Segurança em Redes

Autoria

Esta apresentação foi desenvolvida por Ricardo Campos, docente do Instituto Politécnico de Tomar. Encontra-se disponível na página web do autor no link *Publications* ao abrigo da seguinte licença:

O seu uso, de parte ou da totalidade, pressupõe a utilização da seguinte referência:

Campos, Ricardo. (2011). Apresentação Segurança em Redes. 33 slides.

A sua disponibilização em formato PPT pode ser feita mediante solicitação (email: ricardo.campos@ipt.pt)

Bibliografia

On-line

SSL: http://www.tecmundo.com.br/1896-o-que-e-ssl-.htm

http://pt.kioskea.net/contents/crypto/ssl.php3

Segurança em Redes

Os protocolos actuais utilizam protocolos da Pilha de **protocolos IPV4**;

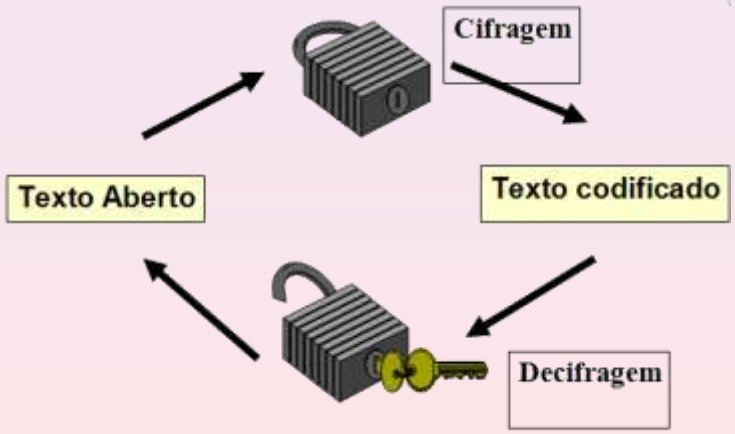
A informação circula entre **origem e destino** através de agentes **intermédios** geralmente **não confiáveis**;

Basta que um agente intermédio não seja confiável para que toda a **comunicação possa ser interceptada e analisada**;

A segurança na arquitectura TCP/IP será incrementada com a introdução do **IPV6** que para lá de resolver questões como o espaço de endereçamento IP, **dedica uma especial atenção aos requisitos de segurança**;

Criptografia

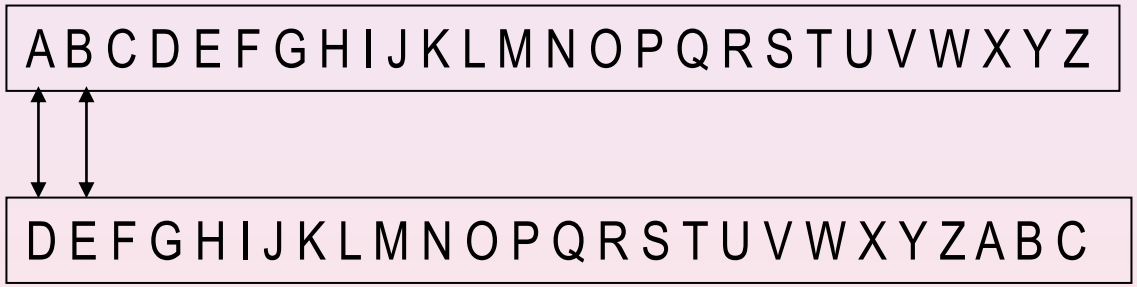
A criptografia é um mecanismo fundamental para se garantir a **confidencialidade na troca de mensagens**. Exemplos que combinam a utilização dos métodos de criptografia são o envio de mensagens de correio electrónico, o estabelecimento de conexões seguras para desenvolver transacções comerciais ou bancárias entre o browser de um utilizador e um site, etc..



