Aula 00 - (Prof. Diego Carvalho e Renato da Costa)

ISS-Porto Alegre (Auditor Fiscal da Receita Municipal) Tecnologia da Informação - 2024 (Pós-Edital)

Autor:
Diego Carvalho, Emannuelle Gouveia Rolim, Equipe Informática 2 (Diego Carvalho), Equipe Informática e TI, Paolla Ramos, Renato da Costa

05 de Agosto de 2024

Índice

APRESENTAÇÃO DO PROFESSOR

PROF. DIEGO CARVALHO

FORMADO EM CIÊNCIA DA COMPUTAÇÃO PELA UNIVERSIDADE DE BRASÍLIA (UNB), PÓS-GRADUADO EM GESTÃO DE TECNOLOGIA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA E, ATUALMENTE, AUDITOR FEDERAL DE FINANÇAS E CONTROLE DA SECRETARIA DO TESOURO NACIONAL.

ESTRATÉGIA CONCURSOS

PROFESSOR DIEGO CARVALHO - WWW.INSTAGRAM.COM/PROFESSORDIEGOCARVALHO

Sobre o curso: galera, todos os tópicos da aula possuem Faixas de Incidência, que indicam se o assunto cai muito ou pouco em prova. Diego, se cai pouco para que colocar em aula? Cair pouco não significa que não cairá justamente na sua prova! A ideia aqui é: se você está com pouco tempo e precisa ver somente aquilo que cai mais, você pode filtrar pelas incidências média, alta e altíssima; se você tem tempo sobrando e quer ver tudo, vejam também as incidências baixas e baixíssimas. *Fechado?*

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

INCIDÊNCIA EM PROVA: BAIXA

INCIDÊNCIA EM PROVA: MÉDIA

INCIDÊNCIA EM PROVA: ALTA

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Além disso, essas faixas não são por banca – é baseado tanto na quantidade de vezes que caiu em prova independentemente da banca quanto nas minhas próprias avaliações sobre cada assunto.

#ATENÇÃO

Avisos Importantes

O curso abrange todos os níveis de conhecimento...

Esse curso foi desenvolvido para ser acessível a **alunos com diversos níveis de conhecimento diferentes.** Temos alunos mais avançados que têm conhecimento prévio ou têm facilidade com o assunto. Por outro lado, temos alunos iniciantes, que nunca tiveram contato com a matéria ou até mesmo que têm trauma dessa disciplina. A ideia aqui é tentar atingir ambos os públicos - iniciantes e avançados - da melhor maneira possível..

Por que estou enfatizando isso?

O **material completo** é composto de muitas histórias pessoais, exemplos, metáforas, piadas, memes, questões, desafios, esquemas, diagramas, imagens, entre outros. Já o **material simplificado** possui exatamente o mesmo núcleo do material completo, mas ele é menor e mais objetivo. *Professor, eu devo estudar por qual material?* Se você quiser se aprofundar nos assuntos ou tem dificuldade com a matéria, necessitando de um material mais passo-a-passo, utilize o material completo. Se você não quer se aprofundar nos assuntos ou tem facilidade com a matéria, necessitando de um material mais direto ao ponto, utilize o material simplificado.

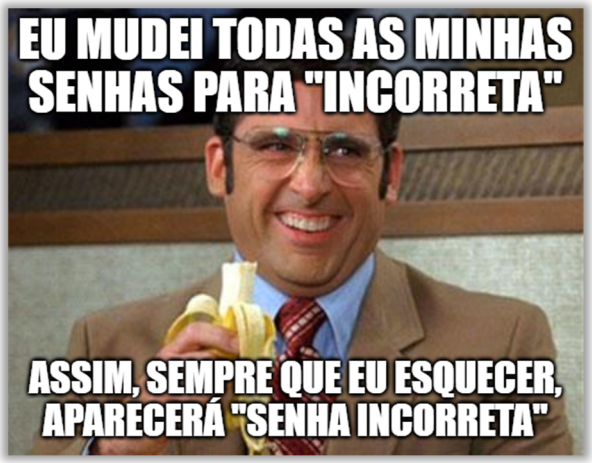
Por fim...

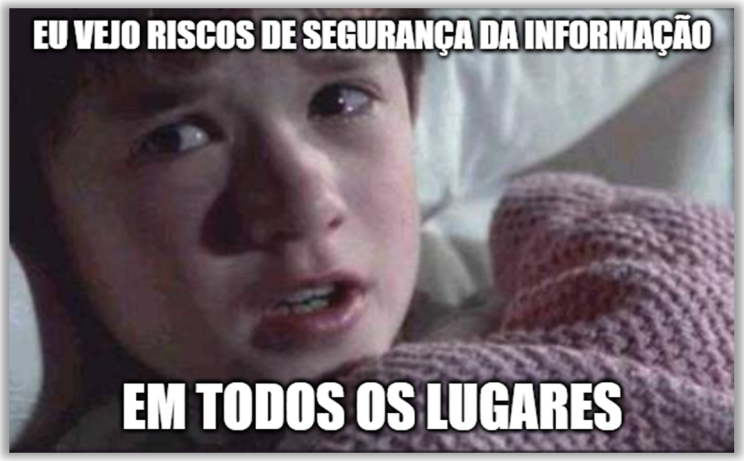
O curso contém diversas questões espalhadas em meio à teoria. Essas questões possuem um comentário mais simplificado porque **têm o único objetivo de apresentar ao aluno como bancas de concurso cobram o assunto previamente administrado**. A imensa maioria das questões para que o aluno avalie seus conhecimentos sobre a matéria estão dispostas ao final da aula na lista de exercícios e **possuem comentários bem mais abrangentes**.

APRESENTAÇÃO DA AULA

Pessoal, o tema da nossa aula é: **Segurança da Informação**. Nós vamos ver os conceitos básicos, terminologias e princípios fundamentais. Depois vamos entender mais sobre criptografia, assinatura digital e certificação digital. Esses são assuntos que estão no dia-a-dia de vocês mesmo que vocês não percebam. *Quem aí não viu as tretas que rolaram com hackeamento de celulares recentemente na política brasileira?* Pois é, ninguém está imune...

PROFESSOR DIEGO CARVALHO - WWW.INSTAGRAM.COM/PROFESSORDIEGOCARVALHO





Galera, todos os tópicos da aula possuem Faixas de Incidência, que indicam se o assunto cai muito ou pouco em prova. *Diego, se cai pouco para que colocar em aula?* Cair pouco não significa que não cairá justamente na sua prova! A ideia aqui é: se você está com pouco tempo e precisa ver somente aquilo que cai mais, você pode filtrar pelas incidências média, alta e altíssima; se você tem tempo sobrando e quer ver tudo, vejam também as incidências baixas e baixíssimas. *Fechado?*

INCIDÊNCIA EM PROVA: BAIXÍSSIMA
INCIDÊNCIA EM PROVA: BAIXA
INCIDÊNCIA EM PROVA: MÉDIA
INCIDÊNCIA EM PROVA: ALTA
INCIDÊNCIA EM PROVA: ALTÍSSIMA

Além disso, essas faixas não são por banca – é baseado tanto na quantidade de vezes que caiu em prova independentemente da banca e também em minhas avaliações sobre cada assunto...

#ATENÇÃO

Avisos Importantes

O curso abrange todos os níveis de conhecimento...

Esse curso foi desenvolvido para ser acessível a **alunos com diversos níveis de conhecimento diferentes.** Temos alunos mais avançados que têm conhecimento prévio ou têm facilidade com o assunto. Por outro lado, temos alunos iniciantes, que nunca tiveram contato com a matéria ou até mesmo que têm trauma dessa disciplina. A ideia aqui é tentar atingir ambos os públicos - iniciantes e avançados - da melhor maneira possível..

Por que estou enfatizando isso?

O **material completo** é composto de muitas histórias, exemplos, metáforas, piadas, memes, questões, desafios, esquemas, diagramas, imagens, entre outros. Já o **material simplificado** possui exatamente o mesmo núcleo do material completo, mas ele é menor e bem mais objetivo. *Professor, eu devo estudar por qual material?* Se você quiser se aprofundar nos assuntos ou tem dificuldade com a matéria, necessitando de um material mais passo-a-passo, utilize o material completo. Se você não quer se aprofundar nos assuntos ou tem facilidade com a matéria, necessitando de um material mais direto ao ponto, utilize o material simplificado.

Por fim...

O curso contém diversas questões espalhadas em meio à teoria. Essas questões possuem um comentário mais simplificado porque **têm o único objetivo de apresentar ao aluno como bancas de concurso cobram o assunto previamente administrado**. A imensa maioria das questões para que o aluno avalie seus conhecimentos sobre a matéria estão dispostas ao final da aula na lista de exercícios e **possuem comentários bem mais completos, abrangentes e direcionados.**

SEGURANÇA DA INFORMAÇÃO

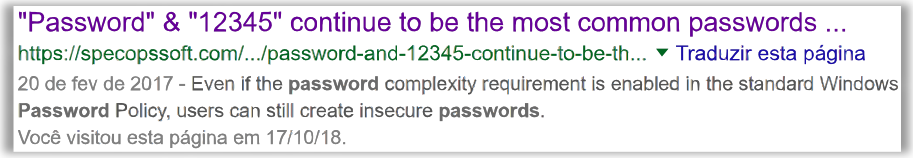
Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXA

Galera, uma **rotina comum** na vida de várias pessoas é: acordar, tomar um banho, escovar os dentes, comer alguma coisa, sair de casa, entrar no carro, chegar na firma, guardar suas coisas na gaveta e finalmente trabalhar. No fim do dia, você abre sua gaveta, pega as suas coisas e vai embora para casa. *Não é mais ou menos assim?* No entanto, há alguns detalhes que não falamos sobre essa rotina!

Ao sair, vocês por acaso deixam a porta de casa destrancada? Vocês deixam uma fresta na janela? Vocês não usam alarme no carro? Vocês deixam seu cofre aberto? Bem, eu espero que vocês tenham respondido um sonoro **não** para todas essas perguntas! Por favor :) *E por que vocês trancam a porta, fecham as janelas, utilizam alarmes no carro e trancam seus cofres com chave?* **Porque vocês possuem ativos de valor que desejam proteger**!

Ninguém quer ter casa, carro ou quaisquer itens pessoais furtados. Por conta disso, vocês tomam várias precauções: colocam uma fechadura melhor, utilizam alarme automotivo, entre outros.


"Password" & "12345" continue to be the most common passwords ...
https://specopssoft.com/.../password-and-12345-continue-to-be-th... ▾ Traduzir esta página
20 de fev de 2017 - Even if the **password** complexity requirement is enabled in the standard Windows **Password** Policy, users can still create insecure **passwords**.
Você visitou esta página em 17/10/18.

Agora, vocês já notaram que – quando se trata de informação – nós somos bem mais negligentes e muito menos cuidadosos? Vejam a notícia acima: ela afirma que, em 2017, as senhas mais comuns do planeta ainda eram "password" e "12345". Pois é, **as pessoas não têm a mesma precaução na hora de proteger suas informações quanto têm na hora de proteger seus objetos**. Assim fica fácil até para um hacker relativamente habilidoso...

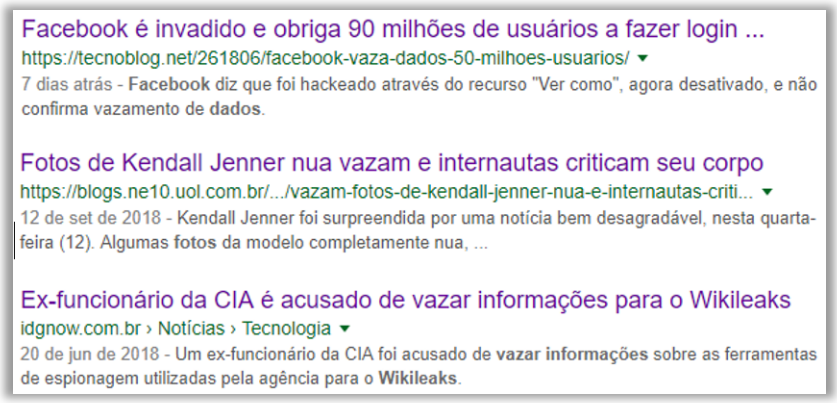
LISTA DE SENHAS MAIS UTILIZADAS DE 2017				
12345	123456789	admin	starwars	hello
password	letmein	welcome	123123	freedom
12345678	1234567	monkey	dragon	whatever
qwerty	football	Login	password	qazwsx
123456	iloveyou	abc123	master	trustno1

Claro que nem toda informação é relevante ao ponto de necessitar de várias barreiras de segurança. Você eventualmente não precisa colocar uma senha no computador de casa ou pagar caro por um antivírus poderoso. Analogamente, se você mora em um bairro tranquilo da Suíça, dificilmente necessitará de alarme no carro ou trancar a porta de casa. Por outro lado, se você mora em um bairro perigoso de Honduras, é recomendável possuir várias barreiras de segurança.

De toda forma, nós estamos na era digital! Como a imagem acima apresenta, a humanidade armazena e acessa trilhões de informações todos os dias por meio de diversos meios diferentes, **como computadores, celulares, conversas ou documentos**. *Vocês sabiam que o conteúdo digital produzido no mundo dobra em quantidade a cada dois anos?* Em 2020, devemos ter mais de 44 trilhões de gigabytes de informações digitais.

Por conta disso, as organizações gastam grande parte de seus orçamentos em equipamentos capazes de coletar, processar, analisar e disseminar dados de forma segura. Hoje em dia, a informação é a principal fonte de renda dos negócios, logo precisa estar adequadamente assegurada. Galera, acreditem em mim: informação é dinheiro! Isso vale tanto para um banco quanto para uma padaria da esquina...

Vejam as notícias seguintes: informações vazam basicamente todos os dias tanto de empresas (Facebook), quanto de pessoas (Kendall Jenner), quanto de órgãos públicos (CIA). **Logo, não são só as instituições que devem ter cuidado, todos nós devemos ser mais diligentes com as informações que possuímos**. *Bacana?* Dito isso, vamos ver na tabela seguinte também algumas definições de Segurança da Informação...

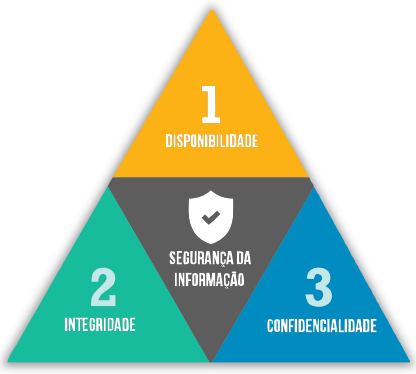


DEFINIÇÕES DE SEGURANÇA DA INFORMAÇÃO
Proteção de informações e de sistemas de informações contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados.
Salvaguarda de dados organizacionais contra acesso não autorizado ou modificação para assegurar sua disponibilidade, confidencialidade e integridade.
Conjunto de estratégias para gerenciar processos, ferramentas e políticas necessárias para prevenir, detectar, documentar e combater ameaças às informações organizacionais.

O Decreto Nº 9.637 da Presidência da República, que institui a Política Nacional de Segurança da Informação (PNSI) nos órgãos e entidades da Administração Pública Federal busca:

> *"Assegurar a disponibilidade, integridade, a confidencialidade e a autenticidade da informação a nível nacional. Para os fins do disposto neste Decreto, a segurança da informação abrange: I – a segurança cibernética; II – a defesa cibernética; III – a segurança física e a proteção de dados organizacionais; e IV – as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação".*

Já a literatura acadêmica afirma que existe uma trindade sagrada da segurança da informação. São três princípios (também chamados de propriedades ou atributos): **Confidencialidade**, **Integridade** e **Disponibilidade** – conhecidos pela sigla **CID**.



Se um ou mais desses princípios forem desrespeitados em algum momento, significa que houve um incidente de segurança da informação (apesar de a figura ao lado apresentar uma pirâmide numerada, não existe hierarquia entre os princípios).

Vamos ver esses princípios em detalhes mais à frente, mas basicamente a **confidencialidade** é o princípio de que a informação não esteja disponível ou seja revelada a indivíduos, entidades ou processos não autorizados; a **integridade** é o princípio de salvaguarda da exatidão e completeza de ativos de informação; e a **disponibilidade** é o princípio da capacidade de estar acessível e utilizável quando demandada por uma entidade autorizada.

Controles de Segurança

INCIDÊNCIA EM PROVA: BAIXA

Galera, selecionar e implementar controles de segurança adequados inicialmente pode ajudar uma organização a reduzir seus riscos a níveis aceitáveis. A seleção de possíveis controles deve se basear na avaliação de riscos. Os controles podem variar em natureza, mas – fundamentalmente – são formas de proteger a confidencialidade, integridade ou disponibilidade de informações. **Em geral, eles são divididos em dois tipos**[1]:

CONTROLES FÍSICOS	São barreiras que impedem ou limitam o acesso físico direto às informações ou à infraestrutura que contém as informações. Ex: portas, trancas, paredes, blindagem, vigilantes, geradores, sistemas de câmeras, alarmes, catracas, cadeados, salas-cofre, alarmes de incêndio, crachás de identificação, entre outros.
CONTROLES LÓGICOS	Também chamados de controles técnicos, são barreiras que impedem ou limitam o acesso à informação por meio do monitoramento e controle de acesso a informações e a sistemas de computação. Ex: senhas, firewalls, listas de controle de acesso, criptografia, biometria[2], IDS, IPS, entre outros.

É importante destacar que o tipo de controle se dá em razão do recurso e, não, do método de autenticação. *Como assim, Diego?* Se o recurso a ser acessado for físico (Ex: entrar em uma casa), trata-se de um controle físico; se o recurso a ser acessado for lógico (Ex: logar em um sistema), trata-se de um controle lógico. **Dessa forma, alguns dos exemplos apresentados acima podem variar entre controle físico ou lógico dependendo do recurso acessado.**

(TRT/10 – 2013) Os mecanismos utilizados para a segurança da informação consistem em controles físicos e controles lógicos. Os controles físicos constituem barreiras de hardware, enquanto os lógicos são implementados por meio de softwares.

Comentários: o controle de acesso físico não se limita ao hardware e o controle de acesso lógico não se limite ao software (Errado).

(TJDFT – 2015) Na segurança da informação, controles físicos são soluções implementadas nos sistemas operacionais em uso nos computadores para garantir, além da disponibilidade das informações, a integridade e a confidencialidade destas.

Comentários: controles físicos são barreiras que limitam o contato ou acesso direto à informação ou à infraestrutura suporta essa informação (Errado).

[1] Nunca vi em bibliografias consagradas, mas já encontrei em uma prova a cobrança de controles de segurança processuais, que tratam basicamente de... processos de segurança (Ex: troca de senha a cada 30 dias).

[2] A biometria é polêmica: há algumas classificações que a colocam como controle lógico e outras como físico ou lógico a depender do que ela se propõe a proteger.

Terminologia

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Sabe-se que existe o **risco** de que um determinado **agente** se aproveite de **vulnerabilidades** para – por meio de **ataques** ou de **ameaças** – gerar um **incidente** que quebre a confidencialidade, integridade ou disponibilidade de um **ativo** de **informação** gerando graves **impactos** organizacionais. *Professor, não entendi nada!* Calma, galera! Vocês só não entenderam porque vocês ainda não sabem o significado da maioria dessas palavras.

Na Segurança da Informação, utiliza-se um jargão muito específico. Caso – no decorrer da aula – vocês tenham alguma dúvida, é só retornar aqui e descobrir o significado. Vejamos

TERMINOLOGIA	DESCRIÇÃO
ATIVO	Qualquer coisa que tenha valor para instituição, tais como: informações, pessoas, serviços, software, hardware, documentos físicos, entre outros.
INFORMAÇÃO	Ativo que, como qualquer outro ativo importante para os negócios, tem valor para a organização e, por isso, deve ser adequadamente protegido.
AGENTE	Fonte produtora de um evento que pode ter um efeito adverso sobre um ativo de informação, como um funcionário, meio ambiente, hacker, etc.
VULNERABILIDADE	Fragilidades presentes ou associadas a ativos que, quando exploradas por ameaças, levam à ocorrência de incidentes de segurança.
AMEAÇA	A ameaça é um agente externo que, se aproveitando das vulnerabilidades, poderá quebrar a confidencialidade, integridade ou disponibilidade da informação, causando um desastre ou perda significativa em um ambiente, sistema ou ativo de informação.
ATAQUE	Evento decorrente da exploração de uma vulnerabilidade por uma ameaça com o intuito de obter, alterar, destruir, remover, implantar ou revelar informações sem autorização de acesso.
EVENTO	Ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a Segurança da Informação.
INCIDENTE	Fato decorrente de um ataque bem-sucedido, com consequências negativas, uma ocorrência indicando uma violação, uma falha ou situação desconhecida, algo que possa ser relevante para a segurança da informação.
IMPACTO	Abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio.
RISCO	Probabilidade potencial da concretização de um evento que possa causar danos a um ou mais ativos da organização.

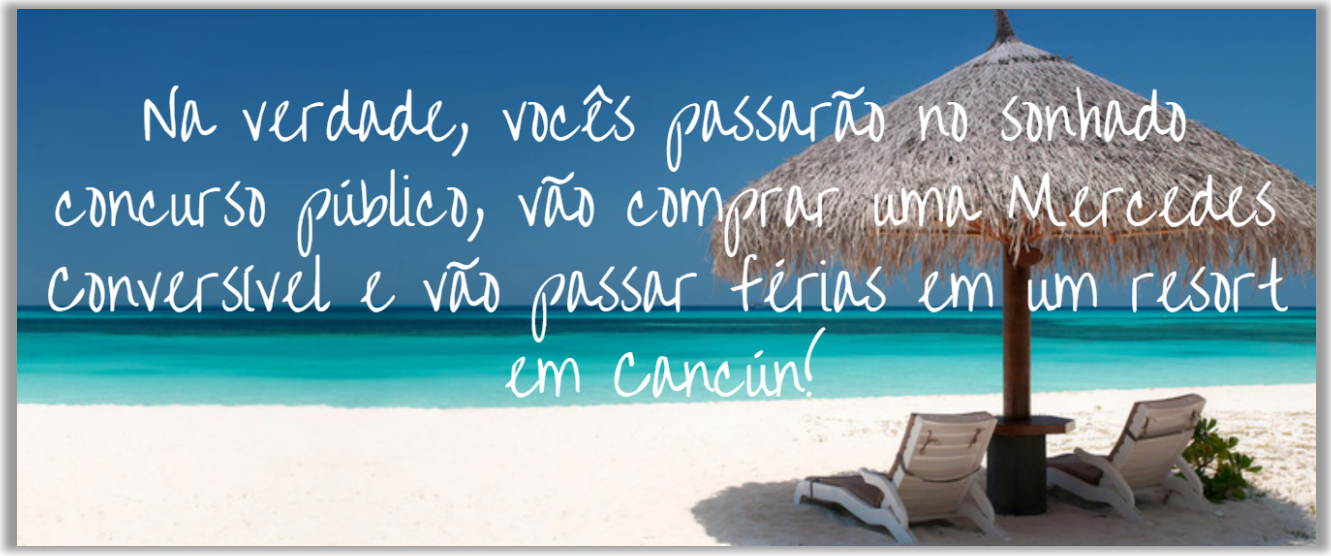
Eu percebo que é muito comum que os alunos tenham dúvidas sobre a diferença entre ameaça e risco. Vamos dirimi-las agora! A ameaça trata de um dano potencial, isto é, caso ocorra um

incidente, poderá haver dano ou não. Já o risco trata de um dano real, isto é, caso ocorra um incidente, necessariamente haverá perdas ou danos. Em geral, o risco trata da concretização de ameaças. *Entendido?*

Agora vamos fazer uma analogia – grosso modo – para entender melhor como essa terminologia se aplicaria à vida cotidiana. Imagine que você passe no sonhado concurso público e compre um carro – **esse carro seria um ativo**. Como o carro ainda está com o cheirinho de novo, você decide estacioná-lo mais longe a fim de evitar a ocorrência de qualquer acontecimento imprevisível – **isso seria um evento.**

Se esse acontecimento imprevisível fosse negativo, como alguém abrir a porta do carro ao lado com força e arranhar o seu carro, **isso seria incidente**. No entanto, esse lugar mais longe é mais perigoso e frequentemente carros são furtados por diversos assaltantes – **esses assaltantes seriam os agentes**. Como o carro foi comprado recentemente, você ainda não teve tempo de instalar um alarme – **isso seria uma vulnerabilidade**.

Dessa forma, você sabe que há chances de o carro ser furtado – isso seria um **ameaça**. Certo dia, quando você se aproxima do carro para voltar para casa, um meliante anuncia um assalto – **isso seria um risco**, visto que ele ainda não o assaltou efetivamente. Ele, então, rouba a sua chave e carteira, entra no veículo e sai cantando pneu – **isso seria um ataque**. O agressor some com o carro, leva para um desmanche e você fica sem o carro para todo sempre – **isso seria um impacto**.



(PEFOCE – 2012) As ameaças são fatores externos que podem gerar incidente de segurança da informação por intermédio da exploração das vulnerabilidades dos ativos de informação.

Comentários: ameaça é um agente externo que, se aproveitando das vulnerabilidades, poderá quebrar a confidencialidade, integridade ou disponibilidade da informação, causando um desastre ou perda significativa em um ambiente, sistema ou ativo de informação (Correto).

Princípios Fundamentais

Confidencialidade

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Confidencialidade é a capacidade de um sistema de não permitir que informações estejam disponíveis ou sejam reveladas a entidades não autorizadas – incluindo usuários, máquinas, sistemas ou processos. Seria algo similar à privacidade, em que pessoas autorizadas podem acessar e visualizar uma informação privada, mas pessoas não autorizadas não podem. *Simples, não?* É algo bem do nosso dia-a-dia...

