Redes de Computadores

Prof. Macêdo Firmino

Princípios de Segurança de Redes

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Pergunta???

Acessar a Internet é seguro?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

Utilizar a Internet requer que alguns cuidados sejam tomados e, para isto, é importante que você esteja informado dos riscos aos quais está exposto. Alguns destes riscos são:

- Acesso a conteúdos impróprios ou ofensivos: pode se deparar com páginas que contenham pornografia, que atentem contra a honra ou que incitem o ódio e o racismo.
- Contato com pessoas mal-intencionadas: existem pessoas que se aproveitam da Internet para aplicar golpes, tentar se passar por outras pessoas e cometer crimes como, por exemplo, estelionato, pornografia infantil e sequestro.
- Furto de identidade: assim como você pode ter contato direto com impostores, também pode ocorrer de alguém tentar se passar por você, colocando em risco a sua imagem ou reputação.

Introdução

- Furto e perda de dados: os dados presentes em seus equipamentos conectados a Internet podem ser furtados e apagados, pela ação de ladrões, atacantes e códigos maliciosos.
- Invasão de privacidade: a divulgação de informações pessoais pode comprometer a sua privacidade, de seus amigos e familiares.
- Divulgação de boatos: pessoas podem usar a Internet para a divulgação de informações falsas, que podem gerar pânico e prejudicar pessoas e empresas.
- Dificuldade de exclusão: aquilo que e divulgado na Internet nem sempre pode ser totalmente excluído ou ter o acesso controlado. Uma opinião dada em um momento de impulso pode ficar acessível por tempo indeterminado e pode, de alguma forma, ser usada contra você.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução

- Dificuldade de manter sigilo: caso não sejam tomados os devidos cuidados, as informações podem trafegar ou ficar armazenadas de forma que outras pessoas tenham acesso ao conteúdo.
- Uso excessivo: o uso desmedido da Internet, assim como de outras tecnologias, pode colocar em risco a sua saúde física, diminuir a sua produtividade e afetar a sua vida social ou profissional.
- Plágio e violação de direitos autorais: a cópia, alteração ou distribuição não autorizada de conteúdos e materiais protegidos pode contrariar a lei de direitos autorais e resultar em problemas jurídicos e em perdas financeiras.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Pergunta???

Como podemos saber se a comunicação é segura?

Introdução

- Uma comunicação é dita segura se apresentar as seguintes propriedades:
  - Confidencialidade: somente o remetente e o destinatário devem poder "entender" o conteúdo da mensagem transmitida;
  - Autenticação: remetente e destinatário precisam confirmar a identidade um do outro (confirmar que a outra parte é que alega ser);
  - Integridade: remetente e destinatário precisam assegurar que o conteúdo de sua comunicação não foi alterado, por acidente ou por má intenção, durante a transmissão;
  - Disponibilidade: a comunicação deve ocorrer (ou seja, os serviços e recursos do sistema devem estar disponíveis sempre que forem necessários para os usuários legítimos).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Pergunta???

O que fazer para tentar garantir a segurança na comunicação?

Introdução

- Para tentar reduzir os riscos e se proteger há diversos mecanismos de segurança. Por exemplo:
  - Criptografia;
  - Antivírus;
  - Firewall;
  - Cópias de segurança (*Backups*);
  - Assinatura Digital e Certificado Digital.

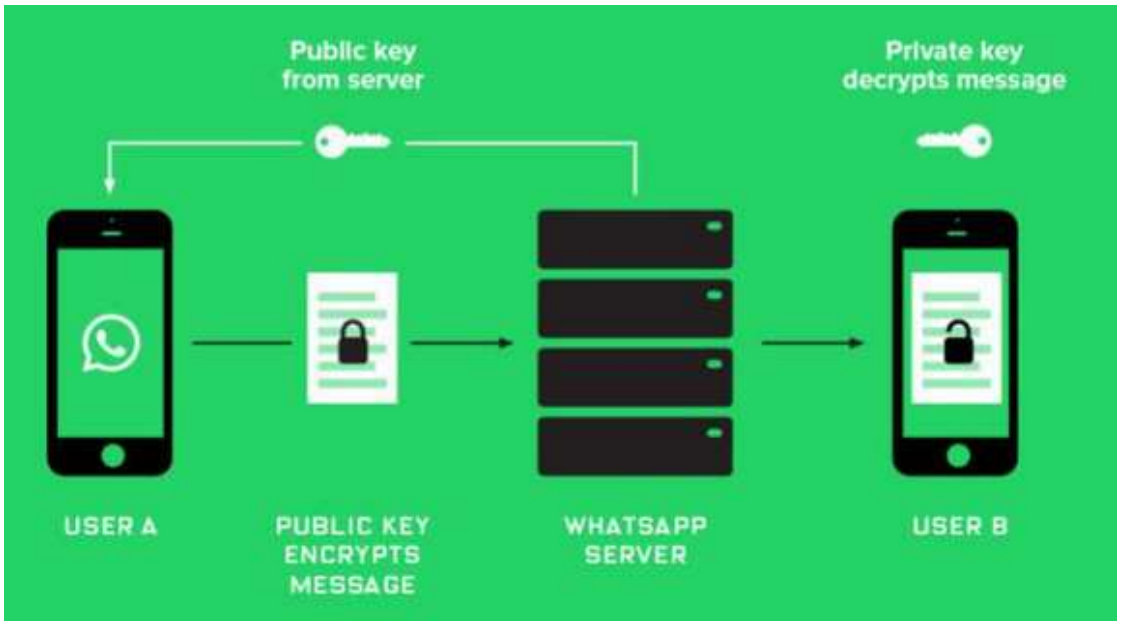
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Pergunta???

O que é criptografia?

Criptografia

É a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de decriptografia específica. Esse técnica visa garantir a confidencialidade da informação.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Criptografia

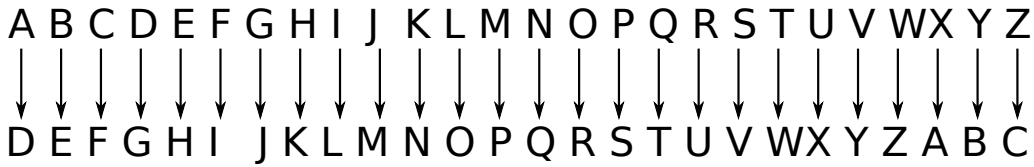
Componentes

A mensagem original, antes de ser transformada, é chamada texto claro. Após transformada, ela é denominada simplesmente texto cifrado. Um algoritmo de criptografia transforma o texto claro em texto cifrado; um algoritmo de decriptografia transforma o texto cifrado de volta para texto claro. O emissor usa um algoritmo de criptografia e o receptor utiliza um algoritmo de decriptografia.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia – Cifra de César

Por exemplo (cifra de César): uma criptografia que utiliza substituição de letras pelas letras deslocadas.



