INFORMÁTICA

Segurança da Informação – Parte II

Livro Eletrônico

GRAN CURSOS ONLINE

SUMÁRIO

Apresentação

Olá, querido(a) amigo(a)!
Acredite nos seus sonhos! E lute com toda a garra e dedicação para conquistá-los!
Vamos então à aula sobre **Segurança da Informação (Parte II)**.
Que Deus o(a) abençoe e sucesso nos estudos!

SEGURANÇA DA INFORMAÇÃO – PARTE II

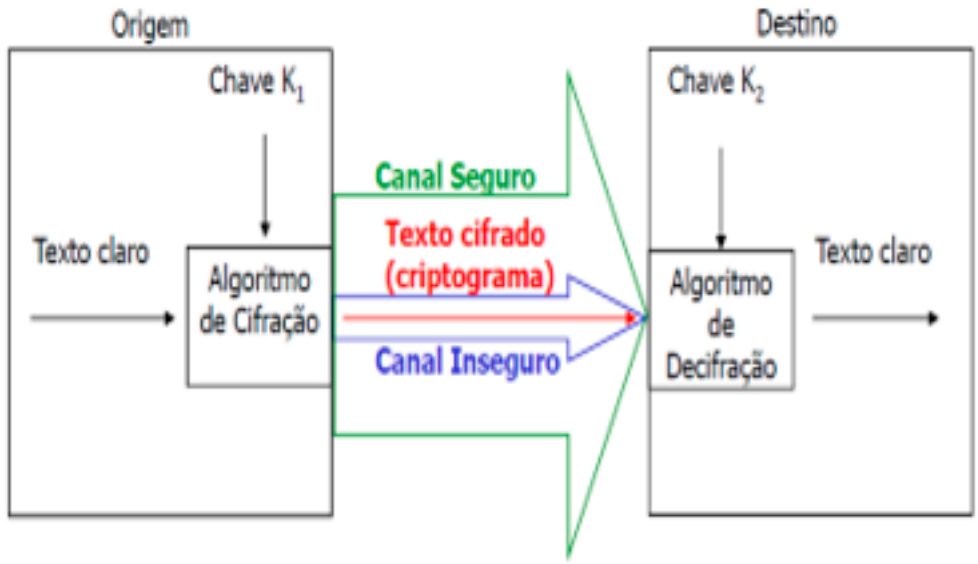
1. Noções sobre Criptografia

A palavra **criptografia** é composta dos termos gregos KRIPTOS (secreto, oculto, ininteligível) e GRAPHO (escrita, escrever). Trata-se de um conjunto de conceitos e técnicas que **visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la**.

Terminologia básica sobre Criptografia:

- **Mensagem ou texto:** informação que se deseja proteger. Esse texto quando em sua forma original, ou seja, a ser transmitido, é chamado de **texto puro** ou **texto claro**;
- **Remetente ou emissor:** pessoa ou serviço que envia a mensagem;
- **Destinatário ou receptor:** pessoa ou serviço que receberá a mensagem;
- **Encriptação:** processo em que um texto puro passa, transformando-se em **texto cifrado**.
- **Desencriptação:** processo de recuperação de um **texto puro** a partir de um **texto cifrado**.
- **Canal de comunicação:** é o meio utilizado para a troca de informações;
- **Criptografar:** ato de **encriptar** um **texto puro**, assim como, **descriptografar** é o ato de **desencriptar** um **texto cifrado**;
- **Chave:** informação que o remetente e o destinatário possuem e que será usada para criptografar e descriptografar um texto ou mensagem.

Elementos de um sistema criptográfico:



Obs.: **Criptografia** = arte e ciência de manter mensagens seguras.
Criptoanálise = arte e ciência de quebrar textos cifrados.
Criptologia = combinação da criptografia + criptoanálise.

2. Criptografia de Chave Simétrica

A **criptografia de Chave Simétrica** (também chamada de **Criptografia de Chave Única**, ou **Criptografia Privada**, ou **Criptografia Convencional** ou **Criptografia de Chave Secreta**) utiliza **APENAS UMA chave para encriptar e decriptar as mensagens**. Assim, como só utiliza UMA chave, obviamente ela deve ser compartilhada entre o remetente e o destinatário da mensagem.

Para ilustrar os sistemas simétricos, podemos usar a imagem de um cofre, que só pode ser fechado e aberto com uso de **UMA** chave. Esta pode ser, por exemplo, uma combinação de números. A mesma combinação abre e fecha o cofre.

Para criptografar uma mensagem, usamos a chave (fechamos o cofre) e para decifrá-la utilizamos a mesma chave (abrimos o cofre).

Obs.: na **criptografia simétrica** (ou de **chave única**) tanto o emissor quanto o receptor da mensagem devem conhecer a chave utilizada. Ambos fazem uso da MESMA chave, isto é, uma ÚNICA chave é usada na codificação e na decodificação da informação.

A figura seguinte ilustra o processo de criptografia baseada em uma única chave, ou seja, a chave que cifra uma mensagem é utilizada para posteriormente decifrá-la.

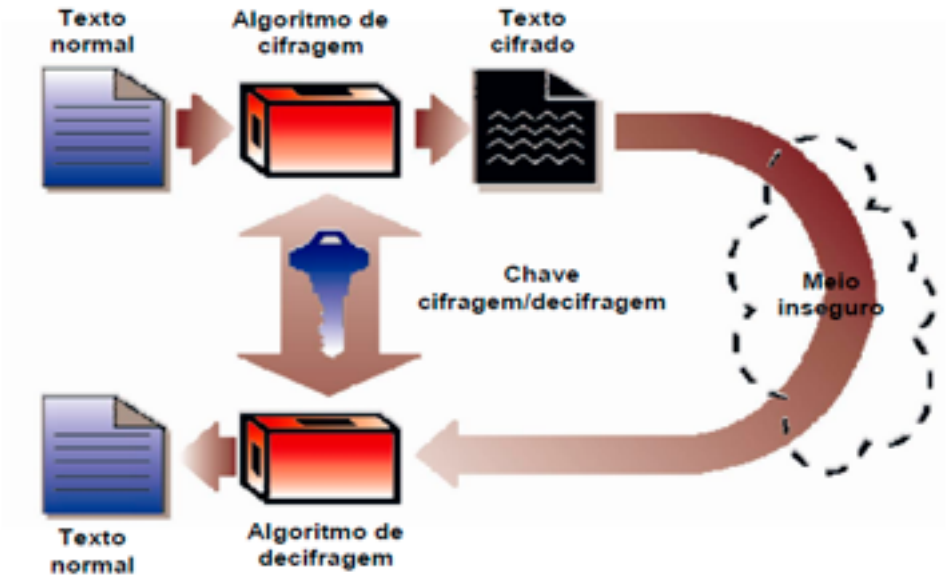
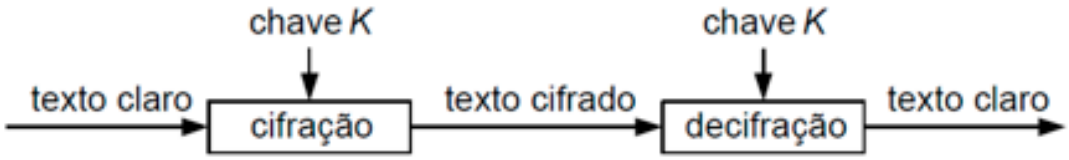


Ilustração de um processo de criptografia por chave secreta.
Fonte: GARFINKEL, Simson; SPAFFORD, Gene (1999, p. 197)

Sistema de Criptografia Simétrica



A chave de cifração é igual à chave de decifração.
ou
A chave de cifração pode ser facilmente gerada a partir da chave de decifração e vice-versa.

Sejam:
- **Ek( ) a função cifração com a chave k;**
- **Dk( ) a função de decifração com a chave k;**
- **M o texto em claro e C o texto cifrado.**

As principais **vantagens** dos algoritmos simétricos são:

- **Rapidez**: um polinômio simétrico encripta um texto longo em milésimos de segundos;
- **Chaves pequenas**: uma chave de criptografia de 128 bits torna um algoritmo simétrico praticamente impossível de ser quebrado.

A maior **desvantagem** da criptografia simétrica é que **a chave utilizada para encriptar é IGUAL à chave que decripta**. Quando um grande número de pessoas tem conhecimento da chave, a informação deixa de ser um segredo.

O uso de chaves simétricas também faz com que sua utilização **não** seja **adequada em situações em que a informação é muito valiosa**. Para começar, é necessário usar uma grande quantidade de chaves caso muitas pessoas estejam envolvidas. Ainda, há o fato de que tanto o emissor quanto o receptor precisam conhecer a chave usada. A transmissão dessa chave de um para o outro pode não ser tão segura e cair em "mãos erradas", fazendo com que a chave possa ser interceptada e/ou alterada em trânsito por um inimigo.

Existem vários **algoritmos** que usam **chaves simétricas**, como: o **DES** (Data Encryption Standard), o **IDEA** (International Data Encryption Algorithm), e o **RC** (Ron's Code ou Rivest Cipher):

- **DES (Data Encryption Standard)**: criado pela IBM em 1977, faz uso de chaves de 56 bits. Isso corresponde a 72 quadrilhões de combinações (2^{56} = 72.057.594.037.927.936). É um valor absurdamente alto, mas não para um computador potente. Em 1997, ele foi quebrado por técnicas de "força bruta" (tentativa e erro) em um desafio promovido na internet. No DES o processo de criptografia envolve, sobre os dados originais, a primeira etapa de **permutação**;

- **IDEA (International Data Encryption Algorithm)**: criado em 1991 por James Massey e Xuejia Lai, o IDEA é um algoritmo que faz uso de chaves de 128 bits e que tem uma estrutura semelhante ao DES;
- **RC (Ron's Code ou Rivest Cipher)**: criado por Ron Rivest na empresa RSA Data Security, esse algoritmo é muito utilizado em e-mails e faz uso de chaves que vão de 8 a 1024 bits. Possui várias versões: RC2, RC4, RC5 e RC6. Essencialmente, cada versão difere da outra por trabalhar com chaves maiores.

Há ainda outros algoritmos conhecidos, como o **AES** (*Advanced Encryption Standard*) - que é baseado no DES, o **3DES**, o **Twofish** e sua **variante Blowfish**, por exemplo.

3. Criptografia de Chave Assimétrica

Os algoritmos de **criptografia assimétrica (também chamada de criptografia de chave pública)** utilizam **DUAS chaves DIFERENTES**, uma **PÚBLICA** (que pode ser distribuída) **e uma PRIVADA** (pessoal e intransferível). Assim, nesse método cada pessoa ou entidade mantém duas chaves: uma pública, que pode ser divulgada livremente, e outra privada, que deve ser mantida em segredo pelo seu dono.

As mensagens codificadas com a chave pública só podem ser decodificadas com a chave privada correspondente.

Do ponto de vista do custo computacional, **os sistemas simétricos apresentam melhor desempenho que os sistemas assimétricos**, e isso já foi cobrado em provas várias vezes!

Obs.: também conhecida como "**Criptografia de Chave Pública**", a técnica de **criptografia por Chave Assimétrica** trabalha com **DUAS chaves**: **uma denominada privada e outra denominada pública**. Nesse método, uma pessoa deve criar uma chave de codificação e enviá-la a quem for mandar informações a ela. Essa é a chave pública. Outra chave deve ser criada para a decodificação. Esta – a chave privada – é secreta.

A figura seguinte ilustra o princípio da criptografia utilizando chave assimétrica.

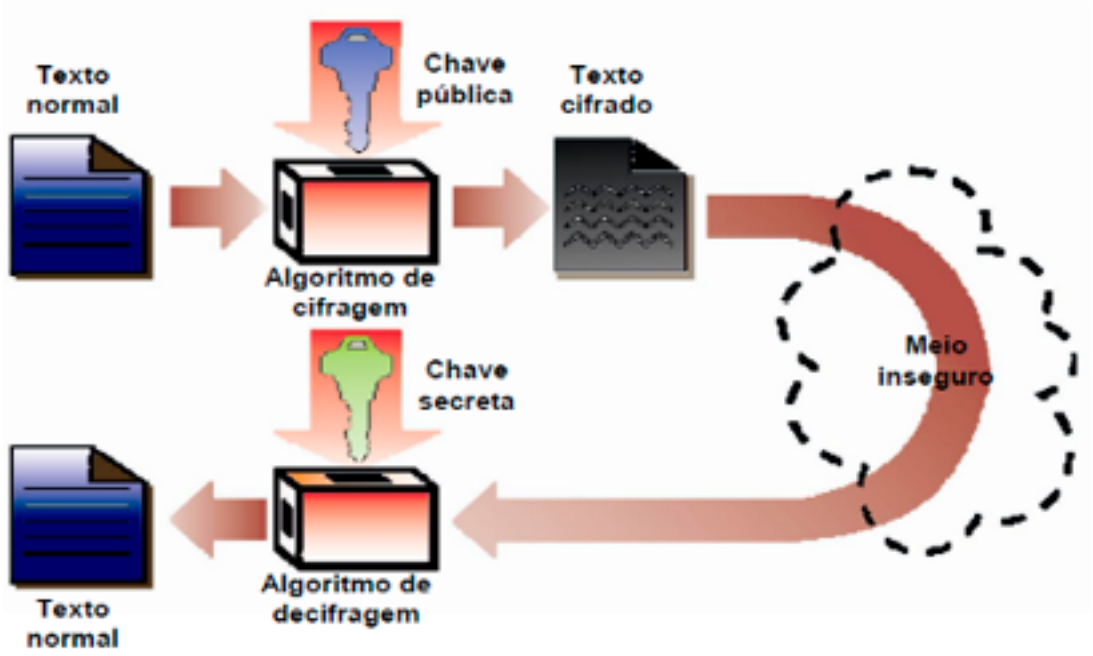


Ilustração de um processo de criptografia por chave pública
Fonte: GARFINKEL, Simson; SPAFFORD, Gene (2001, p.208).

Para entender melhor, imagine o seguinte: o USUÁRIO-A criou uma chave pública e a enviou a vários outros sites. Quando qualquer desses sites quiser enviar uma informação criptografada ao USUÁRIO-A deverá utilizar a chave pública deste. Quando o USUÁRIO-A receber a informação, apenas será possível extraí-la com o uso da chave privada, que só o USUÁRIO-A tem. Caso o USUÁRIO-A queira enviar uma informação criptografada a outro site, deverá conhecer sua chave pública.

Entre os **algoritmos** que usam chaves assimétricas têm-se o **RSA** (o mais conhecido), o **DSA** (Digital Signature Algorithm), o Schnorr (praticamente usado apenas em assinaturas digitais) e **DiffieHellman**.

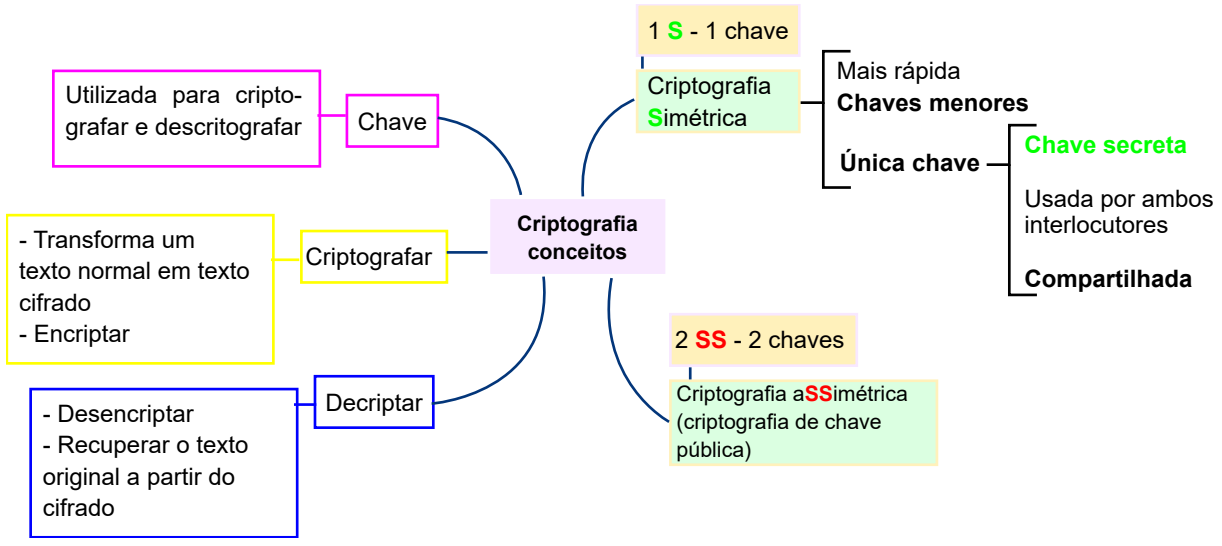


*Figura. Mapa Mental Relacionado à Criptografia A**SS**imétrica. Fonte: QUINTÃO (2020)*

4. Hashes Criptográficos

Hash é uma **função matemática** que recebe uma mensagem de entrada e gera como resultado um número finito de caracteres (“dígitos verificadores”).