Por exemplo: caso eu escreva uma carta e a envie dentro de um envelope para um destinatário, o carteiro pode ter acesso a minha carta, mas em tese não poderá lê-la. Caso ele rasgue o selo, aí sim ele terá acesso direto às informações lá escritas. **No entanto, nesse contexto, ele terá quebrado o princípio da confidencialidade, e uma ou mais pessoas não autorizadas poderão visualizar meus dados privados contidos dentro da carta.**

É importante destacar que a garantia da confidencialidade deve ser obtida em todos os níveis, desde a geração da informação, passando pelos meios de transmissão, até chegar ao seu destino e ser devidamente armazenada ou, se necessário, destruída sem possibilidade de recuperação. Outra coisa: não confundam **confidencialidade** com **confiabilidade**: o segundo trata da tolerância de um sistema a eventuais falhas.

(TCE/RS – 2014) José utilizou uma ferramenta para criptografar uma informação a ser transmitida para Maria, com o objetivo de proteger a informação contra acesso não autorizado. O requisito básico de segurança da informação assegurado pela criptografia é a:

a) irretratabilidade.
b) autenticidade.
c) confidencialidade.
d) disponibilidade.
e) confiabilidade.

_____

Comentários: proteger a informação contra acesso não autorizado assegura confidencialidade (Letra C).

Integridade

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Integridade é a capacidade de garantir que a informação manipulada está correta, fidedigna e que não foi corrompida. Esse princípio geralmente trata da salvaguarda da exatidão e completeza da informação, com o intuito de aferir que a informação não tenha sido alterada sem autorização durante seu percurso, de sua origem ao seu destino, mantendo todas as características originais estabelecidas pelo proprietário da informação.

Em outras palavras, esse princípio sinaliza a conformidade dos dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário, garantindo a não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital.

No exemplo anterior, se a carta que eu enviei chegou ao destinatário exatamente da forma que eu a enviei, ou seja, **lacrada, correta, fidedigna, precisa, original, impecável, sem nenhuma manipulação**, então mantivemos o princípio da integridade da informação. É por essa razão que empresas de e-commerce pedem que os clientes não aceitem produtos que estejam com a embalagem danificada ou sem lacre – porque ela pode ter sido manipulada por terceiros.

Percebam também que confidencialidade e integridade são princípios independentes, isto é, a quebra de um princípio não implica a quebra do outro. Por exemplo: o carteiro pode interceptar minha carta, colocá-la contra uma luz forte e eventualmente conseguir visualizar a minha mensagem sem a minha autorização – quebrando o princípio da confidencialidade. No entanto, ele não terá quebrado o princípio da integridade, visto que minha carta será entregue inalterada.

(TJ/SP – 2014) Assinale a alternativa que apresenta corretamente a característica do requisito básico de segurança, conhecido como integridade.

a) Verificar se uma entidade é realmente quem ela diz ser.
b) Determinar as ações que uma entidade pode executar.
c) Proteger uma informação contra acesso não autorizado.
d) Proteger a informação contra alteração não autorizada.

_____

Comentários: integridade trata da proteção da informação contra alteração não autorizada (Letra D).

Disponibilidade

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Disponibilidade é a propriedade de uma informação estar acessível e utilizável sob demanda por uma entidade autorizada. De certa forma, ela garante que usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. Exemplo: se eu recebi uma carta, eu devo ter acesso a sua informação sempre que eu desejar. São características da disponibilidade a oportunidade, a continuidade e a robustez.

No entanto, o exemplo da carta não é muito elucidativo para esse princípio – eu prefiro explicar esse princípio de outra maneira! *Vocês já precisaram fazer uma transferência de grana importantíssima e, quando foram acessar o aplicativo do seu banco, ele estava fora do ar?* Pois é, isso já aconteceu comigo quando eu tinha uma conta em um banco que eu prefiro nem dizer o nome. Isso me irritou tanto que eu abri uma conta em outro banco mais confiável!

Vocês percebem a importância desse princípio? O prejuízo de um banco quando seu sistema fica fora ar pode ser de milhões de reais – dependendo do tempo indisponível, bilhões de reais! **Por essa razão, há um investimento massivo em recursos que reduzem as chances de o sistema e suas informações ficarem indisponíveis**. *Quais, professor?* Por exemplo: firewalls, backups, redundâncias, equipamentos de energia, entre outros.

PEGADINHA CLÁSSICA: CONFIDENCIALIDADE X DISPONIBILIDADE

A confidencialidade garante que a informação **somente** esteja acessível para usuários autorizados. Já a disponibilidade garante que a informação esteja disponível aos usuários autorizados sempre que necessário (notem que existem dois requisitos).

(CGM/PB – 2018) A disponibilidade pressupõe que uma informação deva estar disponível a qualquer pessoa de direito, sempre que necessário.

_____

Comentários: essa é a premissa da disponibilidade, isto é, informação disponível sempre que necessário aos usuários autorizados (Correto).

(SERPRO – 2013) Um ataque à infraestrutura de conectividade de um banco à Internet, interrompendo o acesso a seus serviços de home banking, afeta a disponibilidade.

_____

Comentários: se interrompe o acesso aos serviços, é claro que afeta a disponibilidade (Correto).

Princípios Adicionais

Galera, alguns autores consideram como princípios fundamentais apenas Confidencialidade, Integridade e Disponibilidade. **Já outros consideram também os princípios da Autenticidade e da Irretratabilidade.** Por fim e mais raro, há também os atributos propostos por Donn B. Parker – também conhecido como Hexagrama Parkeriano – que considera os atributos: Confidencialidade, Integridade, Disponibilidade, Autenticidade, Posse ou Controle, e Utilidade.

Autenticidade

INCIDÊNCIA EM PROVA: ALTÍSSIMA

A autenticidade é a propriedade que trata da garantia de que o emissor de uma mensagem é de fato quem alega ser. Em outras palavras, ela garante a identidade de quem está enviando uma determinada informação. *Sabe quando você assina um contrato?* A sua assinatura é uma forma (frágil) de garantir que você é quem diz ser! O cartório tem a sua assinatura (chamada firma) e ele pode comparar com a assinatura que consta no contrato.

Galera, eu sei fazer a assinatura do meu pai impecavelmente. Logo, eu poderia quebrar essa garantia da autenticidade porque se trata de um método frágil, mas existem outras maneiras de melhorar essa garantia de autenticidade. **De toda forma, a autenticidade busca garantir que a pessoa que está requisitando acesso a alguma informação é realmente quem ela diz ser**. Hoje em dia é muito fácil se passar por outro em redes sociais, por exemplo...

Em tese, nada impediria que eu criasse um instagram com o nome ***@fatima_bernardes***, um facebook com o nome ***@ronaldinho_gaucho_10*** ou um twitter com o nome ***@cabo_daciolo_51***.

No entanto, as redes sociais criaram a verificação de conta (representado pelo ícone ✔). *O que é isso, professor?* **Esse é um recurso criado inicialmente para figuras públicas, celebridades, cantores, artistas, entre outro para evitar que outras pessoas se passem por elas.** Observem nas três redes sociais acima que existe o ícone que mostra que essa conta é autêntica, isto é, ela é realmente de quem diz ser.

Alguém sempre poderá dizer: *professor, não é possível garantir isso, porque o celular do dono da conta pode ter sido roubado, por exemplo.* É verdade, absolutamente nenhum sistema é totalmente seguro. No entanto, quando dissemos que isso garante autenticidade, nós assumimos que não ocorreu nenhum incidente e que o dono utiliza uma autenticação forte em suas redes. Em segurança da informação, é comum utilizar o verbo **garantir** sem problema.

Caiu poucas vezes em prova, mas é bom enfatizar que existem dois tipos de autenticação:

- **Autenticação de Origem dos Dados:** pode ocorrer sem conexão e busca garantir que a origem dos dados recebidos é realmente de quem diz ser.

- **Autenticação de Entidade Par:** ocorre com conexão e busca garantir a confiabilidade da identidade das entidades conectadas.

(TRF/4 – 2014) A segurança da informação objetiva a proteção de ativos da informação contra acessos não autorizados, alterações indevidas, sendo considerada uma prática de gestão de riscos incidentes que impliquem o comprometimento de seus requisitos e conceitos básicos. Dentro desta análise conceitual, a garantia de que as entidades identificadas em um processo de comunicação como remetentes ou autores sejam, exatamente, os mencionados nela, pode ser conceituada como:

a) severidade.
b) confidencialidade.
c) disponibilidade.
d) criticidade.
e) autenticidade.

_____

Comentários: garantia de que as entidades identificadas como autores sejam realmente quem dizem ser é uma característica do Princípio da Autenticidade (Letra E).

(Prefeitura de Vitória – 2010) Autenticar é confirmar a identidade de uma entidade visando, por exemplo, garantir que a entidade é quem ela diz ser. As técnicas para autenticação podem basear-se na verificação de informações como, por exemplo, senhas.

_____

Comentários: autenticar é realmente confirmar a identidade de uma entidade, isto é, garantir que ela é legítima – uma senha é realmente uma forma de verificação de autenticidade, visto que – em tese – apenas o proprietário conhece a senha (Correto).

Irretratabilidade

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Também chamada de Irrefutabilidade ou Não-repúdio, o princípio da irretratabilidade trata da capacidade de garantir que o emissor da mensagem ou participante de um processo não negue posteriormente a sua autoria. No Direito, o não-repúdio implica a intenção de cumprir as obrigações de um contrato. Implica também que uma parte de uma transação não possa negar ter recebido uma transação, nem a outra parte pode negar ter enviado uma transação.

É importante notar que, embora a tecnologia – como os sistemas criptográficos – possa ajudar nos esforços de não-repúdio, o conceito é, em sua essência, um conceito legal que transcende o domínio da tecnologia. *Como assim, professor?* Lembrem-se do exemplo anterior! Alguém sempre pode falar que teve o celular roubado ou que quem fez a postagem foi um estagiário ou que o algoritmo do sistema está com algum erro.

No entanto, é possível utilizar uma autenticação forte, o que aumenta consideravelmente a confiança de que quem enviou a mensagem foi realmente quem parece ser. Dessa forma, alguém dificilmente conseguiria negar sua autoria. Em 2015, o Twitter Oficial do STJ publicou o tweet abaixo e o apagou minutos depois. O órgão dificilmente conseguiria negar sua autoria, visto que – como possui uma conta verificada – necessita de autenticação forte.

Professor, autenticidade e irretratabilidade são a mesma coisa? Não, são conceitos distintos! Se você me envia uma carta com a sua assinatura no papel, eu sei que você é autor da carta (Autenticidade), mas você ainda pode negar que escreveu aquele conteúdo porque – apesar de ter a sua assinatura – **alguém pode ter capturado a carta no meio do caminho e alterado o conteúdo mensagem deixando apenas a assinatura ao final.**

Por meio da Irretratabilidade, inserimos um mecanismo de integridade que garante que a carta está íntegra, isto é, foi recebida exatamente da maneira que foi enviada. Nesse caso, quando garantimos a autenticidade (assinatura) e a integridade (mensagem sem modificações), nós garantimos automaticamente a irretratabilidade – também chamada de não repúdio, porque o autor não pode repudiar sua autoria, isto é, não pode se esquivar de ter enviado aquela mensagem.

AUTENTICIDADE + INTEGRIDADE = IRRETRATABILIDADE

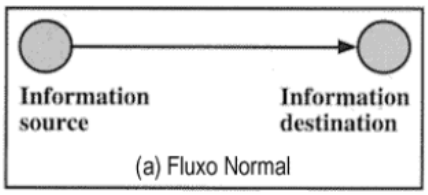
(TCE/PA – 2016) O princípio de não repúdio impede que o autor de um documento negue a criação e a assinatura desse documento.

_____

Comentários: perfeito... o autor não pode negar a criação e assinatura de um documento (Correto).

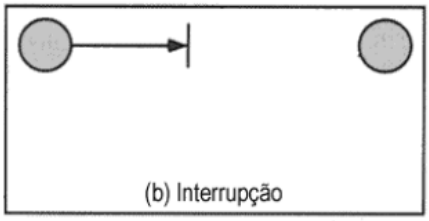
Desafio

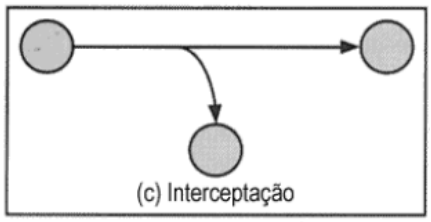
Considerem o cenário normal de fluxo de informação abaixo em que uma fonte da informação envia dados para um destinatário da informação.

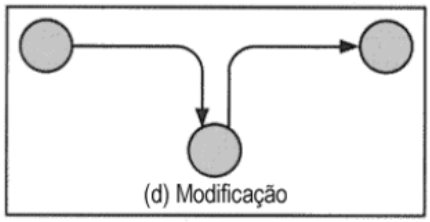


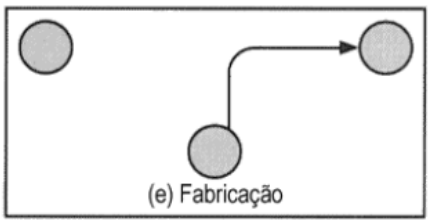
Agora vamos analisar os quatro cenários acima:

- **(b) Interrupção:** a informação que deveria sair da fonte e chegar ao destinatário foi interrompida no meio do caminho e não chegou ao seu destino final;
- **(c) Interceptação:** a informação que sai da fonte chegou ao destinatário, mas foi interceptada por alguém não autorizado no meio do caminho que teve acesso ao seu conteúdo;
- **(d) Modificação:** a informação que saiu da fonte foi recebida por um terceiro (que não necessariamente a leu) e posteriormente enviada ao destinatário com alterações;
- **(e) Fabricação:** a informação não foi enviada pela fonte e, sim, por um terceiro se fazendo parecer ter sido a fonte e enviada ao destinatário.









Quais serviços de segurança da informação foram violados por meio dos quatro ataques apresentados acima? A resposta eu vou deixar no rodapé[1]!

[1] (b) Disponibilidade; (c) Confidencialidade; (d) Integridade; (e) Autenticidade.

CRIPTOLOGIA

Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

A informação sempre foi objeto de poder, portanto é comum a criação de técnicas para obter informações de modo não autorizado e, ao contrário, **acaba sendo necessário o surgimento de mecanismos de defesa visando proteger as informações**. Basicamente a Criptologia se ocupa da ocultação de informações e da quebra dos segredos de ocultação. A primeira pode ser alcançada por Esteganografia ou Criptografia, e a segunda pode ser alcançada por Criptoanálise.

A criptografia possui dois grandes grupos: códigos e cifras. Os códigos são palavras, frases, letras, símbolos usados para substituir elementos do texto claro. As cifras, por sua vez, são algoritmos de criptografia e descriptografia de mensagens. Elas se caracterizam por dois tipos básicos de transformação: transposição e substituição. Vejam abaixo como esses conceitos são dispostos um em relação ao outro.

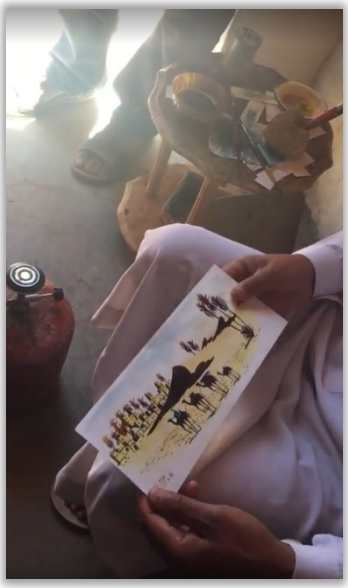
(STF – 2013) A criptologia incorpora estudos e conhecimentos das áreas de criptografia e criptoanálise.

Comentários: a criptologia realmente incorpora estudos e conhecimentos de criptografia e criptoanálise – além da esteganografia (Correto).

Esteganografia

INCIDÊNCIA EM PROVA: BAIXA

Trata-se de uma técnica utilizada para esconder informações. **Seu objetivo é que as informações sejam transmitidas de forma invisível, sem que possam ser capturadas ou monitoradas**. *Quem aí tem filhos?* Vocês podem fazer um experimento legal com eles: escrevam uma carta secreta com suco de limão! Vocês precisarão de uma folha de papel em branco, um cotonete, um ferro de passar roupa e um copinho com limão espremido.

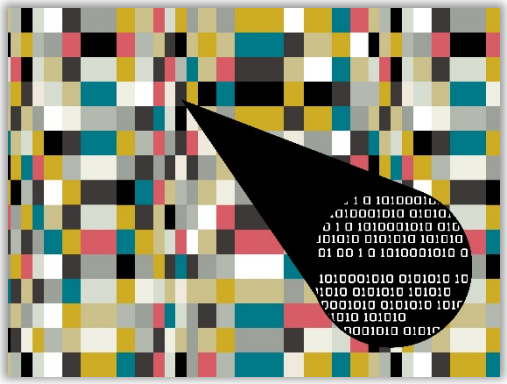


Molhem a ponta do cotonete no suco de limão, escrevam alguma coisa no papel em branco e deixem secar naturalmente. Vocês perceberão que a folha continuará em branco e não será possível visualizar a mensagem escrita. Após um tempo, peguem o ferro de passar roupa e passem o papel. **A mensagem escrita com o limão de forma invisível aparecerá no papel**! Esse é um exemplo bem simples de esteganografia.

Vou compartilhar uma experiência pessoal com vocês! Certa vez, em uma viagem ao Deserto do Saara, fui em um povoado berbere onde um artista fazia pinturas com pigmentos de água com açúcar. Inicialmente, não era possível ver nenhuma definição do que ele estava desenhando. **Até que ele passou o papel em um maçarico de gás propano e de repente apareceu essa imagem ao lado**! *Legal, né?*

O guia nos contou que, há trezentos anos atrás, essa era uma forma de enviar mensagens de forma invisível entre as famílias. Depois de um tempo, tornou-se uma forma de arte chamada Piroaquarela ou Aquarela de Fogo. Já na era moderna, **a esteganografia aparece como uma técnica para ocultar uma mensagem dentro de outra, de forma que não sejam percebidas por terceiros**. Em geral, escondem-se mensagens dentro de imagens, sons, vídeos ou textos.

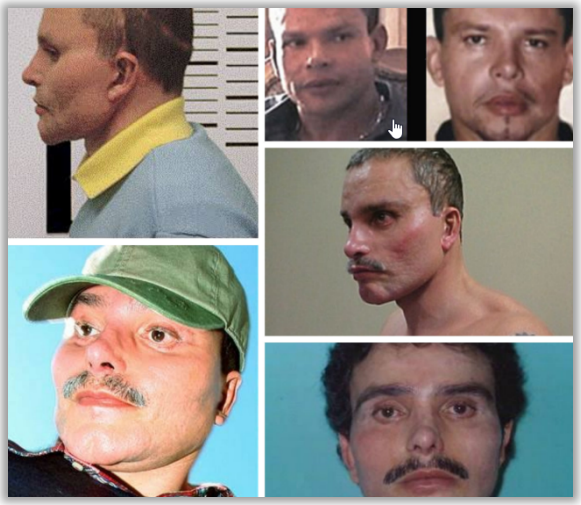
Professor, como é possível esconder uma mensagem em uma imagem? Não vamos entrar em muitos detalhes sobre o funcionamento, mas basicamente uma imagem é um conjunto pixels codificados em milhões e milhões de bits (Ex: 01101010000101110101011101101000) – como mostra a imagem ao lado! **Se eu modificar apenas alguns desses bits para guardar uma mensagem secreta, não vai fazer muita diferença para você porque a mudança será imperceptível para o olho humano**.



Alguém consegue notar alguma diferença entre a imagem da esquerda e a imagem da direita abaixo? Pois é, a imagem da direita está esteganografada, isto é, há uma mensagem escondida dentro dela. Se a pessoa que vai receber a mensagem sabe disso e sabe como decifrá-la, ela conseguirá ver a

mensagem escondida na imagem. **Caso contrário, uma pessoa desavisada só vai achar que é uma foto de um panda**. E isso pode ser feito com vários tipos de arquivos.

Por fim, só mais um caso interessante! Transcrevo a seguir uma reportagem da Folha de São Paulo, de 10 de março de 2008. Vejam que legal :)



> *Você nunca mais verá a **Hello Kitty** com olhos inocentes. A culpa é do traficante colombiano Juan Carlos Ramírez Abadía. Quando foi preso em São Paulo, em agosto do ano passado, os delegados da Polícia **Federal ficaram intrigados com a quantidade de imagens da gatinha japonesa que ele guardava nos computadores**. Eram quase 200 imagens, quase todas enviadas por e-mail.*
>
> *A surpresa maior foi a descoberta de que a Hello Kitty não era só uma Hello Kitty. **Havia mensagens de voz e de texto escondidas nas imagens.** Algumas delas podem mudar o destino de Abadía no Brasil: elas contêm ordens para movimentar cocaína entre países e para sumir com pessoas na Colômbia, segundo análise feita pelo DEA, a agência antidrogas dos EUA. Para os americanos, Abadía continuou a comandar o tráfico na Colômbia mesmo após se mudar para o Brasil.*

> *A mulher de Abadía, Yessica, é fanática por Hello Kitty. Um dos quartos da casa em que ela vivia em Aldeia da Serra (Grande SP) tinha cadeiras, relógios e papel de parede da Hello Kitty. O DEA ajudou a PF porque o Brasil não teria toda a tecnologia necessária para fazer a investigação.* ***A técnica de computação usada para esconder uma mensagem de voz em uma imagem é conhecida como esteganografia****.*
>
> *A Al Qaeda utilizou essa técnica para preparar os atentados de 2001. Hello Kitty não era o único disfarce para as ordens de Abadía. Algumas mensagens continham fotos de crianças (...)*

https://www1.folha.uol.com.br/fsp/cotidian/ff1003200801.htm

(UFC – 2013) Sobre Esteganografia é correto afirmar que:

a) É uma categoria de algoritmo criptográfico simétrico.
b) É a análise de desempenho dos algoritmos criptográficos.
c) É uma técnica para ocultar uma mensagem dentro de outra.
d) É um algoritmo matemático capaz de obter a mensagem original a partir do seu código hash.
e) É uma técnica para decifrar o texto cifrado sem qualquer conhecimento da mensagem original e do algoritmo criptográfico utilizado.

_____
Comentários: esteganografia é uma técnica de ocultação de uma mensagem dentro de outro (Letra C).

(PC/DF – 2012) Esteganografia é um termo pouco utilizado no âmbito da segurança da informação, mas que exige cuidados especiais de quem se preocupa com o tema. Assinale a alternativa que apresenta a definição de esteganografia.

a) Técnica de esconder informações dentro de arquivos como imagens, sons, vídeos ou textos.
b) Sinônimo de criptografia, é técnica de codificar a informação para que não seja entendida por terceiros.
c) Algoritmo matemático que converte um texto claro em uma mensagem cifrada, e vice-versa.
d) Estudo de técnicas de quebra de sigilo de mensagens eletrônicas criptografadas.
e) Método para codificação de arquivos binários, transformando-os em texto ASCII.

_____
Comentários: esteganografia é uma técnica de esconder informações dentro de arquivos como imagens, sons, vídeos ou textos (Letra A).

Criptografia e Criptoanálise

Conceitos Básicos

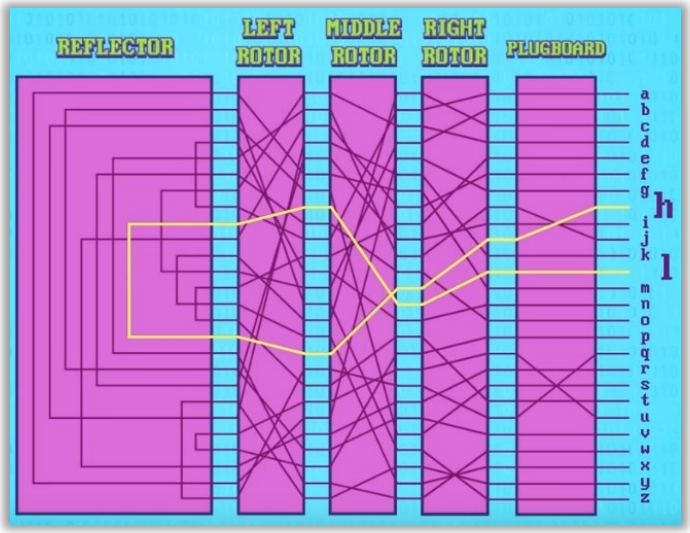
INCIDÊNCIA EM PROVA: BAIXA

A Criptografia é a técnica de tornar uma mensagem ininteligível! Ela remonta ao Egito por volta de 1.900 A.C., **quando um escriba esculpiu alguns símbolos hieroglíficos em uma rocha no túmulo do chefe egípcio Khnumhotep II**. A criptografia não era tão difícil naquela época, já que a maioria das pessoas era analfabeta e só a elite podia ler qualquer linguagem escrita. Desde essa época, faraós, reis, imperadores, presidentes, ditadores e comandantes militares usaram a criptografia para esconder comunicações de seus inimigos.

Um exemplo é Maria, Rainha dos Escoceses! Em 1577, ela queria assassinar a Rainha Elizabeth I e – para tal – começou a trocar mensagens com seus companheiros de conluio. Para que ninguém desconfiasse caso as mensagens acabassem em mãos erradas, eles as criptografavam! Eles utilizaram uma cifra de substituição, em que você substitui umas letras por outras ou palavras comuns por símbolos. **As mensagens de Maria foram capturadas pelos espiões da Rainha Elizabeth I, decifradas e Maria foi imediatamente presa, julgada e condenada por traição**. A pena foi morte por decapitação na guilhotina. Essa é apenas uma historinha para contextualizar sobre a importância da criptologia no decorrer da história da humanidade. *Bacana?* :)

Falando agora de tempos mais modernos, essa máquina acima é chamada Enigma II. **Ela é uma máquina eletromecânica de criptografia utilizada pelos nazistas durante a Segunda Guerra Mundial**. Quem assistiu ao filme O Jogo da Imitação (The Imitation Game), que conta a história de Allan Turing – o pai da computação –, deve conhecê-la. Se não assistiram ainda, assistam! É um filmaço! #ficadica :)

A Enigma era poderosa e complexa por possuir três rotores – como mostrado na imagem ao lado – para bagunçar as letras digitadas e dificultar a decifragem das mensagens. O **H** digitado se tornava um **J**, que se tornava um **M**, que se tornava um **Q**, que se tornava um **P**, que passava por um refletor e se tornava um **I**, que se tornava um **H**, que se tornava um **N**, que finalmente se tornava um **L** na mensagem criptografada. Além disso, você poderia configurar a máquina de diversas maneiras, dificultando a decifragem para quem interceptasse.