Iremos Atacar Amanhã às 10 Horas.

Texto Limpo

Luhprv Dwdfdu Dpdqkd dv 10 Krudv.

Texto Criptografado

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia

Atualmente, os algoritmos criptográficos são divulgados à comunidade e o sigilo das informações é garantido apenas pela chave. Quanto maior a chave, mais dificuldade para um ataque por força bruta.

A quebra da criptografia utilizando força bruta (todas as chaves possíveis) é inviável para chaves acima de 128 *bits*, por exemplo:

- Chaves de 64 *bits*: utilizando o computador gerando 90 bilhões de chaves por segundo (*Deep Crack*) temos o tempo de 4 dias e meio para encontrar uma chave.
- Chave de 128 *bits*: utilizando um computador bem melhor (gerando 1 trilhão de chaves por segundo) temos o o tempo de 10 milhões de trilhões de anos para testarmos todas as chaves.

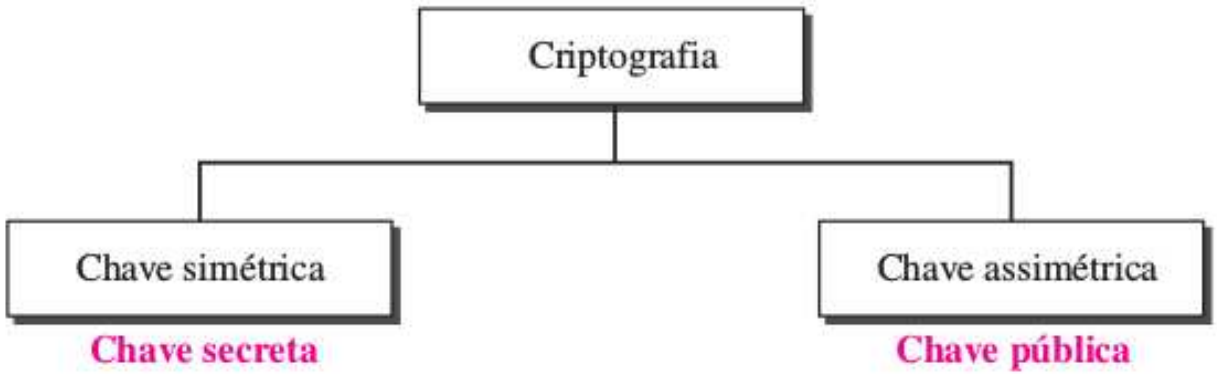
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia

Os algoritmos criptográficos são baseados essencialmente em técnicas de substituição, transposição simples e fórmulas matemáticas.

Existem dois principais tipos de algoritmos de cifragem:

- Criptografia com chave simétrica;
- Criptografia com chave pública.

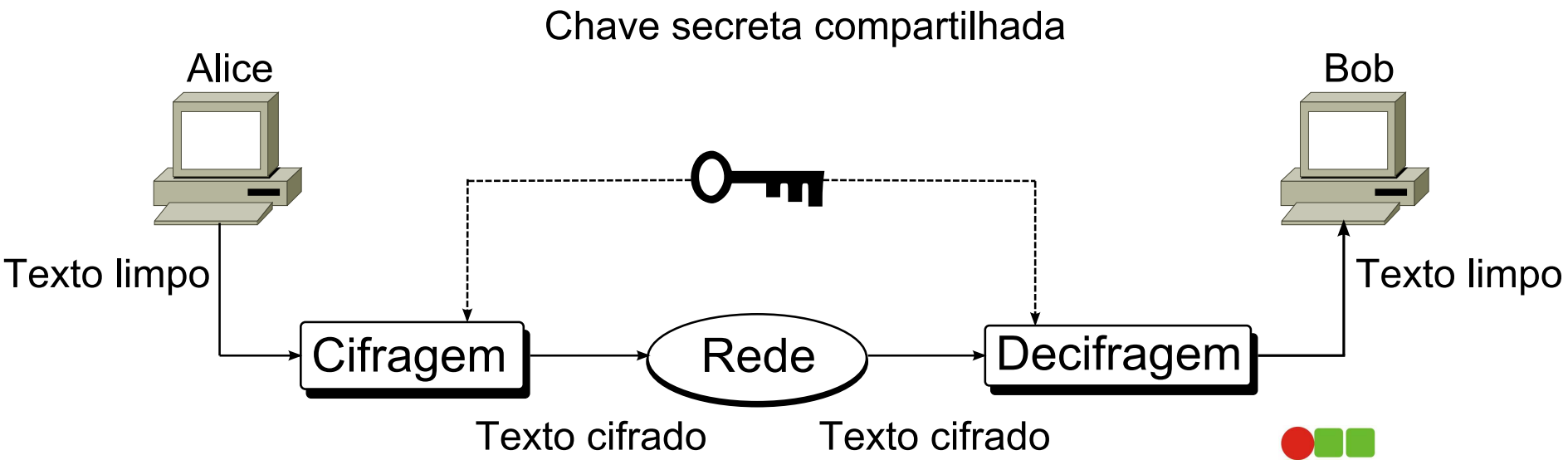


INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia

Criptografia com chave simétrica

O remetente usa uma determinada chave e um algoritmo de cifragem para criptografar a mensagem, enquanto que o destinatário usa a mesma chave e um algoritmo de decifragem recíproco para decifrar a mensagem;



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia Com Chave Simétrica

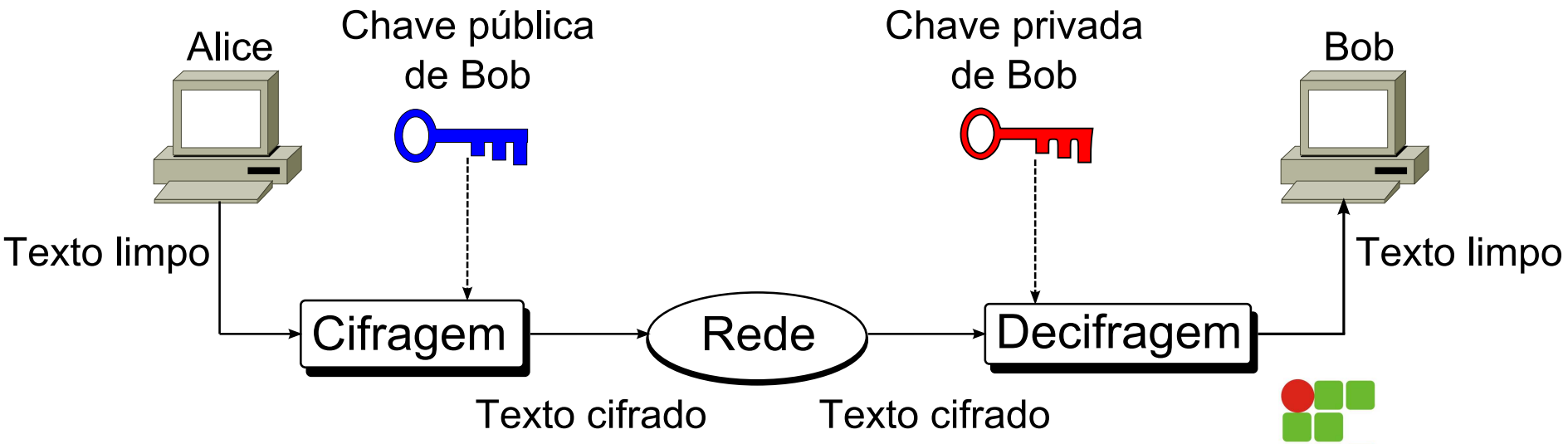
Os algoritmos criptográficos com chaves simétricas mais utilizadas são: DES (*Data Encryption Standard*), AES (*Advanced Encryption Standard*), 3-DES e RC4 (Rivest Cipher 4).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia Com Chave Pública