É uma função **unidirecional**. A figura seguinte ilustra alguns exemplos de uso da função *hash*:

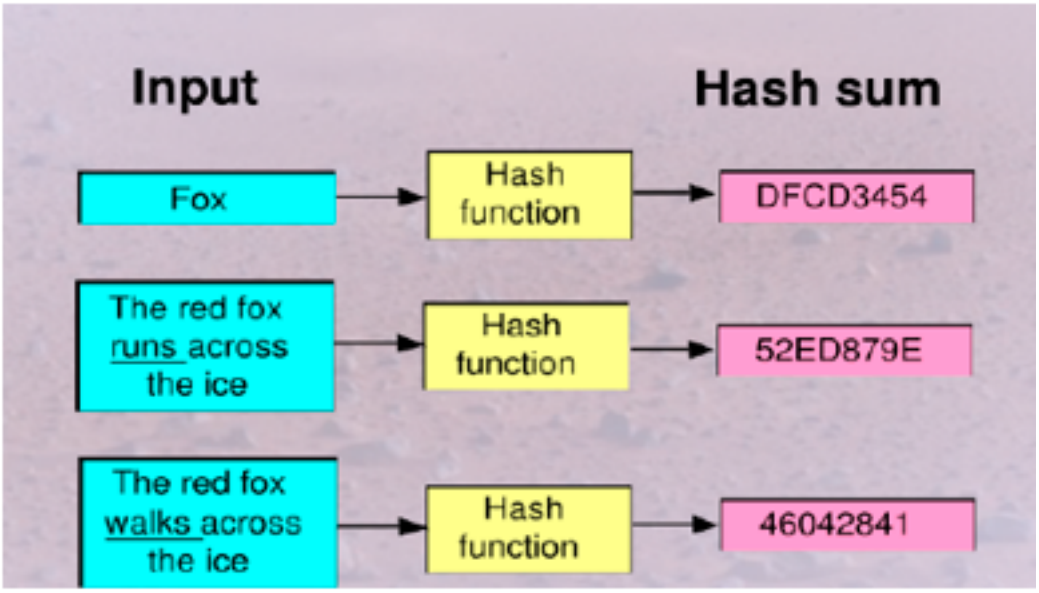


Figura. Exemplos de Saídas da Função

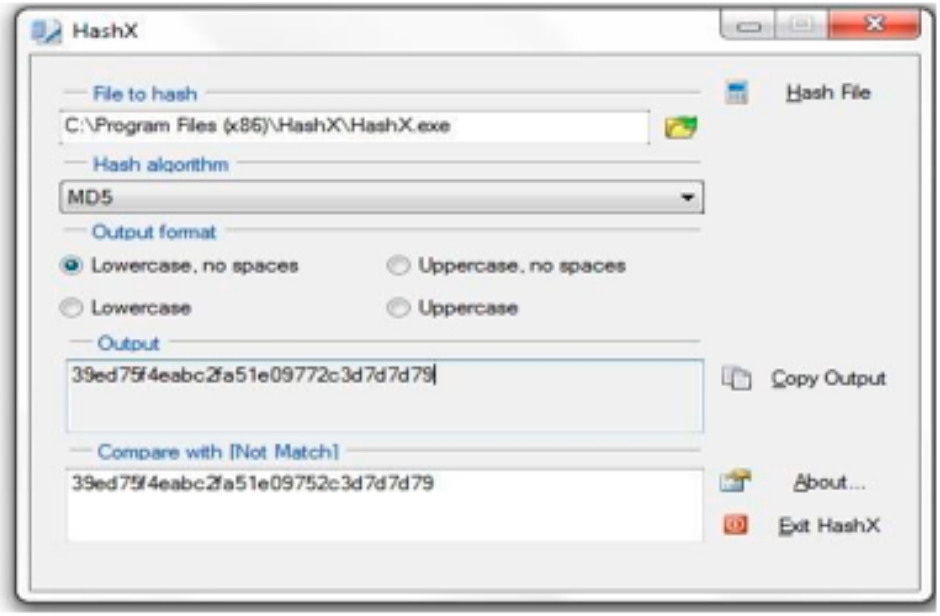
Não é possível reconstituir a mensagem a partir do *hash*.

Pode ser feita em um sentido e não no outro – como a relação entre as chaves em um sistema de criptografia assimétrica.

Alguns algoritmos de *hash*: **MD4, MD5, SHA-1**, SHA-256, TIGER etc.

Obs.: CERT.BR (2013) destaca que “uma **função de resumo** (**hash**) é um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho que ela tenha, gera um resultado único e de tamanho **fixo**, chamado **hash”**.

Usamos o ***hash*** (**resumo da mensagem** ou ***message digest*** em inglês) quando precisamos garantir a **integridade** de determinada informação; realizar armazenamento seguro de senhas; garantir a integridade de arquivos etc.



CERT.BR (2013) destaca o uso do *hash* para vários **propósitos**, como por exemplo:

- gerar assinaturas digitais;
- **verificar a integridade** de um arquivo armazenado no computador ou em backups;
- **verificar a integridade de um arquivo obtido da Internet** (nesse caso, alguns sites, além do arquivo em si, disponibilizam o hash correspondente, para que o usuário verifique se o arquivo foi corretamente transmitido e gravado). Você pode utilizar uma ferramenta como a listada na tela seguinte para calcular o hash do arquivo e, quando julgar necessário, gerar novamente este valor. Se os dois hashes forem iguais podemos concluir que o arquivo não foi alterado. Caso contrário, temos aí um forte indício de que o arquivo esteja corrompido ou que foi modificado durante a transmissão;

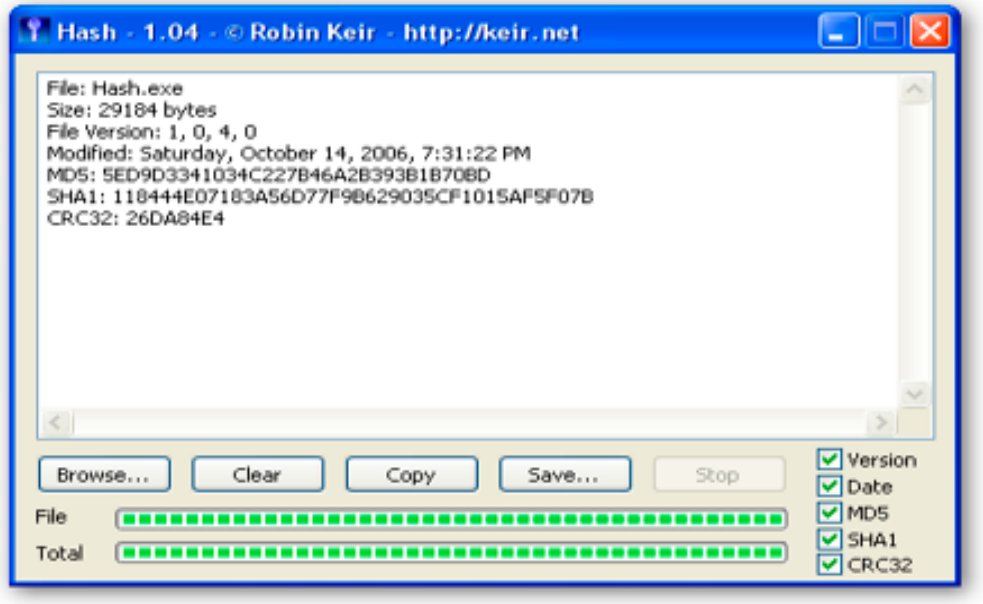


Figura. Geração do hash do arquivo "hash.exe"

Obs.: ***HASH (Message Digest – Resumo de Mensagem):*** **Método matemático "UNIDIRECIONAL"**, ou seja, só pode ser executado em um único sentido (ex.: você envia uma mensagem com o hash, e este não poderá ser alterado, mas apenas conferido pelo destinatário). Utilizado para garantir a "integridade" (não alteração) de dados durante uma transferência.

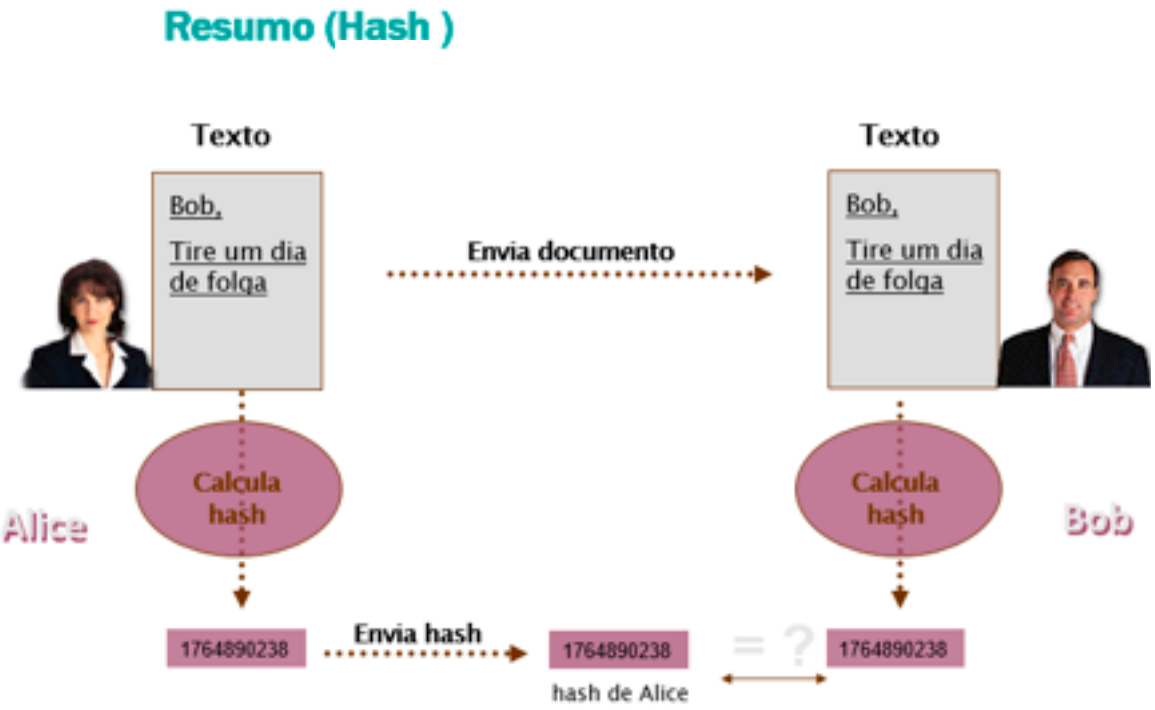


Figura. Resumo (Hash).

5. Assinatura Digital

O glossário criado pela ICP Brasil destaca que a **Assinatura Digital é um código anexado ou logicamente associado a uma mensagem eletrônica** que **permite de forma única e exclusiva a comprovação da autoria de um determinado conjunto de dados** (um arquivo, um *e-mail* ou uma transação).

A assinatura digital comprova que a pessoa criou ou concorda com um documento assinado digitalmente, como a assinatura de próprio punho comprova a autoria de um documento escrito.

Stallings (2008) destaca que a **assinatura digital** é um mecanismo de **AUTENTICAÇÃO** que permite ao criador de uma mensagem anexar um código que atue como uma assinatura.

Obs.: em outras palavras**, a assinatura digital consiste na criação de um código, através da utilização de uma chave privada**, **de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada.**

Obs.: **a verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo** (CERT.BR,2013).

CERT.BR (2013) destaca que "para contornar a baixa eficiência característica da criptografia de chaves assimétricas, **a codificação é feita sobre o *hash*** e não sobre o conteúdo em si, pois é mais rápido codificar o *hash* (que possui tamanho fixo e reduzido) do que a informação toda".

A assinatura é formada tomando o *hash (Message Digest – Resumo de Mensagem)* da mensagem e criptografando-o com a chave privada do criador.

Assim, a assinatura digital fornece uma prova inegável de que uma mensagem veio do emissor.

Para verificar esse requisito, uma assinatura deve ter as seguintes **propriedades:**

- **Autenticidade**: o receptor (destinatário de uma mensagem) pode confirmar que a assinatura foi feita pelo emissor;
- **Integridade**: qualquer alteração da mensagem faz com que a assinatura seja invalidada;
- **Não repúdio** (irretratabilidade): o emissor (aquele que assinou digitalmente a mensagem) não pode negar que foi o autor da mensagem, ou seja, não pode dizer mais tarde que a sua assinatura foi falsificada.

É importante ressaltar que a segurança do método se baseia no fato de que **a chave privada é conhecida apenas pelo seu dono**. Também é importante ressaltar que o fato de **assinar uma mensagem não significa gerar uma mensagem sigilosa**. Para o exemplo anterior, se José quisesse assinar a mensagem e ter certeza de que apenas Maria teria acesso a seu conteúdo, seria preciso codificá-la com a chave pública de Maria, depois de assiná-la.

6. Entendendo os Componentes da Infraestrutura de Chaves Públicas (ICP)

Obs.: **PKI (Public Key Infrastrusture) é a infraestrutura de chaves públicas (ICP). A ICP-Brasil é um exemplo de PKI.**

A **ICP (Infraestrutura de Chaves Públicas ou PKI) é um conjunto formado por arquitetura, organização, técnicas, práticas e procedimentos** que servem de base para a implantação e operação do sistema criptográfico de chave pública usada em certificados.

Autoridade Certificadora (AC)

Vamos ao exemplo da carteira de motorista. Se pensarmos em um certificado como uma carteira de motorista, a Autoridade Certificadora opera como um tipo de órgão de licenciamento. **Em uma ICP, a AC emite, gerencia e revoga os certificados para uma comunidade de usuários finais**. A **AC** assume a tarefa de autenticação de seus usuários finais e então assina digitalmente as informações sobre o certificado antes de disseminá-lo. A **AC**, no final, é responsável pela autenticidade dos certificados emitidos por ela.

Autoridade de Registro (AR)

Embora a **AR** possa ser considerada um componente estendido de uma ICP, os administradores estão descobrindo que isso é uma necessidade. À medida que aumenta o número de usuários finais dentro de uma ICP, também aumenta a carga de trabalho de uma **AC**.

A **AR** serve como uma **entidade intermediária** entre a **AC** e seus usuários finais, ajudando a **AC** em suas funções rotineiras para o processamento de certificados.

Uma **AR** é necessariamente uma entidade operacionalmente vinculada a uma **AC**, a quem compete:

- identificar os titulares de certificados: indivíduos, organizações ou equipamentos;
- encaminhar solicitações de emissão e revogação de certificados à **AC**;
- guardar os documentos apresentados para identificação dos titulares.

A **AC** deve manter uma lista de suas **ARs** credenciadas e estas **ARs** são consideradas confiáveis, pelo ponto de vista dessa **AC**.

Obs.: **a AC emite, gerencia e revoga os certificados para uma comunidade de usuários finais. A AR serve como uma entidade intermediária entre a AC e seus usuários finais, ajudando a AC em suas funções rotineiras para o processamento de certificados.**

Uma Infraestrutura de Chaves Públicas (ICP) envolve um processo colaborativo entre várias entidades: autoridade certificadora (AC), autoridade de registro (AR), repositório de certificados e o usuário final.

Obs.: **AC Raiz no Brasil é o ITI (Instituto Nacional de Tecnologia da Informação)**

É a primeira autoridade da **cadeia de certificação**.

Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.

Emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu.

Encarregada de emitir a lista de certificados revogados e de fiscalizar e auditar as autoridades certificadoras, autoridades de registro e demais prestadores de serviço habilitados na ICP-Brasil.

Somente a AC Raiz pode realizar certificação cruzada com AC raízes noutros países.

7. Certificado Digital

Um certificado digital é um documento eletrônico que identifica pessoas, físicas ou jurídicas, URLs, contas de usuário, servidores (computadores), dentre outras entidades. Este "documento" na verdade é uma estrutura de dados que contém a chave pública do seu titular e outras informações de interesse.

Ele contém informações relevantes para a identificação "real" da entidade a que visa certificar (CPF, CNPJ, endereço, nome, etc.) e informações relevantes para a aplicação a que se destina.

O certificado fica armazenado em **dispositivos (mídias) de segurança**, como por ex.: *Token* ou *Smart Card (cartão inteligente)*, ilustrados a seguir.

Token

Token

Smart Card ou cartão inteligente

Figura. Ilustração de dispositivos de segurança

Quanto aos **objetivos do certificado digital** podemos destacar:

- Transferir a credibilidade que hoje é baseada em papel e conhecimento para o ambiente eletrônico;
- **Vincular uma chave pública a um titular** (eis o objetivo principal).

O certificado digital precisa ser emitido por uma autoridade reconhecida pelas partes interessadas na transação, conforme visto na próxima figura. Chamamos essa autoridade de **Autoridade Certificadora, ou AC.**

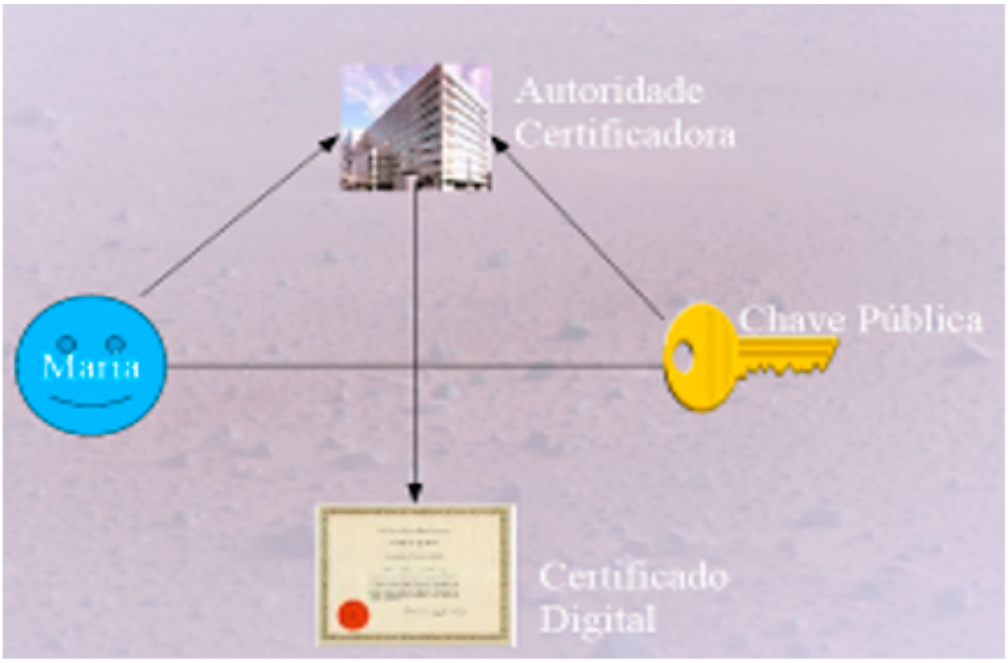
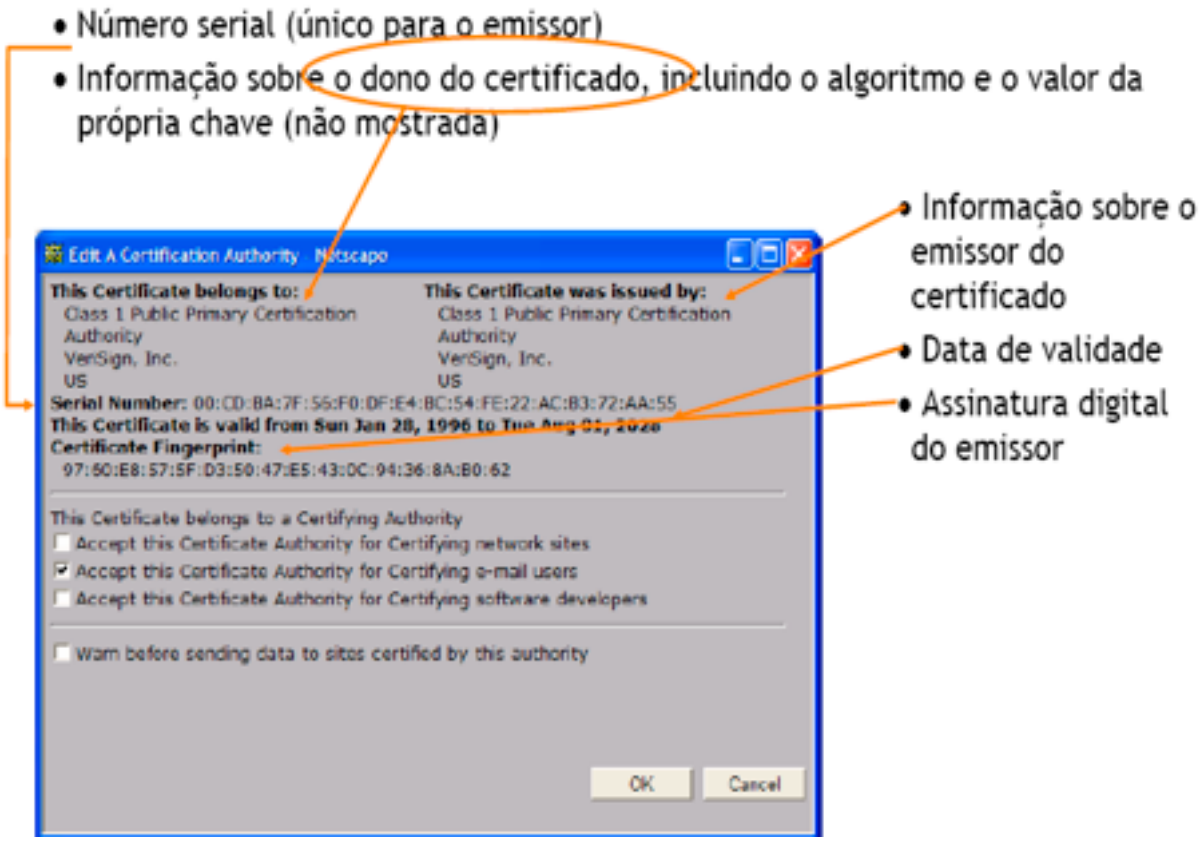


Figura. Vínculo da Chave Pública ao Titular

Dentre as informações (atributos) que compõem a estrutura de um certificado temos:

Versão	Indica qual formato de certificado está sendo seguido.
Número de série	Identifica unicamente um certificado dentro do escopo do seu emissor.
Nome do titular	Nome da pessoa, URL ou demais informações que estão sendo certificadas.
Chave pública do titular	Informações da chave pública do titular.
Período de validade	Data de emissão e expiração.
Nome do emissor	Entidade que emitiu o certificado.
Assinatura do emissor	Valor da assinatura digital feita pelo emissor.
Algoritmo de assinatura do emissor	Identificador dos algoritmos de **hash** + assinatura utilizados pelo emissor para assinar o certificado.
Extensões	Campo opcional para estender o certificado.