Ela era utilizada para troca de mensagens entre os generais nazistas. Foi quando o matemático britânico Allan Turing criou uma máquina chamada *Bombe* capaz de traduzir textos encriptados pelos alemães e decifrando diversas mensagens que continham informações de planos e estratégias de guerra. Dessa forma, **considera-se que a máquina de criptoanálise de Allan Turing ajudou a encerrar a guerra mais cedo, porque vários ataques alemães foram evitados**.

Técnicas de Criptografia

Atualmente são empregadas técnicas de criptografias simétricas, assimétricas e híbridas. Essas técnicas empregam dois fundamentos principais: **substituição**, em que cada elemento no texto claro é mapeado para outro elemento; e **transposição**, em que os elementos no texto claro original são reorganizados. O requisito essencial de ambos é que nenhuma informação seja perdida! Vejamos em detalhes...

Criptografia Simétrica[1]

INCIDÊNCIA EM PROVA: ALTÍSSIMA

A Criptografia Simétrica implica o uso de uma chave secreta utilizada tanto para codificar quanto para decodificar informações. Um dos precursores da criptografia simétrica foi o imperador romano Júlio César, que implementou uma técnica que codificava a mensagem a ser enviada, substituindo cada caractere do texto por um caractere três posições à frente em relação ao alfabeto, conforme a imagem ao lado. Observem que A corresponde a D, D corresponde a G, G corresponde a J, e assim por diante.

D Culswrjudild Slphwulfd lpsolfd r xvr gh xpd fkdyh vhfuhwd xwlolcdgd wdqwr sdud frglilfdu txdqwr sdud ghfrglilfdu lqirupdfrhv. Up grv suhfxuvruhv gd fulswrjudild vlphwulfd irl r lpshudgru urpdqr Jxolr Chvdu, txh lpsohphqwrx xpd whfqlfd txh frglilfdyd d phqvdjhp d vhu hqyldgd, vxevwlwxlqgr fdgd fdudfwhuh gr whawr sru xp fdudfwhuh wuhv srvlfrhv d iuhqwh hp uhodfdr dr doidehwr, frqiruph d lpdjhp dr odgr. Oevhuyhp txh A fruuhvsrqgh d D, D fruuhvsrqgh d G, G fruuhvsrqgh d J, h dvvlp sru gldqwh.

O segundo parágrafo é exatamente o primeiro parágrafo, porém cifrado com a técnica do Imperador Júlio César. *Bacana, né?* Quem quiser brincar, acesse o site abaixo:

HTTPS://CRYPTII.COM/PIPES/CAESAR-CIPHER

Se uma pessoa interceptar a mensagem do segundo parágrafo, não conseguirá decifrar a mensagem. No entanto, se ela souber qual é a chave de encriptação, facilmente ela conseguirá decodificar a mensagem. *E o que seria essa chave de encriptação?* É uma informação que controla a

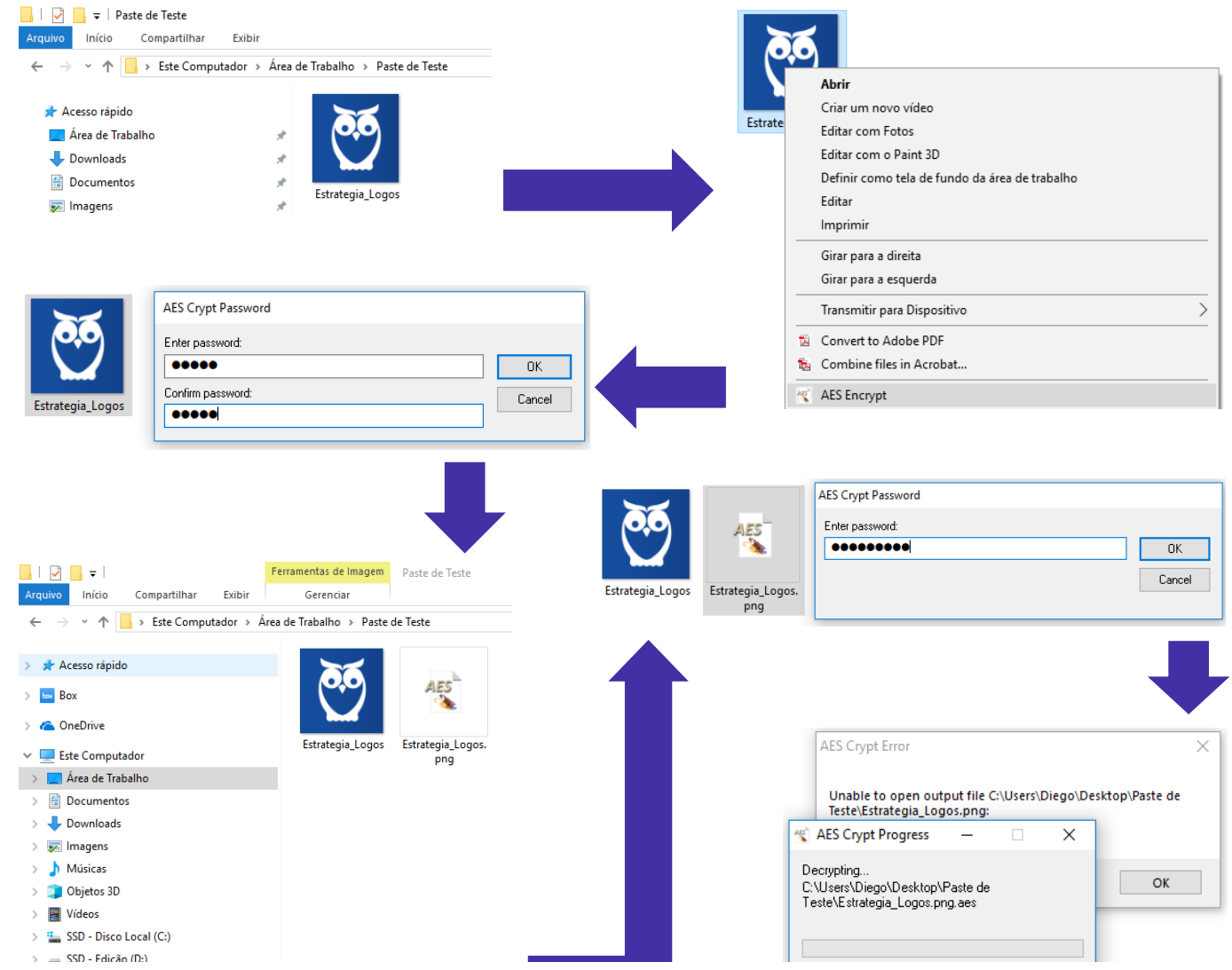
[1] Também chamado de Algoritmo de Chave Secreta, Chave Única, Chave Compartilhada, Chave Privada ou Criptografia Convencional.

operação de um algoritmo de criptografia – **na criptografia simétrica, ela é utilizada tanto para codificar quanto para decodificar a mensagem**. No caso acima, a chave de Júlio César é 3! *Por que?* Porque o caractere verdadeiro e o caractere codificado diferem em três posições.

Bacana! Nós entendemos a criptografia simétrica de uma maneira simplificada. Vamos ver agora como isso se aplicaria aos tempos atuais. Vamos supor que Maria precise enviar um documento sensível para João. Ela faz uso de um software de encriptação para proteger seu documento e, para tal, utiliza uma senha ou chave. Ela então envia o documento criptografado para João! *João vai conseguir abrir o documento?* **Não, porque ele não sabe a senha!** *E agora?*

Maria teria que entregar ou falar pessoalmente qual é a senha para João, mas isso poderia ser um grande inconveniente. Ela poderia enviá-la por e-mail, mas seria arriscado, visto que alguém poderia interceptá-la e utilizá-la para descriptografar o documento sensível. Percebam, então, que essa é uma boa solução para casos mais simples, **mas há riscos e inconvenientes**. Quem quiser brincar com esse tipo de criptografia ou precisar esconder algum arquivo, eu recomendo:

HTTPS://WWW.AESCRYPT.COM



Na primeira figura, eu tenho uma imagem do logo do Estratégia. Na segunda figura, eu clico com o botão direito para utilizar o programa AES Encrypt. Na terceira figura, o programa pede para que eu insira uma senha ou chave – eu utilizo '**12345**'. Na quarta figura, é criado o arquivo criptografado da imagem. Na quinta figura, eu tento abrir a foto e o programa pede a senha – eu insiro '**123456789**'. Na última figura, é negada a abertura da imagem por senha incorreta!

Voltando ao nosso contexto: se a pessoa que vai descriptografar o arquivo futuramente for a mesma pessoa que o criptografou, não há muito problema. No entanto, eu poderia enviar esse arquivo criptografado para o meu parceiro, Professor Renato da Costa. Nesse caso, ele só conseguiria abri-lo se possuísse a senha ou chave que eu escolhi. **Dessa forma, eu teria que encontrá-lo pessoalmente para passar a senha ou chave – isso poderia ser um inconveniente**.

Em um sistema de criptografia simétrica é primordial que a chave seja protegida. Como se trata da mesma chave, ela deve ser trocada antes da comunicação iniciar. O sistema fica vulnerável se a chave não for bem protegida ou se a chave for interceptada por um atacante quando for enviada entre as partes que se comunicam. **O risco de a chave ser comprometida fica maior com o aumento do número de partes envolvidas na troca de mensagens com a mesma chave.**

Por fim, é importante ressaltar um rigor teórico: a criptografia – por si só – garante apenas o princípio da confidencialidade. No entanto, algoritmos criptográficos simétricos permitem garantir confidencialidade, integridade e autenticidade. *Como se garante a integridade?* Enviando o texto em claro junto do texto criptografado, o que permite verificar se a mensagem recebida é exatamente igual a mensagem enviada – concluindo que não foi alterada no meio do caminho.

Além disso, permite também garantir o princípio da autenticidade, caso se possa assegurar que apenas as duas entidades tenham conhecimento da chave secreta. *Diego, por que não garante o não-repúdio?* Porque um terceiro jamais poderá saber quem de fato enviou uma determinada mensagem. Como as duas entidades conhecem a chave secreta, uma das entidades pode sempre negar (repudiar) o envio da mensagem afirmando que quem a enviou foi a outra entidade.

- **Principais algoritmos:** DES, 3DES, AES, IDEA, RC4, Blowfish, Cifragem de Júlio César, etc.

(SEFAZ/PB – 2006) Criptografia simétrica é um método de codificação que utiliza:

a) uma chave pública e uma chave privada para encriptar e decodificar a mesma mensagem.
b) duas chaves públicas para encriptar e decodificar a mesma mensagem.
c) uma só chave para encriptar e decodificar a mesma mensagem.
d) duas chaves privadas para encriptar e decodificar a mesma mensagem.
e) uma chave pública e duas chaves privadas para encriptar e decodificar a mesma mensagem.

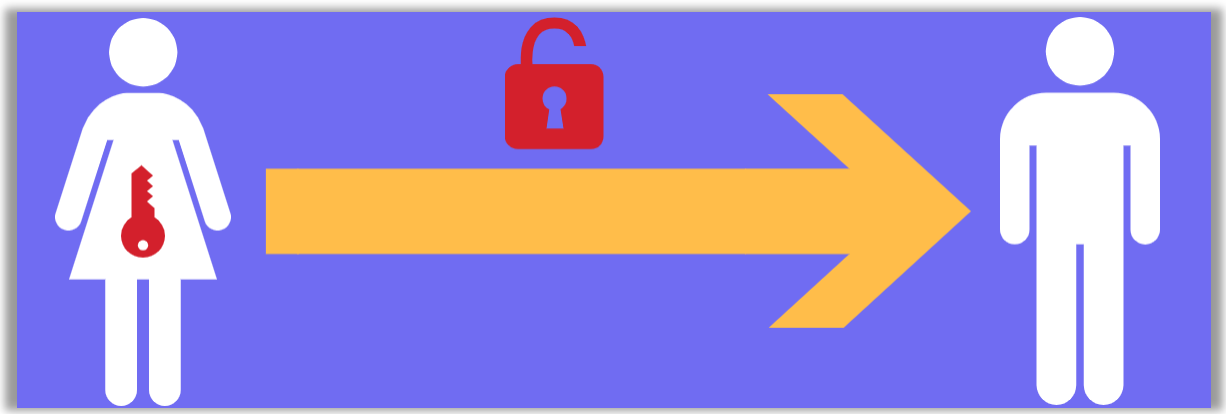
Comentários: a criptografia simétrica utiliza uma só chave para encriptar e decodificar a mesma mensagem – chamada de chave simétrica (Letra C).

Criptografia Assimétrica

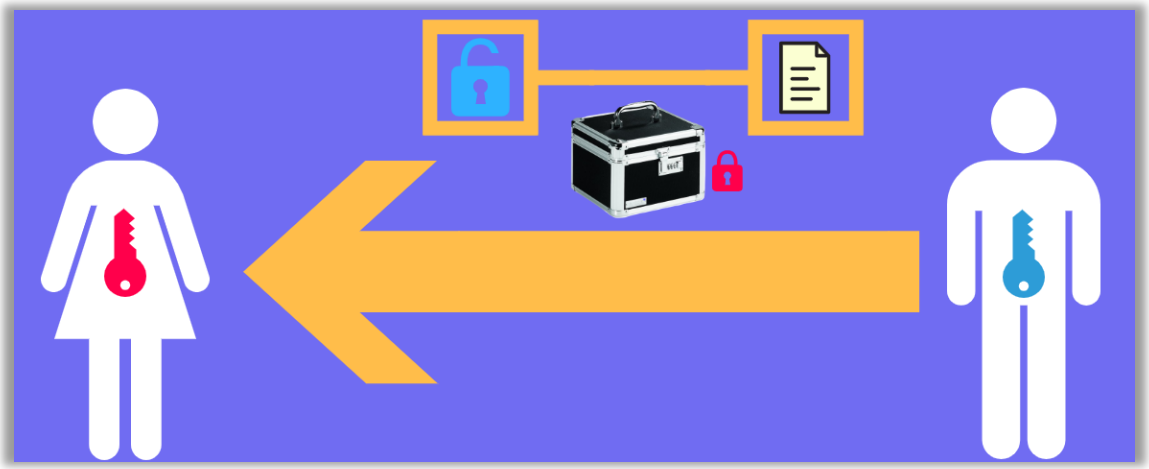
INCIDÊNCIA EM PROVA: ALTÍSSIMA

Nós vimos que a Criptografia Simétrica tinha uma falha: havia a necessidade de compartilhar a chave de cifragem/decifragem. A Criptografia Assimétrica (também chamada de Criptografia de Chave Pública) acabou com essa vulnerabilidade ao criar duas chaves distintas e assimétricas – sendo uma pública e uma privada. **A chave pública é disponibilizada para qualquer um e a chave privada é de uso personalíssimo e restrito a um usuário, instituição ou equipamento**.

Embora sejam chaves criptográficas diferentes, elas formam um par exclusivo em que necessariamente ao se criptografar informações com uma chave pública, **somente a chave privada correspondente do par é capaz de descriptografar essas informações e vice-versa**. Para entender isso melhor, eu preciso bastante da atenção de vocês agora – esse assunto é um pouquinho complexo e cai muito em prova. Vejam só...



Imaginem que agora é a Maria que precisa receber um documento sensível de João. No entanto, dessa vez, antes de receber qualquer documento, ela decide comprar um cadeado vermelho que vem acompanhado de uma chave vermelha. Dessa forma, ela vai aos correios e envia seu novo cadeado vermelho aberto para João, permanecendo com a chave vermelha sob sua posse. *Entenderam essa parte?*



João recebe o cadeado vermelho aberto e decide comprar um cadeado azul com uma única chave. Além disso, ele compra uma caixa. Então, **ele insere seu cadeado azul aberto junto com o documento sensível que Maria precisa, coloca tudo dentro dessa caixa**, permanece com a sua chave azul, mas tranca a caixa com o cadeado vermelho que foi enviado aberto por Maria e envia a caixa para ela por meio dos correios.

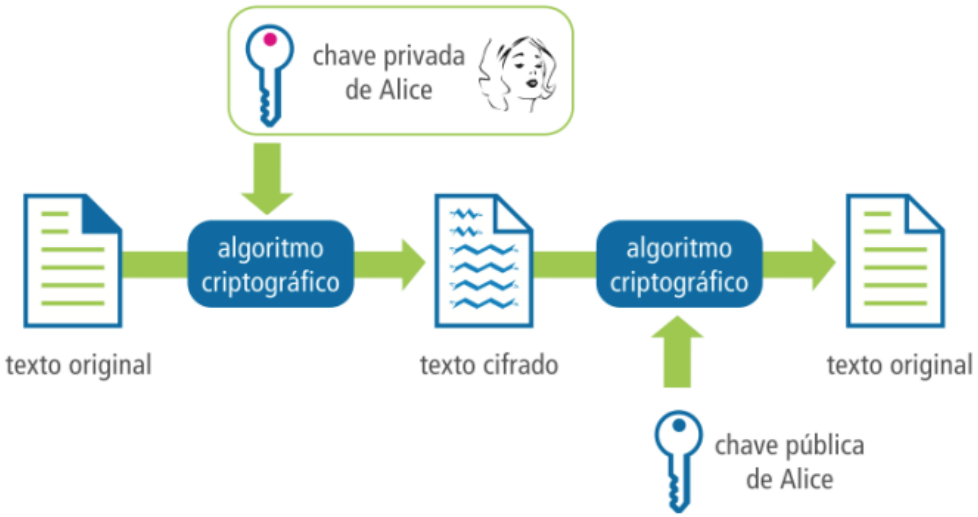
Maria recebe a caixa trancada com seu cadeado vermelho e – **como somente ela possui a chave vermelha para o cadeado vermelho** – destranca a caixa e encontra o cadeado azul aberto de João junto do documento sensível. Pronto! Agora toda vez que eles precisarem enviar documentos sensíveis um para o outro, eles podem inseri-los na caixa junto de seu cadeado aberto e trancá-la com o cadeado do outro. *Simples, né?*

Esse método é interessante porque, caso o carteiro ou qualquer outra pessoa intercepte a caixa, ele não conseguirá abri-la. *Por que, professor?* Porque a chave nunca é enviada! O que é enviado é apenas o cadeado aberto – cada um permanece com sua chave. Em nossa analogia, o cadeado aberto representa a chave pública e a chave do cadeado representa a chave privada. No entanto, toda metáfora tem suas limitações. Logo, vamos retornar agora aos computadores!

Na Criptografia Assimétrica, nós possuímos duas chaves diferentes – uma chave pública e uma chave privada – por essa razão, é chamada de criptografia assimétrica. **Esse par de chaves formam um par exclusivo**, de modo que um texto criptografado pela chave pública só pode ser descriptografado pela chave privada e um texto criptografado pela chave privada só pode ser descriptografado pela chave pública. *Bacana?*

A chave pública é realmente pública – você pode contar qual é a sua chave pública para todo mundo. Evidentemente, a chave privada é exclusivamente sua! **Similarmente, o número da sua conta corrente é público – ela seria sua chave pública. Já a senha de transação da sua conta corrente é privada – ela seria sua chave privada**. *Professor, quando eu quiser criptografar uma mensagem, eu devo usar a minha chave pública ou minha chave privada?* Depende!

O emissor que deseja enviar uma informação sigilosa deverá utilizar a chave pública do destinatário para criptografar essa informação sigilosa. Para isto, é importante que o destinatário disponibilize sua chave pública. **O Princípio da Confidencialidade é garantido, uma vez que somente o destinatário que possui a chave privada específica dessa chave pública conseguirá desfazer a operação de criptografia** – como mostra a imagem anterior.



Professor, o que acontece se eu utilizar minha chave privada para criptografar uma informação? Nesse caso, qualquer um que possua sua chave pública conseguirá descriptografá-la e visualizá-la. E como sua chave pública é literalmente pública, você não garantirá o princípio da confidencialidade (todos terão acesso à informação). **Por outro lado, você garantirá o princípio da autenticidade**. *Como assim, Diego?* Vejam só...

Nós sabemos que o princípio da autenticidade garante que determinada pessoa é realmente quem ela diz ser. Se alguém utilizar a minha chave pública para descriptografar uma informação e conseguir, **ela terá certeza de que fui eu que realmente criptografei aquela informação**. *Por que?* Porque se a informação foi descriptografada com minha chave pública, ela só pode ter sido criptografada com minha chave privada. E adivinhem: somente eu possuo minha chave privada!

Note que, diferentemente dos algoritmos de criptografia simétrica, os algoritmos de chave pública podem garantir também o não-repúdio porque, partindo do princípio de que a mensagem é integra, autêntica e que a chave privada é particular de cada entidade, somente a autora poderia tê-la enviado, logo não poderia negá-la. Percebam, portanto, que sempre que garantimos o não-repúdio garantimos a autenticidade, mas o contrário não é verdadeiro.

Em suma, algoritmos de criptografia simétrica podem garantir confidencialidade, integridade e autenticidade e algoritmos de chave pública garantem todos esses + não-repúdio.

- **Principais algoritmos:** RSA, DSA, ECDSA, ElGamal, Diffie-Hellman (para troca de chaves), etc.

> **(PC/GO – 2015)** Criptografia é a ciência de transformar mensagens para ocultar seu significado de intrusos. Considerando essa informação, assinale a alternativa que apresenta a técnica de criptografia que utiliza a chave pública para codificar as mensagens.
>
> a) cifragem de chave simétrica
> b) hashing
> c) estaganografia
> d) cifragem de chave assimétrica
> e) assinatura digital
>
> _____
> **Comentários:** trata-se da cifragem de chave assimétrica (Letra D).

Comparando os algoritmos de criptografia simétrica com algoritmos de criptografia assimétrica, podemos afirmar que os algoritmos de criptografia simétrica possuem menor custo computacional do que a criptografia assimétrica (isto é, possuem um maior desempenho ao criptografar uma mesma quantidade de dados em menos tempo). Além disso, a criptografia simétrica utiliza, em geral, chaves menores do que a criptografia assimétrica.

Dito de outra forma, os algoritmos de criptografia assimétrica precisam – em geral – de chaves maiores para garantir o mesmo nível de segurança que algoritmos de criptografia simétrica (que utilizam chaves consideravelmente menores). Por fim, o gerenciamento de chaves para comunicação de um grupo de usuários é mais simples na criptografia assimétrica (utilizam 2n chaves, sendo n o número de pessoas), enquanto a criptografia simétrica utiliza n(n-1)/2 chaves.

Criptografia Híbrida

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

A Criptografia Assimétrica tem vantagens em relação a Criptografia Simétrica, mas também tem desvantagens. Em geral, as chaves simétricas são bem menores que as chaves assimétricas. Dessa forma, a Criptografia Assimétrica chega a ser até cem vezes mais lenta que a Criptografia Simétrica.

Por essa razão, é comum a utilização de uma Criptografia Híbrida, ou seja, uma combinação da Criptografia Simétrica e Criptografia Assimétrica.

Basicamente, utiliza-se um algoritmo de Criptografia Assimétrica apenas para trocar chaves simétricas – chamadas de chaves de sessão – de forma segura. Logo, após a troca, toda comunicação é realizada utilizando um algoritmo de Criptografia Simétrica. Protocolos como *Secure Sockets Layer* (SSL) utilizam chaves de sessão para criptografar e descriptografar informações. *Fechou?*

(TJ/PA – 2009) Para manter a segurança das comunicações via Internet, o protocolo SSL (Secure Sockets Layer) utiliza sistemas criptográficos:

a) simétricos de chaves públicas.
b) assimétricos de chaves privadas.
c) simétricos de chaves privadas.
d) assimétricos de chaves de sessão.
e) simétricos de chaves de sessão.

_____

Comentários: esse protocolo utiliza sistemas criptográficos simétricos de chaves de sessão. *Professor, mas ele não utiliza a criptografia assimétrica?* Sim, mas apenas para trocar as chaves de sessão. A segurança da comunicação é mantida pelo SSL por meio de sistemas criptográficos simétricos de chaves de sessão (Letra E).

Para finalizar esse assunto, precisamos falar de mais um conceito: Princípio de Kerckhoff! Esse **princípio afirma que a segurança de um sistema criptográfico deve depender da chave utilizada e, não, do conhecimento do algoritmo.** *Como é, Diego?* Dito de outra forma, isso significa que não existe nenhum problema em um possível atacante conhecer os detalhes de implementação e funcionamento de um algoritmo – ele inclusive deve ser público.

Nós vimos vários exemplos de algoritmos criptográficos! Se você quiser entender seus detalhes para compreender como eles funcionam, basta buscar no Google – é tudo público! O surgimento de um novo algoritmo criptográfico cuja implementação não seja conhecida não aumenta a sua confiabilidade. **Na verdade, o melhor algoritmo é aquele que é público e que vem sofrendo ataques diversos sem quebrar – permanecendo seguro.**

Existem três fatores que influenciam a segurança de um sistema criptográfico: **(1) a força computacional de seu algoritmo – no sentido de que um algoritmo muito simples seria fraco[2]; (2) o sigilo da chave – a chave secreta ou privada não deve ser exposta; (3) e o comprimento da chave – chaves pequenas demais podem ser frágeis.** Por outro lado, os detalhes de implementação do algoritmo são irrelevantes, podendo (na verdade, devendo) ser públicos.