Criptografia com chave pública

Há duas chaves uma chave privada e uma chave pública. Se Alice desejar enviar uma mensagem secreta para Bob, ela deverá usar a chave pública de Bob para cifrar a mensagem. Quando a mensagem for recebida por Bob, a chave privada dele será usada para decifrar a mensagem.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

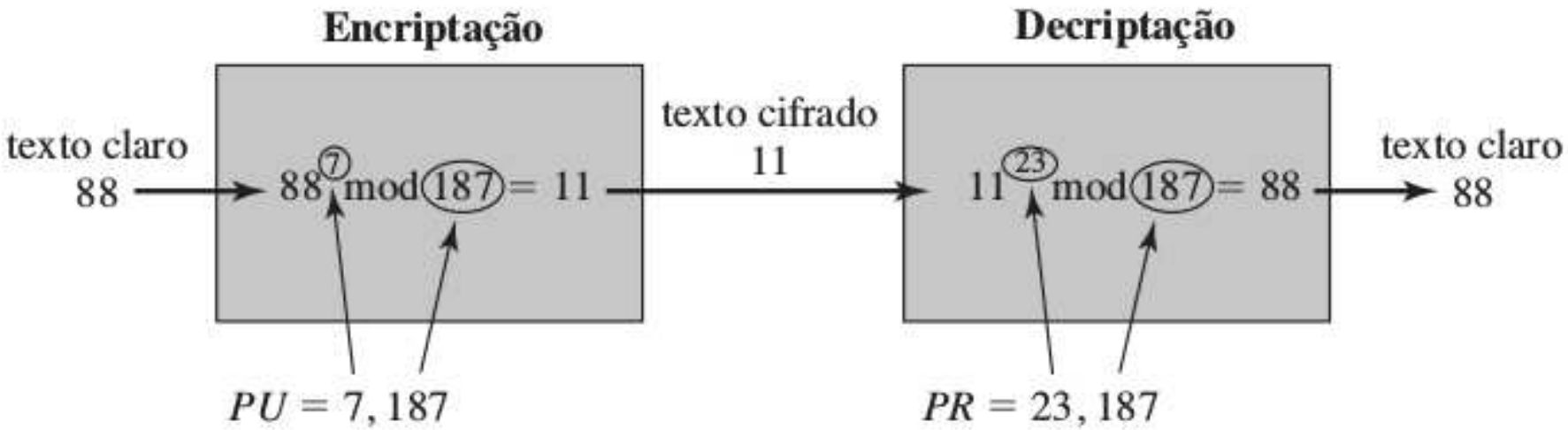
Criptografia Com Chave Pública

A chave privada é mantida em segredo pelo receptor. Enquanto que a chave pública é distribuída publicamente. Uma restrição, com relação a estas chaves, é que a chave privada não pode ser obtida a partir da chave pública.

O método mais utilizado na criptografia com chave pública é denominado RSA devido aos seus inventores (Rivest, Shamir e Adleman). Ele utiliza operações com números primos.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Criptografia Com Chave Pública – RSA



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Vídeos

https://www.youtube.com/watch?v=_Eeg1LxVWa8&t=389s

https://www.youtube.com/watch?v=gP4PqVGudtg

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Pergunta???

O que é antivírus?

Antivírus

- Os antivírus são programas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador.
- Há diversos tipos de antivírus que diferem entre si das seguintes formas:
  - Método de detecção: assinatura (uma lista de assinaturas e usada a procura de padrões) e comportamento (baseia-se no comportamento apresentado pelo código malicioso quando executado);
  - Forma de obtenção: podem ser gratuitos, experimentais (trial, usados livremente por um prazo predeterminado) e pagos (exigem que uma licenca seja adquirida).
  - Execução: podem ser localmente instalados no computador ou executados sob demanda por intermédio do navegador Web.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Antivírus

- Cuidados a serem tomados:
  - Tenha sempre um bom antivírus instalado em seu computador. O site `http://www.av-comparatives.org/` realiza comparações, através de testes, entre diversos antivírus;
  - Utilize antivírus *online* quando suspeitar que o seu antivírus esteja desabilitado/comprometido ou quando necessitar de uma segunda opinião sobre um arquivo. O site `https://www.virustotal.com/` disponibiliza um antivírus *on-line* gratuito para realizar verificações em arquivos e em páginas *Web*;
  - Configure o antivírus para verificar automaticamente arquivos obtidos pela Internet, os discos rígidos e as unidades removíveis (como pen-drives, CDs, DVDs e discos externos);
  - Mantenha o antivírus sempre atualizado;
  - Evite executar simultaneamente diferentes antivírus (eles podem entrar em conflito e afetar o desempenho do computador).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Pergunta???

O que é firewall?

Firewall

- Os antivírus não são capazes de impedir que um atacante tente explorar, via rede, alguma vulnerabilidade existente em seu computador e nem de evitar o acesso não autorizado. Para isso, utiliza-se os *firewalls*.
- Exitem dois tipos de *Firewall*:
  - *Firewall* Pessoal: é utilizado para proteger um computador contra acessos não autorizados vindos da Internet.
  - *Firewall* de Rede: é uma combinação de *hardware* (usualmente um roteador ou computador) e *software* que analisa o tráfego que entra/sai de uma rede, permitindo que alguns pacotes passem e bloqueando outros.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Firewall

- Quando bem configurado, um *firewall* pode ser capaz de:
  - Registrar as tentativas de acesso aos serviços habilitados no seu computador;
  - Bloquear as tentativas de invasão e de exploração de vulnerabilidades do seu computador e possibilitar a identificação das origens destas tentativas.
  - Evitar que um código malicioso já instalado seja capaz de se propagar, impedindo que vulnerabilidades em outros computadores sejam exploradas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Pergunta???