Um exemplo destacando informações do certificado pode ser visto na figura seguinte:



8. Emissão de um Certificado Digital

Existem diversos processos de emissão de um certificado digital, os quais são baseados no contexto de aplicação e nas suas exigências. Um certificado digital de e-mail seguro, por exemplo, possui um processo de emissão mais simples e flexível do que um certificado e-CPF (ICP-Brasil).

A ICP-Brasil definiu os **tipos de certificados válidos**. Foram definidos diversos tipos diferentes, divididos entre:

- **Certificados de assinatura** (só assina): **A1, A2, A3, A4, T3 e T4;**
- **Certificados de sigilo** (assina e criptografa): **S1, S2, S3 e S4.**

A **série A (A1, A2, A3 e A4)** reúne os certificados de assinatura digital, utilizados na confirmação de identidade na Web, em *e-mail*, em redes privadas virtuais (VPN) e em documentos eletrônicos com verificação da integridade de suas informações.

Também certificados de assinatura digital, certificados do tipo **T3 e T4 somente** podem ser emitidos para equipamentos das Autoridades de Carimbo do Tempo (ACTs) credenciadas na ICP-Brasil.

A **série S** (**S1, S2, S3 e S4**) reúne os certificados de sigilo, utilizados na codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas.

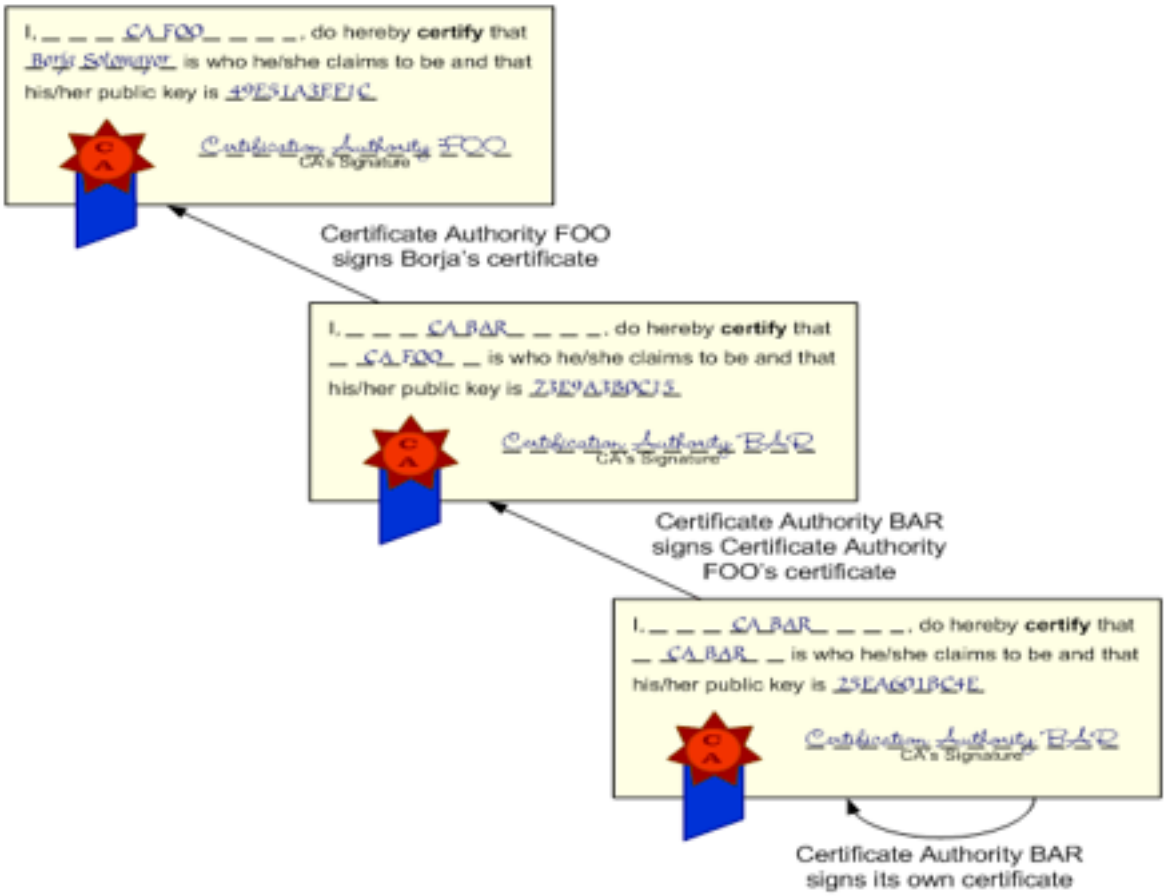
Os dez tipos são diferenciados pelo uso, pelo nível de segurança e pela validade.

Tipo de Certificado	Validade Máxima (anos)
A1 e S1	1
A2 e S2	2
A3, S3, T3	5
A4, S4, T4	6

Obs.: | **quanto maior o número do certificado, maior o nível de segurança de seu par de chaves.**

Com exceção de certificados autoassinados, todo certificado digital está abaixo de uma **cadeia de certificação.**

Uma cadeia de certificação é composta pelo certificado de entidade final e por todos os certificados de AC na hierarquia de emissão.



Como garantir a validade de um certificado digital?

Validar um certificado digital é uma das tarefas mais importantes da PKI. A autenticidade de uma assinatura digital pressupõe a validade do certificado digital associado à chave pública.

Um certificado digital está válido se:

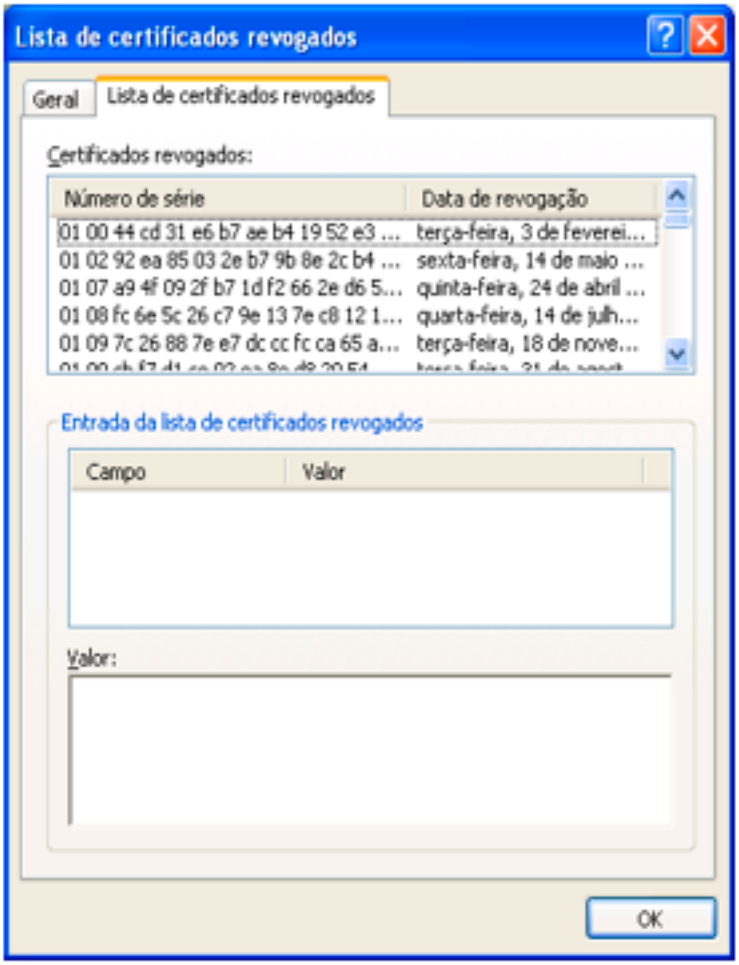
- ele está dentro do seu período de validade;
- data emissão do certificado <= data validação <= data expiração;

Emitido para: BRUNO DE PAULA RIBEIRO

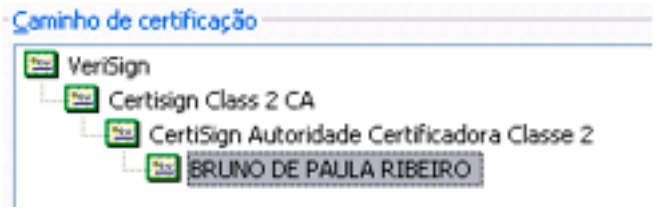
Emitido por: CertiSign Autoridade Certificadora Classe 2

Válido a partir de 23/1/2008 **até** 23/1/2009

- ele não foi revogado pela AC que o emitiu.



- ele está debaixo de uma cadeia de certificação íntegra e válida.



9. Certificação Digital

Atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora.

Para se fazer a certificação de uma assinatura digital, é necessária uma infraestrutura que valide o certificado para as demais entidades. Para isso, existem dois modelos de certificação que podem ser utilizados. São eles:

- **Modelo de malha de confiança**: baseado na criação de uma rede em que as entidades pertencentes devem confiar umas nas outras. Cada vez que um usuário obtém a

chave pública de outro usuário, ele pode verificar a assinatura digital da chave obtida por meio das demais entidades, garantindo a certeza de que a chave é a verdadeira. **Nesse modelo, a confiança é controlada pelo próprio usuário**. Além disso, a confiança **não** é transitiva, ou seja, se uma entidade A confia em B e B confia em C, isso não significa necessariamente que A confia em C. Esse modelo é utilizado no software PGP, que faz a certificação de mensagens eletrônicas;

- **Modelo hierárquico**: baseado na montagem de uma hierarquia de Autoridades Certificadoras (**ACs**). As ACs certificam os usuários e existe uma autoridade certificadora raiz (**AC-Raiz**) que faz a certificação de todas as ACs de sua jurisdição. Nesse modelo, os certificados digitais precisam da assinatura digital de uma AC para ser válido. Caso alguma entidade duvide de sua validade, basta consultar na AC para verificar se o certificado não foi revogado. Caso haja dúvida da validade do certificado da AC, basta conferir na AC-Raiz, que, em regra, possui um certificado assinado por si mesmo e é mantida por uma entidade governamental. Esse é o modelo utilizado para a montagem de Infraestruturas de Chaves Públicas (ICPs).

A seguir, destacamos alguns cuidados extraídos de Cert.Br (2013) a serem tomados para proteger os seus dados, e utilizar de forma adequada a certificação digital.

Proteja seus dados (CERT.BR, 2013):

- utilize **criptografia** sempre que, ao enviar uma mensagem, quiser assegurar-se que somente o destinatário possa lê-la;
- utilize **assinaturas digitais** sempre que, ao enviar uma mensagem, quiser assegurar ao destinatário que foi você quem a enviou e que o conteúdo não foi alterado;
- só envie **dados sensíveis** após certificar-se de que está usando uma conexão segura;
- utilize **criptografia para conexão** entre seu leitor de *e-mails* e os servidores de *e-mail* do seu provedor;
- **cifre o disco do seu computador e dispositivos removíveis**, como disco externo e *pen-drive*. Assim, em caso de perda ou furto do equipamento, seus dados não poderão ser indevidamente acessados;
- verifique o ***hash***, quando possível, dos arquivos obtidos pela Internet.

Seja cuidadoso com as suas chaves e certificados (CERT.BR, 2013):

- utilize **chaves de tamanho adequado**. Quanto maior a chave, mais resistente ela será a ataques de força bruta;
- **não utilize chaves secretas óbvias**;
- **certifique-se de não estar sendo observado ao digitar suas chaves e senhas de proteção**;
- **utilize canais de comunicação seguros** quando compartilhar chaves secretas;

- **armazene suas chaves privadas com algum mecanismo de proteção**, como por exemplo senha, para evitar que outra pessoa faça uso indevido delas;
- **preserve suas chaves**. Procure fazer *backups* e mantenha-os em local seguro (se você perder uma chave secreta ou privada, não poderá decifrar as mensagens que dependiam de tais chaves);
- tenha muito **cuidado ao armazenar e utilizar suas chaves em computadores potencialmente infectados ou comprometidos**, como em LAN *houses*, *cybercafés*, *stands* de eventos etc.;
- **se suspeitar que outra pessoa teve acesso à sua chave privada** (por exemplo, porque perdeu o dispositivo em que ela estava armazenada ou porque alguém acessou indevidamente o computador onde ela estava guardada), **solicite imediatamente a revogação do certificado junto à AC que o emitiu**.

Seja cuidadoso ao aceitar um certificado digital (CERT.BR, 2013):

- **mantenha seu sistema operacional e navegadores Web atualizados** (além disto contribuir para a segurança geral do seu computador, também serve para manter as cadeias de certificados sempre atualizadas);
- **mantenha seu computador com a data correta**. Além de outros benefícios, isto impede que certificados válidos sejam considerados não confiáveis e, de forma contrária, que certificados não confiáveis sejam considerados válidos;
- **ao acessar um *site* Web, observe os símbolos indicativos de conexão segura** e leia com atenção eventuais alertas exibidos pelo navegador;
- **caso o navegador não reconheça o certificado como confiável, apenas prossiga com a navegação se tiver certeza da idoneidade da instituição e da integridade do certificado**, pois, do contrário, poderá estar aceitando um certificado falso, criado especificamente para cometer fraudes.

10. PIN e PUK

*PIN (Personal Identification Number)

A senha PIN é utilizada para o uso do Certificado Digital e será solicitada toda vez que realizar algum tipo de procedimento.

**PUK (Personal Unlocking Key)

A senha PUK tem a função de desbloquear a senha PIN do Cartão Criptográfico/Token.

11. Esteganografia

É a **técnica de esconder um arquivo dentro de outro arquivo**, podendo ser uma imagem, documento de texto, planilha eletrônica etc., **só que utilizando criptografia**. Ao esconder um arquivo em uma imagem, por exemplo, ao enviá-la para o destinatário desejado, você tem que se assegurar que quem receber a imagem deverá conhecer o método de exibição e a senha utilizada na proteção deste arquivo.

Figura. Esteganografia

12. Segurança em Conexões Web

Ao navegar na Internet, geralmente utilizamos o protocolo HTTP nos casos em que não se tem o tráfego de informações sigilosas (como senhas, números de cartão de crédito e dados bancários). Quando o acesso envolver a transmissão de informações sigilosas, é importante certificar-se do uso de **conexões seguras**, com utilização do protocolo **HTTPS**.

Veja a distinção entre esses protocolos a seguir.

Protocolo	Descrição
HTTP (Hypertext Transfer Protocol – Protocolo de Transferência de Hipertexto)	Utilizado para realizar a transferência das páginas Web para nossos programas navegadores (**browsers**). Os dados transferidos por esse protocolo podem conter, por exemplo: texto, áudio ou imagens. Esse protocolo utiliza a porta 80. O 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. Portanto, não é indicado para transmissões que envolvem informações sigilosas, e deve ser substituído pelo HTTPS, que oferece conexões seguras (CERTBR,2013).

Protocolo	Descrição
HTTPS (HyperText Transfer Protocol Secure)	É uma variação do protocolo HTTP que utiliza mecanismos de segurança. O protocolo HTTPS, segundo CERTBR(2013), 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, como o SSL (Secure Sockets Layer) e o TLS (Transport Layer Security), para assegurar a confidencialidade e a integridade das informações. O HyperText Transfer Protocol Secure - HTTPS - é uma variação do protocolo HTTP que utiliza mecanismos de segurança.

De maneira geral, no acesso à Internet, você vai se deparar com os seguintes tipos de conexões...

Conexão padrão: usada em grande parte dos acessos realizados. **Não** provê requisitos de segurança.

Veja a seguir alguns indicadores deste tipo de conexão (Certbr,2013):

- o endereço do *site* começa com "**http://";**
- em alguns navegadores, o tipo de protocolo usado (HTTP), por ser o padrão das conexões, pode ser omitido na barra de endereços;
- um **símbolo do *site* (logotipo) é apresentado próximo à barra de endereço** e, ao passar o *mouse* sobre ele, não é possível obter detalhes sobre a identidade do *site*.

Figura. Conexão não segura em diversos navegadores (CertBr,2013)

Conexão segura: deve ser utilizada na transferência de dados sensíveis. Provê autenticação, integridade e confidencialidade, como requisitos de segurança.

