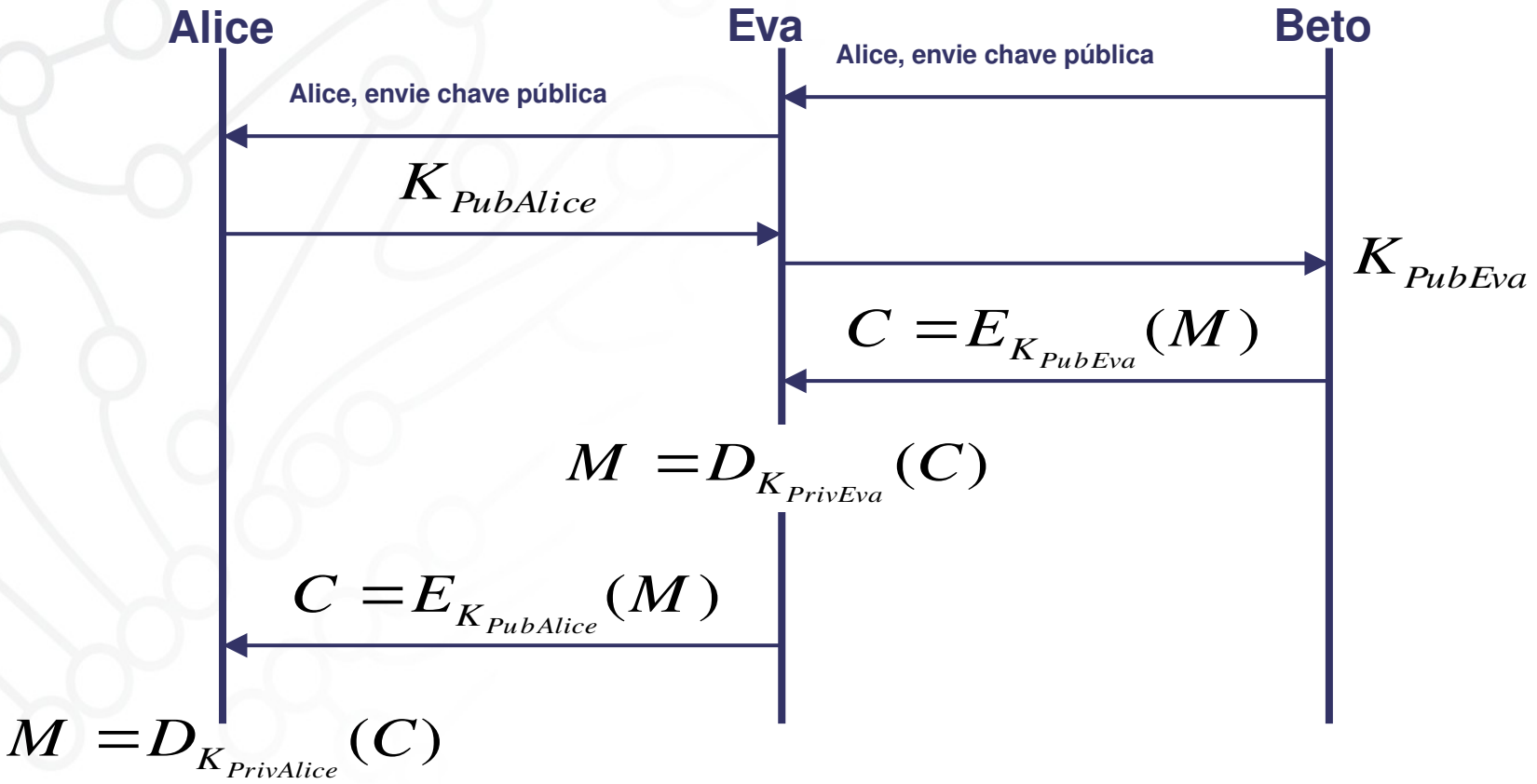
Escola Superior de Redes RNP

Cada usuário possui um par de chaves (pública, privada).

A chave pública é utilizada para ciframento e pode ser distribuída livremente.

A chave privada é utilizada para o deciframento de mensagens cifradas com a chave pública correspondente.