[2] Um algoritmo é considerado **computacionalmente** seguro quando o tempo despendido para efetuar a sua quebra é maior que o tempo de vida útil da informação ou quando o valor gasto para efetuar a quebra é maior que o valor intrínseco da informação.

(TJ/AM – 2019) A segurança de um sistema criptográfico simétrico deve estar na chave e no tamanho dessa chave, e não nos detalhes do algoritmo.

_____

Comentários: tanto no sistema criptográfico simétrico quanto no assimétrico, a segurança deve estar na força do algoritmo, no sigilo de sua chave e no tamanho da chave e, não, nos detalhes do algoritmo – conforme Princípio de Kerckoff (Correto).

(TJ/AM – 2019) A segurança de um sistema criptográfico simétrico tem como características básicas a força do algoritmo e o comprimento da chave.

_____

Comentários: tanto no sistema criptográfico simétrico quanto no assimétrico, a segurança deve estar na força do algoritmo, no sigilo de sua chave e no tamanho da chave e, não, nos detalhes do algoritmo – conforme Princípio de Kerckoff (Correto).

(TCU – 2007) Atualmente, os sistemas criptográficos utilizados são incondicionalmente seguros por se basearem na dificuldade de resolução de problemas matemáticos específicos ou em limitações na tecnologia computacional vigente.

_____

Comentários: na verdade, os sistemas criptográficos utilizados atualmente são ~~incondicionalmente~~ computacionalmente seguros (Errado).

(TRT19 – 2011) Uma regra fundamental da criptografia é:

a) A chave criptográfica deve ser modificada a cada período de alguns anos.

b) Deve-se presumir que o criptoanalista conhece os métodos genéricos de criptografia e descriptografia que são utilizados.

c) Tanto os algoritmos quanto as chaves devem ser secretos, segundo o princípio de Kerckhoff.

d) O sigilo deve decorrer da presença de um algoritmo forte e secreto, independentemente do tamanho da chave.

e) Deve-se supor que, se uma cifra puder resistir a uma estratégia de texto cifrado, ela é segura.

_____

Comentários: (a) Errado, não existe essa exigência de modificação a cada período; (b) Correto, podemos assumir que o criptoanalista (o cara que deseja quebrar o algoritmo) conhece métodos genéricos de criptografia e descriptografia utilizados já que o algoritmo deve ser público; (c) Errado, os algoritmos devem ser públicos e as chaves devem ser secretas; (d) Errado, o algoritmo deve ser público e depende – sim – do tamanho da chave; (e) Errado, a estratégia de texto cifrado indica que o atacante conhece apenas o texto cifrado, logo não conhece o texto original nem a chave. Resistir a essa estratégia não indica que a cifra é segura. Aliás, mesmo que o atacante conheça o texto original e o texto cifrado, o atacante não conheceria a chave, logo não poderia descriptografar outras mensagens. Por outro lado, resistir também a essa estratégia não indica que a cifra é necessariamente segura (Letra B).

Principais Algoritmos

INCIDÊNCIA EM PROVA: BAIXA

Vejamos uma tabela comparativa entre os principais algoritmos de criptografia simétrica, assimétrica e de hash (que veremos mais à frente):

ALGORITMO	DESCRIÇÃO
DES	Algoritmo simétrico de chave privada com 56 bits de tamanho de chave. Desenvolvido na década de 1970, é considerado fraco pelos padrões atuais de segurança.
3DES	Versão atualizada do DES, que usa três vezes a cifra DES para melhorar a segurança. Suas chaves podem ter 112 ou 168 bits.
AES	Algoritmo simétrico de chave privada que substituiu o DES como padrão de criptografia em 2001. Suas chaves podem ter 128, 192 ou 256 bits.
IDEA	Algoritmo simétrico de chave privada desenvolvido na década de 1990, com chave de 128 bits. Foi uma alternativa ao DES, mas é menos utilizado atualmente.
RC4	Algoritmo simétrico de chave privada usado em várias aplicações, como redes sem fio e SSL/TLS. Possui chaves de 40 a 2048 bits.
RSA	Algoritmo assimétrico de chave pública usado para criptografia e assinaturas digitais. É um dos algoritmos mais amplamente usados na criptografia moderna.
DIFFIE-HELLMAN	Algoritmo de troca de chaves que permite a comunicação segura em um canal inseguro. É amplamente utilizado em sistemas criptográficos baseados em chave pública.
BLOWFISH	Algoritmo simétrico de chave privada usado em diversas aplicações de segurança, com chaves de 32 a 448 bits. É conhecido por sua velocidade e segurança.
MD5	Algoritmo de hash criptográfico que gera um resumo de 128 bits da mensagem original. É amplamente usado para verificar a integridade de arquivos.
SHA	Família de algoritmos de hash criptográficos que geram resumos de tamanho fixo (160, 256, 384 ou 512 bits) da mensagem original. É amplamente usado em diversas aplicações de segurança.

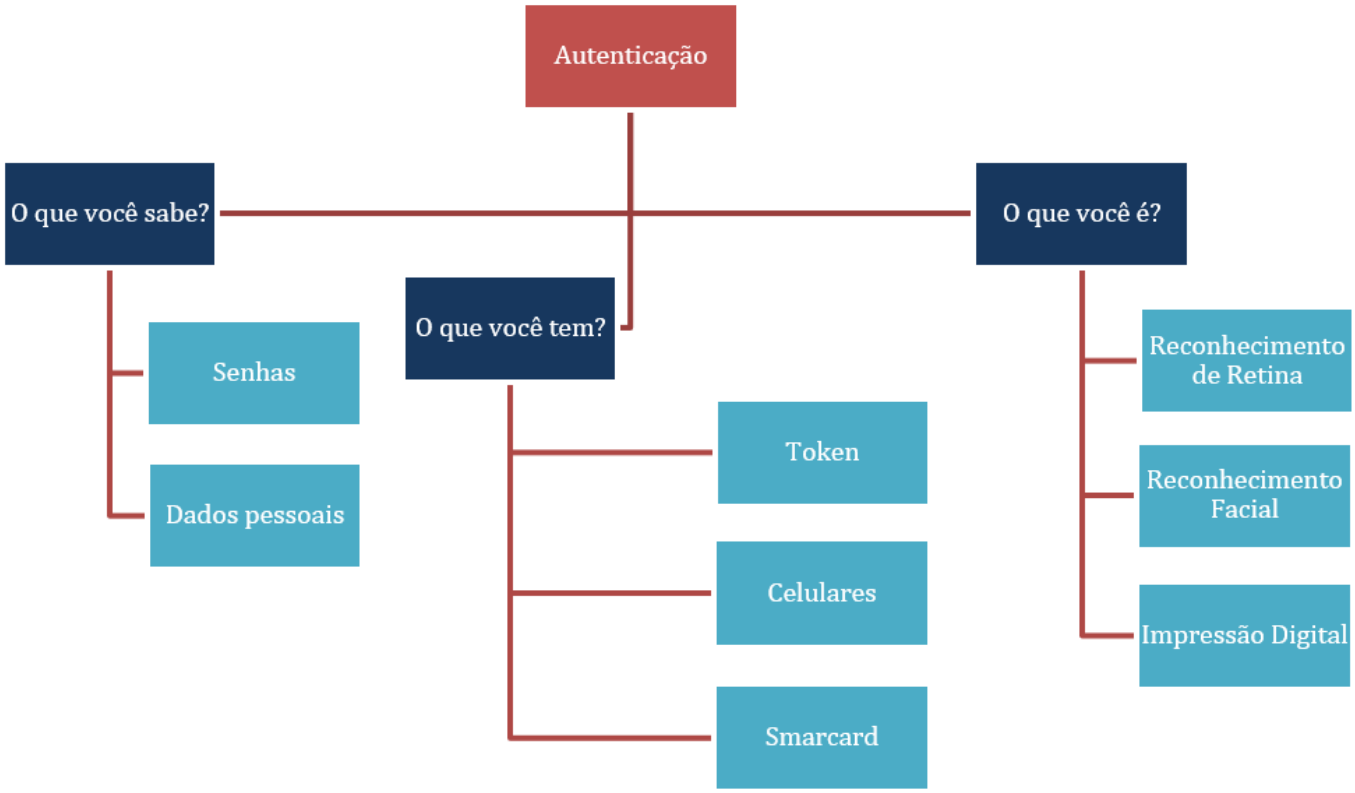
ALGORITMO	SEGURANÇA	VELOCIDADE	TAMANHO DA CHAVE	UTILIZAÇÃO	TIPO
DES	Fraco	Rápido	56 bits	Legado	Simétrico
3DES	Moderado	Lento	112-168 bits	Legado	Simétrico
AES	Forte	Rápido	128-256 bits	Atual	Simétrico
IDEA	Moderado	Rápido	128 bits	Legado	Simétrico
RC4	Moderado	Rápido	40-2048 bits	Legado	Simétrico
RSA	Forte	Lento	2048-4096 bits	Atual	Assimétrico
DIFFIE-HELLMAN	Forte	Moderado	Variável	Chave Pública	Assimétrico
BLOWFISH	Forte	Rápido	32-448 bits	Legado	Simétrico
MD5	Fraco	Rápido	128 bits	Legado	Hash
SHA	Moderado	Moderado	160-512 bits	Atual	Hash

AUTENTICIDADE

Conceitos Básicos

INCIDÊNCIA EM PROVA: BAIXA

No início dessa aula, nós vimos que a Autenticidade é um dos princípios da Segurança da Informação. Em seguida, no contexto de Criptografia, nós vimos que é possível garantir a Autenticidade utilizando Criptografia Assimétrica – para tal, basta criptografar a mensagem com sua chave privada. **Podem-se utilizar diversos métodos de autenticação, inclusive uma combinação entre eles**. Veremos abaixo os principais:



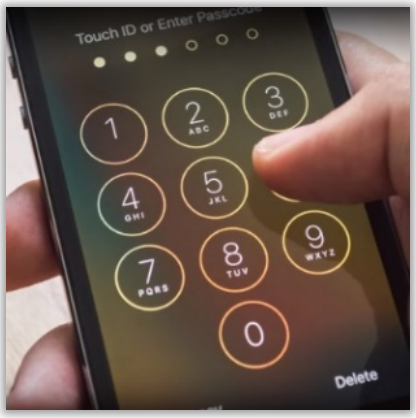
Método de Autenticação: O que você sabe?

Trata-se da autenticação baseada no conhecimento de algo que somente você sabe, tais como: senhas, frases secretas, dados pessoais aleatórios, entre outros.

Senhas

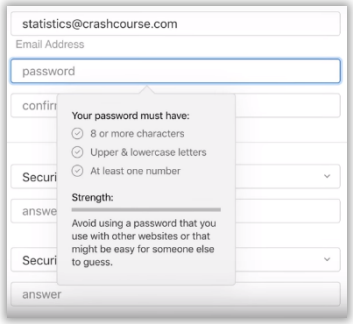
Hoje em dia, a combinação mais utilizada para autenticação em sistemas de informação é: **Usuário e Senha**. Essa é a forma de autenticação mais fácil de se implementar! No entanto, essa forma de autenticação pode ser comprometida se eventualmente hackers descobrirem essa combinação –

como nós já vimos, a senha mais utilizada no mundo no ano passado foi '12345' (cuidado com as senhas de vocês!).



Notem que uma senha de cinco dígitos – como a senha acima – é muito fácil de ser quebrada por um computador. Só existem 100.000 possibilidades – o que não é nada para um computador com processamento razoável. **Ele pode testar todas essas possibilidades em milésimos de segundo – é o chamado Ataque de Força Bruta**. Claro que há estratégias para mitigar esse risco. *Você já errou três vezes a senha do seu celular?* Pois é, ele te bloqueia por um período! Outra estratégia é obrigar que a senha tenha alguns requisitos básicos para ser mais difícil de ser quebrada ou descoberta. Vocês já devem ter visto algo mais ou menos assim:

ESTRATÉGIAS DE SENHAS
Utilize pelo menos oito caracteres (algumas normas recomendam seis caracteres);
Mescle letras minúsculas e maiúsculas, números, espaços, pontuação e outros símbolos;
Evite utilizar um caractere mais de duas vezes; não a anote, memorize-a;
Evite utilizar informações pessoais, como nome do filho, aniversário da mãe, etc;
Alterar as senhas com frequência e não utilizar a mesma senha em contas diferentes;
Substituir alguns caracteres por números parecidos como: D13Go C4RV4LHo;
Não utilizar sequências de teclado como: QWERTY, ASDFGH ou ZXCVBN;
Certificar de encerrar uma sessão ao acessar sites que requeiram uso de senhas;
Não escolher palavras que façam parte do dicionário.



Notem que uma senha de oito dígitos numéricos tem apenas um milhão de combinações possíveis – é ridiculamente fácil para um computador testar todas as possibilidades em pouco tempo utilizando um ataque de força bruta. No entanto, uma senha de oito caracteres que podem ser números, símbolos, maiúsculos, minúsculos, entre outros, pode ter mais de 600 trilhões de combinações. Aí fica bem mais complexo para qualquer computador pessoal! *Entendido?* Prossigamos...

Método de Autenticação: O que você é?

Trata-se da autenticação baseada no conhecimento de algo que você é, como seus dados biométricos. Exemplos: impressão digital, padrão de retina, reconhecimento de voz, reconhecimento facial, assinatura manuscrita (característica comportamental individual), etc. Dessa forma, a não ser que você possua um irmão gêmeo univitelino, somente você possuirá a maioria dessas características físicas ou biométricas.

Biometria

A Biometria (Bio = vida) utiliza características físicas únicas para verificar sua identidade. A biometria mais famosa é a impressão digital, entretanto podemos ter acessos biométricos através do reconhecimento de voz, varredura de retina e imagine, até mesmo DNA! Hoje em dia, diversos computadores portáteis trazem consigo um Leitor de Digital para, inclusive, fazer *logon* no Sistema Operacional.

Método de Autenticação: O que você tem?

Trata-se da autenticação baseada em algo que somente o verdadeiro usuário possui, tais como: celulares, crachás, *Smart Cards*, chaves físicas, *tokens*, etc. É um bom método de autenticação, porque resolve o problema da adivinhação por força bruta. Ademais, ela tipicamente requer a presença física do usuário, portanto é bem mais difícil para atacantes remotos conseguirem acesso. *Como assim, professor?*

Galera, alguém em outra cidade não consegue abrir a porta do meu apartamento sem antes vir à minha cidade. Dessa forma, esse método de autenticação possui uma dificuldade bem maior de ser quebrada. No entanto, **ele ainda pode ser comprometido se o atacante estiver fisicamente próximo**. Chaves podem ser copiadas, celulares podem ser roubados e trancas podem ser arrombadas. *Entendido?* Vamos ver alguns exemplos!

Smart Cards

Um *Smart Card* é um cartão inteligente. Trata-se simplesmente de um **cartão de plástico contendo um microprocessador – um chip – que armazena informações eletrônicas sobre o usuário** (Ex: Chaves), servindo como uma mídia criptográfica. O e-CPF, por exemplo, é um CPF digital em um cartão inteligente que garante a autenticidade e a integridade na comunicação.

Tokens

Os *tokens* são objetos de autenticação! Podem servir para armazenar senhas aleatórias (*One Time Password*) ou podem conter um conector USB servindo como mídia criptográfica, armazenando informações sobre o usuário (Certificado Digital), assim como um *Smart Card*.

Autenticação Forte

INCIDÊNCIA EM PROVA: BAIXA

Nós acabamos de ver três métodos de autenticação e sabemos que todos eles possuem riscos e vulnerabilidades, no entanto – quando nós combinamos métodos de autenticação – nós temos uma confiança maior na autenticidade. **Dessa forma, surgiu a Autenticação Forte, que é um tipo de autenticação que ocorre quando se utiliza pelo menos dois desses três métodos de autenticação de naturezas diferentes**.

Um exemplo é a Autenticação em Dois Fatores (ou Verificação em Duas Etapas)! **Um atacante pode adivinhar sua senha ou roubar o seu celular, mas é muito mais improvável que ele consiga fazer ambos**. Hoje em dia esse tipo de autenticação está ficando cada vez mais comum. Em geral, você utiliza algo que você sabe (Ex: Senha) para acessar um sistema. Ele, então, envia uma mensagem com um código para algo que você tem (Ex: Celular).

Você insere esse código e pronto... estará autenticado, ou seja, o sistema saberá que você é realmente você. **Quando você saca dinheiro em um caixa eletrônico, você também utiliza dois métodos de autenticação**. Primeiro, você insere seu cartão (algo que você tem). Após escolher o valor que você deseja sacar, você insere ou uma senha (algo que você sabe) ou sua impressão digital (algo que você é). Agora notem que eu deixei passar um detalhe lá na definição de autenticação forte: **os métodos devem ter naturezas diferentes.**

Se eu me autenticar utilizando cinco informações da mesma natureza (Ex: algo que você sabe), não se trata de um cenário de autenticação forte. Para ser considerada uma autenticação forte, é necessário utilizar pelo menos dois métodos de naturezas diferentes. *Entendido?*

(TRF/5 – 2017) Um Analista deve implementar o controle de acesso ao sistema computacional do Tribunal, utilizando o mecanismo de autenticação forte baseada em dois fatores. São eles:

a) cartão de identificação e token.
b) frase de segurança e PIN.
c) token e PIN.
d) impressão digital e padrão de voz.
e) senha e frase de segurança.

_____

Comentários: (a) Errado, cartão de identificação não serve para autenticação; (b) Errado, ambos são algo que você sabe; (c) Correto, token é algo que você tem e o PIN (Personal Identification Number) é algo que você sabe – como uma senha; (d) Errado, ambos são algo que você é; (e) Errado, ambos são algo que você sabe (Letra C).

(CRMV/RO – 2021) O uso de senhas fortes e de um gerenciador de senhas é suficiente para proteger o acesso a uma conta, sendo dispensável o uso do duplo fator de autenticação.

_____

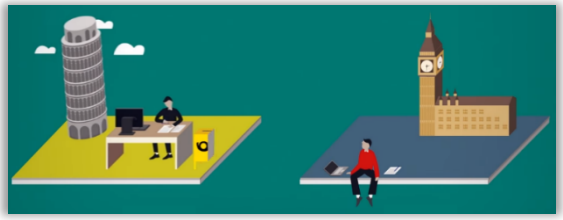
Comentários: senhas fortes e gerenciador de senhas não são suficientes para proteger o acesso a uma conta – recomenda-se a utilização do duplo fator de autenticação (Errado).

Assinatura Digital

Conceitos Básicos

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Galera, **existem alguns momentos em que soluções antigas infelizmente não atendem mais nossas demandas modernas**. *Vocês já pararam para pensar como é antiquado e inseguro assinar documentos e contratos utilizando um papel e uma caneta?* Pois é! No Brasil, cartórios pegam fogo com frequência. Além disso, assinaturas podem ser facilmente copiadas. As demandas modernas exigem uma solução mais flexível e responsiva! *Concordam comigo?*



Imaginem que Felipe mora na Itália e deseja fechar um contrato com o empresário Lucas, que mora em Londres. Para que o contrato chegue até o destinatário, **ele deve ir fisicamente e pode demorar semanas por conta das idas e vindas**.

Se ambos utilizassem assinaturas digitais, eles poderiam fechar contratos em questão de minutos em vez de semanas. Para tal, bastaria selecionar o documento, clicar com o botão direito, assinar digitalmente utilizando um código de segurança e enviá-lo por e-mail. O processo ocorre completamente sem papel e em alguns lugares – como a União Europeia – **um contrato assinado digitalmente vale tanto quanto um contrato assinado fisicamente**. Pois bem...

Nós vimos que é possível utilizar a Criptografia Assimétrica de duas maneiras: se eu criptografo uma mensagem com a chave pública do destinatário, eu garanto o Princípio da Confidencialidade; **se eu criptografo uma mensagem com a minha chave privada, eu garanto o Princípio da Autenticidade**. No entanto, vamos ser mais ambiciosos: a Assinatura Digital garantirá a Autenticidade, a Integridade e a Irretratabilidade.

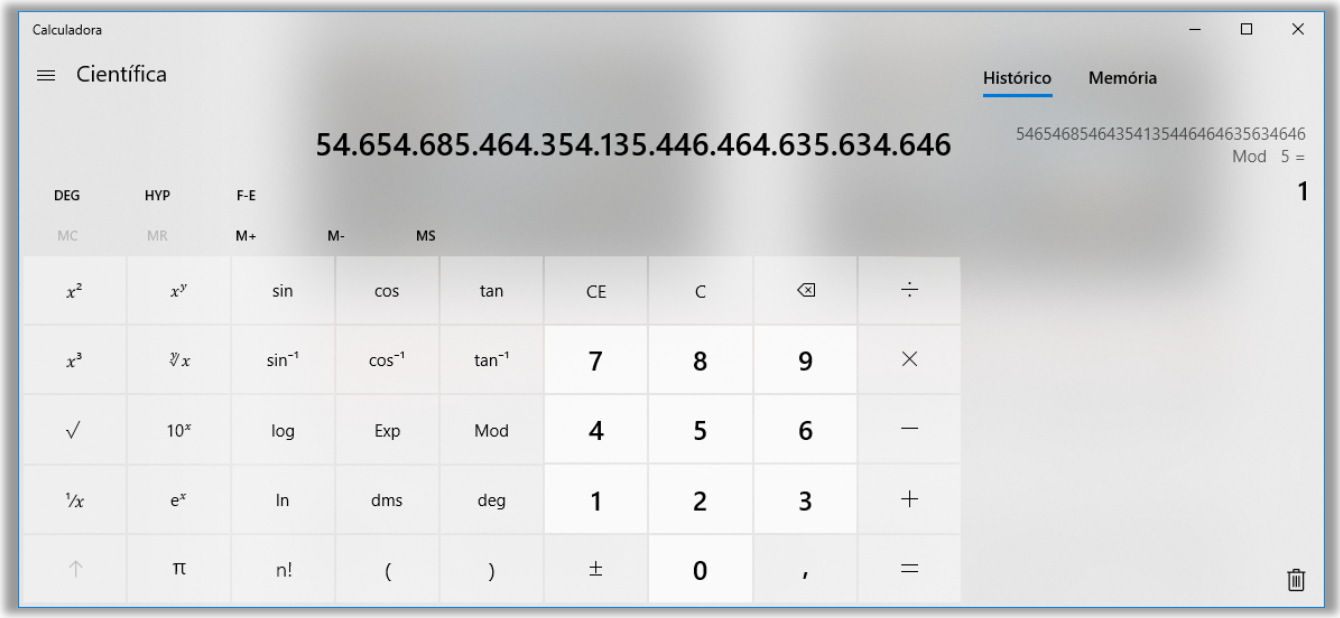
Para descobrir como ela fará isso, precisamos entender um conceito chamado: Algoritmo de Hash (ou Resumo)! O Algoritmo de Hash é basicamente um algoritmo criptográfico que transforma uma entrada de dados em uma saída de dados. No entanto, essa definição é muito genérica, então vamos detalhar mais! Esse algoritmo é capaz de transformar dados de entrada de qualquer tamanho – de poucos *bits* a muitos terabytes – em dados de saída de tamanho fixo[1].

Eu suma: o que vocês precisam memorizar é que o algoritmo de hash basicamente recebe dados de entrada de qualquer tamanho e produz um dado de saída de tamanho fixo. Um exemplo clássico é a Função de Resto ou Módulo. *Vocês se lembram lá na segunda série do ensino fundamental quando a Tia ensinou para a turma como funcionava uma divisão?* Nós tínhamos o dividendo, divisor, quociente e resto! Vejam só:

[1] Um arquivo de 50 Gb, por exemplo, pode gerar um *hash* (também chamado *Message-Digest* ou Resumo de Mensagem) de alguns bits.

A Função Resto ou Módulo funcionava assim: dado um dividendo e um divisor, a função retornava um resto. Na imagem à esquerda, o dividendo era 10 e o divisor era 3, logo a Função Resto resultou em 1. *Por que?* Porque 1 é o resto da divisão de 10 por 3. Na imagem à direita, o dividendo era 942.386 e o divisor era 3, logo a Função Resto resultou em 2. *Por que?* Porque 2 é o resto da divisão de 942.386 por 3.

Professor, o que isso tem a ver com a Função Hash? Galera, notem que – quando a entrada foi um dividendo de dois dígitos (10) – o resto teve apenas um dígito (1). E quando a entrada foi um dividendo de seis dígitos (942.386), o resto também teve apenas um dígito (2). Em outras palavras, **não importa se a entrada tem um dígito ou um trilhão de dígitos, a saída sempre terá apenas um único dígito**. *Legal né?* Vejam quantos dígitos temos abaixo e a saída foi... 1.