Sistema de Criptografia Simples, Julius Caesar

Substituição de letras pelas letras deslocadas de N;

Exemplo N = 3;



Chave Secreta e Chave Pública

Dois sistemas de criptografia são usados actualmente:

- Sistemas de Chave Secreta (trabalha com uma única chave)

- Sistemas de Chave Pública (trabalha com pares de chaves)

Chave Secreta

Sistema de Criptografia Simétrico;

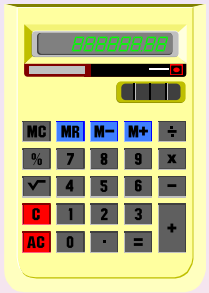
A **mesma chave** é usada para **cifrar e decifrar** a mensagem;

A segurança do sistema depende da chave ser conhecida apenas pelo emissor e receptor da mensagem;

A chave secreta deve ser fornecida de alguma forma para o destinatário para que a mensagem possa ser decifrada.

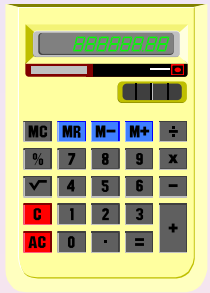
Criptografia

Algoritmo de cifragem



Texto aberto

Texto Codificado



Algoritmo de decifragem

Texto aberto

Chave Secreta

Chave Pública

Sistema de Criptografia Assimétrico

- Utiliza um **par de chaves**;
- Uma chave **publica para cifrar a mensagem**;
- Uma chave **privada para decifrar a mensagem**;

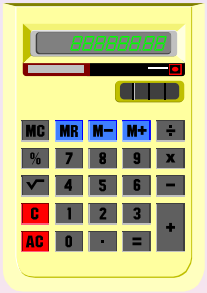
A **chave pública** não é secreta;

A **chave privada** é secreta;

A chave pública deve ser distribuída para os utilizadores que desejarem enviar uma mensagem com segurança.