Necessidade de chaves públicas autênticas



Cifras simétricas x assimétricas

	Vantagens	Desvantagens
Simétricas	• Rápidas • Chaves pequenas	• Muitas chaves para gerenciar • Sigilo das chaves nas duas pontas
Assimétricas	• Poucas chaves para gerenciar • Somente chave privada precisa ser mantida em sigilo	• Lentas • Chaves grandes

Funções de hash criptográficas

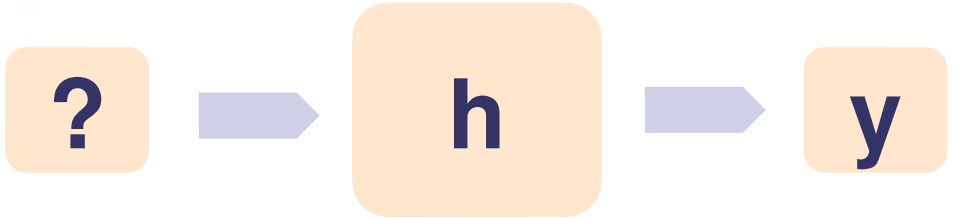
Escola Superior de Redes RNP

"Função computacionalmente eficiente que mapeia cadeias binárias de tamanho arbitrário para cadeias binárias de tamanho fixo qualquer, chamadas de **valores hash**".

Funções de hash – Propriedades
Resistência da pré-imagem

Escola Superior de Redes RNP

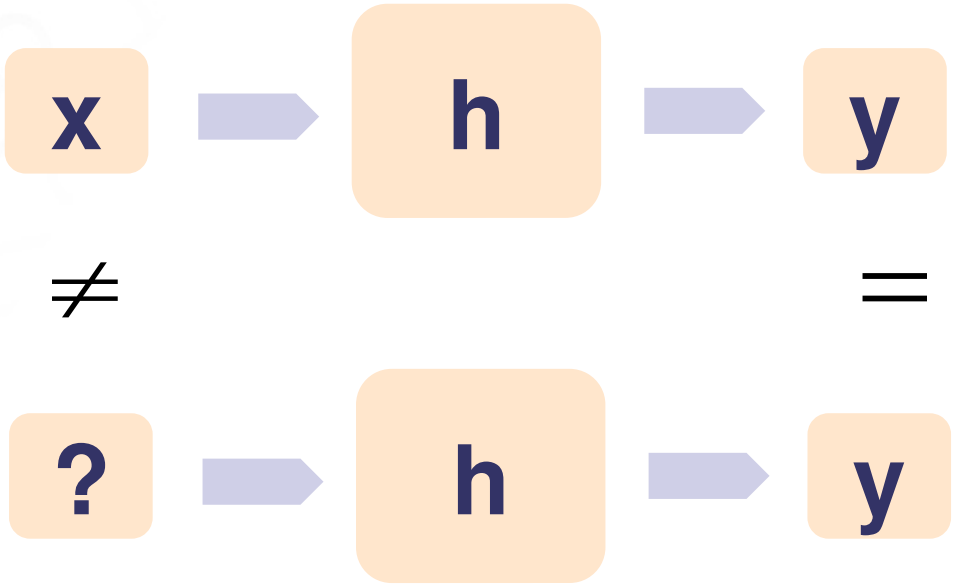
pré-imagem



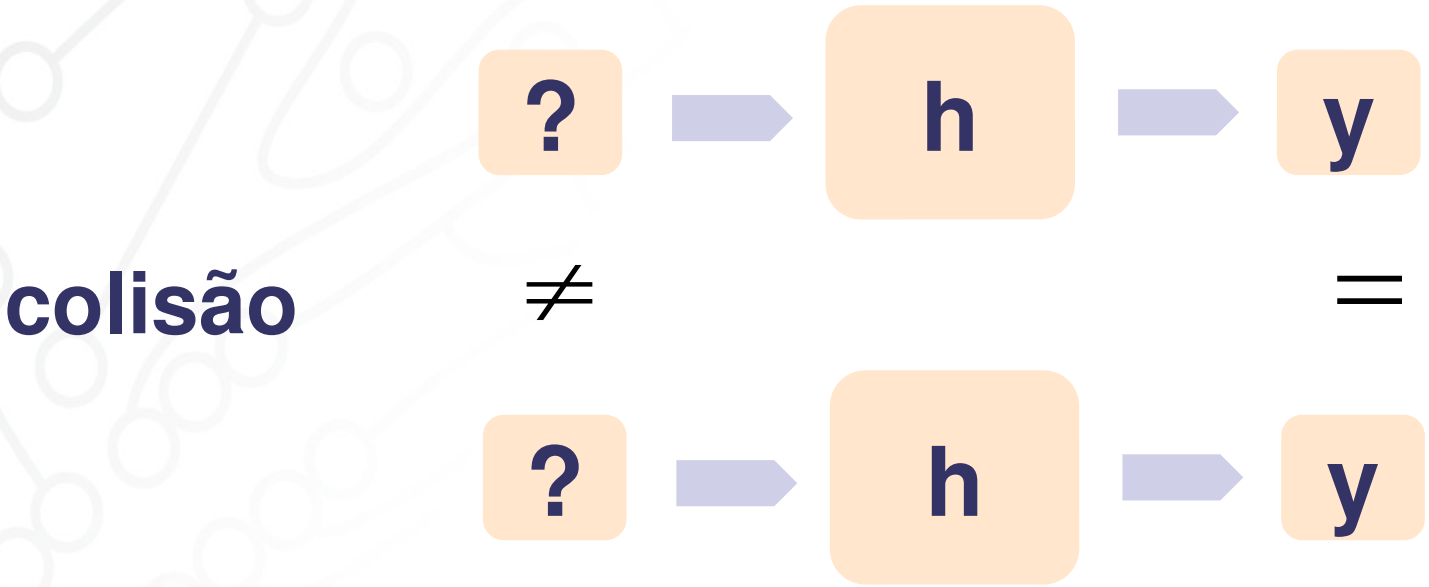
Funções de hash – Propriedades
Resistência da segunda pré-imagem