Veja a seguir alguns indicadores deste tipo de conexão (Certbr,2013):

- 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 (à esquerda ou à direita) e, ao passar o *mouse* ou clicar sobre ele, são exibidos **detalhes sobre conexão e certificado digital em uso**.

Figura. Conexão segura em diversos navegadores

Conexão segura com EV SSL: provê os mesmos requisitos de segurança que a conexão segura anterior, porém com maior grau de confiabilidade quanto à identidade do *site* e de seu dono, pois utiliza certificados EV SSL (*Extended Validation Secure Socket Layer*) - certificado emitido sob um processo mais rigoroso de validação do solicitante. Inclui a verificação de que a empresa foi legalmente registrada, encontra-se ativa e que detém o registro do domínio para o qual o certificado será emitido, além de dados adicionais, como o endereço físico.

Além de apresentar indicadores similares aos apresentados na conexão segura sem o uso de EV SSL, também introduz um indicador próprio, destacado a seguir (CertBr,2013): **a barra de endereço e/ou o recorte são apresentados na cor verde e no recorte é colocado o nome da instituição dona do *site*.**

Figura. Conexão segura usando EV SSL em diversos navegadores

Outro nível de proteção de conexão usada na Internet envolve o **uso de certificados auto-assinados e/ou cuja cadeia de certificação não foi reconhecida**. Este tipo de conexão não

pode ser caracterizado como sendo totalmente seguro (e nem totalmente inseguro) pois, apesar de prover integridade e confidencialidade, não provê autenticação, já que não há garantias relativas ao certificado em uso (CertBr,2013).

Ao acessar um site com HTTPS e o navegador não reconhecer a cadeia de certificação, ele emite **alertas**, como os ilustrados a seguir.

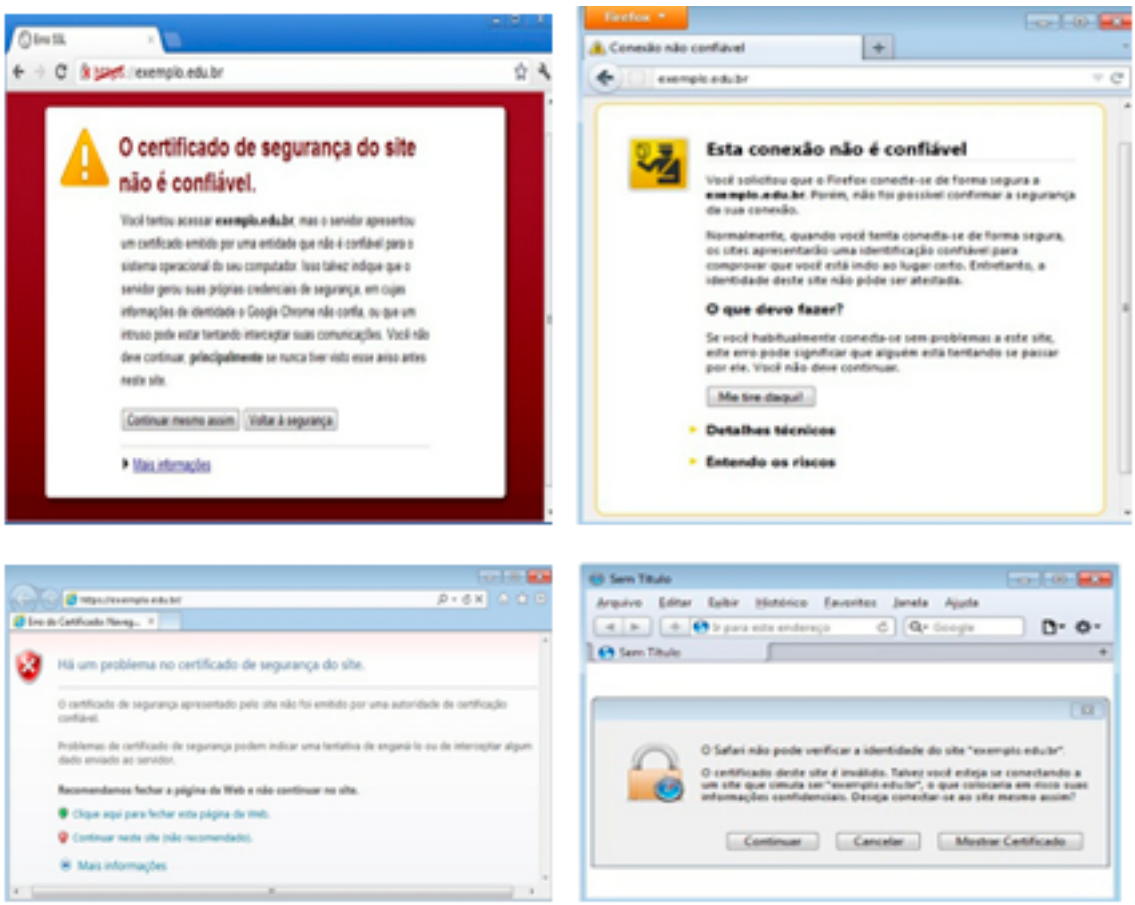


Figura. Alertas de certificado não confiável em navegadores (Certbr,2013)

Esses **alertas**, geralmente são emitidos em situações como (CertBr,2013):

- o certificado está fora do prazo de validade;
- o navegador não identificou a cadeia de certificação (dentre as possibilidades, o certificado pode pertencer a uma cadeia não reconhecida, ser autoassinado ou o navegador pode estar desatualizado e não conter certificados mais recentes de ACs);
- o endereço do *site* não confere com o descrito no certificado;
- o certificado foi revogado.

Caso você, apesar dos riscos, opte por aceitar o certificado, a simbologia mostrada pelo seu navegador será a ilustrada a seguir. Alguns indicadores deste tipo de conexão são (CertBr,2013):

- um cadeado com um “X” vermelho é apresentado na barra de endereço;

- a identificação do protocolo “https” é apresentado em vermelho e riscado;
- a barra de endereço muda de cor, ficando totalmente vermelha;
- um indicativo de erro do certificado é apresentado na barra de endereço;
- um recorte colorido com o nome do domínio do site ou da instituição (dona do certificado) é mostrado ao lado da barra de endereço e, ao passar o mouse sobre ele, é informado que uma exceção foi adicionada.

Figura. Conexão HTTPS com cadeia de certificação não reconhecida.

Certos *sites* fazem uso combinado, na mesma página *Web*, de conexão segura e não segura. Neste caso, pode ser que o cadeado desapareça, que seja exibido um ícone modificado (por exemplo, um cadeado com triângulo amarelo), que o recorte contendo informações sobre o *site* deixe de ser exibido ou ainda haja mudança de cor na barra de endereço, como ilustrado a seguir (CertBr,2013).

Figura. Uso combinado de conexão segura e não segura
Fonte: http://www.slideshare.net/edmoreno/livro-criptografia-em-hw-e-sw-isbn-8575220691

RESUMO

CRIPTOGRAFIA

(CONVERSÃO DE DADOS EM CÓDIGOS)

! sistemas Simétricos apresentam maior desempenho do que sistemas aSSimétricos

DE CHAVE aSSIMÉTRICA

(DUAS CHAVES DIFERENTES | PÚBLICA)

- CHAVE **PÚBLICA (CODIFICAÇÃO** | LIVREMENTE COMPARTILHADA)
- CHAVE **PRIVADA (DECODIFICAÇÃO)**
- O **DESTINATÁRIO CRIA A CHAVE PÚBLICA**, DE CODIFICAÇÃO, E A ENVIA PARA QUEM VAI LHE GERAR A INFORMAÇÃO CRIPTOGRAFADA

→ **PRINCIPAIS ALGORÍTIMOS** ! CAI MTO

RSA

DSA

DIFFIE-HELLMAN

DE CHAVE SIMÉTRICA

(ÚNICA | PRIVADA | CONVENCIONADA CHAVE SECRETA)

- APENAS **UMA CHAVE PARA ENCRIPTAR E DESENCRIPTAR** A MENSAGEM | COMPARTILHADA ENTRE EMISSOR E DESTINATÁRIO

- CHAVE DE CIFRAÇÃO FACILMENTE GERADA A PARTIR DA CHAVE DE DECIFRAÇÃO E VICE VERSA

+ VANTAGENS

RAPIDEZ | CHAVES PEQUENAS

- DESVANTAGENS

ÚNICA CHAVE PARA CIFRAÇÃO E DECIFRAÇÃO

→ **PRINCIPAIS ALGORÍTIMOS** ! CAI MTO

AES 128 | 192 | 256

DES 56 bits (PERMUTAÇÃO) | 3DES

IDEA 128 bits | RC | TWOFISH | BLOWFISH

Figura. Criptografia. Fonte: Clube dos Mapas por @paola.tuzani

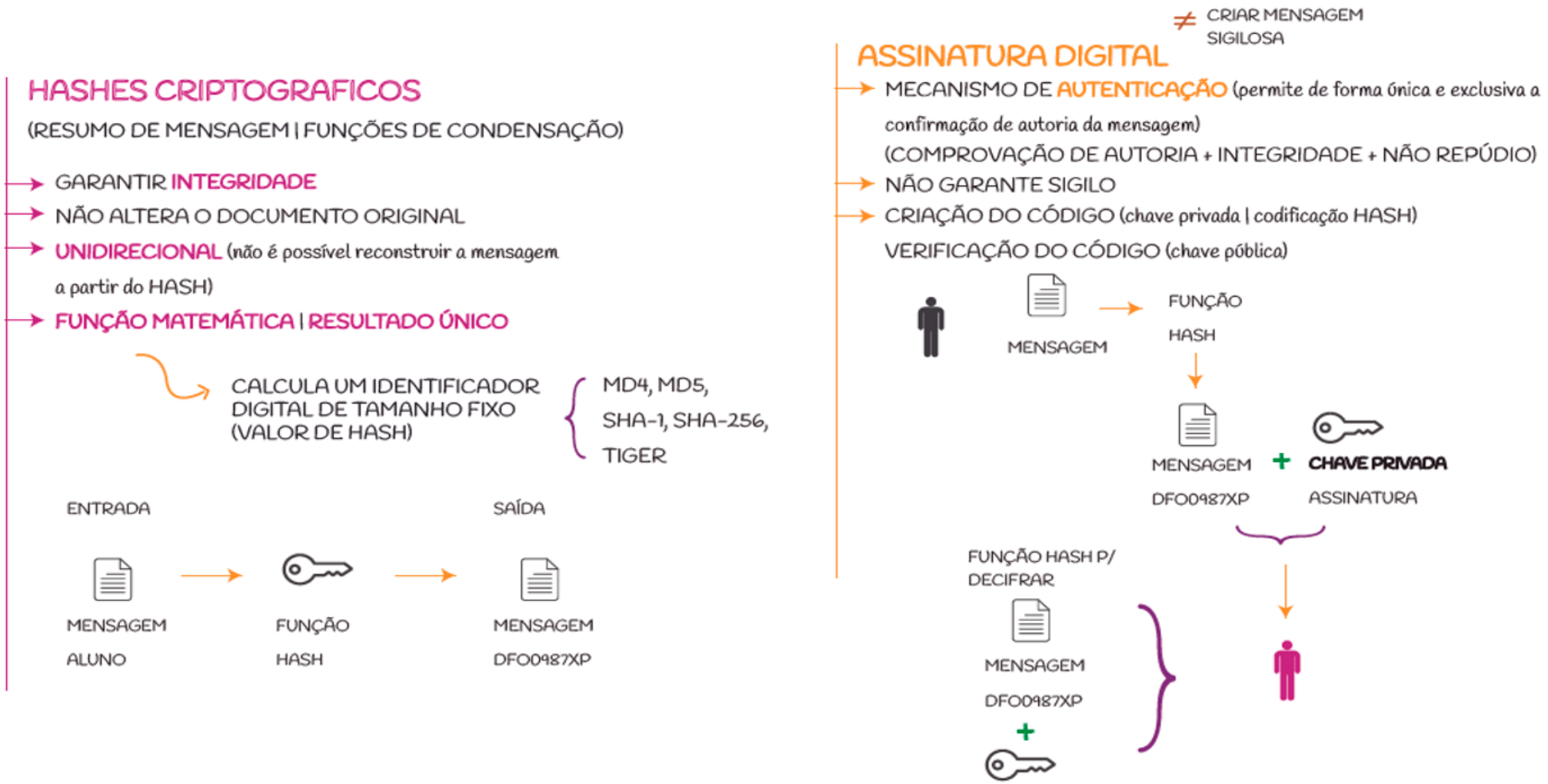


Figura. Hashes Criptográficos e Assinatura Digital. Fonte: Clube dos Mapas por @paola.tuzan

CERTIFICADO DIGITAL

- emitido por **autoridade certificadora – AC**
- **certificação digital**
  - **MALHA DE CONFIANÇA**
    rede de confiança entre as entidades
    confiança NÃO transitiva
    utilizada no software PGP
  - **MODELO HIERÁRQUICO**
    hierarquia de autoridades certificadoras.
    AC-raíz faz certificação das demais ACs
    precisam da assinatura digital da AC
    utilizado na **Infraestrutura de chaves públicas ICP**
- **tipos**
  - **TIPO A – CERTIFICADO DE ASSINATURA DIGITAL**
    (autenticidade e autoria)
  - **TIPO S – CERTIFICADO DE SIGILO/ CONFIDENCIALIDADE**
    (sigilo ou criptografia)
  - **TIPO T – CERTIFICADO DE TEMPO**
    (dia e hora)
- certificados autoassinados
  DONO = EMISSOR
  - **SIM** (INTEGRIDADE E CONFIDENCIALIDADE)
  - **NÃO** (AUTENTICAÇÃO) | **EV SSL** PROCESSO MAIS RIGOROSO DE VALIDAÇÃO

PIN
para uso nos certificados
PUK
desbloquear o PIN

- objetivo principal **vincular a chave pública a um titular**
- PKC: **certificar quem é o titular de uma chave pública**
- garantir a AUTORIA **AUTENTICIDADE** de uma informação por meio da **relação entre chaves pública e privada de uma entidade**
- documento eletrônico que **identifica**
  transferir credibilidade
  - **PESSOAS F/J**
  - **URL's**
  - **CONTAS DE USUÁRIOS/ SERVIDORES**
- contém a **chave pública do titular** ! CAI MTO
- armazenado em dispositivos de segurança
  ex: token, smart-card

NÍVEL DE SEGURANÇA ↓

FINAL	VALIDADE (anos)	TAMANHO (bits)
AS 1	1	2048
AS 2	2	2048
AS T 3	5	2048
AS T 4	6	4096

Figura. Certificado Digital. Fonte: Clube dos Mapas por @paola.tuzani

componentes da PKI

usuários + autoridades certificadoras + certificados e diretórios

função da PKC: estruturar esses componentes e definir padrões p/ documentos e protocolos

RFC 5280

é uma **especificação** da família **de padrões para o X 509 PKI** | traça perfil para formato e semântica para certificados e listas de certificados revogados

atribuições

- REGISTRO
- INICIALIZAÇÃO
- CERTIFICAÇÃO
- RECUPERAÇÃO DO PAR DE CHAVES
- ATUALIZAÇÃO DO PAR DE CHAVES
- PEDIDO DE REVOGAÇÃO
- CERTIFICAÇÃO CRUZADA

- ASSEGURA INTEGRIDADE + AUTORIA
- CADEIA HIERÁRQUICA E DE CONFIANÇA

INFRAESTRUTURA DE CHAVES PÚBLICAS (PKI / ICP)

conjunto de tecnologias que garante às transações e aos documentos eletrônicos a segurança por meio do uso de um par de chaves

autoridade certificadora (AC)

órgão de licenciamento

- EMITE
- GERENCIA
- REVOGA

} CERTIFICADOS P/ USUÁRIOS FINAIS

raiz no brasil = AC raiz (instituto nacional TI MCTIC | vinculado à Casa Civil – PR)

modelo de raiz única

responsável pela AUTENTICIDADE dos certificados emitidos por ela

o par de chaves é gerado pelo próprio titular ! CAI MTO

autoridade de registro (AR)

entidade **intermediária** | auxilia a AC em suas funções rotineiras para processamento de certificados

sistema opcional que assegura o vínculo entre chaves públicas e identidades de seus proprietários

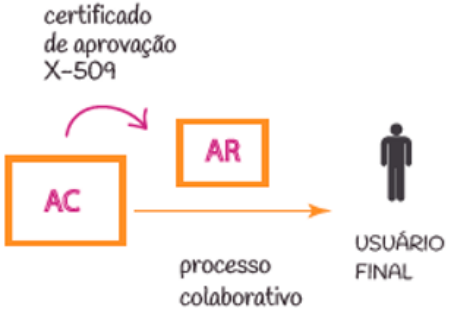


Figura. PKI. Fonte: Clube dos Mapas por @paola.tuzani

QUESTÕES DE CONCURSO

001. (CESPE/TJ-AM/ANALISTA JUDICIÁRIO/ARQUIVOLOGIA/2019) Com relação a conceitos básicos de informática, julgue o item que se segue.
Um certificado digital validado por uma autoridade certificadora permite associar uma mensagem ao seu remetente, garantindo-se, assim, a autenticidade da comunicação.

Um certificado digital é um documento eletrônico que identifica pessoas, físicas ou jurídicas, URLs, contas de usuário, servidores (computadores), dentre outras entidades. Este "documento" na verdade é uma estrutura de dados que contém a chave pública do seu titular e outras informações de interesse.
Ele contém informações relevantes para a identificação "real" da entidade a que visa certificar (CPF, CNPJ, endereço, nome, etc.) e informações relevantes para a aplicação a que se destina.
Dentre as informações que compõem um certificado temos:

- **Versão:** indica qual formato de certificado está sendo seguido;
- **Número de série:** identifica unicamente um certificado dentro do escopo do seu emissor;
- **Algoritmo:** identificador dos algoritmos de hash+assinatura utilizados pelo emissor para assinar o certificado;
- **Emissor:** entidade que emitiu o certificado;
- **Validade:** data de emissão e expiração;
- **Titular:** nome da pessoa, URL ou demais informações que estão sendo certificadas;
- **Chave pública:** informações da chave pública do titular;
- **Extensões:** campo opcional para estender o certificado;
- **Assinatura:** valor da assinatura digital feita pelo emissor.

O certificado digital precisa ser emitido por uma autoridade reconhecida pelas partes interessadas na transação. Chamamos essa autoridade de **Autoridade Certificadora, ou AC.**
Quanto aos objetivos do certificado digital podemos destacar:

- transferir a credibilidade que hoje é baseada em papel e conhecimento para o ambiente eletrônico;
- **vincular uma chave pública a um titular** (eis o objetivo principal).