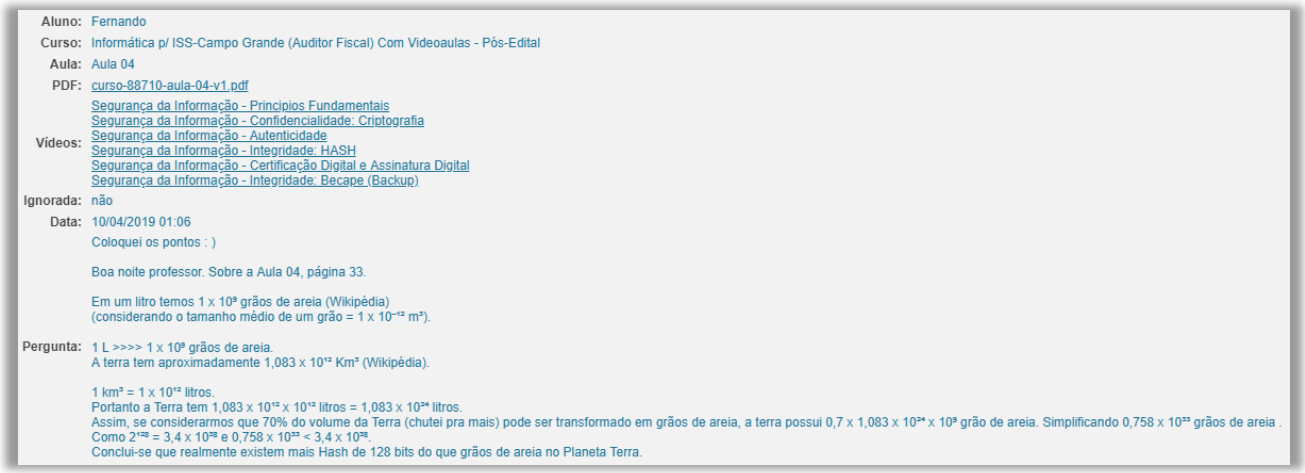
O Algoritmo de *Hash* faz algo similar: dada uma entrada de tamanho qualquer, ele a transforma em uma saída de tamanho fixo. *Querem outro exemplo legal?* Vejam o número de um boleto:

No boleto acima, percebam que há um número **1** totalmente isolado. Esse número é chamado de Dígito Verificador e é calculado em função de todos os outros dígitos do boleto de forma que qualquer alteração nos demais dados geraria um Dígito Verificador diferente. Dessa forma, o sistema de um banco é capaz de perceber facilmente se há algum erro de digitação no boleto. Dada uma entrada, gerou-se uma saída de tamanho fixo – **chamado Dígito Verificador**.

Um último exemplo é o Cadastro de Pessoa Física (CPF). **Nesse caso, os dois últimos dígitos são os Dígitos Verificadores – eles são calculados de acordo com um algoritmo definido pela Receita Federal**. O CPF 123.456.789-12 não é válido porque – dada a entrada 123.456.789 – a saída 12 não é válida. Por outro lado, o CPF 105.828.626-98 é válido porque – dada a entrada 105.828.626 – a única saída válida é 98. *Bacana?*

Agora uma pergunta: *se eu souber a saída, eu consigo descobrir qual é a entrada?* Não, o algoritmo de *hash* tem apenas uma direção (*one-way*), sendo extremamente difícil de inverter! **Em outras palavras, eu não devo conseguir saber qual é o número do boleto baseado apenas no dígito verificador**. Eu posso te dizer sem problema que o número verificador do meu CPF é 71. *E aí, vocês conseguem descobrir qual é o restante?* Não, porque ele só tem uma direção.

Outra característica do Algoritmo de *Hash* é que dada uma mesma entrada, a saída sempre será a mesma, ou seja, o resto da divisão de 10 por 3 é 1 – nunca será 2, 3, 4, etc. **O Algoritmo de Hash tem um problema: diferentes entradas podem gerar a mesma saída – nós chamamos isso de colisão**! Por exemplo: o resto da divisão de 10 por 3 é 1, mas o resto da divisão de 13 por 3 também é 1, isto é, para entradas diferentes, tivemos a mesma saída.



Aluno: Fernando
Curso: Informática p/ ISS-Campo Grande (Auditor Fiscal) Com Videoaulas - Pós-Edital
Aula: Aula 04
PDF: curso-88710-aula-04-v1.pdf
Vídeos: Segurança da Informação - Princípios Fundamentais
Segurança da Informação - Confidencialidade: Criptografia
Segurança da Informação - Autenticidade
Segurança da Informação - Integridade: HASH
Segurança da Informação - Certificação Digital e Assinatura Digital
Segurança da Informação - Integridade: Becape (Backup)
Ignorada: não
Data: 10/04/2019 01:06

Coloquei os pontos :)

Boa noite professor. Sobre a Aula 04, página 33.

Em um litro temos 1×10^9 grãos de areia (Wikipédia)
(considerando o tamanho médio de um grão = 1×10^{-12} m³).

Pergunta: 1 L >>>> 1×10^9 grãos de areia.
A terra tem aproximadamente $1{,}083 \times 10^{12}$ Km³ (Wikipédia).

$1\ km^3 = 1 \times 10^{12}$ litros.
Portanto a Terra tem $1{,}083 \times 10^{12} \times 10^{12}$ litros = $1{,}083 \times 10^{24}$ litros.
Assim, se considerarmos que 70% do volume da Terra (chutei pra mais) pode ser transformado em grãos de areia, a terra possui $0{,}7 \times 1{,}083 \times 10^{24} \times 10^9$ grão de areia. Simplificando $0{,}758 \times 10^{33}$ grãos de areia .
Como $2^{128} = 3{,}4 \times 10^{38}$ e $0{,}758 \times 10^{33} < 3{,}4 \times 10^{38}$.
Conclui-se que realmente existem mais Hash de 128 bits do que grãos de areia no Planeta Terra.

UM ALUNO FEZ QUESTÃO DE FAZER AS CONTAS PARA PROVAR QUE ISSO É VERDADE :)

A Função de Resto ou Módulo não é um bom Algoritmo de *Hash* para criptografia de senhas, porque ele é bastante suscetível a colisões. Uma forma de reduzir a chance de colisões é aumentando o

tamanho fixo de saída. **Atualmente, Algoritmos Criptográficos de Hash exigem pelo menos 128 bits de saída – isso é 2^{128} possibilidades, isso é mais que todos os grãos de areia do Planeta Terra** (conforme exposto pelo nosso querido aluno).

Dessa forma, é muito difícil haver uma colisão, isto é, entradas diferentes gerarem um mesmo resultado! Vamos resumir tudo que vimos: o Algoritmo de *Hash* é uma função unidirecional que – dada uma entrada de dados de tamanho qualquer – sempre gera uma saída de dados de tamanho fixo, **sendo que a mesma entrada sempre gerará a mesma saída e recomenda-se uma saída com um tamanho grande para evitar colisões**.

Uma Função de *Hash* bastante famosa é o MD5! Notem que o tamanho é sempre fixo e que – por menor que seja uma mudança – gera um resultado completamente diferente. Entre as duas primeiras frases, a única diferença é um sinal de exclamação. **No entanto, nós podemos chegar até o nível de bits, isto é, um único bit diferente pode gerar um resultado completamente diferente**. Vamos ver sua aplicação em algumas frases:

FRASE	HASH
Oi	of3abd55f538f9f34352420oa452ffbc (32 caracteres)
Oi!	7349da19c2ad665428oecf64ce42b837 (32 caracteres)
Oi, pessoal! O Professor Diego é flamenguista e o Professor Renato é vascaíno.	9ed868b2aa98ce95aaa08ef1065ad8fc (32 caracteres)

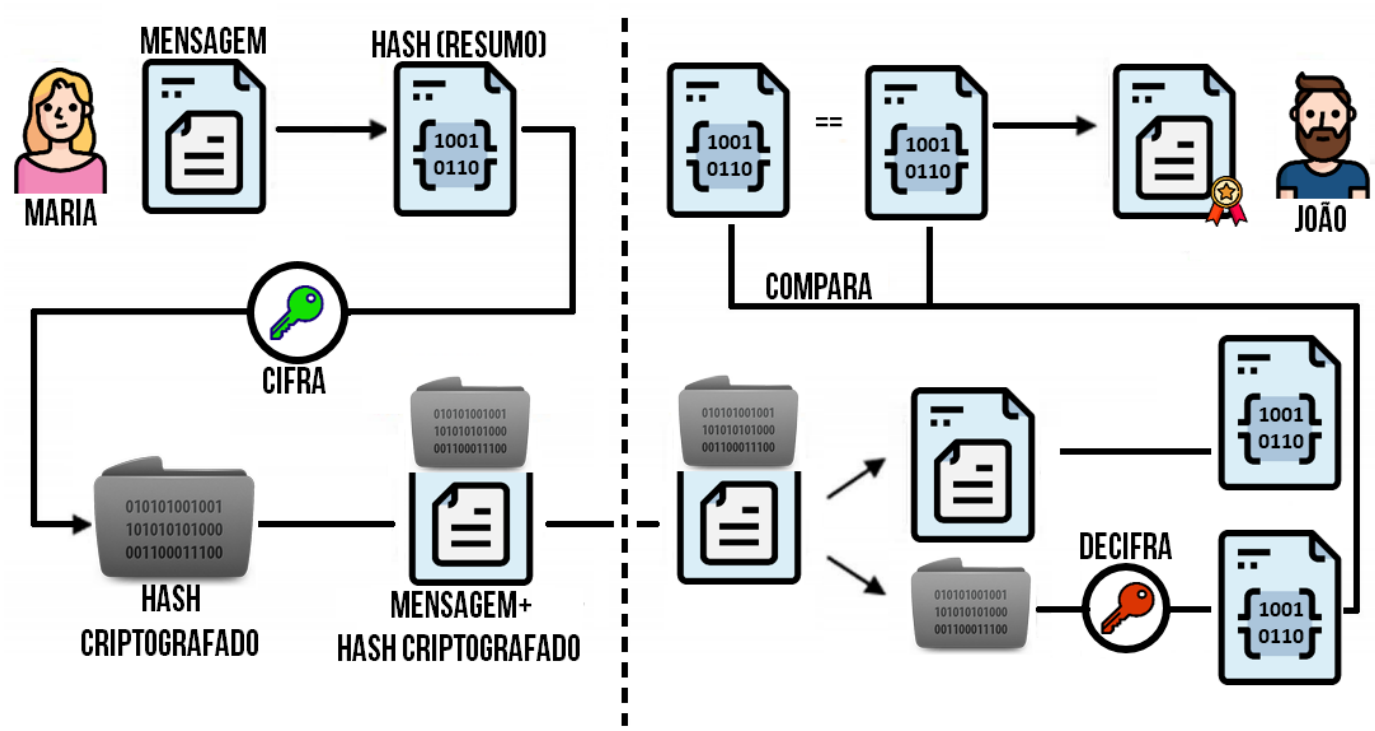
Se eu fizesse o *hash* da Bíblia inteira, daria um resultado com esse mesmo tamanho fixo acima. Quem quiser brincar um pouquinho com *hash*, basta acessar a página abaixo:

HTTPS://WWW.MD5HASHGENERATOR.COM

Quando você faz um cadastro em um site e cria uma senha, o site não armazena a sua senha – ele armazena o hash da sua senha. Por que? Porque armazenar a sua senha seria inseguro, visto que o administrador do site poderia roubá-la e utilizá-la para fins escusos. Após o cadastro, toda vez que você acessar o site com sua senha, ele gerará outro hash e comparará com o hash que ele tem salvo do cadastro. Se forem iguais, significa que você é realmente você :)

Agora qual é a relação entre Algoritmo de Hash e Assinatura Digital? **Nosso objetivo é garantir Autenticidade, Integridade e Irretratabilidade do emissor**. Nós já sabemos que – para garantir autenticidade – basta utilizar a Criptografia Assimétrica e cifrar a informação com a minha chave privada. Nós também sabemos que – para garantir a integridade – basta utilizar um Algoritmo de *Hash*. Então, combinamos essas duas estratégias para alcançar nosso objetivo.

Na figura a seguir, Maria possui uma mensagem em claro (sem criptografia). Ela gera um *hash* dessa mensagem, depois criptografa esse *hash* utilizando sua chave privada. Em seguida, **ela envia para João tanto a mensagem original quanto o seu *hash***. João gera um *hash* da mensagem original e obtém um resultado. Depois descriptografa o *hash* da mensagem utilizando a chave pública de Maria e obtém outro resultado.

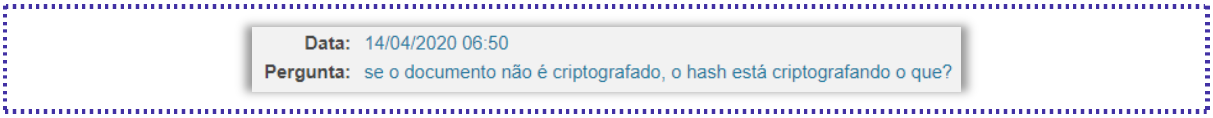


Dessa forma, ele tem dois *hashes* para comparar: o que ele gerou a partir da mensagem em claro e o que ele descriptografou a partir da mensagem criptografada. Se forem iguais, significa que Maria realmente enviou a mensagem e que ela não pode negar que enviou o documento e, por fim, significa que o documento está íntegro. **E essa é a Assinatura Digital baseada em *Hash* – ela não se preocupa com a confidencialidade, qualquer um pode visualizar a mensagem.**

Agora notem que a mensagem enviada por Maria foi recebida integralmente por João sem nenhuma modificação no meio do caminho. Além disso, João tem certeza de que foi Maria quem a enviou porque só uma mensagem criptografada com a chave privada de Maria seria descriptografada com a chave pública de Maria. **Se João tem certeza de que Maria que enviou a mensagem e que ninguém a alterou do caminho, Maria não pode negar que a enviou**.

Em outras palavras, a garantia da autenticidade e da integridade garante automaticamente a irretratabilidade ou não-repúdio. *Que fantástico, professor!* Eu sei, eu sei...

- **Principais algoritmos:** SHA-1 (Hash de 160 bits), MD5 (Hash de 128 bits), etc



Galera, eu recebi essa pergunta no fórum recentemente! **Entendam: o hash criptografa – sim – o documento, mas o documento criptografado pelo hash é enviado junto com o documento em claro.** Imagina que eu preciso lhe enviar uma mensagem, mas eu não ligo se alguém lê-la no meio do caminho – eu quero apenas que você saiba que a mensagem que você recebeu não foi modificada no meio do caminho (manteve-se íntegra).

Eu posso fazer duas cartas idênticas, mas uma eu envio dentro de uma caixa de metal trancada com um cadeado que só eu tenho, mas que a chave dele está exposta para qualquer um utilizar para confirmar minha identidade. Você receberá a carta e a caixa! Dessa forma, você pode pegar a chave (que está exposta) e testar para verificar se ela abre o meu cadeado. **Se conseguir abrir o cadeado, significa que somente eu posso tê-la enviado, visto que apenas eu possuo esse cadeado.**

Agora você tem acesso às duas cartas e pode compará-las! **Se estiverem iguais, significa que a mensagem está íntegra e que não foi modificada no meio do caminho.** *Fechou?*

(BAHIAGÁS – 2010) Uma assinatura digital é um recurso de segurança cujo objetivo é:

a) identificar um usuário apenas por meio de uma senha.
b) identificar um usuário por meio de uma senha, associada a um token.
c) garantir a autenticidade de um documento.
d) criptografar um documento assinado eletronicamente.
e) ser a versão eletrônica de uma cédula de identidade.

_____

Comentários: o objetivo da assinatura digital é garantir a autenticidade de um documento (Letra C).

Por fim, é importante diferenciar três conceitos: Identificação, Autenticação e Autorização (alguns autores incluem também a Auditoria). Na identificação, uma entidade apresenta uma informação capaz de identificá-la unicamente na base de dados de um sistema, por exemplo, um número de conta ou nome de usuário. **Caso a informação recebida pela entidade seja encontrada na base de dados, pode-se afirmar que ocorreu um processo de identificação.**

No entanto, isso não garante que a informação recebida seja autêntica. *Por que?* Porque ela pode ter informado os dados de outra entidade! Para garantir que a informação entregue pela entidade era realmente dela, é necessário utilizar algum método de autenticação como algo que ela sabe, algo que ela tem ou algo que ela é (que nós já estudamos). **Caso a informação da entidade seja autêntica, podemos deduzir que se trata de um usuário válido solicitando acesso.**

Finalmente, temos a fase de Autorização! Galera, não é porque o usuário foi identificado e autenticado que ele tem acesso a todos os recursos de um sistema. **O processo de autorização trata dos privilégios concedidos a uma entidade ao utilizar um sistema e busca verificar se essa determinada entidade tem permissão para acessar funcionalidades ou dados específicos de um sistema ou aplicação conforme é possível ver na imagem acima.**

(MPE/MA – 2013) Para permitir que seja possível aplicar medidas de segurança na internet, é necessário que os serviços disponibilizados e as comunicações realizadas por este meio garantam alguns requisitos básicos, como Identificação, Autenticação e Autorização. A Autorização visa:

a) proteger uma informação contra acesso não autorizado.
b) proteger a informação contra alteração não autorizada.
c) determinar as ações que a entidade pode executar.
d) evitar que uma entidade possa negar que foi ela quem executou uma ação.
e) garantir que um recurso esteja disponível sempre que necessário.

_____

Comentários: (a) Confidencialidade; (b) Integridade; (c) Autorização; (d) Irretratabilidade; (e) Disponibilidade (Letra C).

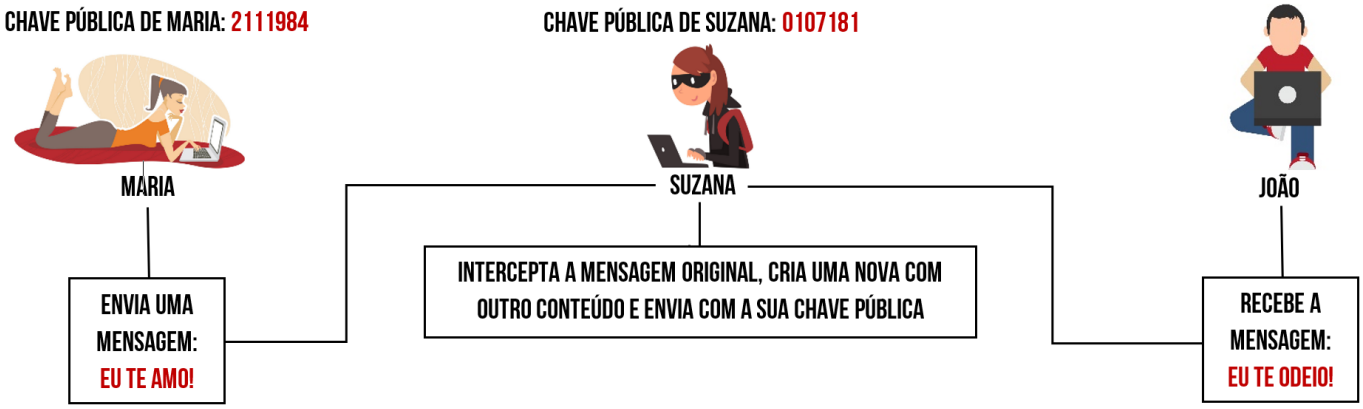
Certificado Digital

Conceitos Básicos

INCIDÊNCIA EM PROVA: ALTÍSSIMA

Foi legal estudar Assinatura Digital, mas ela tem um problema grave! Nós falamos que – se Maria quisesse enviar uma mensagem para João – ela deveria criptografá-la com a sua chave privada. Entende-se, portanto, que a chave pública de Maria esteja divulgada em algum lugar para que possa ser encontrada por qualquer pessoa ou que Maria tenha enviado de alguma forma a sua chave pública para o João.

No entanto, Suzana poderia interceptar a mensagem de Maria para João. Ela poderia jogar mensagem original fora, criar uma nova mensagem com um recado diferente, criptografá-la com a sua chave privada e enviá-la junto com a sua chave pública para João. **Quando João recebesse a mensagem, ele utilizaria a chave pública recebida (de Suzana) para descriptografar a mensagem e acharia que se tratava realmente de uma mensagem de Maria.**



É como se você criasse uma corrente em uma rede social pedindo doações para ajudar alguém que esteja precisando de um tratamento de saúde. No entanto, em vez de publicar o número da conta corrente dessa pessoa, você publicasse o seu número de conta corrente. **Isso significa que a Assinatura Digital possui uma autenticação relativamente frágil, porque não é possível saber se a chave pública que foi utilizada é realmente de quem diz ser.**

Notem que João utilizou a chave pública recebida (que ele pensava ser de Maria, mas era de Suzana) e conseguiu descriptografar a mensagem. Coitado, ele acreditou que tinha sido Maria que havia enviado e agora acha que ela o odeia! Legal, mas agora chegamos em um impasse! *Como eu vou confiar na chave pública de alguém agora, Diego?* **Para resolver esse problema, é necessária uma terceira parte confiável chamada Autoridade Certificadora (AC)**.

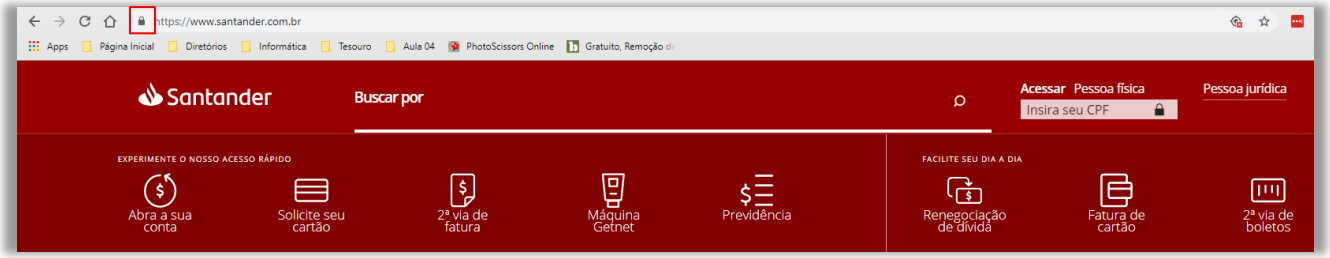
A Autoridade Certificadora é uma entidade responsável por emitir certificados digitais – ela é uma espécie de Cartório Digital. Antes da existência de cartórios, existiam muitas fraudes porque contratos eram fraudados utilizando uma cópia assinatura do contratante. Foi necessária a criação

de um cartório – uma terceira parte confiável – que armazenava a assinatura de várias pessoas. Se alguém quisesse confirmar essa assinatura, bastava ir a um cartório.

Um contrato de locação, por exemplo, possui a assinatura do locatário, locador e fiador. Cada um desses tem que ir ao cartório reconhecer firma – criada anteriormente. *Quem nunca fez isso?* Você vai ao cartório, mostra o contrato assinado e assina na frente do tabelião ou do registrador. **Dessa forma, você atesta a autoria da assinatura que consta em um documento**. *É meio frágil, vocês concordam comigo?*

A Autoridade Certificadora faz algo similar: ela mantém documentos chamados Certificados Digitais. Esse documento contém o nome, registro civil e chave pública do dono do certificado, a data de validade, versão e número de série do certificado, o nome e a assinatura digital da autoridade certificadora, algoritmo de criptografia utilizado, etc. **A Autoridade Certificadora é responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais**.

Para que uma Autoridade Certificadora também seja confiável, sua chave pública deve ser amplamente difundida de tal modo que todos possam conhecer e atestar a sua assinatura digital nos certificados gerados, o que dificulta possíveis fraudes. Vamos pensar no nosso dia-a-dia agora! *Vocês estão vendo aquele cadeado no canto esquerdo da Barra de Endereço?* Pois é... *o que será que significa esse cadeado?*

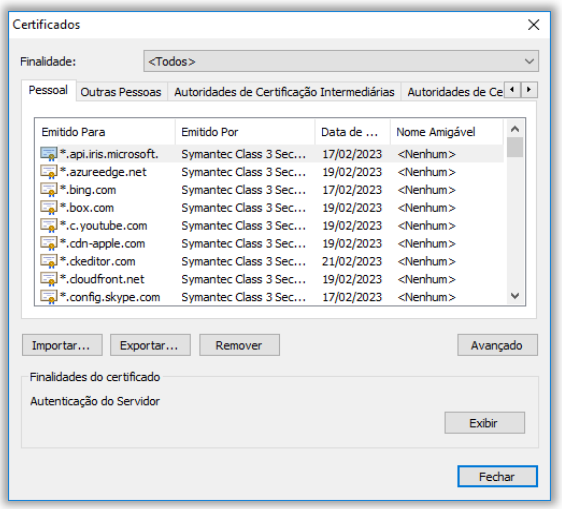


Esse cadeado significa que essa página web fornece um serviço possivelmente crítico em que trafegam informações sigilosas, portanto ela oferece um canal de comunicação criptografado e seguro. No caso, trata-se da utilização do protocolo HTTPS, que é uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo SSL/TLS (Secure Sockets Layer / Transport Layer Security).

Essa camada adicional de segurança permite que os dados possam ser transmitidos por meio de uma conexão criptografada/segura e que se verifique a autenticidade do servidor web por meio do uso de certificados digitais (é a autenticidade do servidor e, não, do cliente). Nesse caso específico, o seu navegador precisa ter garantias de que ele está trocando informações com o banco e não com outra página web se passando pelo banco. *Bacana?*

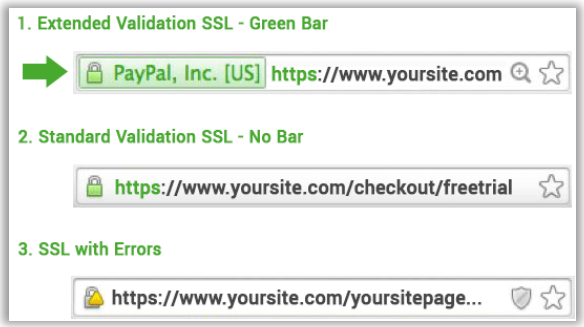
Para tal, a página do banco envia seu certificado digital, que contém seu algoritmo de criptografia, sua chave pública e a assinatura da autoridade certificadora que emitiu seu certificado. O seu navegador web possui uma lista de certificados confiáveis conforme é apresentado na imagem

abaixo. No caso do Google Chrome, essa lista fica em **Configurações > Privacidade e Segurança > Gerenciar Certificados**. *Entendido?*



O navegador verifica se a autoridade certificadora que assinou seu certificado é uma das autoridades certificadoras cadastradas. **Se realmente for, isso significa que o navegador pode confiar que o banco é legítimo e autêntico e aparecerá o cadeado (em alguns casos, verde) mostrando que a comunicação é segura**. Em algumas situações, você tentará utilizar um site cujo certificado não é confiável e o navegador informará sobre esse risco você poderá assumir o risco de acessar assim mesmo ou não. Uma Autoridade Certificadora é também responsável por publicar informações sobre certificados que não são mais confiáveis.