Escola Superior de Redes RNP

segunda pré-imagem



Funções de hash – Propriedades
Resistência a colisões



Funções de hash - Usos

Escola Superior de Redes RNP

Proteção de senhas em sistemas Unix/Linux

Verificação de integridade de arquivos

Funções de hash - Ataques

Escola Superior de Redes RNP

Ataque de Wang e Yu (2005) contra o MD5 resultou na violação da resistência a colisões.

Geração de um certificado digital válido, com chave privada correspondente, de uma autoridade certificadora intermediária.

MACs

Escola Superior de Redes RNP

Códigos de autenticação de mensagem (MAC) têm por objetivo garantir a integridade de uma mensagem, bem como a sua origem.

Recebem como entrada a mensagem e uma chave simétrica.

Não garantem irretratabilidade.

MACs - Propriedades

Escola Superior de Redes RNP

Facilidade de computação

Compressão

Resistência à computação

Assinaturas digitais

Escola Superior de Redes RNP

Associa uma mensagem a uma entidade.

Provê autenticação da origem da mensagem, integridade e não-repúdio.

Diferente de assinaturas manuais. Por quê?

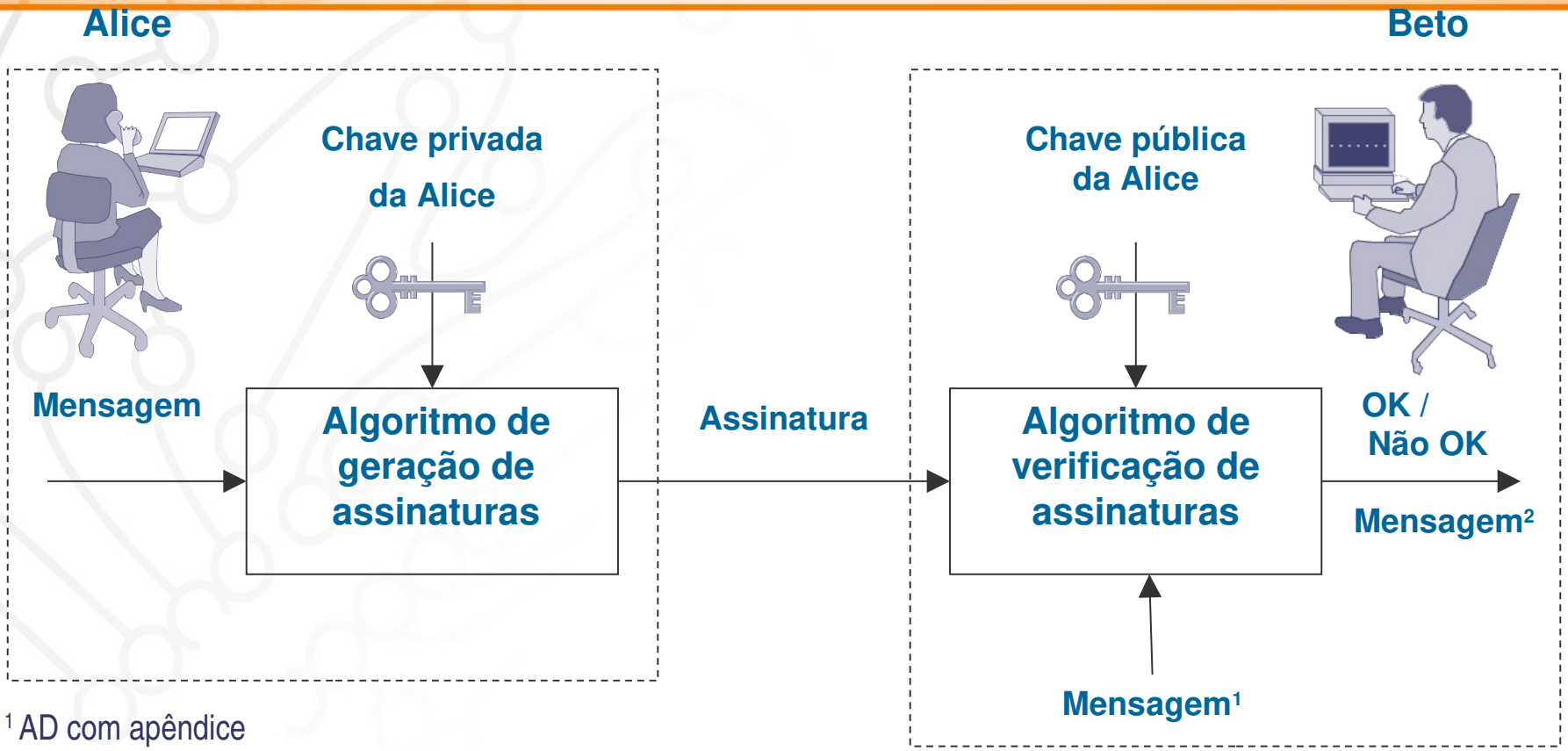
Assinaturas digitais

Escola Superior de Redes RNP

Requisitos importantes:

- Deve ser computacionalmente infactível construir uma mensagem para uma assinatura existente.
- Construir uma assinatura fraudulenta para uma mensagem qualquer.

Assinaturas digitais – Modelo geral



[1] AD com apêndice

[2] AD com recuperação de mensagem

Certificado digital

Escola Superior de Redes RNP

Associa uma chave pública a uma entidade

É assinado digitalmente por uma autoridade certificadora

Padrão utilizado: X.509

SSL/TLS

Escola Superior de Redes RNP

Secure Socket Layer foi criado pela Netscape

TLS 1.0 basicamente é SSLv3

Provê:

- Sigilo
- Integridade
- Autenticidade de entidades
- Autenticidade da origem de mensagens

SSL/TLS Protocolos

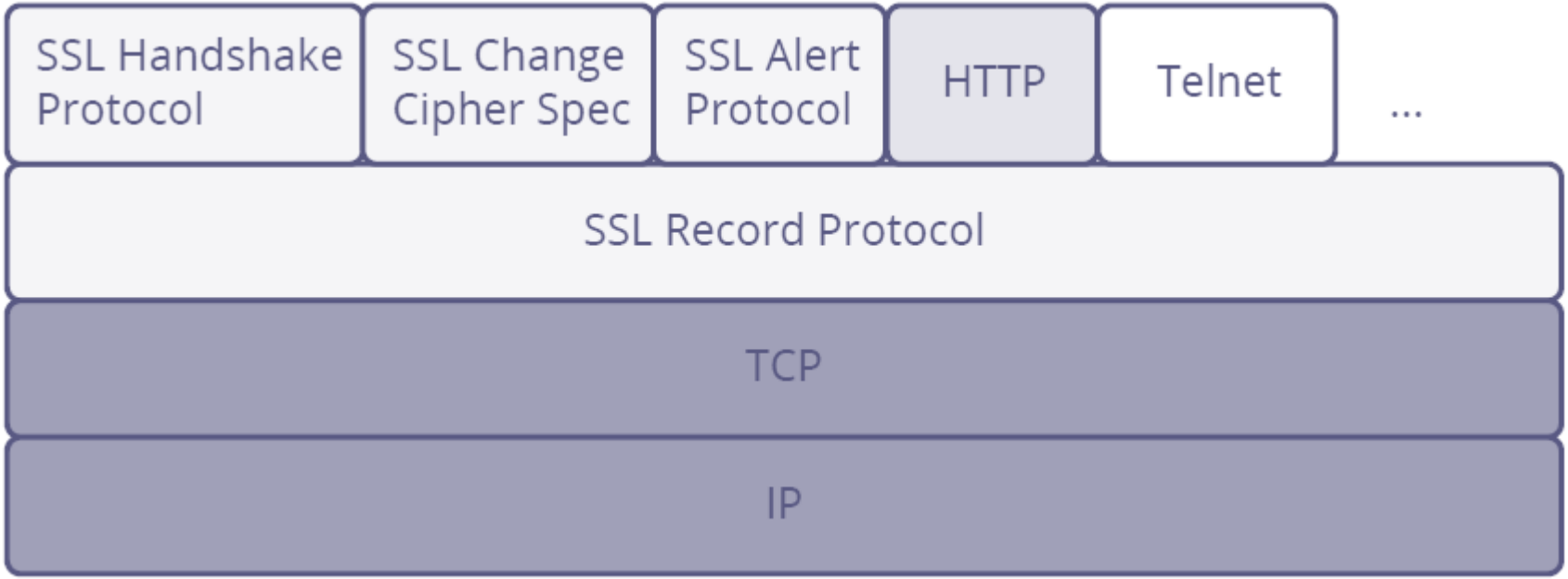


Figura 1.6 - Pilha de protocolos do SSL.