O que é autenticação?

Autenticação

- Mecanismos de autenticação são técnicas utilizadas para realizar a identificação única de um usuário em um computador ou serviço.
- Existem três grupos básicos de mecanismos de autenticação:
  - Aquilo que você é (informações biométricas, como a sua impressão digital, a palma da sua mão, a sua voz e o seu olho);
  - Aquilo que apenas você possui (como seu cartão de senhas bancárias e um *token* gerador de senhas);
  - Aquilo que apenas você sabe (como perguntas de segurança e suas senhas).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Contas e Senhas

Senha, ou *password*, serve para autenticar uma conta, ou seja, e usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. É um dos principais mecanismos de autenticação usados na Internet devido, principalmente, a sua simplicidade.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Contas e Senhas

- Algumas das formas como a sua senha pode ser descoberta são:
  - Ao ser usada em computadores infectados. Muitos códigos maliciosos, armazenam as teclas digitadas, espionam você pela *webcam* e gravam a posição da tela onde o *mouse* foi clicado.
  - Ao ser usada em sites falsos. Ao digitar a sua senha em um site falso, achando que está no site verdadeiro.
  - Por meio de tentativas de adivinhação;
  - Ao ser capturada enquanto trafega na rede, sem estar criptografada;
  - Por meio do acesso ao arquivo onde a senha foi armazenada caso ela não tenha sido gravada de forma criptografada;
  - Com o uso de técnicas de engenharia social, como forma a persuadi-lo a entregá-la voluntariamente;
  - Pela observação da movimentação dos seus dedos no teclado ou dos cliques do *mouse*.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Contas e Senhas

- Cuidados a serem tomados ao usar suas contas e senhas:
  - Certifique-se de não estar sendo observado ao digitar as suas senhas;
  - Não forneca as suas senhas para outra pessoa;
  - Certifique-se de fechar a sua sessão ao acessar sites que requeiram o uso de senhas.
  - Elabore boas senhas;
  - Altere as suas senhas sempre que julgar necessário;
  - Não use a mesma senha para todos os serviços que acessa;
  - Certifique-se de utilizar serviços criptografados quando o acesso a um site envolver o fornecimento de senha;
  - Seja cuidadoso ao usar a sua senha em computadores potencialmente infectados ou comprometidos;
  - Não usar a mesma senha para acessar diferentes contas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Contas e Senhas

- Uma senha boa, bem elaborada, e aquela que e difícil de ser descoberta e fácil de ser lembrada. Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la.
- Alguns elementos que você não deve usar na elaboração de suas senhas são:
  - Qualquer tipo de dado pessoal: evite nomes, sobrenomes, números de documentos, placas de carros, números de telefones e datas;
  - Sequências de teclado;
  - Palavras que façam parte de listas: evite palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes idiomas, etc.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Contas e Senhas

- Alguns elementos que você deve usar na elaboração de suas senhas são:
  - Números aleatórios;
  - Grande quantidade de caracteres: quanto mais longa for a senha mais difícil será descobri-la;
  - Diferentes tipos de caracteres: procure misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas;
  - Selecione caracteres de uma frase: baseie-se em uma frase e selecione a primeira, a segunda ou a última letra de cada palavra.
  - Faca substituições de caracteres: invente um padrão de substituição baseado, por exemplo, na semelhança visual (“w” e “vv”) ou de fonética (“ca” e “k”) entre os caracteres.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Contas e Senhas

- Não permita que o seu navegador memorize as suas senhas.