Sempre que ela descobre ou é informada de que um certificado não é mais confiável, ela o inclui em uma "Lista Negra", chamada de Lista de Certificados Revogados (LCR). **A LCR é um arquivo eletrônico publicado periodicamente pela Autoridade Certificadora, contendo o número de série dos certificados que não são mais válidos e a data de revogação**. Quando isso ocorre, geralmente aparece a mensagem abaixo ao tentar acessar um site.



Por fim, falemos sobre EV-SSL (Extended Validation)! Eles são tipos especiais de certificados digitais X.509 que requerem algumas exigências a mais de segurança para serem emitidos, tais como recursos visuais na barra de endereço do navegador. *Quem nunca viu uma barrinha verde ao lado do endereço?* Isso significa que não se trata de um certificado comum, mas de um certificado EV-SSL – que possui uma segurança maior!

Galera, eu recebo frequentemente algumas perguntas no fórum de dúvidas, logo vamos saná-las de uma vez por todas. A primeira é sobre a diferença entre assinatura digital e certificado digital:

ASSINATURA DIGITAL	CERTIFICADO DIGITAL
Trata-se um método matemático utilizado para verificar a autenticidade e integridade de uma entidade (mensagem, software, servidor, documento, etc).	Trata-se de um documento eletrônico assinado digitalmente por uma terceira parte confiável para vincular uma chave pública a uma entidade.
Garante a autenticidade do emissor, a integridade do documento e o não-repúdio.	Garante a confidencialidade ou a autenticidade do proprietário do certificado. Em combinação com outros recursos, pode garantir integridade e não repúdio.

Outra dúvida bastante comum trata da localização da chave privada! Sempre perguntam: *professor, a chave privada fica dentro do certificado digital?*

Não, o certificado digital é público, logo a chave privada não pode estar inserida nele. **As chaves privadas podem ficar armazenadas em um computador, token ou smartcard protegidas por alguma senha.** *Ela fica armazenada no token junto com o próprio certificado?* Sim, o token armazena ambos! *E eu tenho que memorizar a senha e a chave privada?* Não, você só precisa memorizar a senha – memorizar a chave privada é inviável!

Exemplo de chave privada: MDJKoZIAQ5MCAhvcNAQEBBQADKgAwDXcZ3OBJwlgYjDE7cZ83S O3QZZSfTiwvXqBezakBQsjQVZ1h5MCfTiwvwlgYAwEAAQ==XVOAoZIhvcNgEAAiBimNdWkSET Ibtxnzc7dBliCNBvj9qTgjQVwjSEgwEgjQVZSjQzc7dBlipLSfh5pLBjSMiGOdWCAlaQVZgYCAlghvc NAQEBYjDXVMINjDXVcNADKgAvXqBezSfTiwvKAQEBBQDQY5MCbtxnCKoZkBjSE7cZMoZIhVV jQVZSvj9qTgjQzc7BKgAwDwEgjQVZSjSE7cZMZIhvcNggjQVO3QZoZIAAwEAAQEBBAiBiZ83Se1

(TJ/RS – 2013) Assinale a alternativa que apresenta um dos dados presentes em um certificado digital.

a) Chave privada de criptografia do dono do certificado.
b) Chave única da entidade certificadora raiz.
c) Chave privada de criptografia do emissor do certificado.
d) Chave pública de criptografia do emissor do certificado.
e) Chave pública de criptografia do dono do certificado.

Comentários: ele armazena a chave pública de criptografia do dono do certificado. *E por que a Letra D está errada?* Porque o emissor do certificado é a Autoridade Certificadora e a chave pública de criptografia da Autoridade Certificadora não fica armazenada no Certificado Digital. (Letra E).

Infraestrutura de Chave Pública (ICP-Brasil)

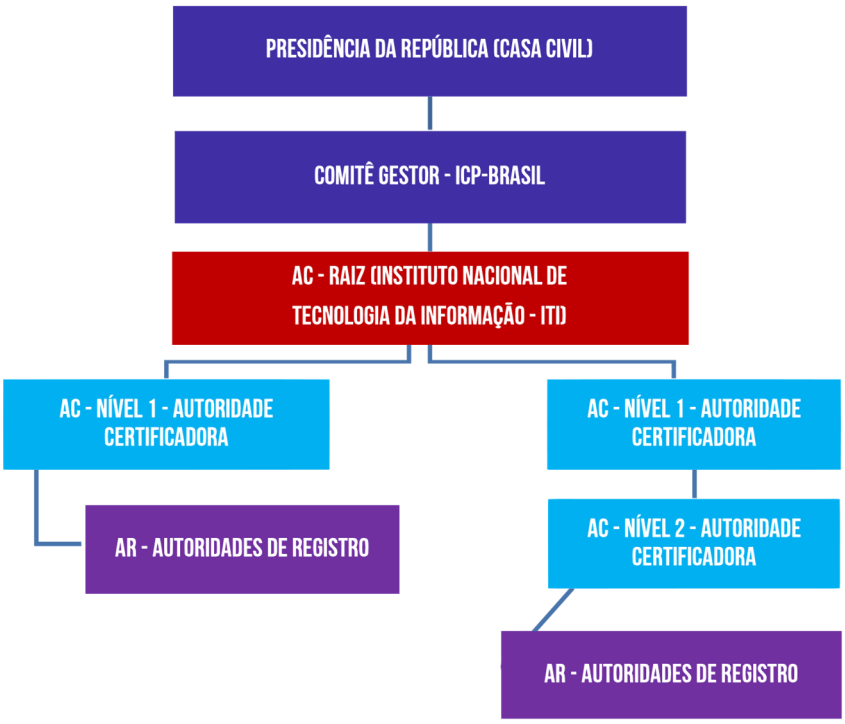
INCIDÊNCIA EM PROVA: MÉDIA

Nós vimos que uma Autoridade Certificadora é responsável por – entre outras atividades – emitir certificados digitais. No entanto, nós vimos que ela também possui um certificado digital contendo sua chave pública. *E quem emite o certificado digital para essa Autoridade Certificadora?* Pois é, nós precisamos de outra parte confiável! Para tal, existem as Infraestruturas de Chave Pública[1] (ICP). *O que é isso, Diego?*

Trata-se de uma entidade pública ou privada que tem como objetivo manter uma estrutura de emissão de chaves públicas, baseando-se no princípio da terceira parte confiável e oferecendo uma mediação de credibilidade e confiança em transações entre partes que utilizem certificados digitais. O Certificado Digital funcionará como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação.

A ICP também pode ser definida como um conjunto de técnicas, práticas, arquitetura, organização e procedimentos implementados pelas organizações públicas e privadas que suportam, em conjunto, a implementação e a operação de um sistema de certificação. Ela busca estabelecer fundamentos técnicos e metodológicos baseado em criptografia de chave pública, para garantir a autenticidade, a integridade e a validade jurídica. **A ICP brasileira é denominada ICP-Brasil!**

Nesta infraestrutura, há duas entidades: Autoridades Certificadoras e Autoridades de Registro, que emitem e vendem certificados digitais respectivamente. Vejam a cadeia de certificação:



[1] Em inglês, *Public Key Infrastructure* (PKI).

Sabe quando vamos tirar a carteira de identidade? Pois é, a maioria das pessoas procura a Secretaria de Segurança Pública (SSP), que é responsável por expedir um documento oficial de identificação atestando quem você realmente é – **seria análogo a uma Autoridade Certificadora de Nível 1**. Ela está subordinada ao Ministério da Justiça, análogo a Autoridade Certificadora Raiz. Já o Instituto de Identificação da SSP seria a Autoridade de Registro.

- **Autoridade Certificadora Raiz**

Trata-se da primeira autoridade da cadeia de certificação. Ela é responsável por executar as políticas de certificados e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. **Dessa forma, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu – isso costuma cair em prova.**

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, ela é responsável por verificar se as ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.

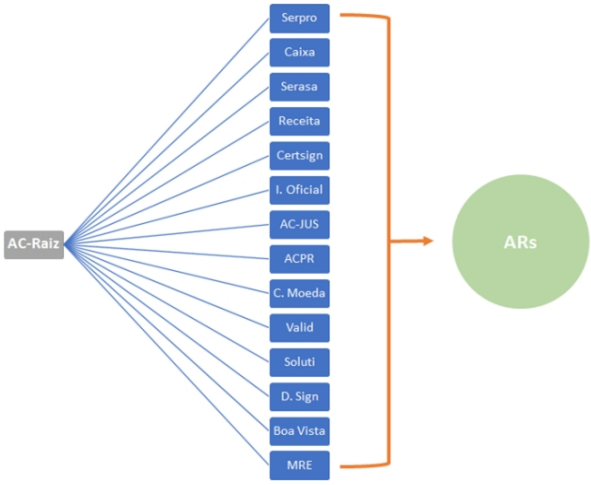
- **Autoridade Certificadora**

Trata-se de uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Busca verificar se o titular do certificado possui a chave privada que corresponde à chave pública do certificado. Ela 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.

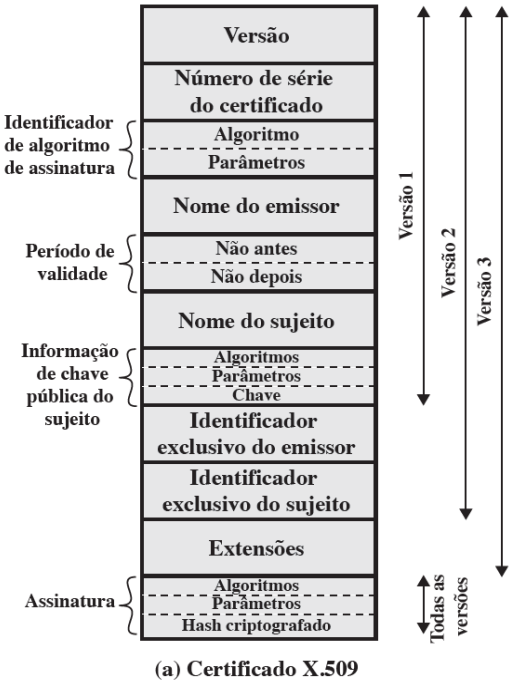
Cabe também à Autoridade Certificadora emitir Listas de Certificados Revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação – DPC. Além de estabelecer e fazer cumprir, pelas Autoridades de Registro – ARs a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada.

- **Autoridade de Registro**

Trata-se de uma entidade responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC, tem por objetivo o **recebimento, a validação, o 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. A imagem ao lado mostra um exemplo de organização.

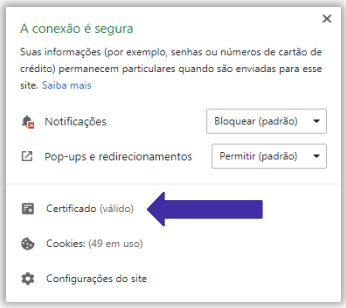


Em suma: a Autoridade Certificadora Raiz emite certificados digitais para as Autoridades Certificadoras hierarquicamente abaixo dela, que emitem certificados para equipamentos, pessoas físicas ou jurídicas. **As Autoridades de Registro não emitem certificados digitais**. Elas o recebem, validam ou encaminham e guardam um registro dessas operações. *Quem emite certificado para pessoas físicas?* Apenas a Autoridade Certificadora!

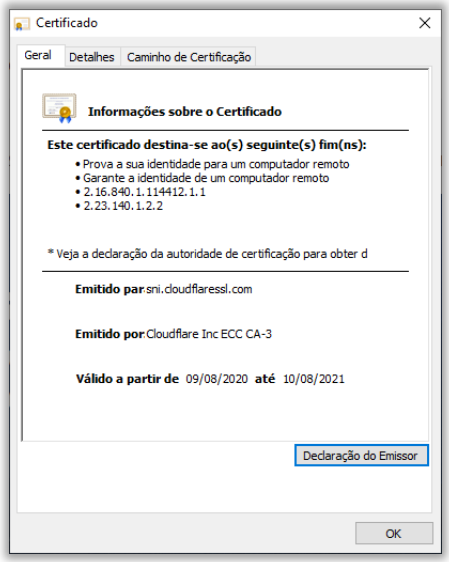


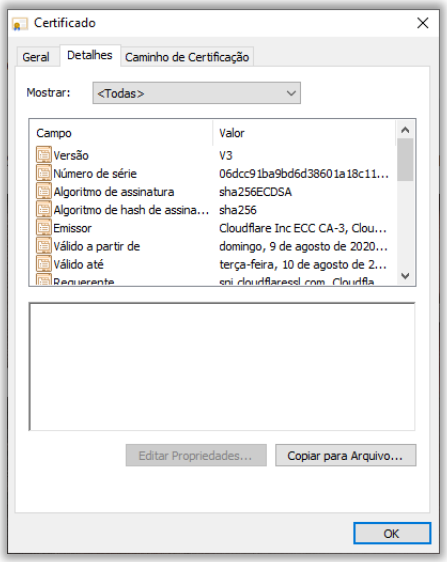
(a) Certificado X.509

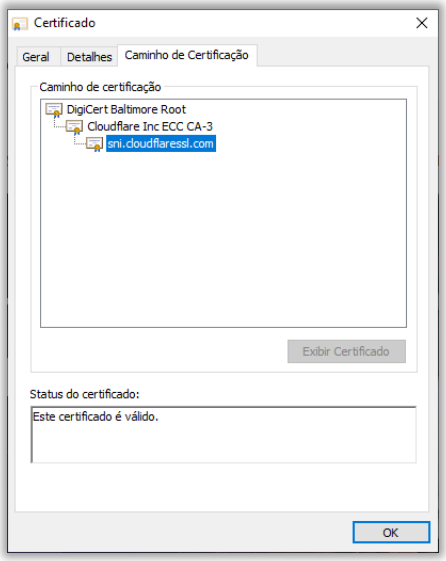
É importante ressaltar que existe um padrão para Infraestrutura de Chaves Públicas! **O Padrão X.509 (Versão 3) especifica, entre outras coisas, o formato dos certificados digitais, de tal maneira que se possa amarrar firmemente um nome a uma chave pública – esse é o padrão utilizado pela ICP-Brasil!** *Professor, quais campos existem em um certificado digital?* Existem diversos campos, sendo que nem todos são obrigatórios. Os campos são: versão, número de série, tipo de algoritmo, nome do algoritmo, nome do titular, nome do emissor, data de validade, chave pública, assinatura da autoridade certificadora, identificador da chave do titular, identificador da chave do emissor, além de diversos atributos ou extensões – vocês não precisam se preocupar em decorar esses campos. *Você quer ver um certificado digital?* Vou mostrar como você pode acessá-lo...



Abra o seu navegador favorito (Ex: Chrome, Edge, Firefox) e acesse na barra de endereços alguma página web via HTTPS (Ex: https://www.estrategiaconcursos.com.br). Em seguida, clique no cadeado à esquerda da barra de endereços e, logo depois, clique em Certificado. Um certificado digital será exibido em uma nova janela conforme podemos ver na imagem seguinte! **Nunca se esqueçam de que o certificado digital é um documento/arquivo!**





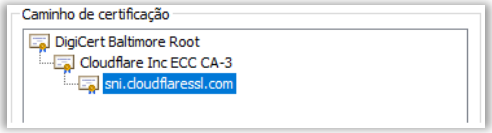


Vocês se lembram das informações contidas em um certificado digital? **Uma informação muito importante anexada ao certificado era a assinatura da autoridade certificadora que o emitiu.** Quando uma autoridade certificadora vai emitir um certificado digital, ela gera um hash de todas as informações do certificado e o assina com a sua chave privada. Dessa forma, todos que receberem o certificado digital poderão verificar sua autenticidade. *Como, professor?*

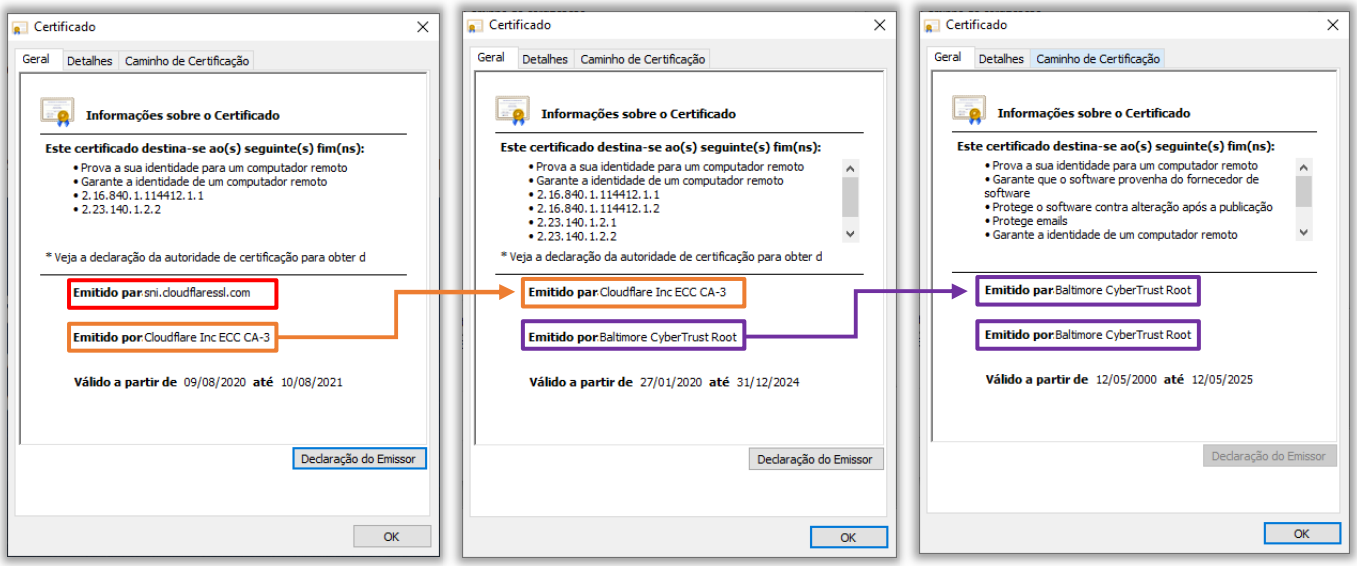
A entidade que recebeu o certificado terá em mãos o próprio certificado e seu hash anexado. Logo, ela poderá utilizar a chave pública da autoridade certificadora que emitiu o certificado para descriptografar seu hash. Em seguida, ela poderá gerar um novo hash das informações do certificado digital e comparar com o hash anexado. Se os hashes forem idênticos, significa que o certificado não foi alterado e que é confiável.

Outro conceito importante apresentado nas imagens acima é o Caminho de Certificação. *Galera, vocês se lembram que uma infraestrutura de chave pública é uma estrutura hierarquizada?* Pois é, essa hierarquia cria um caminho de certificação quando uma autoridade certificadora raiz emite um certificado com sua assinatura digital para uma ou mais autoridades certificadoras intermediárias; e uma dessas emite um certificado com a sua assinatura digital para uma entidade qualquer!

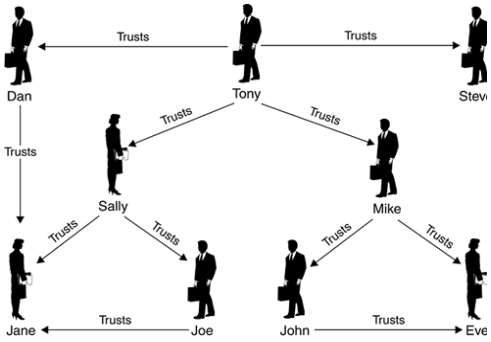
Professor, e quem é que assina o certificado da autoridade certificadora raiz? Ela mesma! **Nesse caso, dizemos que se trata de um certificado autoassinado.**



Acima nós temos o caminho de certificação do certificado da página do Estratégia Concursos. Observem a seguir que ele foi emitido para **sni.cloudflaressl.com** (que é o endereço do servidor onde a página está hospedada) e foi emitido/assinado por **Cloudflare Inc ECC CA-3** (AC intermediária). Já o certificado digital da **Cloudflare Inc ECC CA-3** foi emitido pela **Baltimore CyberTrust Root** (AC Raiz), que – no caso – emite/assina seu próprio certificado digital.



A infraestrutura de chave pública é uma abordagem interessante, mas ela é bastante hierárquica e centralizada. *E isso é um problema?* Pode ser! É possível ocorrer uma falha, vazamento ou corrupção na autoridade certificadora raiz, por exemplo. Logo, essa infraestrutura pode ser bastante vulnerável – um problema grave pode colocar em risco toda a infraestrutura. Dito isso, surgiu uma abordagem chamada Cadeia/Teia de Confiança (Web of Trust – WoT).



O que seria isso, Diego? **Trata-se de um modelo de confiança transitiva e descentralizada que busca disponibilizar criptografia para o público geral sem custos em contrapartida à abordagem de infraestrutura de chave pública.** *E como isso funciona, professor?* A confiança vai sendo estabelecida através de uma rede de transitividade em que, se Tony confia em Mike e Mike confia em John, então Tony confia em John.

Essa rede é construída por meio de uma relação pessoal indivíduos através da assinatura de chave pública de um usuário pelo outro e assim sucessivamente. **Essas etapas acabam por gerar um laço**

de confiança que se converte, então, em uma rede, teia ou cadeia de confiança. Dito isso, é importante fazer essa distinção: em uma infraestrutura de chave pública, todo certificado deve necessariamente ser assinado por uma autoridade certificadora.

Já em uma cadeia/teia de certificados, qualquer entidade pode assinar e atestar a validade de outros certificados. **Ela é – portanto – descentralizada e não hierárquica.**

(MEC – 2011) Um certificado digital consiste na cifração do resumo criptográfico de uma chave pública com a chave privada de uma autoridade certificadora.

_____

Comentários: sendo rigoroso, um certificado digital consiste na cifração do resumo criptográfico de todas as informações que abrangem o certificado digital e não apenas a chave pública – ignorando esse deslize, não há erros na questão (Correto).

(SERPRO – 2013) Um certificado digital consiste na cifração do resumo criptográfico de uma chave pública com a utilização da chave privada de uma autoridade certificadora.

_____

Comentários: sendo rigoroso, um certificado digital consiste na cifração do resumo criptográfico de todas as informações que abrangem o certificado digital e não apenas a chave pública – ignorando esse deslize, não há erros na questão (Correto).

(TRF/2 – 2017) "*O certificado digital ICP-Brasil funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web*".

(Sítio do Instituto Nacional de Tecnologia da Informação. Disponível em: http://www.iti.gov.br/certificacao-digital/o-que-e).

Referente à certificação digital, assinale a alternativa correta.

a) A Autoridade Certificadora Raiz é quem emite os certificados para o usuário final.
b) A criptografia simétrica utiliza duas chaves distintas: chave privada e chave pública.
c) A Autoridade Certificadora é a primeira autoridade da cadeia de certificação da ICP-Brasil.
d) O Instituto Nacional de Tecnologia da Informação é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

_____

Comentários: (a) Errado, Autoridade Certificadora Raiz emite certificados para Autoridades Certificadores hierarquicamente abaixo; (b) Errado, essa é a Criptografia Assimétrica; (c) Errado, essa é a Autoridade Certificadora Raiz; (d) Correto, ITI é a AC-Raiz do ICP-Brasil (Letra D).

Tipos de Certificado

INCIDÊNCIA EM PROVA: MÉDIA

Os certificados digitais da Categoria A costumam ser usados para fins de identificação e autenticação. Você pode usá-los para assinar documentos ou validar transações eletrônicas. Já a Categoria S é direcionada a atividades sigilosas, como a proteção de arquivos confidenciais.

- **Certificado de Assinatura Digital (A):** reúne os certificados de assinatura digital, utilizados na confirmação de identidade na web, em e-mails, em Redes Privadas Virtuais (VPNs) e em documentos eletrônicos com verificação da integridade das informações.

- **Certificado de Sigilo (S):** reúne os certificados de sigilo, que são utilizados na codificação de documentos, de bases de dados relacionais, de mensagens e de outras informações eletrônicas sigilosas.

TIPO	GERAÇÃO DO PAR DE CHAVES	TAMANHO DA CHAVE (BITS)	ARMAZENAMENTO	VALIDADE (ANOS)
CERTIFICADO A1/S1	POR SOFTWARE	RSA 1024 OU 2048	DISCO RÍGIDO (HD) E PENDRIVE	1
CERTIFICADO A2/S2	POR SOFTWARE	RSA 1024 OU 2048	SMARTCARD (COM CHIP) OU TOKEN USB	2
CERTIFICADO A3/S3	POR HARDWARE	RSA 1024 OU 2048	SMARTCARD (COM CHIP) OU TOKEN USB	5
CERTIFICADO A4/S4	POR HARDWARE	RSA 2048 OU 4096	SMARTCARD (COM CHIP) OU TOKEN USB	6

(SEFAZ/PE – 2014) Duas séries de certificados previstos na ICP-Brasil são descritas a seguir:

I. Reúne os certificados de assinatura digital, utilizados na confirmação de identidade na web, em e-mails, em Redes Privadas Virtuais (VPNs) e em documentos eletrônicos com verificação da integridade das informações.

II. Reúne os certificados de sigilo, que são utilizados na codificação de documentos, de bases de dados, de mensagens e de outras informações eletrônicas sigilosas.

As séries de certificados I e II são categorizadas, respectivamente, de:

a) B e C.
b) A e B.
c) B e D.
d) A e F.
e) A e S.

_____

Comentários: (I) trata-se dos Certificados de Assinatura Digital (A); (II) trata-se dos Certificados de Sigilo (S); (Letra E).