Uma **assinatura digital** garante as seguintes propriedades:

- **Autenticidade**: o receptor (destinatário de uma mensagem) pode confirmar que a assinatura foi feita pelo emissor;
- **Integridade**: qualquer alteração da mensagem faz com que a assinatura seja invalidada;
- **Não repúdio** (ou **irretratabilidade**): o emissor (aquele que assinou digitalmente a mensagem) não pode negar que foi o autor da mensagem, ou seja, não pode dizer mais tarde que a sua assinatura foi falsificada.

A **assinatura digital** não torna o documento eletrônico sigiloso, pois ele em si não é criptografado. O sigilo do documento eletrônico poderá ser resguardado mediante a cifragem da mensagem com a chave pública do destinatário, pois somente com o emprego de sua chave privada o documento poderá ser decifrado. Já a integridade e a comprovação da autoria são características primeiras do uso da certificação digital para assinar.

Certo.

---

002. (CESPE/2017/TRE-PE/CONHECIMENTOS GERAIS/CARGO 6) O mecanismo de embaralhamento ou codificação utilizado para proteger a confidencialidade de dados transmitidos ou armazenados denomina-se

a) assinatura digital

b) certificação digital.

c) biometria.

d) criptografia.

e) proxy.

A criptografia = arte e ciência de manter mensagens seguras. Visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la. Trata-se de um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet.

Conforme destaca Cert.Br, por meio do uso da criptografia pode-se:

- proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda;
- criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- proteger *backups* contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- **proteger as comunicações realizadas pela Internet, como os *e-mails* enviados/recebidos e as transações bancárias e comerciais realizadas**.[1]

Letra d.

---

003. (CESPE/TRE-PE/CONHECIMENTOS GERAIS/CARGOS 1, 2, 4 E 5/2017) Os mecanismos que contribuem para a segurança da informação em ambientes computacionais incluem

a) certificado digital, criptografia e cavalo de troia.

b) backdoor, firewall e criptografia.

c) rootkits, arquivos de configuração e becape.

[1] Referências: https://cartilha.cert.br/criptografia/

d) firewall, worm e proxy.
e) VPN, honeypot e senha.

Malwares (Códigos maliciosos) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. São espécies de *malware*: vírus, *worms*, *bots* ("Robôs"), cavalos de troia (*trojans*), *spyware*, adware, *keylogger, screenlogger, ransomwares, backdoors, rootkits, cracks*, *hijackers*, *bolware* etc. Dessa forma, estão erradas as assertivas A, C, D e E, o que torna a letra B a resposta da questão.

Os mecanismos de proteção aos ambientes computacionais destinados a garantir a segurança da informação incluem: controle de acesso físico, utilização de token, assinatura digital, política de chaves e senhas, política de segurança, criptografia, antivírus, bloqueador de pop-ups, bloqueador de cookies, *honeypots*, VPN (Virtual Private Network – Rede Virtual Privada), etc.

Honeypot (= "Pote de Mel") é um sistema que possui falhas de segurança reais ou virtuais, colocadas de maneira proposital, a fim de que seja invadido e que o fruto desta invasão possa ser estudado.

Um honeypot é um recurso de rede cuja função é de ser atacado e comprometido (invadido). Significa dizer que um Honeypot poderá ser testado, atacado e invadido. Os honeypots não fazem nenhum tipo de prevenção, os mesmos fornecem informações adicionais de valor inestimável" (Lance Spitzner/2003). Não possui dados ou aplicações importantes para a organização. Objetivo: passar-se por equipamento legítimo. Não existem falsos positivos pois o tráfego nos honeypots é real.

Veja os itens indevidos nas assertivas:

a) certificado digital, criptografia e cavalo de troia.
b) backdoor, firewall e criptografia.
c) rootkits, arquivos de configuração e becape.
d) firewall, worm e proxy.
e) VPN, honeypot e senha.

Letra e.

004. (CESPE/TRE-BA/CONHECIMENTOS GERAIS/NÍVEL MÉDIO/2017) O procedimento utilizado para atribuir integridade e confidencialidade à informação, de modo que mensagens e arquivos trocados entre dois ou mais destinatários sejam descaracterizados, sendo impedidos leitura ou acesso ao seu conteúdo por outras pessoas, é denominado

a) criptografia.
b) engenharia social.
c) antivírus.
d) firewall.
e) becape.

a) Certa**. A criptografia = arte e ciência de manter mensagens seguras.** Visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la. Trata-se de um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso da Internet.

Conforme destaca Cert.Br, por meio do uso da criptografia pode-se:

- proteger os dados sigilosos armazenados em seu computador, como o seu arquivo de senhas e a sua declaração de Imposto de Renda;
- criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- proteger *backups* contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- **proteger as comunicações realizadas pela Internet, como os *e-mails* enviados/recebidos e as transações bancárias e comerciais realizadas**.[2]

Por meio da criptografia e alguns métodos auxiliares, pode-se atribuir integridade e confidencialidade à informação.

b) Errada. Engenharia social compreende as práticas utilizadas para obter acesso a informações importantes ou sigilosas mediante ações para ludibriar ou explorar a confiança das pessoas.

c) Errada. **Antivírus** são **ferramentas preventivas e corretivas,** que detectam (e, em muitos casos, removem) vírus de computador e outros programas maliciosos (como *spywares* e cavalos de troia).

d) Errada. **Firewall** serve, basicamente, para filtrar os pacotes que entram e(ou) saem de um computador e para verificar se o tráfego é permitido ou não.

e) Errada. **Becape (ou Backup)** é uma cópia de segurança. A lista de itens cujo backup deve ser feito com frequência **inclui dados, arquivos de configuração e logs**.

Letra a.

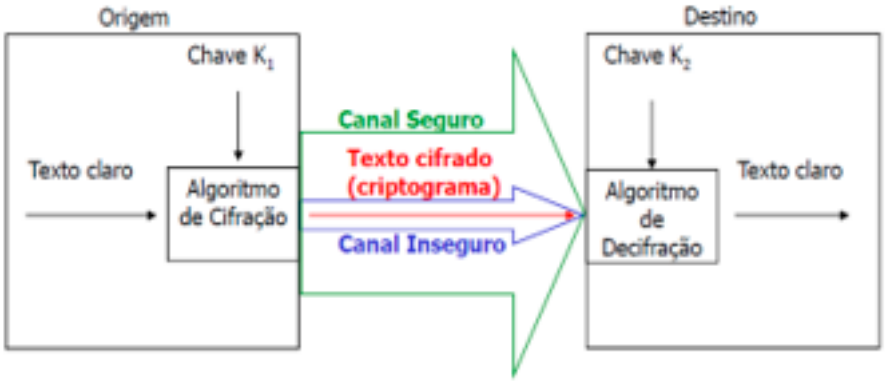
005. (CESPE/TRE-BA/CONHECIMENTOS GERAIS/NÍVEL SUPERIOR/2017) Assinale a opção que apresenta a solução que permite filtrar tentativas de acessos não autorizados oriundos de outros ambientes e redes externas, contribuindo para a melhora do estado de segurança da informação de ambientes computacionais.

a) certificado digital
b) chave de criptografia
c) rootkits
d) firewall
e) antivírus

[2] Referências: https://cartilha.cert.br/criptografia/

a) Errada. **Certificado Digital** é um documento eletrônico que identifica pessoas, físicas ou jurídicas, URLs, contas de usuário, servidores (computadores), dentre outras entidades. Este "documento" na verdade é uma estrutura de dados que contém a chave pública do seu titular e outras informações de interesse.

b) Errada. **Chave de criptografia:** informação que o remetente e o destinatário possuem e que será usada para criptografar e descriptografar um texto ou mensagem.



c) Errada. Rootkit é um tipo de malware cuja principal intenção é se camuflar, para assegurar a sua presença no computador comprometido, impedindo que seu código seja encontrado por qualquer antivírus. Isto é possível porque esta aplicação tem a capacidade de interceptar as solicitações feitas ao sistema operacional, podendo alterar o seu resultado. O invasor, após instalar o rootkit, terá acesso privilegiado ao computador previamente comprometido, sem precisar recorrer novamente aos métodos utilizados na realização da invasão, e suas atividades serão escondidas do responsável e/ou dos usuários do computador.

d) Certa. **Firewall** serve, basicamente, para filtrar os pacotes que entram e(ou) saem de um computador e para verificar se o tráfego é permitido ou não. Permite filtrar tentativas de acessos não autorizados oriundos de outros ambientes e redes externas, contribuindo para a melhora do estado de segurança da informação de ambientes computacionais.

e) Errada. **Antivírus** são **ferramentas preventivas e corretivas,** que detectam (e, em muitos casos, removem) vírus de computador e outros programas maliciosos (como *spywares* e cavalos de troia).

Letra d.

006. (CESPE/TJ-DFT/NÍVEL SUPERIOR/2013) A autoridade certificadora, que atua como um tipo de cartório digital, é responsável por emitir certificados digitais.

Uma Autoridade Certificadora (AC) é responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Além disso, ela verifica se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado.
Certo.

007. (CESPE/TJ-DFT/TÉCNICO JUDICIÁRIO/ÁREA ADMINISTRATIVA/2013) A criptografia, mecanismo de segurança auxiliar na preservação da confidencialidade de um documento, transforma, por meio de uma chave de codificação, o texto que se pretende proteger.

A Criptografia é uma ciência de escrever mensagens cifrados ou em código, sendo muito utilizada como mecanismo de segurança de informação, de modo a auxiliar na minimização dos riscos associados ao uso da Internet para troca de informação.
Certo.

008. (CESPE/AGENTE TÉCNICO DE INTELIGÊNCIA/ÁREA DE TECNOLOGIA DA INFORMAÇÃO/ABIN/2010) A chave assimétrica é composta por duas chaves criptográficas: uma privada e outra pública.

A criptografia de chave pública (a*S*Simétrica) utiliza *duas* chaves: *uma* denominada *privada* e outra denominada *pública*. Nesse método, uma pessoa deve criar uma chave de codificação e enviá-la a quem for mandar informações a ela. Essa é a chave *pública*. Outra chave deve ser criada para a decodificação.
Esta – a chave *privada* – é *secreta*.
Certo.

009. (CESPE/OFICIAL TÉCNICO DE INTELIGÊNCIA/ÁREA DE ARQUIVOLOGIA/ABIN/2010) A respeito de mecanismos de segurança da informação, e considerando que uma mensagem tenha sido criptografada com a chave pública de determinado destino e enviada por meio de um canal de comunicação, pode-se afirmar que a mensagem criptografada com a chave pública do destinatário garante que somente quem gerou a informação criptografada e o destinatário sejam capazes de abri-la.

Quando se criptografa a mensagem com a chave pública do destinatário ela poderá ser aberta (descriptografada) apenas pelo destinatário, já que só ele tem acesso à sua chave privada. O remetente (quem gerou a mensagem) já tem acesso à mensagem em claro, não criptografada.
Errado.

010. (CESPE/CAIXA-NM1/TÉCNICO BANCÁRIO/CARREIRA ADMINISTRATIVA/2010) Um certificado digital é pessoal, intransferível e não possui data de validade.

Um **certificado digital** é um **documento eletrônico que identifica pessoas, físicas ou jurídicas, URLs, contas de usuário, servidores** (computadores) dentre outras entidades. Este "documento" na verdade é **uma estrutura de dados que contém a chave pública do seu titular e outras informações de interesse**. Contêm informações relevantes para a identificação "real" da entidade a que visam certificar (CPF, CNPJ, endereço, nome, etc.) e informações relevantes para a aplicação a que se destinam. O certificado digital precisa ser emitido por uma autoridade reconhecida pelas partes interessadas na transação. Chamamos essa autoridade de Autoridade Certificadora, ou **AC**. Dentre as informações que compõem um certificado temos:

- **Versão:** indica qual formato de certificado está sendo seguido;
- **Número de série:** identifica unicamente um certificado dentro do escopo do seu emissor;
- **Algoritmo:** identificador dos algoritmos de hash+assinatura utilizados pelo emissor para assinar o certificado;
- **Emissor:** entidade que emitiu o certificado;
- **Validade: data de emissão e expiração**;
- **Titular:** nome da pessoa, URL ou demais informações que estão sendo certificadas;
- **Chave pública:** informações da chave pública do titular;
- **Extensões:** campo opcional para estender o certificado;
- **Assinatura:** valor da assinatura digital feita pelo emissor.

Errado.

011. (CESPE/POLÍCIA FEDERAL/PERITO/ÁREA 3/COMPUTAÇÃO/2002) Sistemas criptográficos são ditos simétricos ou de chave secreta quando a chave utilizada para cifrar é a mesma utilizada para decifrar. Sistemas assimétricos ou de chave pública utilizam chaves distintas para cifrar e decifrar. Algoritmos simétricos são geralmente mais eficientes computacionalmente que os assimétricos e por isso são preferidos para cifrar grandes massas de dados ou para operações online.

A **criptografia de chave simétrica** (também chamada de **criptografia de chave única**, ou **criptografia privada,** ou **criptografia convencional**) utiliza **APENAS UMA** chave para encriptar e decriptar as mensagens. Assim, como só utiliza UMA chave, obviamente ela deve ser compartilhada entre o remetente e o destinatário da mensagem.

Para ilustrar os sistemas simétricos, podemos usar a imagem de um cofre, que só pode ser fechado e aberto com uso de uma chave. Esta pode ser, por exemplo, uma combinação de números. A mesma combinação abre e fecha o cofre. Para criptografar uma mensagem, usamos a chave (fechamos o cofre) e para decifrá-la utilizamos a mesma chave (abrimos o cofre).

Os sistemas simétricos têm o problema em relação à distribuição de chaves, que devem ser combinadas entre as partes antes que a comunicação segura se inicie. Esta distribuição se torna um problema em situações em que as partes não podem se encontrar facilmente. Mas há outros problemas: a chave pode ser interceptada e/ou alterada em trânsito por um inimigo.

Obs.: na **criptografia simétrica** (ou de **chave única**) **tanto o emissor quanto o receptor da mensagem devem conhecer a chave utilizada!**

Nos algoritmos de **criptografia assimétrica (criptografia de chave pública)** utilizam **DUAS** chaves **DIFERENTES**, uma **PÚBLICA** (que pode ser distribuída) e uma **PRIVADA** (pessoal e intransferível). Assim, nesse método cada pessoa ou entidade mantém duas chaves: uma pública, que pode ser divulgada livremente, e outra privada, que deve ser mantida em segredo pelo seu dono. As mensagens codificadas com a chave pública só podem ser decodificadas com a chave privada correspondente.
Do ponto de vista do custo computacional, **os sistemas simétricos apresentam melhor desempenho que os sistemas assimétricos**, e isso já foi cobrado em provas várias vezes!
Certo.

---

012. (VUNESP/FUNDUNESP/ANALISTA DE REDES PLENO/SEGURANÇA DA INFORMAÇÃO/2014) A troca de informações pela rede de computadores pode sofrer ataques como quebra do sigilo e até modificação indevida. Nesse contexto, um Certificado Digital tem como função

a) assegurar a privacidade da informação transmitida por meio do uso de criptografia RC4.
b) criptografar a informação transmitida utilizando o algoritmo DES.
c) garantir a integridade da informação transmitida pelo uso do algoritmo de *Hashing*.
d) gerar o algoritmo de criptografia para assegurar privacidade da informação.
e) relacionar uma Chave pública a uma Chave privada de uma entidade.

Um **certificado digital** é **um arquivo de computador que contém um conjunto de informações referentes à entidade para o qual o certificado foi emitido** (seja uma empresa, pessoa física

ou computador) **mais a chave pública referente à chave privada que se acredita ser de posse unicamente da entidade especificada no certificad**o.

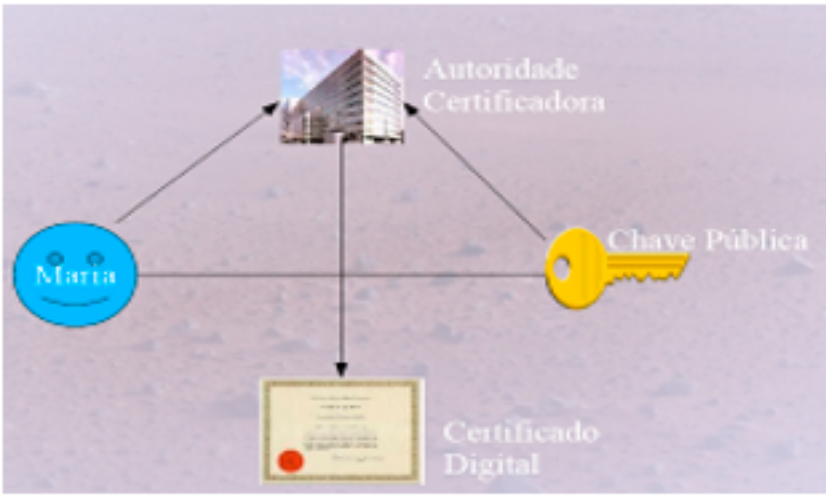


Figura. Vínculo da Chave Pública ao Titular

Letra e.

---

013. (VUNESP/CÂMARA MUNICIPAL DE SÃO JOSÉ DOS CAMPOS-SP/ANALISTA LEGISLATIVO /ANALISTA DE SISTEMAS/2014) No contexto da segurança da informação, diversos recursos são utilizados para dirimir a vulnerabilidade do processo da troca de informações, principalmente o realizado pela rede de computadores. Um desses recursos é o denominado PKC (Public Key Certificate), que tem como função

a) autenticar a veracidade de uma chave simétrica compartilhada publicamente.
b) certificar a segurança de uma chave de criptografia gerada pelo usuário.
c) gerar um código de criptografia de acesso público.
d) identificar e autenticar o proprietário de uma chave pública.
e) publicar certificados de criptografia de domínio público.

PKC (*Public Key Certificate*) é um documento eletrônico que por meio de procedimentos lógicos e matemáticos assegura a integridade das informações e a autoria das transações. PKC tem como missão associar uma entidade a uma chave pública.
Letra d.

---

014. (VUNESP/FUNDUNESP/ANALISTA DE REDES PLENO/SEGURANÇA DA INFORMAÇÃO/2014) Atualmente existem diversas implementações de protocolos criptográficos, mas que se utilizam de, basicamente, dois tipos de algoritmo, o de chave simétrica e o de chave assimétrica. Dentre os vários protocolos, o que utiliza o algoritmo de chave assimétrica é o

a) AES.
b) *Blowfish*.
c) *Cast*.
d) *Diffie-Hellman*.
e) IDEA.

Existem vários algoritmos que usam **chaves simétricas**, como:

- IDEA;
- TwoFish;
- Blowfish;
- Serpent;
- DES;
- AES;
- RC5;
- RC6;
- CAST.

Como exemplos de algoritmos que usam **chaves assimétricas** têm-se:

- RSA;
- **Diffie-Hellman**;
- DAS;
- Schnorr.