Protocolo SSL Record

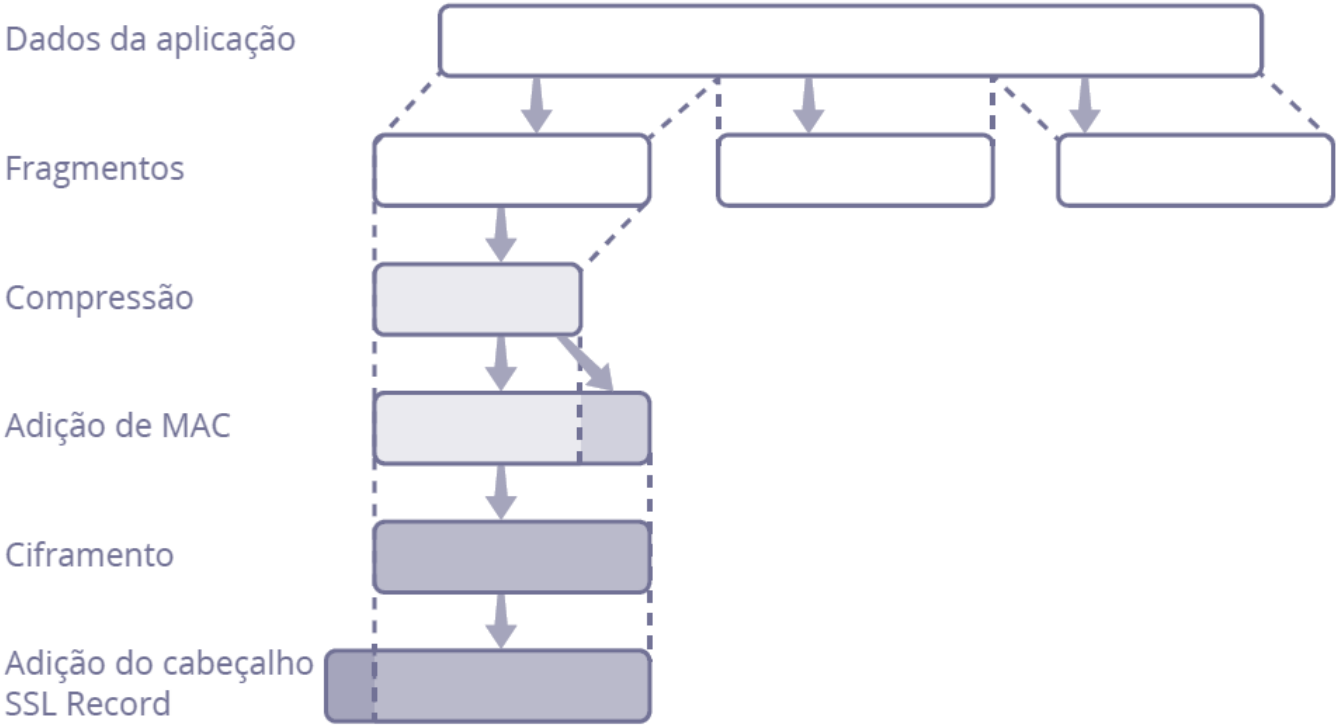


Figura 1.7 - SSL Record Protocol.