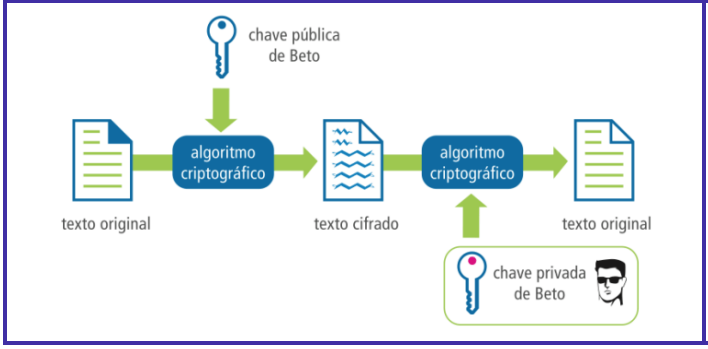
RESUMO

PRINCÍPIOS DE SEGURANÇA	DESCRIÇÃO
CONFIDENCIALIDADE	Capacidade de um sistema de não permitir que informações estejam disponíveis ou sejam reveladas a entidades não autorizadas – incluindo usuários, máquinas, sistemas ou processos.
INTEGRIDADE	Capacidade de garantir que a informação manipulada está correta, fidedigna e que não foi corrompida – trata da salvaguarda da exatidão e completeza da informação.
DISPONIBILIDADE	Propriedade de uma informação estar acessível e utilizável sob demanda por uma entidade autorizada.

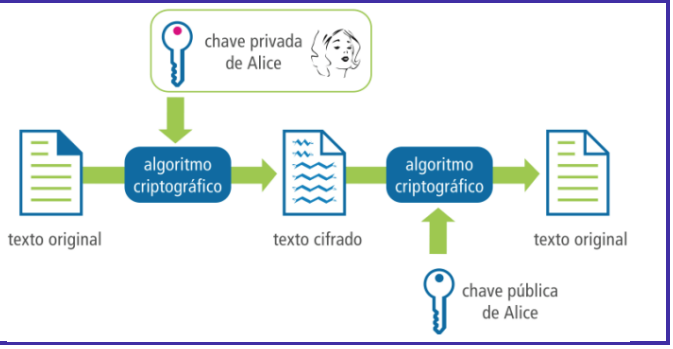
PRINCÍPIOS ADICIONAIS	DESCRIÇÃO
AUTENTICIDADE	Propriedade que trata da garantia de que um usuário é de fato quem alega ser. Em outras palavras, ela garante a identidade de quem está enviando uma determinada informação.
IRRETRATABILIDADE	Também chamada de Irrefutabilidade ou Não-repúdio, trata da capacidade de garantir que o emissor da mensagem ou participante de um processo não negue posteriormente a sua autoria.

TIPO DE CRIPTOGRAFIA	DESCRIÇÃO
CRIPTOGRAFIA SIMÉTRICA (CHAVE SECRETA)	Utiliza um algoritmo e uma única chave secreta para cifrar/decifrar que tem que ser mantida em segredo.
CRIPTOGRAFIA ASSIMÉTRICA (CHAVE PÚBLICA)	Utiliza um algoritmo e um par de chaves para cifrar/decifrar – uma pública e a outra tem que ser mantida em segredo.
CRIPTOGRAFIA HÍBRIDA (CHAVE PÚBLICA/SECRETA)	Utiliza um algoritmo de chave pública apenas para trocar chaves simétricas – chamadas chaves de sessão – de forma segura. Após a troca, a comunicação é realizada utilizando criptografia simétrica.

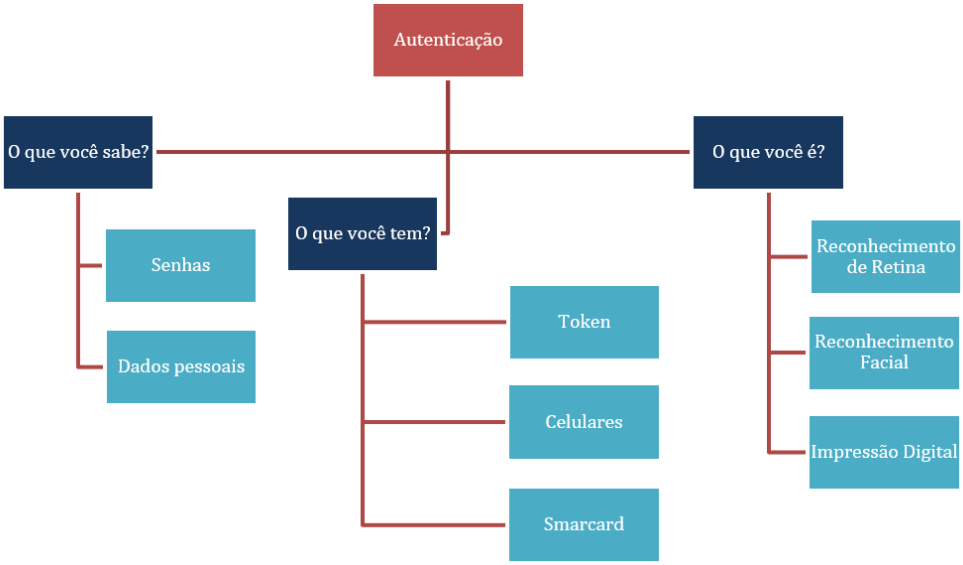
CRIPTOGRAFIA ASSIMÉTRICA UTILIZADA PARA GARANTIR O PRINCÍPIO DA CONFIDENCIALIDADE



CRIPTOGRAFIA ASSIMÉTRICA UTILIZADA PARA GARANTIR O PRINCÍPIO DA AUTENTICIDADE



O emissor criptografa o texto original com a chave pública do receptor de forma que somente ele consiga descriptografá-lo com sua chave privada para visualizar o texto original.	O emissor criptografa o texto original com sua chave privada de forma que o receptor possa descriptografá-lo com a chave pública do emissor.



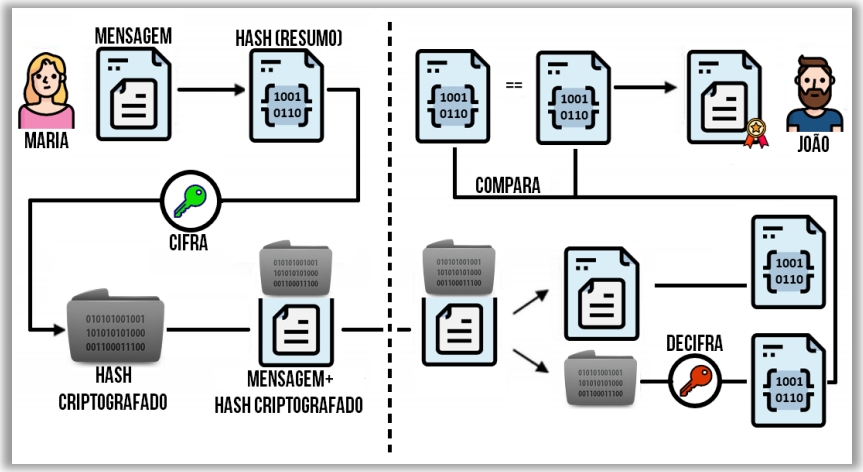
MÉTODOS DE AUTENTICAÇÃO	DESCRIÇÃO
O QUE VOCÊ SABE?	Trata-se da autenticação baseada no conhecimento de algo que somente você sabe, tais como: senhas, frases secretas, dados pessoais aleatórios, entre outros.
O QUE VOCÊ É?	Trata-se da autenticação baseada no conhecimento de algo que você é, como seus dados biométricos.
O QUE VOCÊ TEM?	Trata-se da autenticação baseada em algo que somente o verdadeiro usuário possui, tais como: celulares, crachás, Smart Cards, chaves físicas, tokens, etc.

AUTENTICAÇÃO FORTE

Trata-se de um tipo de autenticação que ocorre quando se utiliza pelo menos dois desses três métodos de autenticação. Um exemplo é a Autenticação em Dois Fatores (ou Verificação em Duas Etapas).

ASSINATURA DIGITAL

Trata-se de um método matemático de autenticação de informação digital tipicamente tratado como substituto à assinatura física, já que elimina a necessidade de ter uma versão em papel do documento que necessita ser assinado. Por meio de um Algoritmo de Hash, é possível garantir a integridade dos dados.



FUNCIONAMENTO DA ASSINATURA DIGITAL

Maria possui uma mensagem em claro (sem criptografia). Ela gera um hash dessa mensagem, depois criptografa esse hash utilizando sua chave privada. Em seguida, ela envia para João tanto a mensagem original quanto o seu hash. João gera um hash da mensagem original e obtém um resultado, depois descriptografa o hash da mensagem utilizando a chave pública de Maria e obtém outro resultado. Dessa forma, ele tem dois hashes para comparar: o que ele gerou a partir da mensagem em claro e o que ele descriptografou a partir da mensagem criptografada. Se forem iguais, significa que Maria realmente enviou a mensagem, significa que ela não pode negar que enviou a mensagem e, por fim, significa que a mensagem está íntegra.

CERTIFICADO DIGITAL

Certificado Digital é um documento eletrônico assinado digitalmente por uma terceira parte confiável – chamada Autoridade Certificadora – e que cumpre a função de associar uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas com o intuito de tornar as comunicações mais confiáveis e auferindo maior confiabilidade na autenticidade. Ele é capaz de garantir a autenticidade, integridade e não-repúdio, e até confidencialidade.

TIPO	GERAÇÃO DO PAR DE CHAVES	TAMANHO DA CHAVE (BITS)	ARMAZENAMENTO	VALIDADE MÁXIMA (ANOS)
CERTIFICADO A1/S1	POR SOFTWARE	RSA 1024 OU 2048	DISCO RÍGIDO (HD) E PENDRIVE	1
CERTIFICADO A2/S2	POR SOFTWARE	RSA 1024 OU 2048	SMARTCARD (COM CHIP) OU TOKEN USB	2
CERTIFICADO A3/S3	POR HARDWARE	RSA 1024 OU 2048	SMARTCARD (COM CHIP) OU TOKEN USB	5
CERTIFICADO A4/S4	POR HARDWARE	RSA 2048 OU 4096	SMARTCARD (COM CHIP) OU TOKEN USB	6

GARANTIAS

A criptografia por si só garante apenas **confidencialidade**! No entanto, quando utilizamos algoritmos criptográficos, nós acrescentamos mecanismos que nos ajudam a garantir outros serviços de segurança da informação. Em outras palavras, algoritmos de criptografia simétrica permitem garantir **confidencialidade**, **autenticidade** e **integridade**. Já algoritmos de criptografia assimétrica permitem garantir **confidencialidade**, **autenticidade**, **integridade** e **não-repúdio**. Notem que nem todos poderão ser garantidos simultaneamente!

PARA MAIS DICAS: WWW.INSTAGRAM.COM/PROFESSORDIEGOCARVALHO

MAPA MENTAL


Segurança da Informação
Controles de Segurança
• CONTROLES FÍSICOS: BARREIRAS FÍSICAS QUE IMPEDEM OU LIMITAM O ACESSO DIRETO ÀS INFORMAÇÕES OU À INFRAESTRUTURA QUE CONTÉM AS INFORMAÇÕES.
EX: PORTAS, TRANCAS, COFRES, ALARMES, ETC.
• CONTROLES LÓGICOS: (CONTROLES TÉCNICOS) BARREIRAS QUE IMPEDEM OU LIMITAM O ACESSO À INFORMAÇÃO POR MEIO DE MONITORAMENTO E CONTROLE DE ACESSO.
EX: SENHAS, FIREWALLS, CRIPTOGRAFIA, ETC.
Princípios Fundamentais
(PREVALECIDOS)
• CONFIDENCIALIDADE: NÃO PERMITIR QUE INFORMAÇÕES SEJAM DISPONÍVEIS OU SEJAM REVELADAS POR PESSOAS NÃO AUTORIZADAS.
• INTEGRIDADE: GARANTIR QUE A INFORMAÇÃO MANIPULADA ESTÁ CORRETA, FIDEDIGNA, E QUE NÃO FOI CORROMPIDA (ALTERADA SEM AUTORIZAÇÃO) NO PERCURSO.
• DISPONIBILIDADE: GARANTIR QUE A INFORMAÇÃO ESTARÁ ACESSÍVEL E UTILIZÁVEL SOB DEMANDA POR UMA ENTIDADE AUTORIZADA.
Princípios Adicionais
• AUTENTICIDADE: GARANTIR QUE O USUÁRIO EMISSOR DA MENSAGEM É DE FATO QUEM ALEGA SER.
• IRRETRATABILIDADE: (IRRECUSABILIDADE OU NÃO-REPÚDIO) GARANTIR QUE O EMISSOR DA MENSAGEM OU PARTICIPANTE DE UM PROCESSO NÃO NEGUE POSTERIORMENTE SUA AUTORIA.
@mapasdathai
Criptologia
• OCULTAÇÃO DE INFORMAÇÕES: ESTEGANOGRAFIA OU CRIPTOGRAFIA
• QUEBRA DOS SEGREDOS DE OCULTAÇÃO: CRIPTOANÁLISE
Esteganografia: OCULTAR UMA MENSAGEM DENTRO DE OUTRA MENSAGEM.
Criptografia: TÉCNICA DE TORNAR UMA MENSAGEM INTELIGÍVEL.
• PRINCIPAIS FUNDAMENTOS:
• SUBSTITUIÇÃO: CADA ELEMENTO É MAPEADO POR OUTRO ≠ EMEANTO.
• TRANSPOSIÇÃO: OS ELEMENTOS SÃO REORGANIZADOS.
• SEGREDO ESSENCIAL: NENHUMA INFORMAÇÃO PODE SER PERDIDA.
CÓDIGOS: PALAVRAS, FRASES, SÍMBOLOS QUE SUBSTITUEM ELEMENTOS.
CIFRAS: ALGORITMOS DE CRIPTOGRAFIA E DESCRIPTOGRAFIA.
CHAVE DE ENCRIPTAÇÃO
• CRIPTOGRAFIA SIMÉTRICA: USA UMA CHAVE SIMÉTRICA COMPARTILHADA TANTO P/ CODIFICAR QUANTO PARA DECODIFICAR.
• GARANTE CONFIDENCIALIDADE, MAS NÃO GARANTE INTEGRIDADE E AUTENTICIDADE.
• DESVANTAGEM: O INCONVENIENTE DE TER QUE COMPARTILHAR A CHAVE.
• PRINCIPAIS ALGORITMOS: DES, 3DES, AES, BLOWFISH, CIFRAGEM DE JÚLIO CÉSAR, ETC.
CRIPTOGRAFIA DE CHAVE PÚBLICA
• CRIPTOGRAFIA ASSIMÉTRICA: USA UMA CHAVE PÚBLICA E UMA CHAVE PRIVADA QUE FORMAM UM PAR EXCLUSIVO.
•GARANTE CONFIDENCIALIDADE SE:
- EMISSOR → UTILIZA A CHAVE PÚBLICA DO DESTINATÁRIO PARA CRIPTOGRAFAR.
- DESTINATÁRIO → UTILIZA SUA CHAVE PRIVADA PARA DESCRIPTOGRAFAR.
• GARANTE AUTENTICIDADE SE:
- EMISSOR → UTILIZA SUA CHAVE PRIVADA PARA CRIPTOGRAFAR.
- DESTINATÁRIO → UTILIZA A CHAVE PÚBLICA DO EMISSOR P/ DESCRIPTOGRAFAR.
• PRINCIPAIS ALGORITMOS: RSA, DSA, ECDSA, ETC.
• DESVANTAGEM: AS CHAVES SÃO MAIORES E POR ISSO A CRIPTOGRAFIA É MAIS LOCA X MAIS LENTA
• CRIPTOGRAFIA HÍBRIDA: USA A CRIPTOGRAFIA ASSIMÉTRICA APENAS PARA TROCAR CHAVES SIMÉTRICAS (CHAVES DE SESSÃO) DE FORMA SEGURA.
• UTILIZADO POR PROTOCOLOS COMO O SSL (SECURE SOCKETS LAYER) E O TLS (TRANSPORT LAYER SECURITY)
Autenticidade
Métodos
• O QUE VOCÊ SABE? SENHAS, PINOS PESSOAIS.
• O QUE VOCÊ TEM? TOKEN, CELULAR, SMARTCARD.
• O QUE VOCÊ É? BIOMETRIA.
Autenticação Forte
• UTILIZA A COMBINAÇÃO DE PELO MENOS 2 MÉTODOS
Assinatura Digital
• É O HASH DA MENSAGEM CRIPTOGRAFADO COM A CHAVE PRIVADA DO EMISSOR, ANEXADA AO ARQUIVO, PARA PROVER:
• INTEGRIDADE
• NÃO-REPÚDIO.
• AUTENTICIDADE
ASSINATURA

Assinatura Digital

Algoritmo de Hash

- ALGORITMO CRIPTOGRÁFICO QUE TRANSFORMA UMA ENTRADA DE DADOS DE QUALQUER TAMANHO EM UMA SAÍDA DE DADOS DE TAMANHO FIXO.
- UMA BOA FUNÇÃO DE HASH NÃO PERMITE QUE SE DESCUBRA OS DADOS DE ENTRADA PELA ANÁLISE DOS DADOS DA SAÍDA.
- DIFERENTES ENTRADAS PODEM GERAR A MESMA SAÍDA → COLISÃO.
- P/ REDUZIR O RISCO DE COLISÃO → AUMENTA-SE O TAMANHO FIXO DE SAÍDA (PELO MENOS 128 BITS).
- USA CHAVES ASSIMÉTRICAS: O EMISSOR USA SUA CHAVE PRIVADA P/ ENCRIPTAR E O RECEPTOR USA A CHAVE PÚBLICA DO EMISSOR P/ DECRIPTAR O HASH.

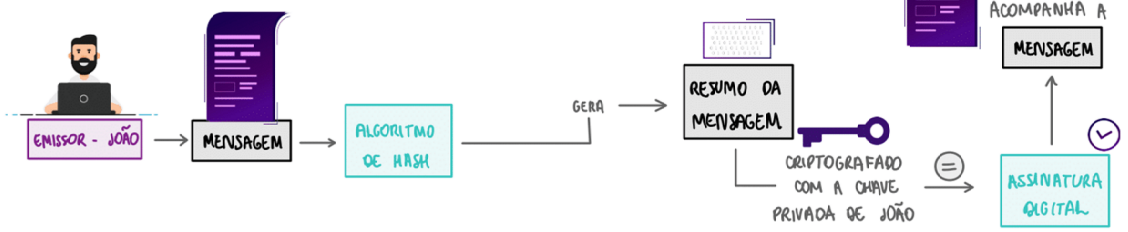
Observações Gerais

GARANTE:

- INTEGRIDADE: UTILIZANDO O ALGORITMO DE HASH;
- NÃO-REPÚDIO: COMBINANDO INTEGRIDADE E AUTENTICIDADE; ASSINATURA
- AUTENTICIDADE: CRIPTOGRAFANDO COM A CHAVE PRIVADA.
- NÃO GARANTE CONFIDENCIALIDADE!
  - NÃO CRIPTOGRAFA O CONTEÚDO DA MENSAGEM
- PRINCIPAIS ALGORITMOS: SHA-1 (HASH DE 160bits), MD5 (HASH DE 128bits), ETC.

Passo a Passo do Algoritmo de Hash

1. MENSAGEM É ESCRITA PELO EMISSOR;
2. CÁLCULO DO HASH DA MENSAGEM P/ GARANTIR INTEGRIDADE;
3. HASH ENCRIPTADO (COM A CHAVE PRIVADA DO EMISSOR) = ASSINATURA DIGITAL;
4. MENSAGEM ASSINADA DIGITALMENTE É TRANSMITIDA POR UM CANAL DE COMUNICAÇÃO;
5. MENSAGEM RECEBIDA E LEGÍVEL (NÃO HÁ CONFIDENCIALIDADE);
6. HASH DECRIPTADO (COM A CHAVE PÚBLICA DO EMISSOR);
7. CÁLCULO DO HASH DA MENSAGEM RECEBIDA;
8. HASH DECRIPTADO CONFRONTADO COM O HASH DA MENSAGEM RECEBIDA PARA VERIFICAÇÃO DE INTEGRIDADE;
9. SE OS HASHS FOREM IGUAIS → MENSAGEM AUTÊNTICA, ÍNTEGRA E IRREFUTÁVEL.



@mapasdathai

Certificado Digital

Conceito

- DOCUMENTO ELETRÔNICO ASSINADO DIGITALMENTE POR UMA TERCEIRA PARTE CONFIÁVEL (AUTORIDADE CERTIFICADORA) E QUE CUMPRE A FUNÇÃO DE ASSOCIAR UMA ENTIDADE (PESSOA, PROCESSO, SERVIDOR, ETC) A UM PAR DE CHAVES CRIPTOGRÁFICAS COM O INTUITO DE TORNAR AS COMUNICAÇÕES MAIS CONFIÁVEIS.

Autoridade Certificadora Raiz

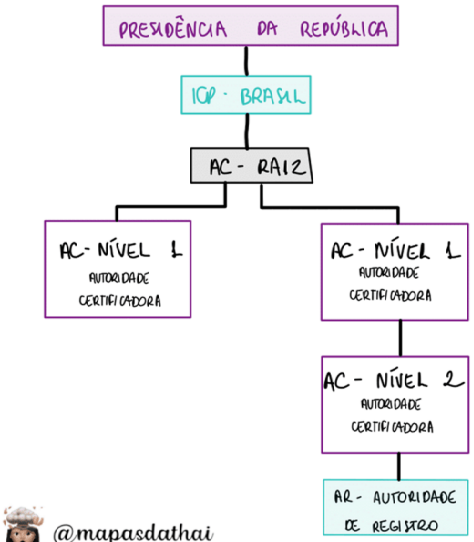
- PRIMEIRA AUTORIDADE NA CADEIA DE CERTIFICAÇÃO;
- EXECUTA AS POLÍTICAS E NORMAS DEFINIDAS PELO ICP-BRASIL;
- EMITE, EXPEDE, DISTRIBUI, REVOGA E GERENCIA OS CERTIFICADOS DAS AUTORIDADES CERTIFICADORAS DE NÍVEIS SUBSEQUENTES;
- EMITE A LCR (LISTA DE CERTIFICADOS REVOGADOS);
- FISCALIZA E AUDITA AS ACs, AS ARs E OUTRAS PRESTADORAS DE SERVIÇO HABILITADAS NA ICP-BRASIL.

Autoridade Certificadora

- EMITE, DISTRIBUI, RENOVA, REVOGA E GERENCIA CERTIFICADOS DIGITAIS;
- BUSCA VERIFICAR SE O TITULAR DO CERTIFICADO POSSUI A CHAVE PRIVADA QUE CORRESPONDE À CHAVE PÚBLICA DO CERTIFICADO;
- CRIA E ASSINA DIGITALMENTE O CERTIFICADO DO ASSINANTE;
- EMITE A LCR;
- MANTÉM REGISTRO DE SUAS OPERAÇÕES;
- ESTABELECE E FAZ AS ARs A ELA VINCULADAS CUMPRIREM AS POLÍTICAS DE SEGURANÇA P/ GARANTIR A AUTENTICIDADE DA IDENTIFICAÇÃO.

Infraestrutura de Chave Pública (ICP Brasil)

- ENTIDADE QUE MANTÉM UMA ESTRUTURA DE EMISSÃO DE CHAVES PÚBLICAS;
- TERCEIRA PARTE CONFIÁVEL;
- É QUEM EMITE O CERTIFICADO DIGITAL DA AUTORIDADE CERTIFICADORA;
- DEFINE UM CONJUNTO DE TÉCNICAS, PRÁTICAS E PROCEDIMENTOS A SEREM ADOTADOS PELAS ENTIDADES;
- ICP-BRASIL = AUTORIDADES CERTIFICADORAS + AUTORIDADES DE REGISTRO.



@mapasdathai

Autoridade de Registro

- É RESPONSÁVEL PELA INTERFACE ENTRE O USUÁRIO E A AUTORIDADE CERTIFICADORA;
- É VINCULADA A UMA AC;
- RECEBE, VALIDA E ENCAMINHA SOLICITAÇÃO DE EMISSÃO OU REVOGAÇÃO DE CERTIFICADOS;
- IDENTIFICA, DE FORMA PRESENCIAL, OS SOLICITANTES;
- MANTÉM REGISTRO DE SUAS OPERAÇÕES.

AS ARs NÃO EMITEM CERTIFICADOS!

Tipos de Certificado

- CERTIFICADOS DE ASSINATURA DIGITAL (A): CONFIRMAÇÃO DE IDENTIDADE NA WEB, EM E-MAILS, EM VPNs E DOCUMENTOS ELETRÔNICOS
- CERTIFICADOS DE SIGILO (S): CODIFICAÇÃO DE DOCUMENTOS, DE BASES DE DADOS E OUTRAS INFORMAÇÕES SIGILOSAS.

TIPO	GERAÇÃO DO PAR DE CHAVES	TAMANHO MÍNIMO	ARMAZENAMENTO	VALIDADE (ANOS)
A1 / S1	SOFTWARE	1024 BITS	DISCO RÍGIDO (HD) E PENDRIVE	1
A2 / S2	SOFTWARE	1024 BITS	SMARTCARD OU TOKEM USB	2
A3 / S3	HARDWARE	1024 BITS	SMARTCARD OU TOKEN USB	5
A4 / S4	HARDWARE	2048 BITS	SMARTCARD OU TOKEN USB	6

QUESTÕES COMENTADAS – DIVERSAS BANCAS

1. **(IADES / BRB – 2022)** As propriedades que garantem que o dado é correto e consistente com o estado ou informação pretendida, e que asseguram os limites de quem pode obtê-la são definidas respectivamente, como

a) integridade e confidencialidade.
b) integridade e disponibilidade.
c) disponibilidade e integridade.
d) consistência e autenticidade.
e) Consistência e confidencialidade.

Comentários:

A propriedade que garante que o dado é correto e consistente com o estado ou informação pretendida é a integridade; já a propriedade que garante que os limites de quem pode obtê-la é chamado de confidencialidade.