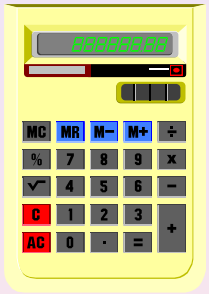
Criptografia

Algoritmo de cifragem



Texto aberto

Texto Codificado



Algoritmo de decifragem

Texto aberto

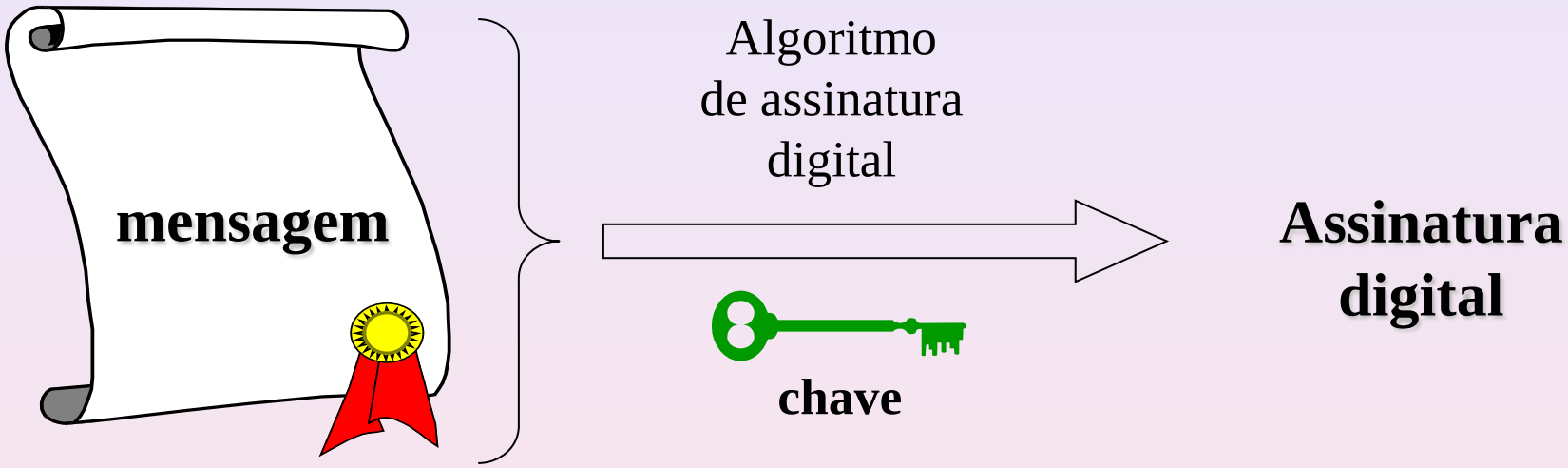
Chave Pública

Chave Privada

Assinatura Digital

O mecanismo da assinatura digital baseia-se na **criptografia assimétrica**, onde o **utilizador** que queira assinar uma mensagem **usa** a sua **chave privada** para criptografar a mensagem e o **receptor** poderá **verificar** a autenticidade da assinatura descriptografando a mensagem **com a chave pública do remetente** e com isto ter a certeza da autenticidade e integridade da mensagem.

Criptografia



Dificuldades no uso de chaves

Sistema de Chave Secreta

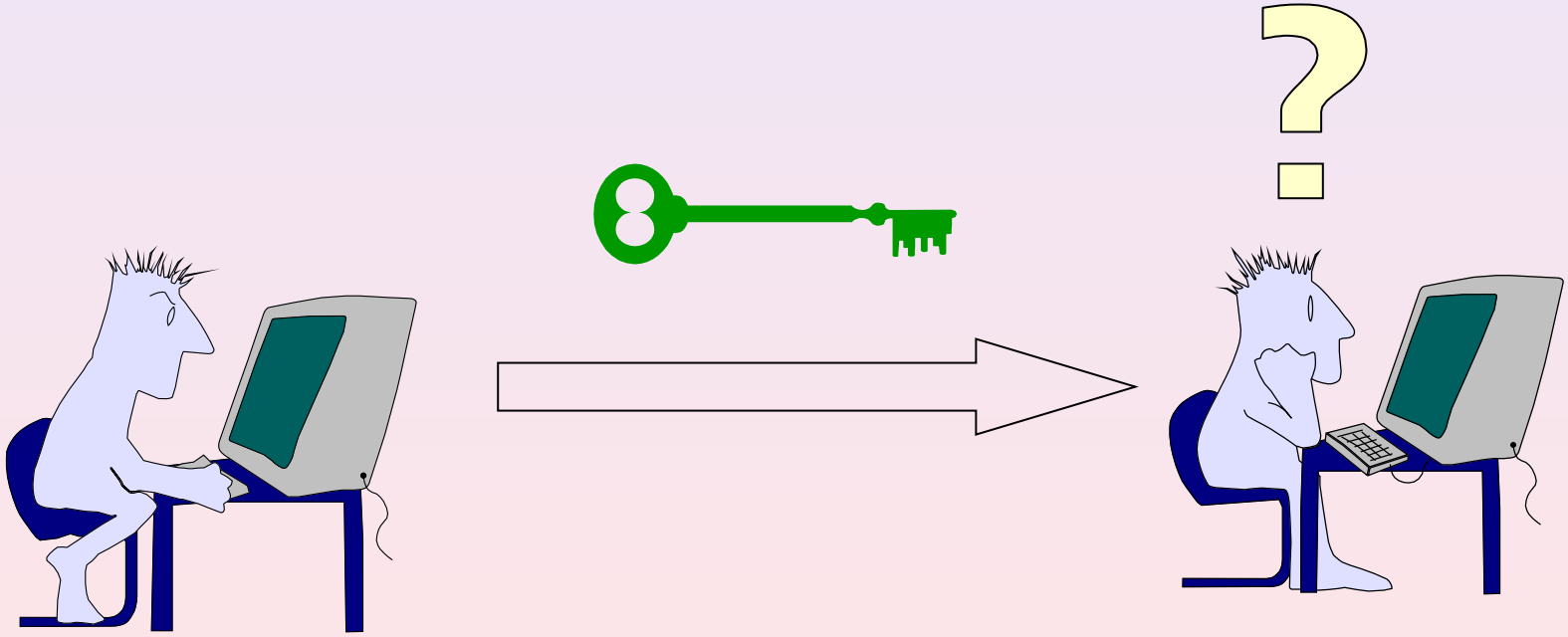
- problemas para comunicar com utilizadores que não se conhecem;
- problemas para comunicar com utilizadores distantes.