SSL Handshake

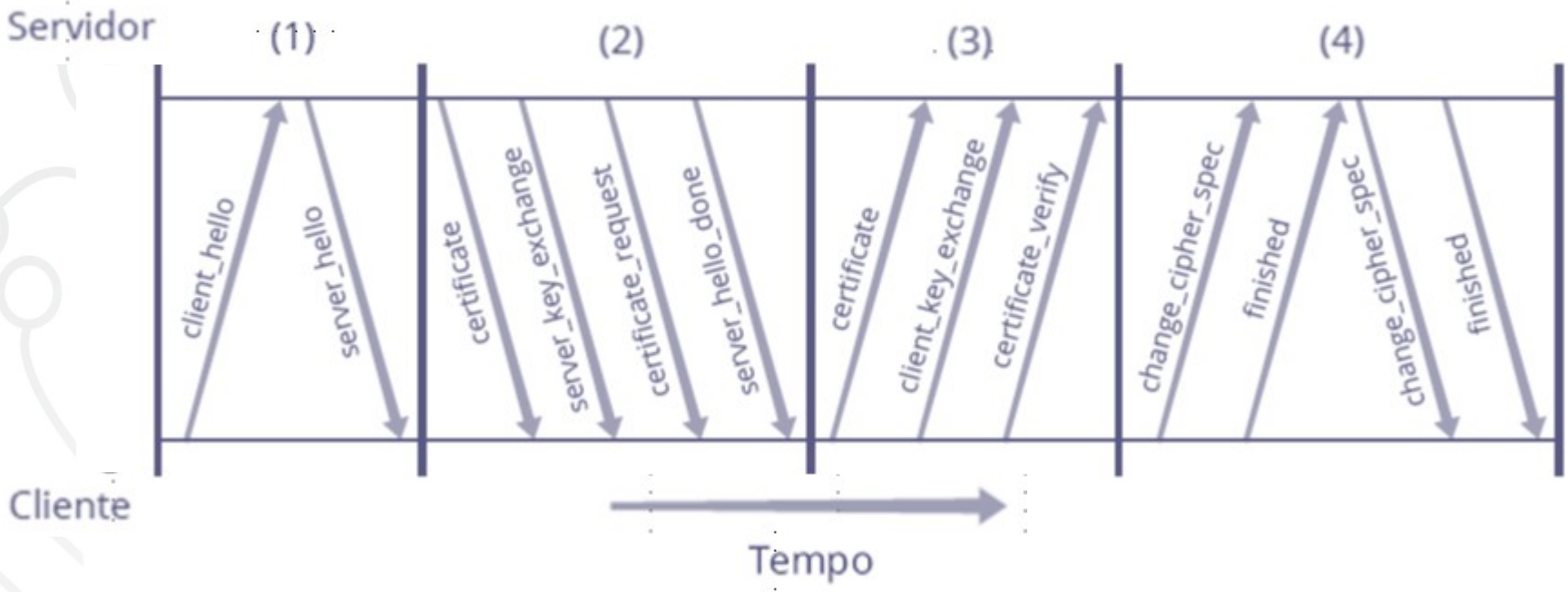


Figura 1.8 - SSL Handshake.

Escola Superior de Redes RNP

Exercício de Fixação 2

Segurança da informação

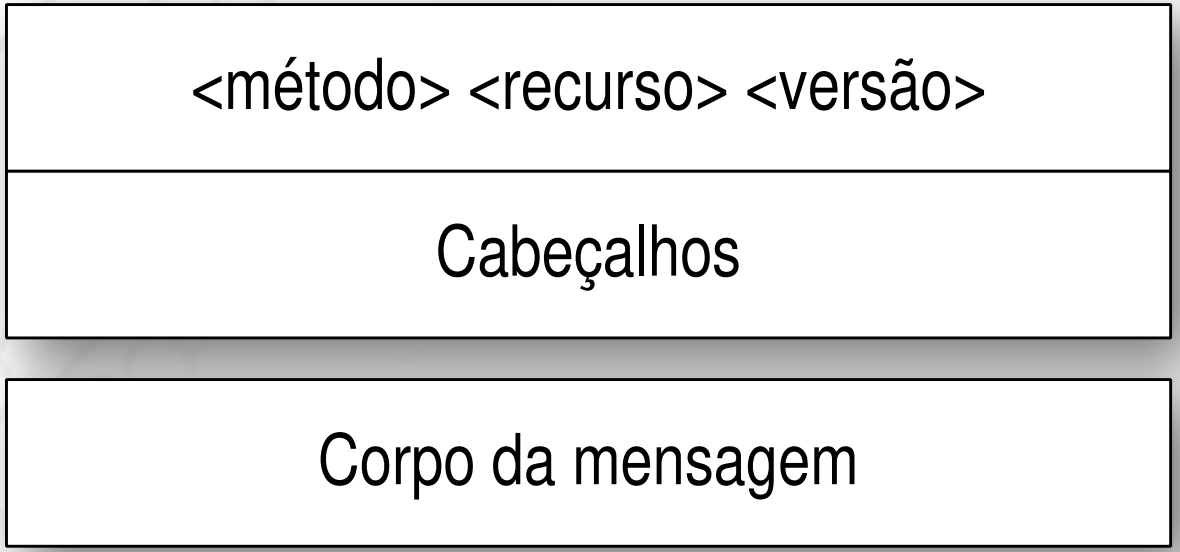
1. Que primitivas criptográficas satisfazem a cada um dos requisitos de segurança da informação?
2. Qual é o propósito de um certificado digital?