Letra d.

015. (VUNESP/DESENVOLVESP/ANALISTA/GRUPO 6/2014) A criptografia tem por objetivo tornar a informação visível apenas para os entes autorizados, utilizando, para isso, esquemas de codificação (cifragem) e chaves. Dentre os vários esquemas, um exemplo de criptografia assimétrica, ou de chaves públicas, é o

a) AES.
b) DES.
c) IDEA.
d) RC4.
e) RSA.

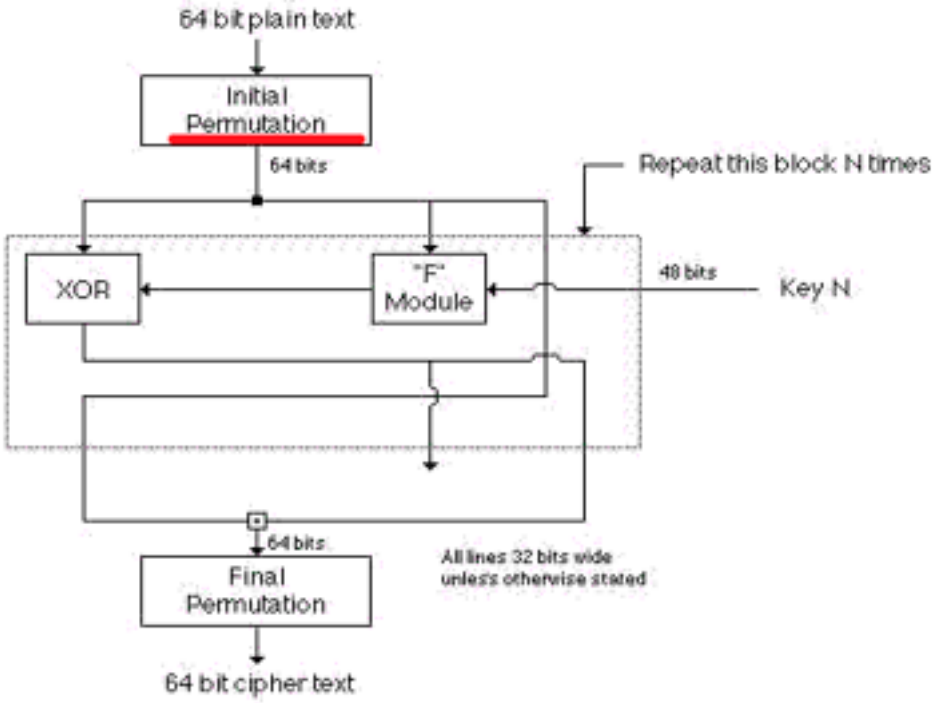
Como exemplos de algoritmos que usam **chaves assimétricas** têm-se: RSA; Diffie-Hellman; DAS; Schnorr etc.

Letra e.

016. (VUNESP/CÂMARA MUNICIPAL DE SÃO JOSÉ DOS CAMPOS- SP/ANALISTA LEGISLATIVO/ANALISTA DE SISTEMAS/2014) Para melhorar a segurança da informação, são utilizados processos de criptografia sobre a informação transmitida. Uma das técnicas de criptografia amplamente difundida é o DES (Data Encryption Standard), na qual o processo de criptografia envolve, sobre os dados originais, a primeira etapa de

a) inversão.
b) permutação.
c) separação.
d) substituição.
e) inserção da chave.

No DES (*Data Encryption Standard*) o processo de criptografia envolve, sobre os dados originais, a primeira etapa de permutação.



Letra b.

017. (FCC/ELETROBRAS/ELETROSUL/TÉCNICO DE SEGURANÇA DO TRABALHO/2016) Considere, por hipótese, que a Eletrosul deseja aumentar a segurança das informações utilizando registros das atividades de seus colaboradores. A partir da análise destes registros armazenados em arquivo ou em base de dados, a empresa pode ser capaz de:

- detectar o uso indevido de computadores, como um usuário tentando acessar arquivos de outros usuários, ou alterar arquivos do sistema;
- detectar um ataque, como de força bruta, ou a exploração de alguma vulnerabilidade;

- rastrear ou auditar as ações executadas por um usuário no seu computador, como programas utilizados, comandos executados e tempo de uso do sistema;
- detectar problemas de hardware ou nos programas e serviços instalados no computador.

Estes registros são denominados

a) backups.

b) phishing.

c) logs.

d) hashes.

e) firewalls.

a) Errada. ***Backups*** são cópias de segurança. Guarde o seguinte para a prova:

- A lista de itens cujo *backup* deve ser feito com frequência **inclui dados, arquivos de configuração e *logs***.
- *Backups* que incluem binários não são aconselháveis, pois abrem a possibilidade de que *malwares* ou executáveis corrompidos sejam reinstalados na restauração do sistema.
- Os *backups* devem ser verificados logo após a sua geração e, posteriormente, em intervalos regulares.
- O melhor é fazer os *backups* da forma mais automatizada, de modo a reduzir o seu impacto sobre o trabalho dos administradores e operadores de sistemas.

b) Errada. ***Phishing, scam*** ou ***phishing scam*** é uma fraude que se dá por meio do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários desavisados.

c) Certa. O termo ***log*** é utilizado para designar um arquivo que contém o registro de eventos relevantes da rede, de um determinado dispositivo, de um sistema etc.

- Muitas vezes, os *logs* são o único recurso que um administrador possui para descobrir as causas de um problema ou comportamento anômalo.
- A partir da **análise** destes registros **armazenados em arquivo ou em base de dados, a empresa pode ser capaz de**:
  - detectar o uso indevido de computadores, como um usuário tentando acessar arquivos de outros usuários, ou alterar arquivos do sistema;
  - detectar um ataque, como de força bruta, ou a exploração de alguma vulnerabilidade;
  - rastrear ou auditar as ações executadas por um usuário no seu computador, como programas utilizados, comandos executados e tempo de uso do sistema;
  - detectar problemas de hardware ou nos programas e serviços instalados no computador.

d) Errada. ***HASH (Message Digest – Resumo de Mensagem)*** é uma **função matemática** que recebe uma mensagem de entrada e gera como resultado um número finito de caracteres ("dígitos verificadores"). A figura seguinte ilustra alguns exemplos de uso da função *hash*:

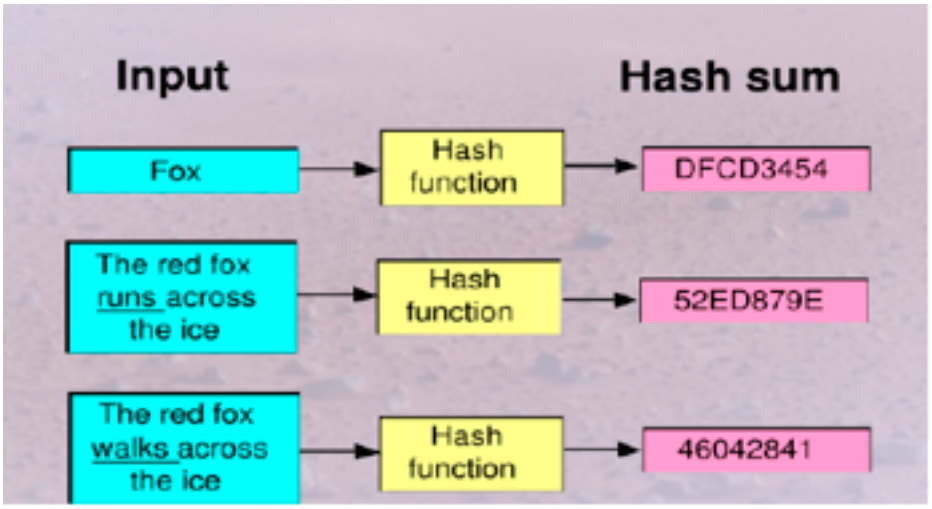


Figura. Exemplos de Saídas da Função

- CERT.BR (2013) destaca que "uma **função de resumo** (***hash***) é um **MÉTODO CRIPTOGRÁFICO** que, quando aplicado sobre uma informação, independentemente do tamanho que ela tenha, gera um resultado único e de tamanho **fixo**, chamado **hash"**.
- Usamos o ***hash*** quando precisamos garantir a **integridade** de determinada informação; realizar armazenamento seguro de senhas; garantir a integridade de arquivos etc.

e) Errada. ***Firewall*** serve, basicamente, para filtrar os pacotes que entram e(ou) saem de um computador e para verificar se o tráfego é permitido ou não.

- São aplicadas ao *firewall* regras RESTRITIVAS, de forma que TUDO QUE NÃO É PERMITIDO É PROIBIDO.
- A utilização de *firewalls* em uma rede visa impedir acesso indevido dentro da própria rede e também acessos oriundos da Internet.
- Pode ser:
  - apenas um ***software*** sendo executado no ponto de conexão entre as redes de computadores (ex.: firewall do Windows, Iptables no Linux etc.); ou
  - um **conjunto de hardware e software** (esse cenário é o mais comum de se encontrar!). O Cisco ASA é um exemplo de um firewall de hardware, que possui um software internamente para aplicação das regras de segurança que serão aplicadas a esse dispositivo.

Letra c.

018. (FCC/COPERGÁS-PE/ANALISTA ADMINISTRADOR/2016) Uma empresa como a COPERGÁS procura implantar regras e mecanismos de proteção e segurança de suas informações. Uma regra ou mecanismo correto é

a) utilizar equipamento do tipo log para detectar o uso indevido de computadores, como um usuário tentando alterar arquivos do sistema de forma indevida.

b) utilizar, sempre que possível, conexão segura com EV SSL, na qual a barra de endereço e/ou o recorte são apresentados na cor verde e há o nome da instituição proprietária do site.

c) certificar-se da procedência do site e da utilização de conexões seguras, como o protocolo HTTP, ao realizar compras e pagamentos via web.

d) evitar cifrar ou colocar senhas em dispositivos removíveis, como disco externo e pendrive, para que dados de backup possam ser mais facilmente recuperados.

e) desabilitar o log dos arquivos obtidos pela internet para conseguir detectar arquivos corrompidos ou indevidamente alterados durante a transmissão.

A regra ou mecanismo deve estar relacionada a uma **boa prática de segurança**, então vamos à análise das alternativas:

a) Errada. Log não é equipamento! **Trata-se de um arquivo que contém o registro de eventos relevantes da rede, de um determinado dispositivo, de um sistema etc.** Muitas vezes, os *logs* são o único recurso que um administrador possui para descobrir as causas de um problema ou comportamento anômalo. Esse registro serve por exemplo para detectar o uso indevido de computadores, como um usuário tentando alterar arquivos do sistema de forma indevida.

b) Certa**. Conexão segura,** segundo CertBr (2012), é a que deve ser utilizada quando dados sensíveis são transmitidos, geralmente usada para acesso a *sites* de *Internet Banking* e de comércio eletrônico. A **conexão segura com EV SSL** provê autenticação, integridade e confidencialidade como requisitos de segurança, porém com maior grau de confiabilidade quanto à identidade do *site* e de seu dono, pois utiliza **certificados EV SSL (*Extended Validation Secure Socket Layer*) -** certificado emitido sob um processo mais rigoroso de validação do solicitante. Inclui a verificação de que a empresa foi legalmente registrada, encontra-se ativa e que detém o registro do domínio para o qual o certificado será emitido, além de dados adicionais, como o endereço físico.

Além de apresentar indicadores similares aos apresentados na conexão segura sem o uso de EV SSL, também introduz um indicador próprio, que é: a barra de endereço e/ou o recorte são apresentados na cor verde e no recorte é colocado o nome da instituição dona do *site (Certbr,2012)*.

Figura - Conexão segura usando EV SSL em diversos navegadores (Fonte: CertBr,2012)

c) Errada. Deve certificar-se da procedência do site e da utilização de conexões seguras, como o protocolo **HTTPS**, ao realizar compras e pagamentos via web.
d) Errada. A cifragem de senhas e dados disponíveis em dispositivos removíveis, como disco externo e *pendrive* é uma boa prática de segurança.
e) Errada. Deve-se habilitar esses ***logs***, para que possamos ser informados sobre anormalidades ocorridas na transmissão.
Letra b.

---

019. (FCC/ELETROBRAS-ELETROSUL/DIREITO/2016) Ao se enviar arquivos pela internet há um método criptográfico que permite verificar se o arquivo foi alterado, ou seja, se teve sua integridade violada. Esse método, quando aplicado sobre as informações do arquivo, independente do seu tamanho, gera um resultado único de tamanho fixo. Assim, antes de enviar o arquivo pode-se aplicar esse método no conteúdo do arquivo, gerando um resultado A. Quando o arquivo é recebido pelo destinatário, pode-se aplicar novamente o método gerando um resultado B. Se o resultado A for igual ao resultado B significa que o arquivo está íntegro e não foi modificado; caso contrário, significa que o arquivo teve sua integridade violada. O método criptográfico citado é conhecido como
a) função de hash.
b) criptografia simétrica.
c) esteganografia.
d) criptografia assimétrica.
e) certificação digital.

Uma **função de resumo** é um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado **hash**.

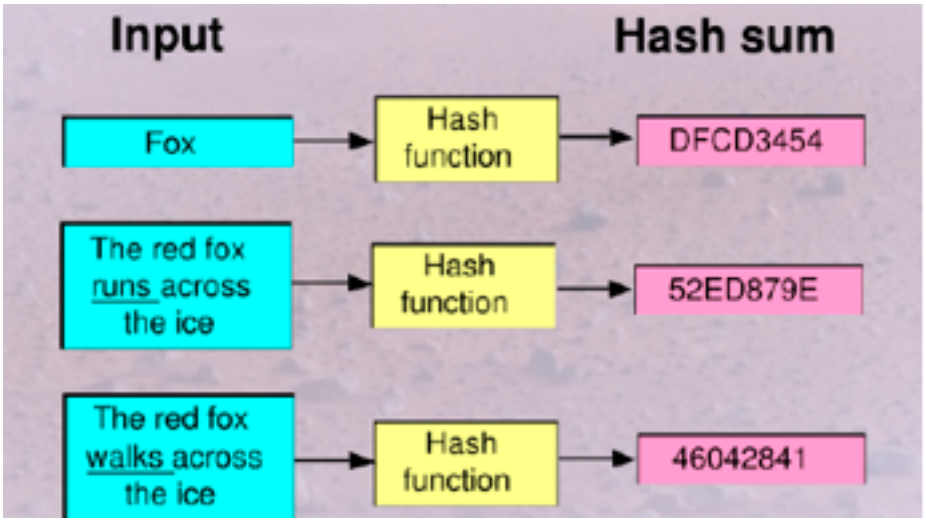


Figura – Exemplos de Saídas da Função Hash

O **hash** é utilizado para:

- verificar a integridade de um arquivo obtido da Internet;
- verificar a integridade de um arquivo armazenado no computador;
- gerar as assinaturas digitais.

Para verificar a **integridade** de um arquivo, por exemplo, 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. Alguns *sites*, além do arquivo em si, também disponibilizam o *hash* correspondente, para que você possa verificar se o arquivo foi corretamente transmitido e gravado.

Letra a.

---

020. (FCC/MANAUSPREV/ANALISTA PREVIDENCIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2015) A criptografia é um dos principais mecanismos de segurança que podem ser usados para se proteger dos riscos associados ao uso da Internet. Em relação a este tema, é correto afirmar que

a) a assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada. A verificação da assinatura é feita com o uso desta chave privada, pois se o texto foi codificado com a chave pública, somente a chave privada correspondente pode decodificá-lo.

b) para contornar a baixa eficiência característica da criptografia de chaves simétricas, a codificação é feita sobre o conteúdo da mensagem, pois é mais rápido codificar a informação toda do que o *hash*.

c) um impostor pode criar uma chave pública falsa para o amigo de uma pessoa e enviá-la para esta pessoa. Ao usá-la para codificar uma informação para este amigo, a pessoa estará codificando-a para o impostor. Uma das formas de impedir que isto ocorra é pelo uso de criptografia simétrica, ou de chave dupla.

d) o certificado digital é um registro eletrônico composto por um conjunto de dados que distingue uma pessoa e associa a ela uma chave privada. É emitido apenas para que pessoas criem sua assinatura digital.

e) a assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada.

a) Errada. A **verificação da assinatura** é feita com o uso da **chave pública do remetente,** pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

b) Errada. CERT.BR (2013) destaca que "para contornar a baixa eficiência característica da criptografia de **chaves assimétricas**, **a codificação é feita sobre o *hash*** e não sobre o conteúdo em si, pois é mais rápido codificar o *hash* (que possui tamanho fixo e reduzido) do que a informação toda".

c) Errada. Chave privada pode ser criada! A criptografia assimétrica ou de chave pública utiliza 2 chaves. A simétrica é de chave única.

Algoritmos:

→ **Simétricos** (ou **convencional**, **chave privada**, **chave única**)

→ **Assimétricos** (ou **chave pública**).

d) Errada. Um certificado digital é um **documento eletrônico que identifica pessoas, físicas ou jurídicas, URLs, contas de usuário, servidores (computadores),** dentre outras entidades. Este "documento" na verdade é uma estrutura de dados que contém a chave pública do seu titular e outras informações de interesse.

Ele contém informações relevantes para a identificação "real" da entidade a que visa certificar (CPF, CNPJ, endereço, nome etc.) e informações relevantes para a aplicação a que se destina.

Quanto aos objetivos do certificado digital podemos destacar:

- transferir a credibilidade que hoje é baseada em papel e conhecimento para o ambiente eletrônico;
- vincular uma chave pública a um titular (eis o objetivo principal).

e) Certa. A assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada (garante que os dados recebidos estão exatamente como foram enviados por uma entidade autorizada, ou seja, não contêm modificação, inserção, exclusão ou repetição).

Letra e.

021. (FCC/TRE-RR/ANALISTA JUDICIÁRIO/ANÁLISE DE SISTEMAS/2015) Um sistema de computador envia uma mensagem para um receptor, acompanhada de um resumo dessa mensagem cifrado com chave privada. O objetivo é garantir que o sistema receptor decifre o resumo com uma chave pública enviada pelo remetente, calcule um novo resumo com base

na mensagem recebida e compare o resultado com a mensagem original para garantir a integridade. Essa função criptográfica é chamada:

a) Criptografia pública cptu.
b) Criptografia privada cptp.
c) Resumo criptográfico hash.
d) Criptografia simétrica simt.
e) Resumo criptográfico gram.

Trata-se da **função de resumo criptográfico *hash***, uma função que relaciona uma mensagem de qualquer tamanho a um valor de *hash* de tamanho fixo, que serve como autenticador (Stallings, 2008).

Letra c.

022. (FCC/TRT-16ª/MA/TÉCNICO JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2014) Considere o texto abaixo.