Sistema de Chave Pública

- como saber se a chave pública realmente pertence ao utilizadores com o qual se quer comunicar?

Certificação das Chaves

Mecanismo para certificar que a chave realmente pertence à pessoa com que se deseja comunicar:



Criptografia

Uma das maiores preocupações nos sistemas de chave pública, é a de **saber se uma mensagem está a ser encriptada com a chave pública correcta** de uma pessoa.;

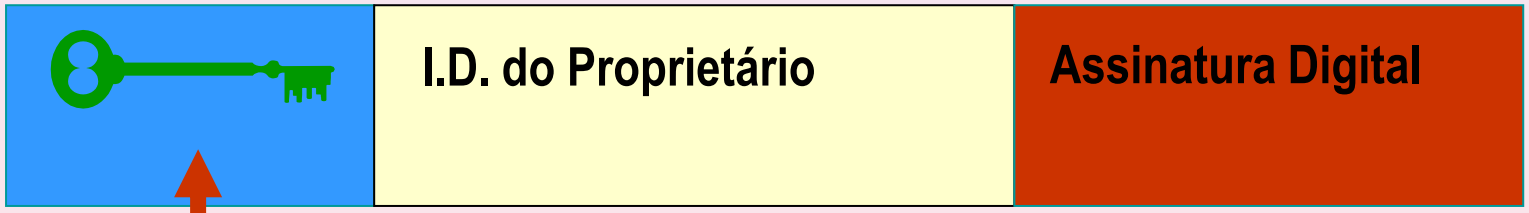
Para evitar estes problemas, **são utilizados os certificados digitais**. Estes certificados vão permitir **verificar, se uma chave pública pertence realmente a uma determinada pessoa**.

Um **certificado digital consiste** essencialmente de três coisas: **uma chave pública**; **informações sobre a identidade da pessoa** (nome, etc..); **uma ou mais assinaturas digitais**.

O objectivo das assinaturas digitais num certificado, é o de assegurar que a informação aí contida foi confirmada, por outra pessoa ou entidade na qual os outros confiam.

Criptografia

C.A. (certification authority)



Chave a ser certificada

Protocolos de Segurança

HTTPS e SSL

O HTTPS é a utilização do protocolo HTTP (HyperText Transfer Protocol) juntamente com o protocolo SSL (Secure Sockets Layer);

Trata-se de uma aplicação de segurança utilizada no ambiente Web;

Os sistemas de Home Banking e compras online são exemplos típicos em que este protocolo é utilizado;

Protocolos de Segurança

O sistema **SSL é independente do protocolo utilizado**, o que significa que pode igualmente proteger transacções feitas na Web pelo protocolo HTTP ou ligações via o protocolo FTP, POP, etc.

Quando é feita uma ligação a um URL com https (um site de Home Banking por exemplo), **o browser utiliza uma porta diferente da 80** (como seria normal num URL com http) **e o SSL é activado**;

O SSL é implementado no próprio browser;

O utilizador pode observar esta situação, verificando um aviso que é enviado pelo browser (no caso do Internet Explorer, aparece um cadeado).

Como gerar um certificado SSL?

A activação do SSL no servidor web implica o **fornecimento de informações sobre o detentor do Website, tais como endereço, documentação e pessoa de contacto**

O servidor web criará então um par de chaves: uma **chave privada**, que deverá ficar somente no servidor e uma **chave pública** que será utilizada, juntamente com os dados preenchidos anteriormente (detentor do website, etc…) para gerar um certificado CSR (Certificate Signing Request)

Este CSR é então submetido a uma autoridade certificadora (CA) que irá validar os dados, através da comprovação da autenticidade dos documentos e da propriedade do Website, garantindo que aquele certificado foi realmente emitido para o proprietário do Website. A autoridade certificadora, gera então o certificado definitivo.