Protocolo HTTP – Introdução

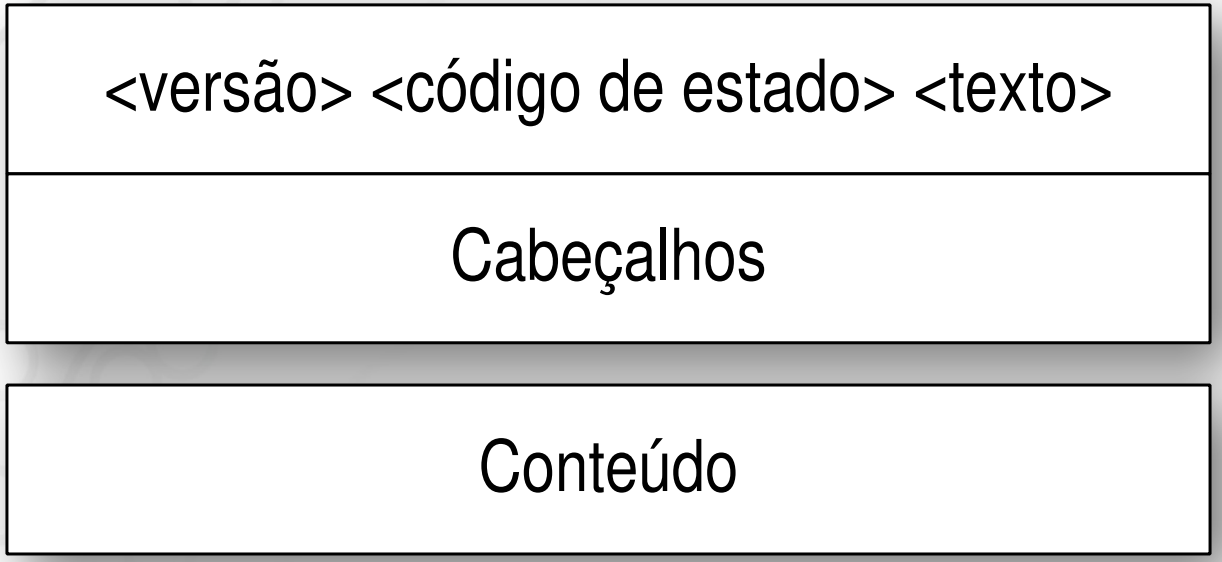
Escola Superior de Redes RNP

Protocolo da camada de aplicação	**Cliente-servidor**	**Transporte normalmente realizado por TCP/IP.**
Não é orientado à conexão.	**Recursos são identificados por URLs.**	**Não possui proteções nativas.**

Protocolo HTTP – Requisição



Protocolo HTTP – Resposta



Protocolo HTTP – Métodos

Escola Superior de Redes RNP

Indicam a ação solicitada pela requisição.

Métodos existentes:

- GET
- POST
- OPTIONS
- HEAD
- PUT
- DELETE
- TRACE
- CONNECT

Protocolo HTTP – Cabeçalhos

Escola Superior de Redes RNP

Compõem a segunda seção de requisições e respostas.

Definem características de ambas.

Um cabeçalho por linha.

Formato:

<nome>: <valor>

Exemplos:

Host – nome de domínio do servidor;

User-Agent – aplicação cliente que gerou a requisição;

Accept – tipos de conteúdos aceitos pelo cliente;

Set-Cookie – define um *cookie* no navegador.

Protocolo HTTP – Códigos de estado

Escola Superior de Redes RNP

1xx – códigos de informação.

2xx – indicam sucesso.

Ex.: 200 OK.

3xx – ações adicionais são necessárias.

Ex.: 301 Moved Permanently.

4xx – requisição não pode ser atendida.

Ex.: 404 Not Found.

5xx – erros no servidor.

Ex.: 501 Not Implemented.

Protocolo HTTP – Cookies

Escola Superior de Redes RNP

Mecanismo utilizado para lembrar informações do usuário.

Formado por pares nome/valor separados por ponto-e-vírgula.

Enviado automaticamente pelos navegadores.

Protocolo HTTP – Cookies

Escola Superior de Redes RNP

Atributos:

- expires
- path
- HttpOnly
- domain
- secure

Protocolo HTTP – Autenticação (1)

Escola Superior de Redes RNP

Métodos de autenticação definidas pela RFC 2617:

- Basic
- Digest

Protocolo HTTP – Autenticação (1)

Escola Superior de Redes RNP

Problemas:

- Não é possível travar contas
- Não é possível desconectar-se do sistema

Autenticação

Protocolo HTTP – Autenticação (2)

GET http://www.exemplo.com/basic/ HTTP/1.1

HTTP/1.1 401 Authorization Required
WWW-Authenticate: ...

GET http://www.exemplo.com/basic/ HTTP/1.1
Authorization: ...

Esquemas de codificação

Escola Superior de Redes RNP

Um processo de codificação consiste em substituir elementos de um conjunto por itens de outro, segundo uma regra pré-estabelecida.

O simples conhecimento das transformações de ida e volta é suficiente para realizar as traduções entre os dois domínios.

Esquemas de codificação

Esquemas de codificação podem ser empregados na proteção contra alguns ataques, como o cross-site scripting, por exemplo.