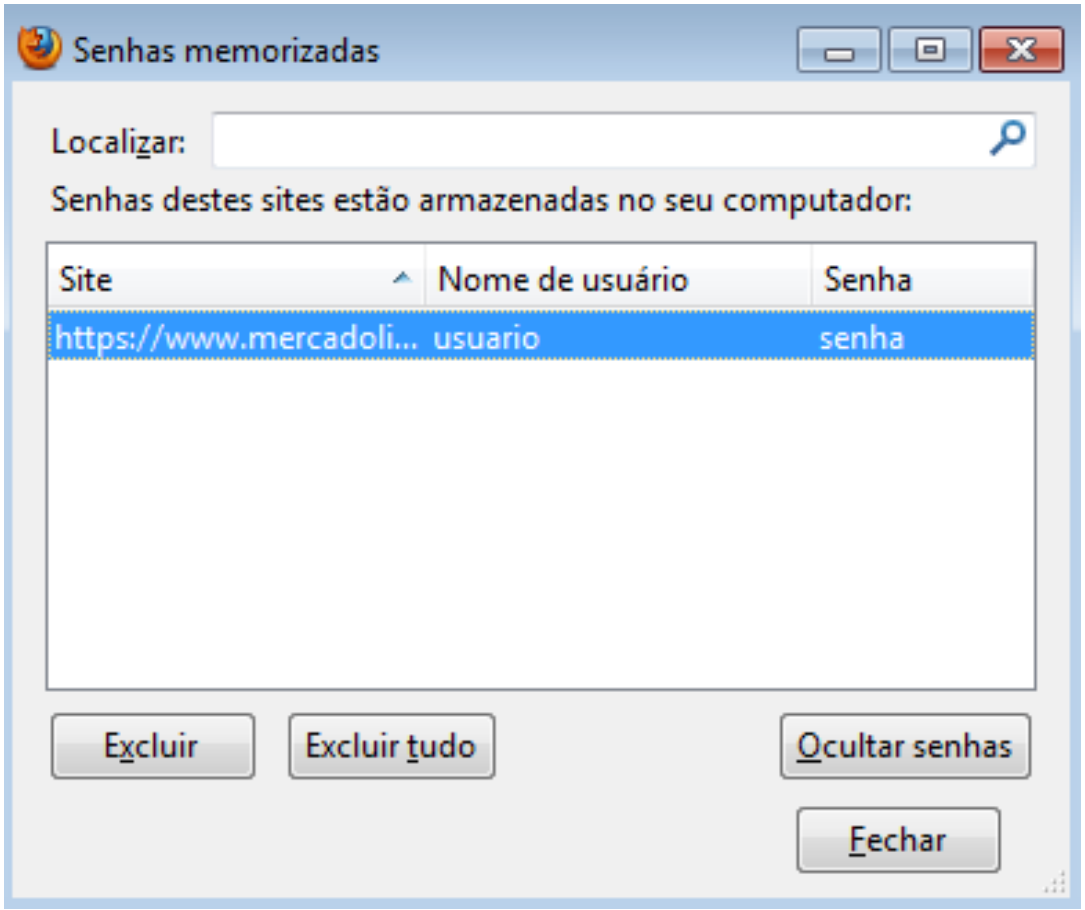


Figura: Senhas salvas no Firefox

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Contas e Senhas

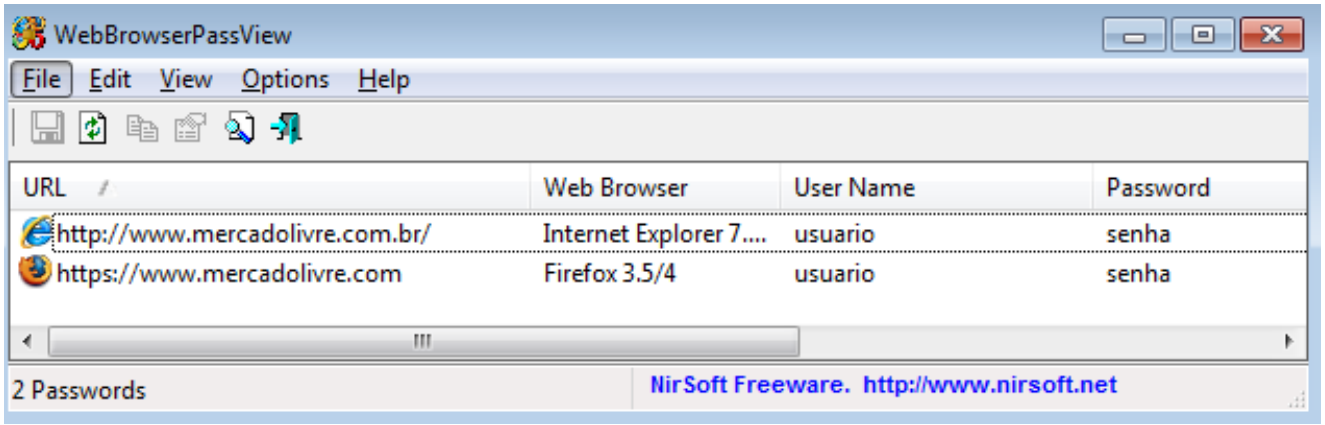


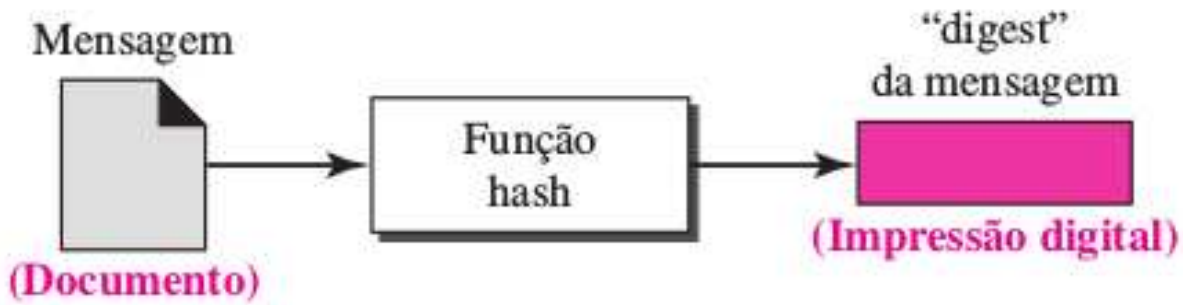
Figura: Senhas salvas no Internet Explorer

Figura: Senhas salvas no Google Chrome

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

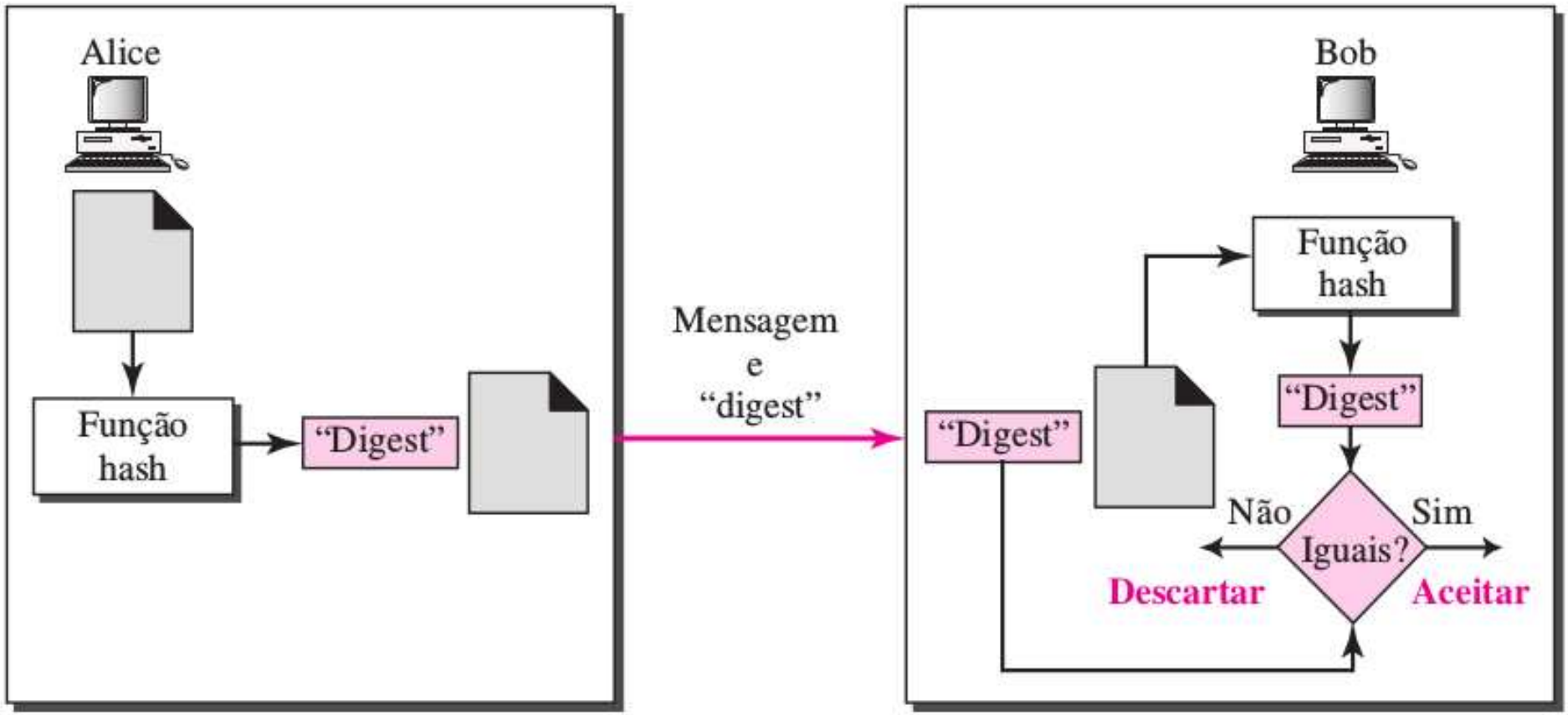
Função de resumo (*Hash*)

A função *hash* é uma função matemática que recebe uma mensagem de tamanho variável, e produz uma saída de tamanho fixo (chamada de resumo da mensagem, "*digest*" ou impressão digital). O objeto principal de uma função de *hash* é buscar garantir a **integridade** de um documento. Uma mudança em qualquer *bit* resulta, com alta probabilidade, em uma mudança no código de *hash*.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Funcionamento



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Função de resumo (*Hash*)

Para verificar a integridade de um arquivo, você pode calcular o *hash* dele e, quando julgar necessário, gerar novamente este valor. Se os dois *hashes* forem iguais então você pode concluir que o arquivo não foi alterado. Caso contrário, este pode ser um forte indício de que o arquivo esteja corrompido ou que foi modificado.