Protocolos de Segurança

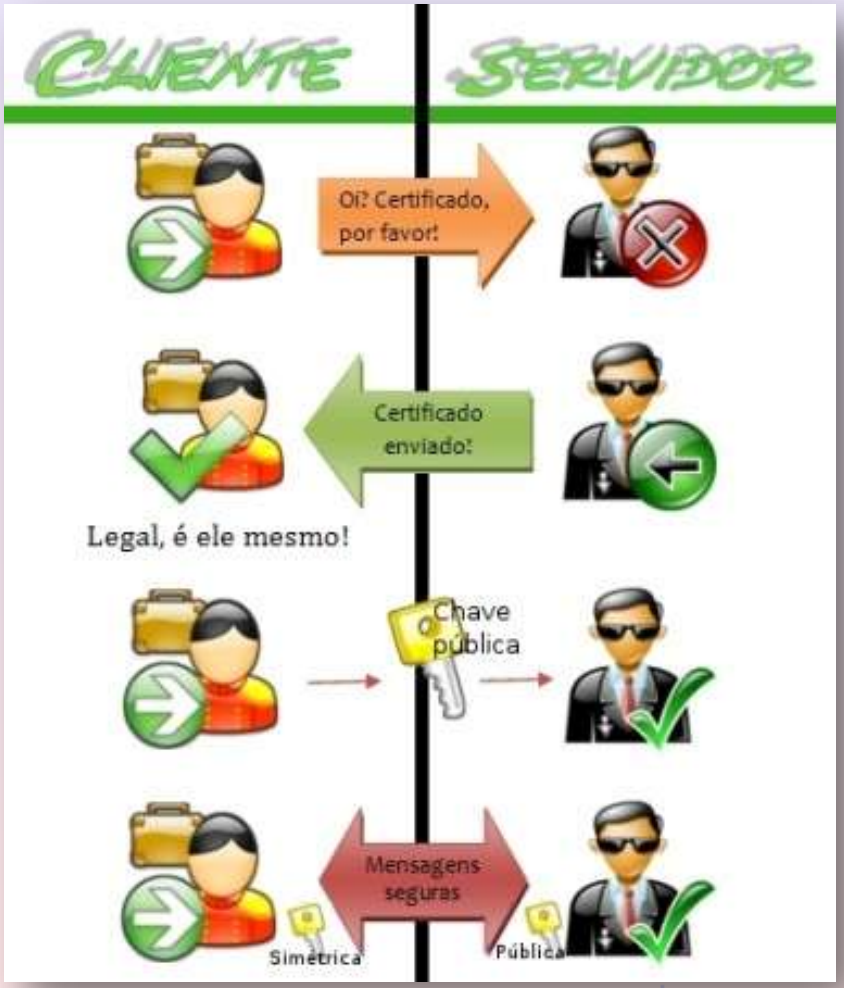
Funcionamento:

O cliente conecta-se ao site (a outro serviço) protegido por SSL e **pede-lhe que se autentique** (identifique).

O servidor, quando recebe o pedido, **envia um certificado ao cliente**, contendo a **chave pública do servidor**, **assinado por uma autoridade de certificação (CA)**

O cliente verifica a validade do certificado (e, por conseguinte, a autenticidade do site). Nesse momento autentica o certificado no armazenamento de autoridades de certificação.

Protocolos de Segurança



Protocolos de Segurança

Se o CA for desconhecido o browser dá ao utilizador a possibilidade de aceitar o certificado por sua conta e risco

Protocolos de Segurança

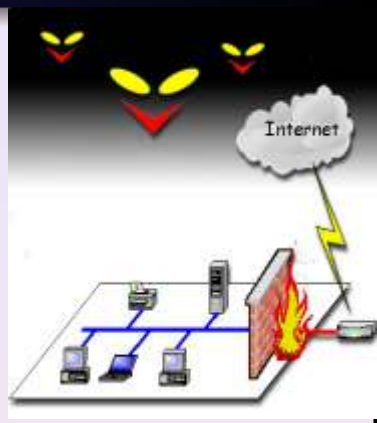
Porque acontece isto com os certificados?

Habitualmente isto acontece por uma de duas razões:

- A data actual não se encontra dentro da data de validade do certificado
- O certificado não pertence a uma autoridade de certificação confiável

Por forma a activar a confiabilidade do site deve instalar o certificado no armazenamento de autoridades de certificação.