Em testes de invasão, são usados na construção correta dos vetores de teste, quando estes são passados por meio de URLs, além da evasão de filtros de entrada.

Codificação de URL (1)

Escola Superior de Redes RNP

Uma URL, ou mais geralmente uma URI, pode conter somente caracteres ASCII imprimíveis.

Alguns deles possuem significado especial em URLs, atuando como delimitadores, e, assim, são classificados como reservados.

Codificação de URL (1)

Escola Superior de Redes RNP

Quando precisam ser utilizados como dados, neste contexto, devem ser codificados, para que possam ser corretamente identificados como tais.

O método empregado, chamado de codificação de URL ou codificação percentual, consiste no uso de um caractere "%" seguido de dois dígitos hexadecimais, que representam o valor numérico do dado sendo codificado.

Escola Superior de Redes RNP

Exercício de Fixação 3

Protocolo HTTP

1. Quais as principais características do protocolo HTTP?

Codificação de URL (2)

Caractere reservado	Caractere codificado	Caractere reservado	Caractere codificado
!	%21	=	%3D
*	%2A	+	%2B
‘	%27	$	%24
(	%28	,	%2C
)	%29	/	%2F
;	%3B	?	%3F
:	%3A	#	%23
@	%40	[	%5B
&	%26	]	%5D

Figura 1.9 - Codificação dos caracteres reservados em URL.

Codificação HTML

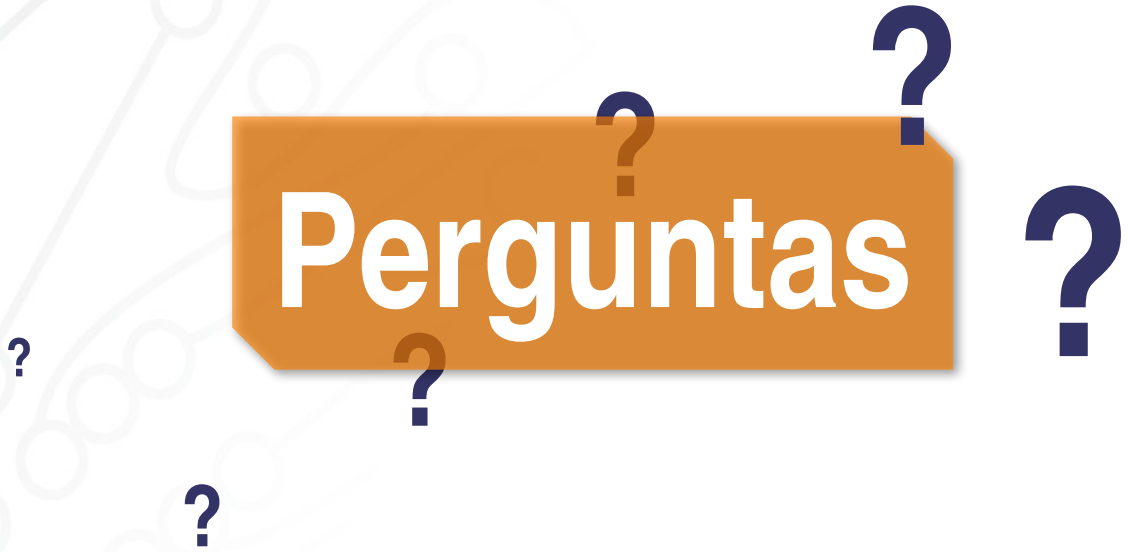
Escola Superior de Redes RNP

Alguns caracteres possuem significado especial em HTML.

Se for necessário exibi-los como parte do conteúdo, é necessário codificá-los, para que não sejam considerados como metacaracteres, pelo navegador web.

Existem três maneiras de efetuar esta tarefa:

- **&<nome da entidade>;**
  - **Ex.: "<" é codificado como "<".**
- **&#<número decimal>;**
  - **Ex.: "<" é codificado como "<".**
- **&#x<número hexadecimal>;**
  - **Ex.: "<" é codificado como "<".**


Perguntas

Escola Superior de Redes RNP

Caderno de Atividade 1

1

Arquiteturas e tecnologias de aplicações web

Escola Superior de Redes RNP

Caderno de Atividade 1

2

Mecanismos criptográficos

Escola Superior de Redes RNP

Caderno de Atividade 1

3

Protocolos HTTP e HTTPS

Escola Superior de Redes RNP

Teste de Invasão de Aplicações Web

Capítulo 1

Introdução e Revisão de Conceitos

RNP MINISTÉRIO DA DEFESA MINISTÉRIO DA CIDADANIA MINISTÉRIO DA SAÚDE MINISTÉRIO DA EDUCAÇÃO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES PÁTRIA AMADA BRASIL GOVERNO FEDERAL