É a entidade subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Cabe também a esta entidade emitir listas de certificados revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação (DPC). Desempenha como função essencial a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada). Na hierarquia dos Serviços de Certificação Pública, esta entidade está subordinada às entidades de nível hierarquicamente superior.

O texto refere-se à Autoridade

a) Certificadora Raiz (AC Raiz).
b) Gestora de Políticas da ICP-Brasil.
c) de Registro (AR).
d) de Validação de Chaves (AVC).
e) Certificadora (AC).

A **Autoridade Certificadora Raiz da ICP-Brasil (AC-Raiz)** é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, **compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu.** A AC-Raiz também está encarregada de emitir a lista de certificados revogados (LCR) e de fiscalizar e auditar as Autoridades Certificadoras (ACs), Autoridades de

Registro (ARs) e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.

> Conforme destaca http://www.iti.gov.br/index.php/certificacao-digital/autoridades-certificadoras, "*uma **Autoridade Certificadora (AC)** é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, **responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais**. Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do assinante, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada). Cabe também à AC **emitir listas de certificados revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação (DPC).** Além de estabelecer e fazer cumprir, pelas Autoridades Registradoras (ARs) a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada*".

Uma **Autoridade de Registro (AR)** é responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC, tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.

Letra e.

---

023. (FCC/TRT-12ª/SC/TÉCNICO JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2013) O trecho a seguir descreve uma parte do processo de geração de assinatura digital e troca de mensagens assinadas digitalmente: O primeiro passo no processo de assinatura digital de um documento eletrônico é a aplicação da..... que fornece uma sequência única para cada documento conhecida como..... No passo seguinte essa sequência única fornecida é codificada com a chave..... do emissor da mensagem. A consequência disso é a geração de um arquivo eletrônico que representa a assinatura digital dessa pessoa. A partir daí, a assinatura digital gerada é anexada ao material que será enviado eletronicamente, compondo a mensagem ou o documento. As lacunas I, II e III são preenchidas, correta e respectivamente, com:

a) esteganografia, digest, primária
b) criptografia, digest, pública
c) função de Hash, resumo, privada
d) criptografia, message key, privada
e) função de Hash, resumo, pública

O primeiro passo no processo de assinatura digital de um documento eletrônico é a aplicação da **função de *Hash*** que fornece uma sequência única para cada documento conhecida como ***resumo.***

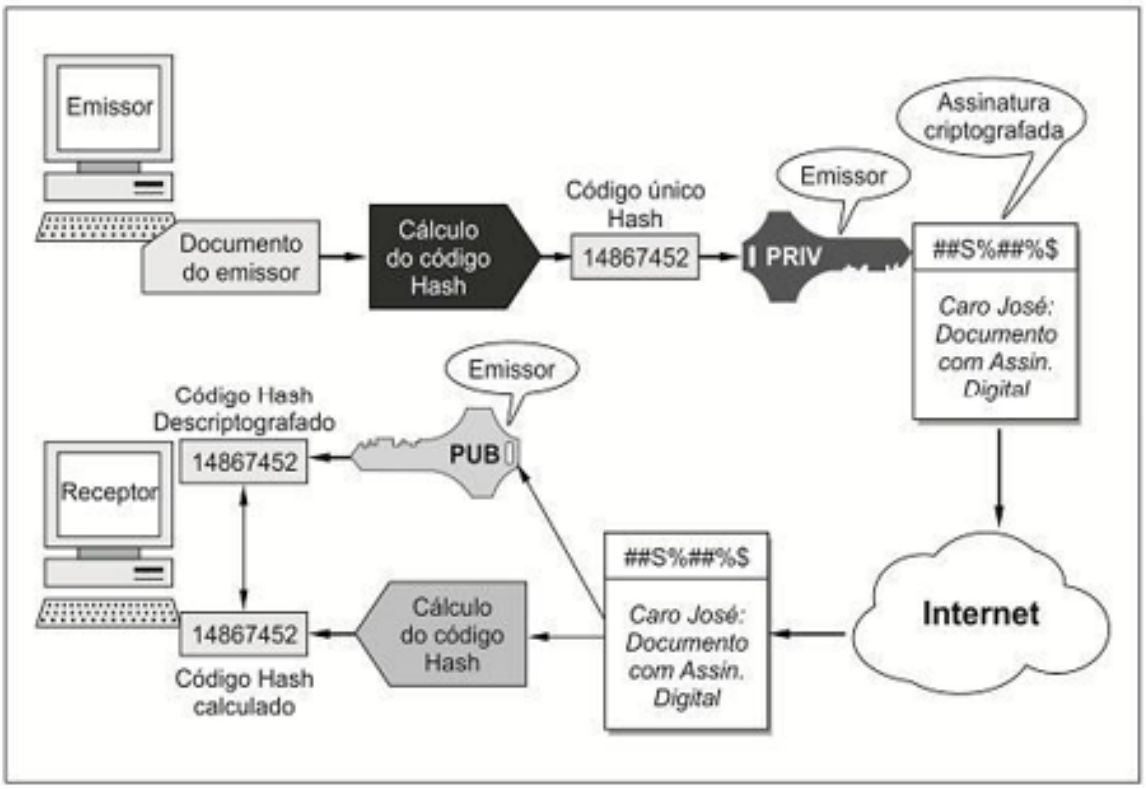
No passo seguinte essa sequência única fornecida é codificada com a chave **privada** do emissor da mensagem. **A consequência disso é a geração de um arquivo eletrônico que representa a assinatura digital dessa pessoa**. A partir daí, a assinatura digital gerada é anexada ao material que será enviado eletronicamente, compondo a mensagem ou o documento.

Obs.: Cert.Br (2013) destaca que o ***hash* é gerado de tal forma que não é possível realizar o processamento inverso para se obter a informação original e que qualquer alteração na informação original produzirá um *hash* distinto**. Apesar de ser teoricamente impossível que informações diferentes gerem *hashes* iguais, a probabilidade de isto ocorrer é bastante baixa.

Letra c.

---

024. (FCC/TRT-2ª/SC/ANALISTA JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO /2013) Considere a figura abaixo.



Em relação aos detalhes mostrados na figura acima, é correto afirmar que

a) a assinatura digital é gerada com base no fato de que apenas o dono conhece a chave pública e que, se ela foi usada para codificar a informação, então apenas seu dono poderia ter feito isto. A verificação da assinatura é feita com o uso da chave privada, pois se o texto foi codificado com a chave pública, somente a chave privada correspondente pode decodificá-lo.

b) para contornar a baixa eficiência característica da criptografia de chaves assimétricas, a codificação é feita sobre o conteúdo em si e não sobre o *hash* gerado, pois é mais rápido codificar a informação que o código *hash*.

c) se trata de um processo que gera um certificado digital autoassinado utilizando criptografia simétrica com função *hash*, no qual o dono e o emissor não são a mesma entidade.
d) se trata de um processo que gera uma assinatura digital utilizando criptografia assimétrica com função *hash*.
e) se trata de um processo que gera uma assinatura digital utilizando criptografia simétrica com função *hash*.

Em relação aos detalhes mostrados na figura é correto afirmar que se trata de um processo que gera uma **assinatura digital** utilizando **criptografia assimétrica** com **função *hash***.
Conforme visto na questão anterior, o primeiro passo no processo de assinatura digital de um documento eletrônico é a aplicação da **função de *Hash,*** que fornece uma sequência única para cada documento conhecida como **resumo**.
No passo seguinte **essa sequência única fornecida é codificada com a chave privada do emissor da mensagem**. A consequência disso é a geração de um arquivo eletrônico que representa a assinatura digital dessa pessoa. A partir daí, a assinatura digital gerada é anexada ao material que será enviado eletronicamente, compondo a mensagem ou o documento.
A verificação da assinatura é feita com o uso da **chave pública**, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.
Pela figura, foi gerado novamente o *hash* da mensagem recebida. 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.
Complementando, temos mais algumas observações:

- Para contornar a baixa eficiência característica da criptografia de chaves assimétricas, a **codificação é feita sobre o hash** e não sobre o conteúdo em si, pois é mais rápido codificar o *hash* (que possui tamanho fixo e reduzido) do que a informação toda;
- **Um certificado autoassinado** é aquele no qual o dono e o emissor são a mesma entidade. Costuma ser usado de duas formas (CERT.BR,2013):
  - **Legítima:** além das ACs raízes, certificados autoassinados também costumam ser usados por instituições de ensino e pequenos grupos que querem prover confidencialidade e integridade nas conexões, mas que não desejam (ou não podem) arcar com o ônus de adquirir um certificado digital validado por uma AC comercial;
  - **Maliciosa:** um atacante pode criar um certificado autoassinado e utilizar, por exemplo, mensagens de *phishing*, para induzir os usuários a instalá-lo. A partir do momento em que o certificado for instalado no navegador, passa a ser possível estabelecer conexões cifradas com *sites* fraudulentos, sem que o navegador emita alertas quanto à confiabilidade do certificado.

Letra d.

025. (FCC/TRT-12ª/SC/TÉCNICO JUDICIÁRIO/TECNOLOGIA DA INFORMAÇÃO/2013) Trabalha com algoritmos que necessitam de pares de chaves, ou seja, duas chaves diferentes para cifrar e decifrar uma informação. A mensagem codificada com a chave 1 de um par somente poderá ser decodificada pela chave 2 deste mesmo par. O método de criptografia e os nomes das duas chaves referenciadas no texto são, respectivamente, criptografia.

a) de curvas elípticas, chave pública e chave de hash.
b) assimétrica, chave pública e chave privada.
c) de chave secreta, chave privada e chave pública.
d) simétrica, chave pública e chave privada.
e) de chave pública, chave primária e chave estrangeira

A **criptografia de chaves aSSimétricas (ou criptografia de chave pública**) **utiliza duas chaves distintas**: uma **pública**, que pode ser livremente divulgada, e uma **privada**, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la.
Dentre as opções da questão, a letra B é a que se encaixa perfeitamente nesse contexto, ao destacar que "a mensagem codificada com a chave 1 (chave pública) de um par somente poderá ser decodificada pela chave 2 (chave privada) deste mesmo par.
Letra b.

026. (FCC/TRT-18ª/GO/TÉCNICO JUDICIÁRIO/ TECNOLOGIA DA INFORMAÇÃO/2013) Fazendo uma analogia com documentos do mundo real, I seria o similar eletrônico do RG, enquanto II, seria o equivalente ao carimbo acompanhado de selo que os cartórios brasileiros utilizam para reconhecer firma em documentos. Juntos, esses dois elementos, aliados à III, garantem a autenticidade, a integridade, o não repúdio à transação e a confidencialidade da informação. Ou seja, as partes são mesmo quem dizem ser e a transação on-line é legítima, autêntica, segura e não sofreu alterações ao longo do caminho.
Preenchem, correta e respectivamente, as lacunas:

a) a assinatura digital - o certificado digital - segurança das informações.
b) a criptografia simétrica - a criptografia assimétrica - certificação digital.
c) o certificado digital - a assinatura digital - criptografia.
d) a criptografia assimétrica - a criptografia simétrica - assinatura digital.
e) a chave pública - a chave privada - criptografia de chave única e à criptografia de chave dupla.

Fazendo uma analogia com documentos do mundo real, **o certificado digital** seria o similar eletrônico do RG, enquanto **a assinatura digital** seria o equivalente ao carimbo acompanhado

de selo que os cartórios brasileiros utilizam para reconhecer firma em documentos. Juntos, esses dois elementos, aliados à **criptografia**, garantem a autenticidade, a integridade, o não repúdio à transação e a confidencialidade da informação. Ou seja, as partes são mesmo quem dizem ser e a transação *on-line* é legítima, autêntica, segura e não sofreu alterações ao longo do caminho.

Letra c.

---

027. (FCC/TJ-PE/ANALISTA JUDICIÁRIO/ANALISTA DE SUPORTE/2012) Sobre criptografia é correto afirmar:

a) Todos os algoritmos de criptografia são baseados na substituição, em que cada elemento do texto claro é mapeado em outro elemento.

b) A técnica para esconder uma mensagem secreta dentro de uma maior, de modo que outros não possam discernir a presença ou o conteúdo da mensagem oculta é conhecida como esteganografia.

c) Um ataque criptoanalítico a um sistema de criptografia envolve a tentativa de cada chave possível até que seja obtida uma tradução inteligível de texto cifrado para texto claro.

d) Se tanto o emissor quanto o receptor utilizarem a mesma chave, o sistema é considerado como criptografia assimétrica ou de chave única.

e) Uma cifra de bloco processa os elementos da entrada continuamente, produzindo a saída de um elemento de cada vez, enquanto prossegue.

Esteganografia (do grego **escrita escondida**) é a capacidade de esconder mensagens secretas em um meio, de maneira que as mesmas passem despercebidas. Um exemplo seria escrever uma carta com tinta invisível.

Em outras palavras, **esteganografia** é o ramo particular da criptologia que consiste em fazer com que uma forma escrita seja camuflada em outra a fim de mascarar o seu verdadeiro sentido.

Ao esconder um arquivo em uma imagem, por exemplo, ao enviá-la para o destinatário desejado, você tem que se assegurar que quem receber a imagem deverá conhecer o método de exibição e a senha utilizada na proteção deste arquivo.

Figura. Esteganografia

Enquanto a criptografia oculta o significado da mensagem, a esteganografia oculta a existência da mensagem.

Letra b.

---

028. (FCC/BANCO CENTRAL DO BRASIL/ANALISTA ÁREA 1/2006) Em uma criptografia, o conceito de força bruta significa uma técnica para

a) eliminar todas as redundâncias na cifra.

b) tornar complexa a relação entre a chave e a cifra.

c) acrescentar aleatoriedade aos dados, tornando maior o caos.

d) quebrar uma criptografia simétrica por meio de busca exaustiva da chave.

e) ocultar uma determinada informação para torná-la imperceptível.

No **ataque por força bruta,** o atacante experimenta cada chave possível em um trecho de texto cifrado, até obter uma tradução inteligível para o texto claro. Em média, metade de todas as chaves possíveis precisam ser testadas para se obter sucesso.

Letra d.

---

029. (VUNESP/SEDUC-SP/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/2014) De acordo com o tipo de segurança desejado, sistemas de criptografia podem utilizar tanto esquemas de chaves simétricas ou assimétricas para a proteção dos dados. A principal diferença desses sistemas tem relação com:

a) o tamanho das chaves, pois os sistemas de chave simétrica necessitam de chaves cujo tamanho seja proporcional ao da informação que será protegida.

b) a velocidade de processamento, pois os sistemas de chave assimétrica são mais rápidos e indicados para servidores que necessitam de alto desempenho.

c) o consumo de memória, pois os sistemas de chave assimétrica exigem menos recursos do sistema.

d) o algoritmo de encriptação e decriptação, que pode utilizar chaves iguais ou diferentes para executar tais operações.

e) o nível de segurança, pois as chaves utilizadas pelos sistemas de chave simétrica são mais fáceis de serem quebradas.

A principal diferença desses sistemas tem relação com o algoritmo de encriptação e decriptação, que pode utilizar chaves iguais ou diferentes para executar tais operações.

Os **algoritmos de Criptografia ASSimétrica (Criptografia de Chave Pública)** utilizam **DUAS** chaves **DIFERENTES**, uma **PÚBLICA** (que pode ser distribuída) e uma **PRIVADA** (pessoal e

intransferível). Assim, nesse método cada pessoa ou entidade mantém duas chaves: uma pública, que pode ser divulgada livremente, e outra privada, que deve ser mantida em segredo pelo seu dono. As mensagens codificadas com a chave pública só podem ser decodificadas com a chave privada correspondente.

A **Criptografia de Chave Simétrica (também chamada de criptografia de chave única, ou criptografia privada, ou criptografia convencional)** uiliza **APENAS UMA** chave para encriptar e decriptar as mensagens. Assim, como só utiliza UMA chave, obviamente ela deve ser compartilhada entre o remetente e o destinatário da mensagem.

Criptografia Simétrica	Criptografia Assimétrica
Usa uma única chave para encriptar e decriptar mensagens.	Usa chaves diferentes para encriptar e decriptar mensagens.
A chave tem que ser compartilhada entre os usuários que irão se comunicar.	Apenas a chave de encriptação é compartilhada (pública). A chave de decriptação é mantida em segredo (privada) com seu titular.
Existe apenas uma única chave para todos os envolvidos na comunicação.	Cada usuário que irá se comunicar possui um par de chaves próprio.
Os processos de encriptação e decriptação são simples (exigem pouco processamento) – ideal para grandes quantidades de dados.	Os processos são mais lentos (exigem mais cálculos dos processadores) – viável apenas em pequenas quantidades de dados.
É mais suscetível a quebras de segredo da chave; Ataques de força bruta é a mais indicada forma de quebrar a chave (descobri-la).	É praticamente impossível quebrar as chaves atuais em tempo suficientemente hábil (nem mesmo usando vários computadores reunidos).
Principais algoritmos: DES: Chaves de 40 e 56 bits 3DES: Chaves de 168 bits AES: Chaves de 256 bits.	Principal algoritmo: RSA: Chaves de 256 bits, 512, 1024 e até 2048 bits (Governo dos EUA).

Letra d.

---

030. (FCC/TJ-AP/ANALISTA JUDICIÁRIO/ÁREA APOIO ESPECIALIZADO/TECNOLOGIA DA INFORMAÇÃO/ADMINISTRAÇÃO EM REDES DE COMPUTADORES/2014) Um Analista de TI do Tribunal de Justiça recebeu a incumbência de planejar e implementar um esquema de criptografia de Chave Pública para a troca de informações entre as duas comarcas de Macapá. Dentre os diferentes algoritmos existentes, ele deve escolher o

a) AES.
b) RC6.
c) DES.
d) IDEA.
e) RSA.

O algoritmo de chave pública (criptografia assimétrica) a ser escolhido é o RSA. AES, DES, IDEA, RC6 são algoritmos de chave privada (criptografia simétrica).
Letra e.

031. (FGV/CM CARUARU/ANALISTA LEGISLATIVO/INFORMÁTICA/2015) Em relação ao tema criptografia, analise as afirmativas a seguir.

I – Assinatura digital consiste na codificação de um texto com uma chave privada e na decodificação desse texto com a chave pública correspondente.
II – Certificados digitais são gerados com base em criptografia simétrica.
III – Certificados digitais no formato X.509 são usados principalmente nos modelos de chave pública baseados em teia de confiança.

Assinale:
a) se somente a afirmativa I estiver correta.
b) se somente a afirmativa II estiverem corretas.
c) se somente a afirmativa III estiverem corretas.
d) se somente a afirmativa I e II estiverem corretas.
e) se somente a afirmativa I e III estiverem corretas.