Firewall



Filtra todo o tráfego entre a internet e a rede local;

Impede que utilizadores externos acedam aos serviços disponibilizados pela rede;

Todo o trafego de entrada e saída deve fluir através da *firewall*;

Apenas o trafego autorizado deve fluir através da *firewall*;

Imprescindível para qualquer empresa de pequena/média dimensão;

Cada vez mais utilizada nos computadores pessoais com ligação permanente à internet

Exemplos de Firewalls

- Firewall do Windows;

- ZoneAlarm (http://www.download.com);

- Outpost Firewall Pro (http://www.agnitum.com.pt);

Virus

Vírus

É um programa capaz de infectar outros programas e ficheiros de um computador. Para realizar a infecção, o vírus embute uma cópia de si mesmo num programa ou ficheiro, que quando executado também executa o vírus, dando continuidade ao processo de infecção.

Anti-Vírus

Entre os antivírus mais populares estão o Norton Antivírus e o AVG.

Download

AVG, http://www.grisoft.com

Norton, http://www.norton.com

Virus

Worms 

Um *Worm,* assim como um vírus, cria cópias de si mesmo de um computador para outro, mas faz isso automaticamente, não necessitando de ser explicitamente executado para se propagar.

A sua propagação dá-se através da exploração de vulnerabilidades existentes ou falhas na configuração de *software* instalado nos computadores.

O grande perigo dos *worms* é a sua capacidade de se replicar em grande volume. Por exemplo, um *worm,* pode enviar cópias de si mesmo a todas as pessoas que constam do seu catálogo de endereços de correio electrónico e os computadores dessas pessoas fazerem o mesmo, provocando um efeito dominó. *Os worms,* são responsáveis por consumir muitos recursos (memória e largura de banda), degradando o desempenho de redes (tornando por exemplo o acesso à Internet mais lento).

Cavalos de Tróia

Na informática, um Cavalo de Tróia é um programa que para além de executar funções para as quais foi aparentemente projectado, também executa outras funções normalmente maliciosas e sem o conhecimento do utilizador:

– Alteração ou destruição de ficheiros;

– Furto de palavras passe e outras informações sensíveis, como números de cartões de crédito.

É necessário que o cavalo de tróia seja executado para que ele se instale num computador. Exemplos comuns de cavalos de tróia são programas que o utilizador recebe ou obtêm de um *site* e que dizem ser jogos ou protectores de ecrã.

Virus

BackDoor

Sub-tipo de Cavalo de Tróia. Um BackDoor é um componente específico que abre uma "porta dos fundos" do computador. O maior objectivo é colectar todas as teclas pressionadas pelo utilizador (através de um componente *keylogger*), com o objectivo de transmitir as senhas bancárias e de cartões de crédito, digitadas pelo utilizador ao navegar por sites de compras, ou em operações de *net-banking*.

Spyware

Consiste num programa que recolhe informações sobre o utilizador, sobre os seus costumes na Internet (no âmbito comercial, por forma a monitorizar os hábitos dos utilizadores) e transmite esta informação a uma entidade externa na Internet, sem o seu conhecimento e o seu consentimento.

Virus

AdWare

Sub-grupo dos spyware. O *Adware* é similar ao spyware, mas não transmite informação pessoal. São conhecidos como programas que trazem para o ecrã do utilizador propaganda. É comum virem embutidos em programas de livre download (exemplo o software gratuito Kazaa é combinado com adwares proporcionando uma fonte de receita)

Phishing

Trata-se de uma armadilha que leva o utilizador a entregar, de forma voluntária, informação pessoal e confidencial, como números de cartões de crédito, informação de contas bancárias ou palavras-passe.

WWW – World Wide Web

Ferramentas gratuitas para testes de segurança em web sites

Netsparker Community Edition: http://www.mavitunasecurity.com/communityedition/

Websecurify: http://www.websecurify.com/

Wapiti: http://www.ict-romulus.eu/web/wapiti/home

N-Stalker: http://www.nstalker.com/products/editions/free/

Skipfish: http://code.google.com/p/skipfish/

Watcher: http://websecuritytool.codeplex.com/

X5s: http://xss.codeplex.com/

Acunetix: http://www.acunetix.com/cross-site-scripting/scanner.htm