Uma função *hash* é semelhante à encriptação. Uma diferença é que o algoritmo de *hash* não precisa ser reversível, como para a decriptação.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Exemplos

O Secure Hash Algorithm (SHA) foi desenvolvido pelo NIST. Ele processa a entrada em blocos de 512 e produz uma saída de 160 bits.

Mensagem Original: "**Curso de Redes de Computadores no IFRN**"
SHA-1: aae724d3c22188f8e40bfa1041f0f194ef387609

Mensagem Alterada: "**Curso de Redes de Computadores no IFRN.**"
SHA-1: 3cc2582ec28503e7e37bcb3cbc45e08c7c5018b1

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Pergunta?

Mas como a função hash é enviada para o destinatário? Se um atacante puder alterar os dados, ele também pode alterar o resumo enviado!

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

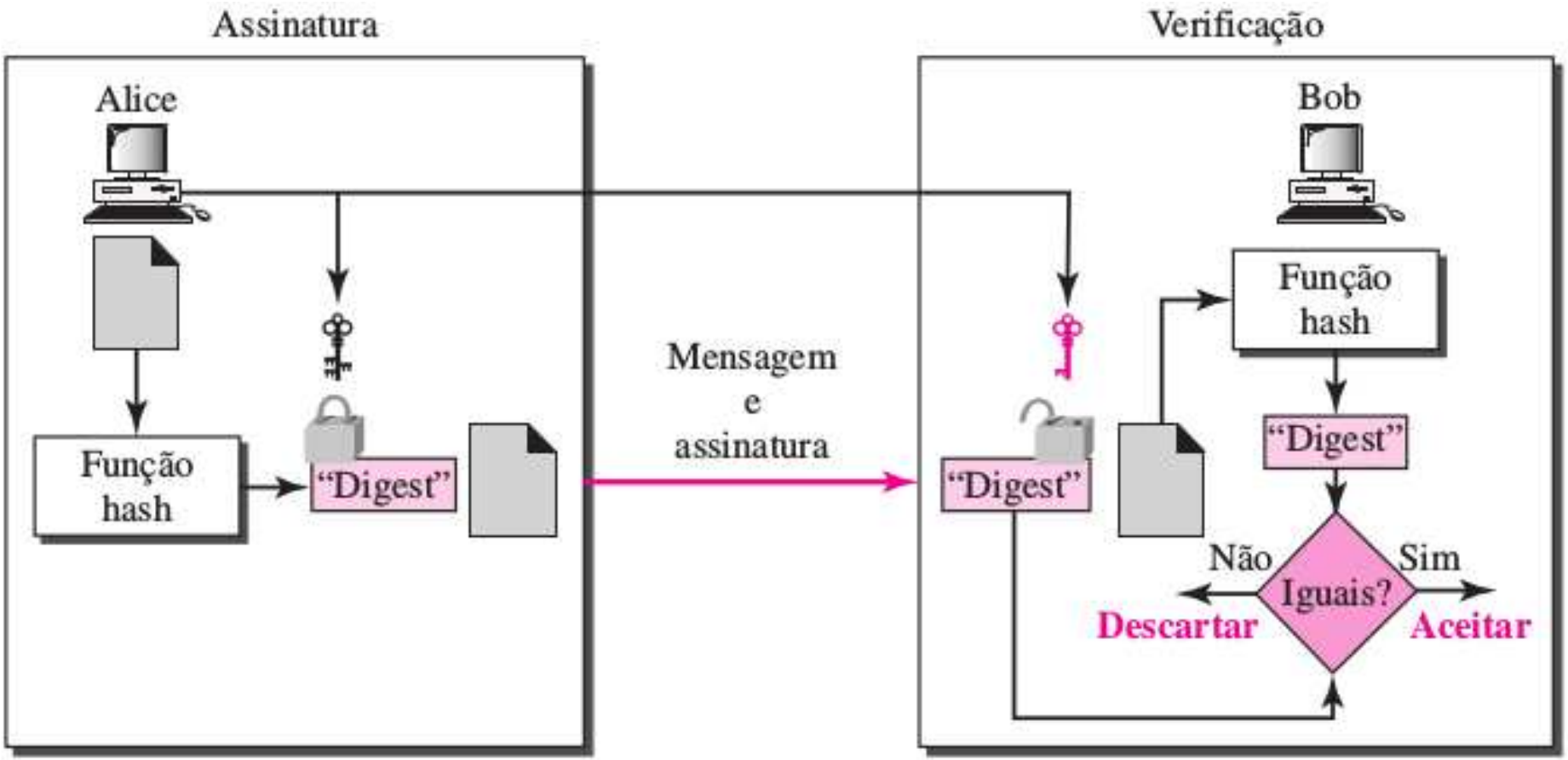
Assinatura Digital

A assinatura digital é uma técnica que utiliza criptografia para garantir as seguintes propriedades de mensagens e documentos eletrônicos:

- Autenticidade: o receptor deve poder confirmar que a assinatura foi feita pelo emissor;
- Integridade: qualquer alteração da mensagem faz com que a assinatura não corresponda mais ao documento;
- Irretratabilidade ou não-repúdio: o emissor não pode negar a autenticidade da mensagem.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Assinatura Digital



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Assinatura Digital

Bob pode assinar uma mensagem usando um algoritmo de geração de assinatura digital. As entradas do algoritmo são a mensagem e a chave privada de Bob. Qualquer outro usuário, digamos, Alice, pode verificar a assinatura usando um algoritmo de verificação, cujas entradas são a mensagem, a assinatura e a chave pública de Bob.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Pergunta?

Como confiar em uma chave pública? A chave pública de Alice é realmente de Alice?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Certificado Digital

Um certificado consiste em uma chave pública mais um identificador do proprietário da chave, com o bloco inteiro assinado por um terceiro confiável. Normalmente, o terceiro é uma autoridade certi- ficadora, como uma agência do governo ou uma instituição financeira, na qual a comunidade de usuários confia. Somente a autoridade certificadora pode criar e atualizar certificados.