I – Certo. **A assinatura digital consiste na criação de um código, através da utilização de uma chave privada**, de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada. **A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo** (CERT.BR,2013).
II – Errado. A criptografia assimétrica será utilizada.
III – Errado**.** Os certificados, em geral, são emitidos segundo o padrão ITUT X.509, facilitando a compatibilidade entre as aplicações que os aceitam. Para se fazer a certificação de uma assinatura digital, é necessária uma infraestrutura que valide o certificado para as demais entidades. Para isso, existem dois modelos de certificação que podem ser utilizados. São eles:

- **Modelo de malha de confiança**: baseado na criação de uma rede em que as entidades pertencentes devem confiar umas nas outras. Cada vez que um usuário obtém a

chave pública de outro usuário, ele pode verificar a assinatura digital da chave obtida por meio das demais entidades, garantindo a certeza de que a chave é a verdadeira. **Nesse modelo, a confiança é controlada pelo próprio usuário**. Além disso, a confiança **não** é transitiva, ou seja, se uma entidade A confia em B e B confia em C, isso não significa necessariamente que A confia em C. Esse modelo é utilizado no software PGP, que faz a certificação de mensagens eletrônicas;

- **Modelo hierárquico**: baseado na montagem de uma hierarquia de Autoridades Certificadoras (**ACs**). As ACs certificam os usuários e existe uma autoridade certificadora raiz (**AC-Raiz**) que faz a certificação de todas as ACs de sua jurisdição. Nesse modelo, os certificados digitais precisam da assinatura digital de uma AC para ser válido. Caso alguma entidade duvide de sua validade, basta consultar na AC para verificar se o certificado não foi revogado. Caso haja dúvida da validade do certificado da AC, basta conferir na AC-Raiz, que, em regra, possui um certificado assinado por si mesmo e é mantida por uma entidade governamental. **Esse é o modelo utilizado para a montagem de Infraestruturas de Chaves Públicas (ICPs).**

Portanto, somente a afirmativa I está correta.

Letra a.

---

032. (IDECAN/AGU/ADMINISTRADOR/2014) O recurso que estuda os princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, com o objetivo de dificultar a leitura de pessoas não autorizadas, denomina-se

a) Backup.
b) Webgrafia.
c) criptografia.
d) quarentena.
e) endereçamento.

A palavra **criptografia** é composta dos termos gregos KRIPTOS (secreto, oculto, ininteligível) e GRAPHO (escrita, escrever). Trata-se de um conjunto de conceitos e técnicas que **visa codificar uma informação de forma que somente o emissor e o receptor possam acessá-la**.

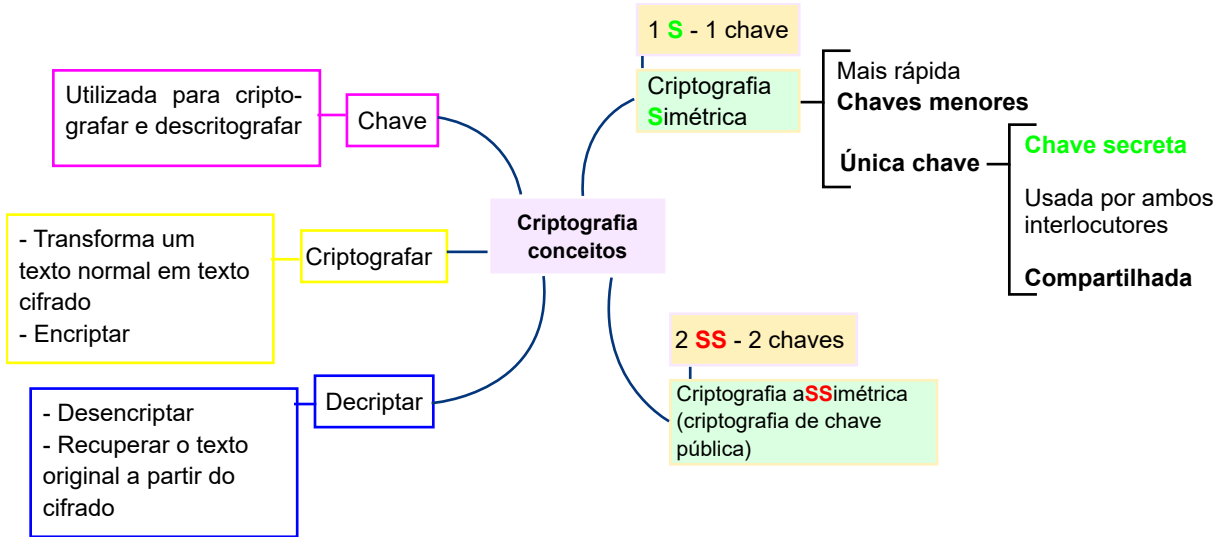


Figura – Mapa Mental Criptografia (Quintão, 2020)

Letra c.

033. (FGV/SUSAM/ANALISTA DE SISTEMAS/2014) Com relação aos princípios de criptografia, analise as afirmativas a seguir.

I – Na criptografia simétrica, a mesma chave é utilizada para encriptar e decriptar a mensagem, devendo a mesma ser acordada entre o transmissor e o receptor.

II – A criptografia assimétrica dá origem à figura das chaves pública e privada.

III – Da mesma forma que na criptografia simétrica, na assimétrica é necessário um acordo prévio de chaves entre o transmissor e o receptor.

Assinale:

a) se somente a afirmativa I estiver correta.

b) se somente a afirmativa II estiver correta.

c) se somente a afirmativa III estiver correta.

d) se somente as afirmativas I e II estiverem corretas.

e) se todas as afirmativas estiverem corretas.

I – Certo. Na criptografia simétrica o emissor e o receptor utilizam a mesma chave para cifrar e decifrar uma informação, devendo a mesma ser acordada entre o transmissor e o receptor.

II – Certo. Chaves assimétricas funcionam com duas chaves: a chave privada e a chave pública. Nesse esquema, uma pessoa ou uma organização deve utilizar uma chave de codificação e disponibilizá-la a quem for mandar informações a ela. Essa é a chave pública. Uma outra chave deve ser usada pelo receptor da informação para o processo de decodificação: é a chave

privada, que é sigilosa e individual. As chaves são geradas de forma conjunta, portanto, uma está associada à outra.

III – Errado. A criptografia assimétrica funciona com duas chaves!

Letra d.

---

034. (FGV/SUSAM/ANALISTA DE SISTEMAS/2014) Um certificado digital é um arquivo de dados contendo segmentos ou seções que possuem informações obrigatórias e adicionais armazenada em extensões. A utilização de certificados digitais permite que sejam agregados requisitos de segurança na tramitação de informações. Dentre esses requisitos, está a garantia da impossibilidade de que o autor recuse a autoria.

Esse é o requisito de

a) integridade.

b) não repúdio.

c) privacidade.

d) autenticidade.

e) sigilo.

Com o não repúdio (irretratabilidade) o emissor (aquele que assinou digitalmente a mensagem) não pode negar que foi o autor da mensagem, ou seja, não pode dizer mais tarde que a sua assinatura foi falsificada.

Letra b.

---

035. (FGV/DPE-RJ/TÉCNICO SUPERIOR ESPECIALIZADO/REDE DE COMPUTADORES/2014) Após a revogação de um certificado digital

a) o certificado deixa de funcionar porque a chave privada não é mais fornecida pela autoridade de registro.

b) a chave pública do certificado é modificada de modo a não haver mais relação matemática com a respectiva chave privada.

c) a autoridade certificadora remove a sua assinatura digital do certificado, tornando-o inválido para uso.

d) o período de validade do certificado é antecipado para a data de revogação.

e) o certificado é adicionado à lista de certificados revogados (crl)

Após a revogação de um certificado digital o certificado é adicionado à **lista de certificados revogados** (LCR ou CRL - *Certificate Revocation List*). A CRL é uma estrutura de dados que

contém a lista de certificados revogados por uma determinada AC. Segundo ITI, essa lista, geralmente, indica o nome de quem a emite, a data de emissão e a data da próxima emissão programada, além dos números de série dos certificados revogados e a data da revogação.

Letra e.

---

036. (FGV/SEFAZ-RJ/FISCAL DE RENDAS/2010) Chaves simétricas são simples e nelas o emissor e o receptor utilizam a mesma chave para cifrar e decifrar uma informação, acarretando riscos menores, diminuindo consideravelmente as possibilidades de extravio ou fraudes. É por esta razão que chaves públicas são utilizadas em assinaturas digitais.

Na **Criptografia Simétrica (ou Convencional, Chave Privada, Chave Única)** o emissor e o receptor fazem uso da **MESMA** chave, isto é, uma ÚNICA chave é usada na codificação e na decodificação da informação.

Figura – Criptografia Simétrica – Encriptar

Figura – Criptografia Simétrica – Decriptar

Nas 2 figuras anteriores, podemos observar o funcionamento da criptografia simétrica. Uma informação é encriptada através de um polinômio utilizandose de uma chave (Chave A) que também serve para decriptar a informação.

As principais vantagens dos algoritmos simétricos são:

- **Rapidez**: um polinômio simétrico encripta um texto longo em milésimos de segundos;
- **Chaves pequenas**: uma chave de criptografia de 128bits torna um algoritmo simétrico praticamente impossível de ser quebrado.

A maior **desvantagem** da criptografia simétrica é que a **chave utilizada para encriptar é IGUAL à chave que decripta**. Quando um grande número de pessoas tem conhecimento da chave, a informação deixa de ser um segredo.

O uso de chaves simétricas tem algumas desvantagens, fazendo com que sua utilização não seja adequada em situações em que a informação é muito valiosa. Para começar, é necessário usar uma grande quantidade de chaves caso muitas pessoas estejam envolvidas.

Ainda, há o fato de que tanto o emissor quanto o receptor precisam conhecer a chave usada. A transmissão dessa chave de um para o outro pode não ser tão segura e cair em "mãos erradas". Existem vários algoritmos que usam chaves simétricas, como o **DES** (Data Encryption Standard), o **IDEA** (*International Data Encryption Algorithm*), e o **RC** (*Ron's Code ou Rivest Cipher*).
Finalizando, a assertiva A é indevida já que afirma que os riscos são menores ao se utilizar chaves **S**imétricas, o que não é verdade. **Como existe apenas uma chave, ela deverá ser conhecida por todos os destinatários, aumentando o risco de extravio ou fraudes.** Em assinaturas digitais são utilizadas as chaves públicas (ou de criptografia a**SS**imétrica).
Errado.

---

037. (FGV/SEFAZ-RJ/FISCAL DE RENDAS/2010) Chaves assimétricas funcionam com duas chaves: a chave privada e a chave pública. Nesse esquema, uma pessoa ou uma organização deve utilizar uma chave de codificação e disponibilizá-la a quem for mandar informações a ela. Essa é a chave pública. Uma outra chave deve ser usada pelo receptor da informação para o processo de decodificação: é a chave privada, que é sigilosa e individual. As chaves são geradas de forma conjunta, portanto, uma está associada à outra.

A técnica de criptografia conhecida como "chave pública" (ou aSSimétrica) trabalha com **DUAS chaves**: **uma denominada privada e outra denominada pública**. Nesse método, uma pessoa deve criar uma chave de codificação e enviá-la a quem for mandar informações a ela. Essa é a chave pública. Outra chave deve ser criada para a decodificação. Esta – a chave privada – é secreta.

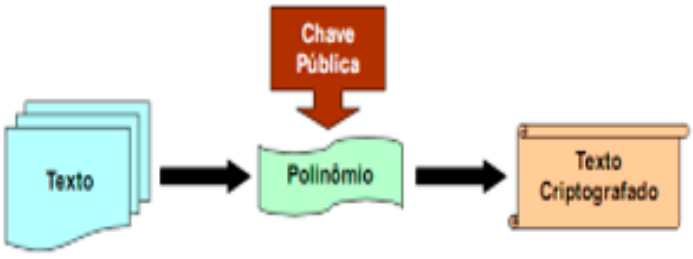


Figura – Criptografia Assimétrica – Encriptar

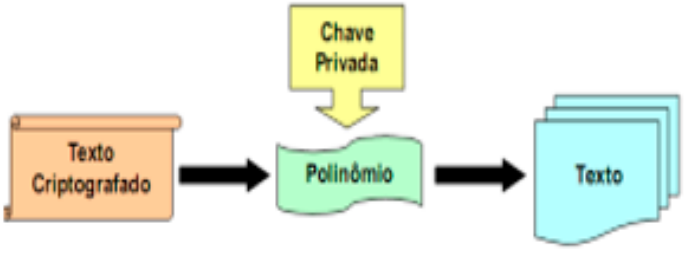


Figura – Criptografia Assimétrica – Decriptar

Entre os algoritmos que usam chaves assimétricas, têm-se o RSA (o mais conhecido), o Diffie-Hellman, o DSA (*Digital Signature Algorithm*), o Schnorr (praticamente usado apenas em assinaturas digitais) e DiffieHellman.

Certo.

---

038. (ESAF/AFRFB/2005) Analise as seguintes afirmações relacionadas à Segurança da Informação.

I – Um plano de contingência consiste em procedimentos de recuperação preestabelecidos, com a finalidade de minimizar o impacto sobre as atividades da organização no caso de ocorrência de um dano ou desastre que os procedimentos de segurança não consigam evitar.

II – Entende-se por Política de Segurança um conjunto de regras que pode ser aplicado a qualquer empresa, que não necessite de processos de revisão e que possa atuar de forma independente em qualquer setor desta empresa.

III – Um Proxy Server é um sistema que atua como intermediário entre duas pontas de uma conexão, evitando a comunicação direta entre elas.

IV – A segurança da informação de uma organização deve ser de exclusiva responsabilidade do setor de segurança, deve ter uma estrutura de segurança estática e, uma vez implementada, todas as informações serão consideradas seguras.

Indique a opção que contenha todas as afirmações verdadeiras.

a)I e II
b) II e III
c) III e IV
d) II e IV
e) I e III

I – Certo. A **política de segurança** deve assegurar a existência de um plano de contingência capaz de orientar todo o processo de restauração parcial ou total do ambiente de sistemas, incluindo também as atividades de teste e manutenção do documento. Em seu conteúdo devem ser abordados diversos aspectos com relação à avaliação de risco e impacto no negócio. A política deve ressaltar que, o plano a ser desenvolvido, resultará num conjunto de documentos onde estarão registradas as ações relativas às adequações da infraestrutura e às alterações nos procedimentos.

II – Errado. A política de segurança deve ser revisada e atualizada sempre que necessário. Deve haver análise periódica da efetividade da política, demonstrada pelo tipo, volume e impacto dos incidentes de segurança registrados!

III – Certo. O Proxy Server pode gerenciar gerencia o tráfego da Internet de/para uma rede local e pode oferecer outros recursos, como o cache de documentos e o controle de acesso.

IV – Errado. Que absurdo!!! “A segurança é responsabilidade de todos nós”, eu até uso essa frase em campanhas de segurança dentro da empresa em que trabalho. A estrutura é bem dinâmica, e obter 100% de segurança é uma utopia!

Letra e.

GABARITO

1. c
2. d
3. e
4. a
5. d
6. c
7. c
8. c
9. e
10. e
11. c
12. e
13. d
14. d
15. e
16. b
17. c
18. b
19. a
20. e
21. c
22. e
23. c
24. d
25. b
26. c
27. b
28. d
29. d
30. e
31. a
32. c
33. d
34. b
35. e
36. e
37. c
38. e

REFERÊNCIAS

CERTBR. **Cartilha de Segurança para Internet**. Versão 4.0. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. 2012.

ALBUQUERQUE, R.; RIBEIRO, B. **Segurança no Desenvolvimento de Software**. Rio de Janeiro: Campus, 2002.

GEUS, Paulo Lício; NAKAMURA, Emilio Tissato. **Segurança de Redes em Ambiente Corporativos**. São Paulo: Novatec, 2007.

MAUSER, D; Diógenes, y. **Certificação Security +** - 2ª edição. 2013.

QUINTÃO, PATRÍCIA LIMA**. Tecnologia da Informação para Concursos.** 2020.

QUINTÃO, PATRÍCIA LIMA**. Informática para Concursos.** 2020.

QUINTÃO, PATRÍCIA LIMA. **Informática-FCC-Questões Comentadas e Organizadas por Assunto**, 3ª. Edição. Ed. Gen/Método, 2014**.**

QUINTÃO, PATRÍCIA LIMA. **1001 Questões Comentadas de Informática Cespe**, 2ª. Edição. Ed. Gen/Método, 2017.

RAMOS, A.; BASTOS, A.; LAYRA, A. **Guia Oficial para Formação de Gestores em Segurança da Informação**. 1. ed. Rio Grande do Sul: ZOUK. 2006.

STALLINGS, W., **Criptografia e Segurança de Redes: Princípios e Práticas**., 4. ed. São Paulo: Pearson Prentice-Hall, 2008.

SCHNEIER, B., **Applied Cryptography: Protocols, Algorithms and Source Code in C**. 2. ed. John Wiley & Sons, 1996.

Patrícia Quintão

Mestre em Engenharia de Sistemas e computação pela COPPE/UFRJ, Especialista em Gerência de Informática e Bacharel em Informática pela UFV. Atualmente é professora no Gran Cursos Online; Analista Legislativo (Área de Governança de TI), na Assembleia Legislativa de MG; Escritora e Personal & Professional Coach.

Atua como professora de Cursinhos e Faculdades, na área de Tecnologia da Informação, desde 2008. É membro: da Sociedade Brasileira de Coaching, do PMI, da ISACA, da Comissão de Estudo de Técnicas de Segurança (CE-21:027.00) da ABNT, responsável pela elaboração das normas brasileiras sobre gestão da Segurança da Informação.

Autora dos livros: Informática FCC - Questões comentadas e organizadas por assunto, 3ª. edição e 1001 questões comentadas de informática (Cespe/UnB), 2ª. edição, pela Editora Gen/Método.

Foi aprovada nos seguintes concursos: Analista Legislativo, na especialidade de Administração de Rede, na Assembleia Legislativa do Estado de MG; Professora titular do Departamento de Ciência da Computação do Instituto Federal de Educação, Ciência e Tecnologia; Professora substituta do DCC da UFJF; Analista de TI/Suporte, PRODABEL; Analista do Ministério Público MG; Analista de Sistemas, DATAPREV, Segurança da Informação; Analista de Sistemas, INFRAERO; Analista - TIC, PRODEMGE; Analista de Sistemas, Prefeitura de Juiz de Fora; Analista de Sistemas, SERPRO; Analista Judiciário (Informática), TRF 2ª Região RJ/ES, etc.

@coachpatriciaquintao **/profapatriciaquintao**

@plquintao **t.me/coachpatriciaquintao**