O usuário pode, então, publicar o certificado. Qualquer um que precise da chave pública desse usuário pode obter o certificado e verificar se ele é válido por meio de uma assinatura confiável anexada.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

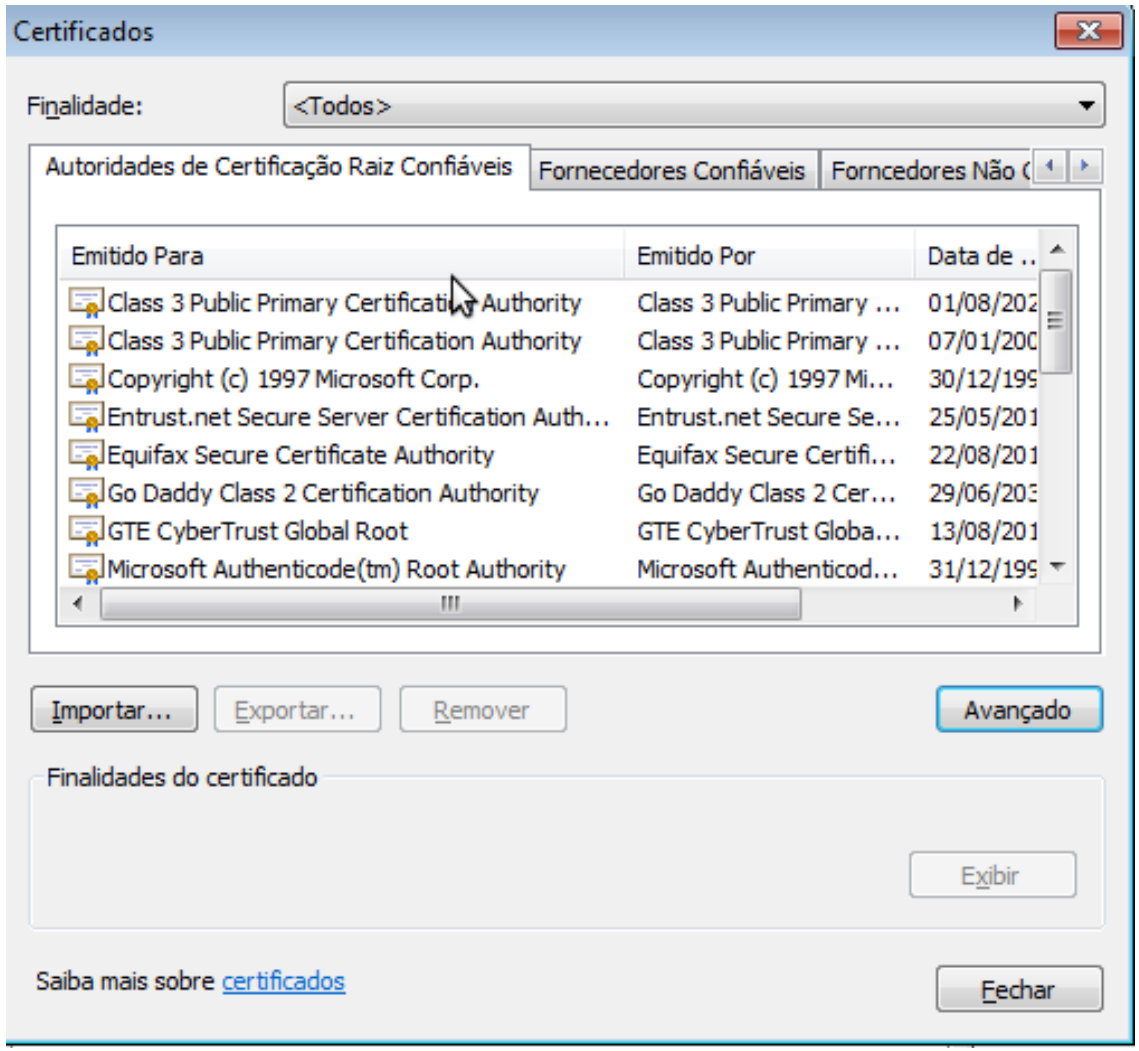
Entidade Certificadora

Para isso foi criado as AC (autoridade de certificação). Elas são organizações estaduais ou federal responsável por criar, distribuir e invalidar certificados digitais, análogas aos cartórios, que verificam assinaturas normais.

Um certificado digital é um documento de identificação digital. Assim como uma Carteira de Identidade, ele possui informações sobre seu proprietário, sua chave pública. Os certificados podem ser utilizada para validar transações online, procurações, autenticar informações empresariais no e-commerce e inúmeras outras aplicações.

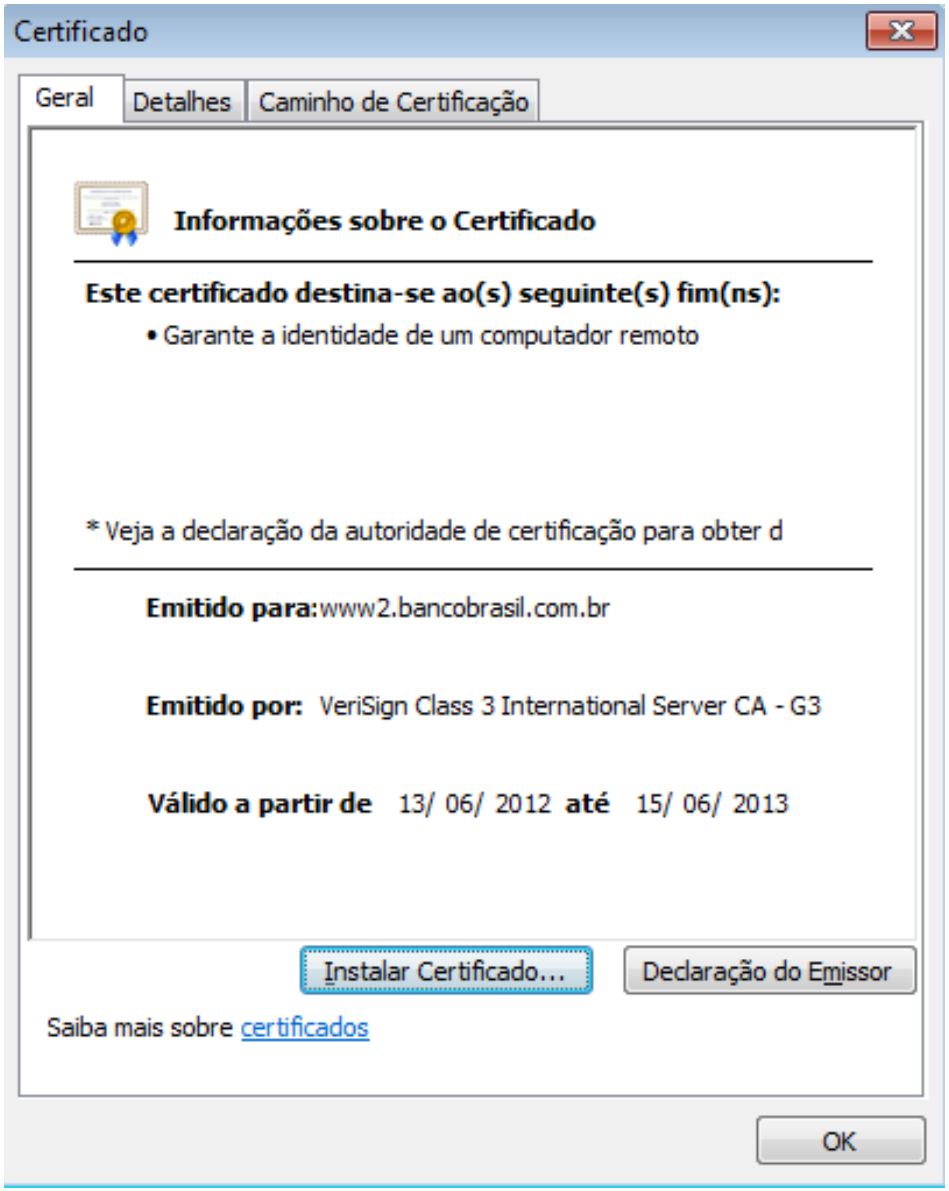
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Certificado Digital



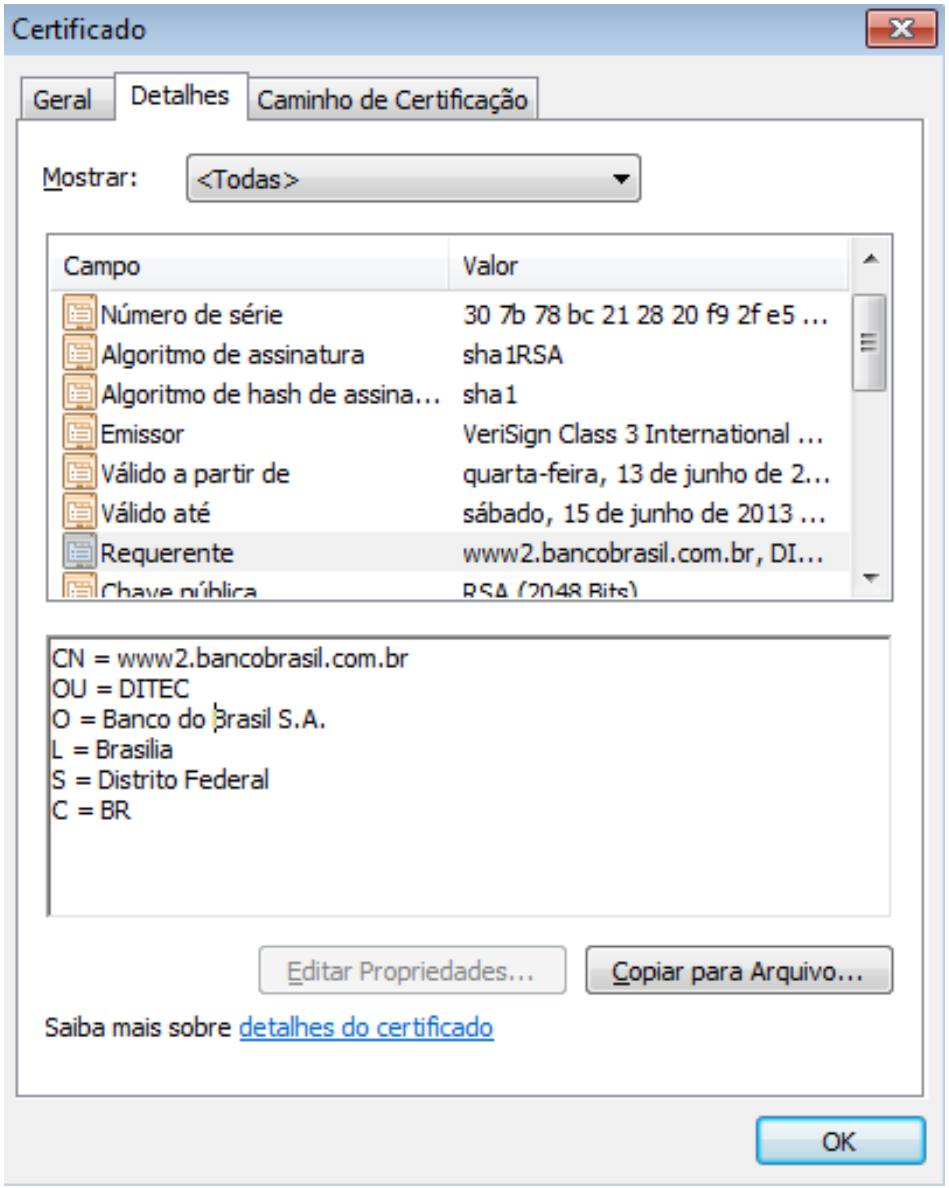
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Certificado Digital



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Certificado Digital



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança em Conexões *Web*

O protocolo HTTP, além de não oferecer criptografia, também não garante que os dados não possam ser interceptados, coletados, modificados ou retransmitidos e nem que você esteja se comunicando exatamente com o site desejado. Por estas características, ele não é indicado para transmissões que envolvem informações sigilosas, como senhas, números de cartão de crédito e dados bancários

Por outro lado, o HTTPS oferece conexões seguras. Ele utiliza certificados digitais para assegurar a identidade, tanto do site de destino como a sua própria, caso você possua um. Também utiliza métodos criptográficos e outros protocolos para assegurar a confidencialidade e a integridade das informações.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança em Conexões *Web* - Conexão Padrão

- Conexão Padrão:
  - O endereço do site começa com "http://";
  - Em alguns navegadores, o tipo de protocolo usado (HTTP) pode ser omitido na barra de endereços;
  - Um símbolo do site (logotipo) é apresentado próximo a barra de endereço e, ao passar o *mouse* sobre ele.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança em Conexões *Web* - Conexão Segura

- Conexão Segura:
  - O endereço do site começa com "https://";
  - O desenho de um "cadeado fechado" é mostrado na barra de endereço e, ao clicar sobre ele, detalhes sobre a conexão e sobre o certificado digital em uso são exibidos;
  - Um recorte colorido (branco ou azul) com o nome do domínio do site é mostrado ao lado da barra de endereço e, ao passar o *mouse* ou clicar sobre ele, são exibidos detalhes sobre conexão e certificado digital.