Gabarito: Letra A

---

2. **(FUNDATEC / IPE SAÚDE – 2022)** A política de segurança da informação estabelece como as informações são acessadas, tendo como objetivo manter os três pilares da segurança da informação, que são:

a) Confidencialidade, velocidade e armazenamento.
b) Confidencialidade, integridade e disponibilidade.
c) Conectividade, confiabilidade e disponibilidade.
d) Velocidade, controle de acesso e atualização da informação.
e) Velocidade, confiabilidade e controle de acesso.

Comentários:

Os pilares da segurança da informação são conhecidos como CID (Confidencialidade, Integridade e Disponibilidade).

Gabarito: Letra B

---

3. **(FADESP / SEFA-PA – 2022)** Na assinatura digital são utilizadas:

a) a chave pública do receptor e a chave privada do receptor
b) a chave pública do emissor e a chave privada do emissor.
c) a chave pública do receptor e a chave privada do emissor

d) a chave privada do receptor e a chave pública do emissor.
e) as chaves secretas do emissor.

Comentários:

Na assinatura digital, são utilizadas a chave privada do emissor (para criptografar) e a chave pública do emissor (para descriptografar).

Gabarito: Letra B

---

4. **(FADESP / SEFA-PA – 2022)** A forma de realizar assinatura digital baseada em logaritmos discretos, em que o trabalho principal para a geração de assinatura que não depende da mensagem pode ser feito durante o tempo ocioso do processador, e a parte da geração da assinatura que depende da mensagem exige multiplicar um inteiro de 2n bits por um inteiro de n bits, é conhecida como:

a) SCHNORR.
b) ELGAMAL.
c) DSA.
d) Curva Elíptica.
e) RSA-PSS.

Comentários:

Questão de nível surreal! É o tipo de questão que eu sugiro simplesmente chutar e ser feliz. Esse nível de aprofundamento não é cobrado nem para analistas de sistemas – talvez para cargos específicos de segurança da informação. De todo modo, a questão trata de Assinatura de Schnorr, que é um protocolo de assinatura digital baseado no problema do logaritmo discreto.

Gabarito: Letra A

---

5. **(FADESP / SEFA-PA – 2022)** A característica do modo de operação de cifra de bloco em que a entrada do algoritmo de encriptação é o XOR dos próximos 64 bits de texto claro e os 64 bits anteriores de texto cifrado é conhecida como:

a) Electronic Codebook (EBC).
b) Cipher Block Chaining (CBC).
c) Cipher Feedback (CFB).
d) Ouput Feedback (OFB).
e) Counter (CTR).

Comentários:

Questão de nível completamente absurdo! É o tipo de questão que eu sugiro simplesmente chutar e ser feliz. Esse nível de aprofundamento não é cobrado nem para analistas de sistemas – talvez para cargos específicos de segurança da informação. De todo modo, existem cinco modos de operação de cifra de bloco: ECB, CBC, CFB, OFB e CTR. A característica do modo de operação de cifra de bloco em que a entrada do algoritmo de encriptação é o XOR dos próximos 64 bits de texto claro e os 64 bits anteriores de texto cifrado é conhecida como CBC (Cipher Block Chaining).

Gabarito: Letra B

---

6. **(FADESP / SEFA-PA – 2022)** A forma de controle de acesso lógico, em que o dono dos dados e os usuários individuais são capazes de definir, ao seu critério, qual acesso será permitido aos seus dados independentemente da política, é definida como um controle de acesso:

a) mandatório
b) baseado na função.
c) discricionário
d) baseado em reivindicações
e) seletista

Comentários:

O Controle de Acesso Discricionário (DAC) é um tipo de controle de acesso de segurança que concede ou restringe o acesso ao objeto por meio de uma política de acesso determinada pelo grupo de proprietários de um objeto. O Controle de Acesso Discricionário é dito discricionário porque o proprietário pode transferir objetos autenticados ou acesso a informações para outros usuários. Em outras palavras, o proprietário determina os privilégios de acesso ao objeto.

Gabarito: Letra C

---

7. **(FADESP / SEFA-PA – 2022)** Considerando os passos utilizados pelo algoritmo de assinatura digital RSA, julgue verdadeira (V) ou falsa (F) cada uma das afirmativas a seguir.

I. A mensagem a ser assinada é inserida em uma função de hash que produz um código hash seguro de tamanho variado.

II. O código hash gerado é encriptado usando a chave privada do emissor para formar a assinatura digital.

III. O destinatário recebe a mensagem e produz um código hash. Ele também decripta a mensagem usando a chave pública do emissor. Se o código hash calculado coincidir com a assinatura decriptada, ela é aceita como válida.

A sequência correta é:

a) I - F; II - F; III - F.
b) I - F; II - F; III - V.
c) I - V; II - V; III - F.
d) I - F; II - V; III - V.
e) I - V; II - V; III - V.

Comentários:

(I) Errado, o código hash tem um tamanho fixo; (II) Correto, a chave privada do emissor é utilizada para criptografar e a chave pública do emissor é utilizada para descriptografar; (III) Correto, se os hashes forem idênticos, significa que a mensagem é íntegra e de quem diz ser.

Gabarito: Letra D

Figura 1 – Notícia da Agência Brasil

8. **(FUNDATEC / ISS-Porto Alegre – 2022)** A Figura 1 apresenta notícia a respeito da 2ª fase da Operação Spoofing, na qual os policiais federais cumpriram dois mandados de prisão temporária e outros de busca e apreensão em endereços de pessoas ligadas à organização criminosa investigada. Os criminosos invadiram os celulares de autoridades, tendo acessado e tomado conhecimento de informações, muito delas sensíveis, sem autorização dos respectivos proprietários. Nesse caso, é correto afirmar que o seguinte princípio básico da Segurança da Informação foi violado:

a) Sigilo
b) Integridade.
c) Não repúdio.
d) Autenticidade.
e) Disponibilidade.

Comentários:

Se os criminosos tiveram acesso a dados sigilosos, foi violado o princípio do sigilo. Nenhum dos outros itens trata de quebra de confidencialidade.

Gabarito: Letra A

Figura 2 – Venda de certificados digitais

9. **(FUNDATEC / ISS-Porto Alegre – 2022)** Um certificado digital "e-CNPJ", do tipo "A1", após devidamente emitido, pode ser armazenado:

I. Diretamente no computador do titular do certificado.
II. Em um token.
III. Em um cartão smart card.

Quais estão corretas?

a) Apenas I.
b) Apenas III.
c) Apenas I e II.
d) Apenas II e III.
e) I, II e III.

Comentários:

TIPO	GERAÇÃO DO PAR DE CHAVES	TAMANHO DA CHAVE (BITS)	ARMAZENAMENTO	VALIDADE (ANOS)
CERTIFICADO A1/S1	POR SOFTWARE	RSA 1024 OU 2048	DISCO RÍGIDO (HD) E PENDRIVE	1
CERTIFICADO A2/S2	POR SOFTWARE	RSA 1024 OU 2048	SMARTCARD (COM CHIP) OU TOKEN USB	2
CERTIFICADO A3/S3	POR HARDWARE	RSA 1024 OU 2048	SMARTCARD (COM CHIP) OU TOKEN USB	5
CERTIFICADO A4/S4	POR HARDWARE	RSA 2048 OU 4096	SMARTCARD (COM CHIP) OU TOKEN USB	6

(I) Correto, ele pode ser armazenado no disco rígido do computador do titular do certificado; (II) Errado, não pode ser armazenado com um token; (III) Errado, não pode ser armazenado em um smartcard.

Gabarito: Letra A

---

10. (FUNDATEC / DPE SC – 2018) A certificação digital é utilizada para garantir, de forma eletrônica, a autoria de determinado documento, como por exemplo, o perito responsável por determinado laudo. Um dos componentes da certificação digital é a utilização de criptografia. Diante do exposto, é correto afirmar que, para verificar a assinatura digital de um perito em relação a um laudo pericial emitido por ele, a primeira etapa é a aplicação:

a) Da chave criptográfica privada do perito.
b) Da chave criptográfica pública do perito.
c) Da chave criptográfica simétrica de quem quer validar.
d) De um algoritmo de hash simétrico de tamanho qualquer.
e) De um algoritmo de hash assimétrico de tamanho mínimo de 128 bits.

Comentários:

(a) Errado. Para verificar a assinatura digital do perito, eu não posso utilizar sua chave privada porque somente ele tem acesso a ela; (b) Correto. Para verificar a assinatura digital do perito, utiliza-se a chave pública dele correspondente à chave privada, de modo que seja possível identificá-lo inequivocamente; (c) Errado. Não se utiliza criptografia simétrica na certificação digital; (d) Errado. Algoritmo de Hash é apenas o algoritmo utilizado no processo de assinatura digital e não é capaz de verificar a assinatura do perito – e não existe algoritmo de hash simétrico; (e) Errado. Algoritmo de Hash é apenas o algoritmo utilizado no processo de assinatura digital e não é capaz de verificar a assinatura do perito – e não existe algoritmo de hash assimétrico;

Gabarito: Letra B

---

11. (CONSULPLAN / TJ-MG – 2017) Segurança da informação é o mecanismo de proteção de um conjunto de informações com o objetivo de preservar o valor que elas possuem para uma pessoa ou organização. Está correto o que se afirma sobre princípios básicos de segurança da informação, EXCETO:

a) Disponibilidade garante que a informação esteja sempre disponível.
b) Integridade garante a exatidão da informação.
c) Confidencialidade garante que a informação seja acessada somente por pessoas autorizadas.
d) Não repúdio garante a informação é autêntica e que a pessoa recebeu a informação.

Comentários:

A **Autenticidade** garantir que quem envia a informação é quem diz ser. Uma maneira de garanti-la é com a autenticação de usuários (Senhas ou Tokens). Já o **Não-repúdio (ou irretratabilidade)** garante que o autor não negará ter criado e assinado o conteúdo da informação. Uma maneira de garanti-la é com o uso de certificados digitais. O princípio que garante que a informação é autêntica é o Princípio da Autenticidade.

Gabarito: Letra D

---

12. (IBADE / PM-AC – 2017) Quanto mais a tecnologia se desenvolve, mais atividades são feitas pelos computadores pessoais, como pagamento de contas e armazenamento de arquivos com informações pessoais. Diante disso, cada vez mais deve-se pensar na segurança da informação. A melhor maneira de um usuário proteger informações quando está longe de seu computador é:

a) bloquear o computador com uma senha.
b) deixar o computador em modo de baixa energia.
c) ativar a proteção de tela.
d) desligar a rede sem fio.
e) desligar o monitor.

Comentários:

(a) Correto. Esse procedimento realmente protege informações do usuário; (b) Errado. Esse procedimento não protege informações do usuário; (c) Errado. Esse procedimento não protege informações do usuário; (d) Errado. Esse procedimento não protege informações do usuário; (e) Errado. Esse procedimento não protege informações do usuário;

Gabarito: Letra A

---

13. (IF-TO / IF-TO - 2016) O suporte para as recomendações de segurança da informação pode ser encontrado em controles físicos e controles lógicos. Existem mecanismos de segurança que apoiam os controles físicos assim como os controles lógicos. Das alternativas abaixo qual não é um mecanismo de segurança que apoia os controles lógicos?

a) Assinatura digital. Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade do documento associado, mas não a sua confidencialidade.

b) Mecanismos de controle de acesso. Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.

c) Sistema de controle de acesso eletrônico ao centro de processamento de dados, com senha de acesso ou identificações biométricas como digitais e íris.

d) Mecanismos de certificação. Atesta a validade de um documento.

e) Mecanismos de criptografia. Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros.

Comentários:

(a) Errado, Assinatura Digital é um controle lógico; (b) Errado, mecanismos de controle de acesso são controles lógicos; (c) Correto. Como a questão fala que é um sistema de controle de acesso eletrônico ao Centro de Processamento de Dados (CPD) da organização, trata-se de um controle físico. Lembrando que CPD é o local onde estão concentrados os sistemas computacionais de uma organização; (d) Errado, mecanismos de certificação é um controle lógico; (e) Errado, mecanismos de criptografia são controles lógicos.

Gabarito: Letra C

---

14. **(ESAF / CASSE/MS – 2016)** Ao receber uma mensagem eletrônica, deve-se fazer a verificação da assinatura digital. Nas alternativas, assinale a que indica a resposta correta para se efetuar esse procedimento.

a) Ter acesso ao CPF e identidade do remetente.
b) Ter acesso ao certificado digital do remetente.
c) Ter acesso ao certificado digital do destinatário.
d) Ter acesso à chave criptográfica dupla do destinatário.

Comentários:

A verificação da assinatura digital é feita por meio do certificado digital do remetente.

Gabarito: Letra B

---

15. **(INAZ do Pará / CRO RJ - 2016)** Quando navegamos na internet, sempre nos preocupamos na segurança das informações. Marque a alternativa **correta** em que o browser demonstra que o site está seguro.

a) http
b) https
c) http://
d) Antivírus
e) Worm

Comentários:

Pessoal, o protocolo de internet mais conhecido é o http. Quando navegamos de forma segura, em sites de compra ou no seu banco, por exemplo, é utilizado o https. Para não esquecer, lembre-se sempre de S de Segurança.

Gabarito: Letra B

---

16. (ESAF / Ministério da Fazenda – 2014) Assinale a opção correta relativa à Segurança da Informação.

a) Criptografia: técnica para converter uma mensagem de texto entre sistemas operacionais distintos.
b) Autenticação: sequência de símbolos destinada a permitir que o algoritmo cifre uma mensagem em texto claro ou decifre uma mensagem criptografada.
c) Autenticação: procedimento destinado a autorizar a sintaxe de determinada mensagem.
d) Autenticação: procedimento destinado a verificar a validade de determinada mensagem.
e) Inicializador: sequência de símbolos destinada a permitir que o algoritmo inicie uma mensagem em texto claro para decifrar uma mensagem criptografada.

Comentários:

(a) Errada. A criptografia é um método que codifica os dados do usuário para que só o destinatário possa ler, dessa maneira garantindo a confidencialidade da informação;

(b) Errada. Autenticação é um procedimento que visa garantir que quem envia a informação é quem diz ser. Lembrando que a sequência de símbolos na questão é chamada de chave de criptografia;

(c) Errada. Autenticação é um procedimento que visa garantir que quem envia a informação é quem diz ser;

(d) Correto. Autenticação é um procedimento que visa garantir que quem envia a informação é quem diz ser. Ou seja, que verifica que uma mensagem é válida (verdadeira) ou não.

(e) Errada. A sequência de símbolos em questão é chamada de chave de criptografia.

Gabarito: Letra D

---

17. (INAZ do Pará / Prefeitura de Curuçá – 2014) Em função de muitos ataques de hacker em diversos dados sigilosos, atualmente a maioria das empresas estão utilizando a certificação digital como uma forma de envio mais seguro das informações a diversos órgãos governamentais e privados. Qual a técnica que garante a veracidade do envio da informação pelo real remetente?

a) VPN.
b) Senha.
c) Não repúdio.
d) Integridade.
e) Confidencialidade.

Comentários:

Galera, o princípio do não-repúdio é o que garante que a informação/mensagem foi realizada por aquela pessoa determinada. Isto é, o autor não negará ter criado e assinado o conteúdo da informação. Uma maneira de garanti-la é com o uso de certificados digitais.

Gabarito: Letra C

---

18. (INAZ do Pará / BANPARÁ – 2014) Segundo os padrões internacionais, o tripé da segurança da informação são:

a) Antivírus, Firewall e Certificação Digital
b) Senha, Antivírus e AntiSpam
c) Consistência, Autenticidade, Integridade
d) Confidencialidade, Disponibilidade e Integridade
e) Navegabilidade, Acessibilidade e Usabilidade

Comentários:

Os três princípios consagrados da segurança da informação são: Confidencialidade, Integridade e Disponibilidade – conhecidos como CID. Se um ou mais desses princípios forem desrespeitados em algum momento, significa que houve um incidente de segurança da informação.

Relembrando rapidamente o conceito de cada um, temos que a **confidencialidade** é o princípio de que a informação não esteja disponível ou seja revelada a indivíduos, entidades ou processos não autorizados; a **integridade** é o princípio de salvaguarda da exatidão e completeza de ativos de informação; e a **disponibilidade** é o princípio da capacidade de estar acessível e utilizável quando demandada por uma entidade autorizada.

Gabarito: Letra D

---

19. (IDECAN / AGU – 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.

Comentários:

Quando necessitamos ocultar uma informação, deixando-a ilegível para pessoas não autorizadas utilizamos a criptografia.

Gabarito: Letra C

---

20. (FUNDATEC / SEFAZ-RS – 2014) Considerando os aspectos da segurança da informação, a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, prejudicando a organização, é chamada de:

a) Eventos de segurança da informação.
b) Incidentes de segurança da informação.
c) Riscos de segurança da informação.
d) Impacto organizacional.
e) Criticidade de ativo.

Comentários:

(a) Errado, evento é uma ocorrência identificada que indica uma possível violação de política de segurança; (b) Errado, incidente é um evento considerado indesejado ou inesperado, com grande possibilidade de comprometer o negócio; (c) Correto, risco é a combinação da probabilidade de um evento e de suas consequências – a exploração de uma vulnerabilidade por parte de uma ameaça é um evento de segurança específico que produz prejuízos à organização como consequência; (d) Errado, impacto é uma mudança adversa no nível de resultados obtidos para o alcance dos objetivos de negócio traçados; (e) Errado, criticidade é definição do quanto determinado ativo é crítico, ou seja, o quanto é importante para a concretização dos objetivos da organização.

Gabarito: Letra C

---

21. (TJ-SC / TJ-SC – 2011) Em segurança da informação, "assinatura digital" diz respeito a:

a) Ação de digitalizar uma assinatura em papel e incluí-la em documentos eletrônicos.

b) Uma tecnologia que permite dar garantia de integridade a autenticidade a arquivos eletrônicos, através da aplicação de operações criptográficas e da utilização de chaves.

c) Ação de escrever sobre a tela de um computador com uma caneta especial.

d) Uma tecnologia que permite a digitalização das impressões digitais do usuário.

e) Ação de digitar o nome completo do usuário no momento de escrever uma mensagem de e-mail.

Comentários:

Assinatura digital é uma tecnologia que permite dar garantia de integridade e autenticidade a arquivos eletrônicos, através da aplicação de operações criptográficas e da utilização de chaves.

Gabarito: Letra B

---

22. (FUNDATEC / SEFAZ RS – 2009) O Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), em seu artigo 313-A, incluído pela Lei no 9.983, de 2000, diz o seguinte: "Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa.". Esse artigo do Código Penal auxilia na preservação das informações existentes nas entidades e órgãos públicos, através da fixação de pena de reclusão, caso seja violado, nas condições desse artigo, o(s) seguinte(s) princípio(s) fundamental(ais) da Segurança da Informação:

I. Integridade.
I. Disponibilidade.
III. Confidencialidade.

Quais estão corretas?

a) Apenas I.
b) Apenas II.
c) Apenas III.
d) Apenas I e II.
e) I, II e III.

Comentários:

Essa é uma questão polêmica! Fica evidente que não houve quebra da confidencialidade porque se trata de um funcionário autorizado. Fica claro também que houve quebra da integridade porque dados foram inseridos, alterados ou excluídos – modificando a informação original. Por outro lado, a análise da disponibilidade é complexa! Eu e o Prof. Renato da Costa discutimos e nós não concordamos que tenha havido uma quebra da disponibilidade. A simples exclusão de um dado não caracteriza a perda da disponibilidade. Caso assim fosse, toda quebra de integridade implicaria

necessariamente em quebra da disponibilidade. Dessa forma, eu discordo do gabarito oficial da banca de que foram violados os princípios da integridade e disponibilidade.

Gabarito: Letra D

---

23. (COPESE-UFPI / Prefeitura de Bom Jesus/PI – 2008) Com relação à segurança da informação, o evento decorrente da exploração de uma vulnerabilidade por uma ameaça é um:

a) impacto.
b) risco.
c) antispyware.
d) repúdio.
e) ataque.

Comentários:

Um ataque é um evento decorrente da exploração de uma vulnerabilidade por uma ameaça com o intuito de obter, alterar, destruir, remover, implantar ou revelar informações sem autorização de acesso.

Gabarito: Letra E

LISTA DE QUESTÕES – DIVERSAS BANCAS

1. **(IADES / BRB – 2022)** As propriedades que garantem que o dado é correto e consistente com o estado ou informação pretendida, e que asseguram os limites de quem pode obtê-la são definidas respectivamente, como

a) integridade e confidencialidade.
b) integridade e disponibilidade.
c) disponibilidade e integridade.
d) consistência e autenticidade.
e) Consistência e confidencialidade.

2. **(FUNDATEC / IPE SAÚDE – 2022)** A política de segurança da informação estabelece como as informações são acessadas, tendo como objetivo manter os três pilares da segurança da informação, que são:

a) Confidencialidade, velocidade e armazenamento.
b) Confidencialidade, integridade e disponibilidade.
c) Conectividade, confiabilidade e disponibilidade.
d) Velocidade, controle de acesso e atualização da informação.
e) Velocidade, confiabilidade e controle de acesso.

3. **(FADESP / SEFA-PA – 2022)** Na assinatura digital são utilizadas:

a) a chave pública do receptor e a chave privada do receptor
b) a chave pública do emissor e a chave privada do emissor.
c) a chave pública do receptor e a chave privada do emissor
d) a chave privada do receptor e a chave pública do emissor.
e) as chaves secretas do emissor.

4. **(FADESP / SEFA-PA – 2022)** A forma de realizar assinatura digital baseada em logaritmos discretos, em que o trabalho principal para a geração de assinatura que não depende da mensagem pode ser feito durante o tempo ocioso do processador, e a parte da geração da assinatura que depende da mensagem exige multiplicar um inteiro de 2n bits por um inteiro de n bits, é conhecida como:

a) SCHNORR.
b) ELGAMAL.
c) DSA.
d) Curva Elíptica.
e) RSA-PSS.

5. **(FADESP / SEFA-PA – 2022)** A característica do modo de operação de cifra de bloco em que a entrada do algoritmo de encriptação é o XOR dos próximos 64 bits de texto claro e os 64 bits anteriores de texto cifrado é conhecida como:

a) Electronic Codebook (EBC).
b) Cipher Block Chaining (CBC).
c) Cipher Feedback (CFB).
d) Ouput Feedback (OFB).
e) Counter (CTR).

6. **(FADESP / SEFA-PA – 2022)** A forma de controle de acesso lógico, em que o dono dos dados e os usuários individuais são capazes de definir, ao seu critério, qual acesso será permitido aos seus dados independentemente da política, é definida como um controle de acesso:

a) mandatório
b) baseado na função.
c) discricionário
d) baseado em reivindicações
e) seletista

7. **(FADESP / SEFA-PA – 2022)** Considerando os passos utilizados pelo algoritmo de assinatura digital RSA, julgue verdadeira (V) ou falsa (F) cada uma das afirmativas a seguir.

I. A mensagem a ser assinada é inserida em uma função de hash que produz um código hash seguro de tamanho variado.

II. O código hash gerado é encriptado usando a chave privada do emissor para formar a assinatura digital.

III. O destinatário recebe a mensagem e produz um código hash. Ele também decripta a mensagem usando a chave pública do emissor. Se o código hash calculado coincidir com a assinatura decriptada, ela é aceita como válida.

A sequência correta é:

a) I - F; II - F; III - F.
b) I - F; II - F; III - V.
c) I - V; II - V; III - F.
d) I - F; II - V; III - V.
e) I - V; II - V; III - V.

Figura 1 – Notícia da Agência Brasil

8. **(FUNDATEC / ISS-Porto Alegre – 2022)** A Figura 1 apresenta notícia a respeito da 2ª fase da Operação Spoofing, na qual os policiais federais cumpriram dois mandados de prisão temporária e outros de busca e apreensão em endereços de pessoas ligadas à organização criminosa investigada. Os criminosos invadiram os celulares de autoridades, tendo acessado e tomado conhecimento de informações, muito delas sensíveis, sem autorização dos respectivos proprietários. Nesse caso, é correto afirmar que o seguinte princípio básico da Segurança da Informação foi violado:

a) Sigilo
b) Integridade.
c) Não repúdio.
d) Autenticidade.
e) Disponibilidade.

Figura 2 – Venda de certificados digitais

9. **(FUNDATEC / ISS-Porto Alegre – 2022)** Um certificado digital "e-CNPJ", do tipo "A1", após devidamente emitido, pode ser armazenado:

I. Diretamente no computador do titular do certificado.

II. Em um token.
III. Em um cartão smart card.

Quais estão corretas?

a) Apenas I.
b) Apenas III.
c) Apenas I e II.
d) Apenas II e III.
e) I, II e III.

10. **(FUNDATEC / DPE SC – 2018)** A certificação digital é utilizada para garantir, de forma eletrônica, a autoria de determinado documento, como por exemplo, o perito responsável por determinado laudo. Um dos componentes da certificação digital é a utilização de criptografia. Diante do exposto, é correto afirmar que, para verificar a assinatura digital de um perito em relação a um laudo pericial emitido por ele, a primeira etapa é a aplicação:

a) Da chave criptográfica privada do perito.
b) Da chave criptográfica pública do perito.
c) Da chave criptográfica simétrica de quem quer validar.
d) De um algoritmo de hash simétrico de tamanho qualquer.
e) De um algoritmo de hash assimétrico de tamanho mínimo de 128 bits.

11. **(CONSULPLAN / TJ MG – 2017)** Segurança da informação é o mecanismo de proteção de um conjunto de informações com o objetivo de preservar o valor que elas possuem para uma pessoa ou organização. Está correto o que se afirma sobre princípios básicos de segurança da informação, EXCETO:

a) Disponibilidade garante que a informação esteja sempre disponível.
b) Integridade garante a exatidão da informação.
c) Confidencialidade garante que a informação seja acessada somente por pessoas autorizadas.
d) Não repúdio garante a informação é autêntica e que a pessoa recebeu a informação.

12. **(IBADE / PM AC – 2017)** Quanto mais a tecnologia se desenvolve, mais atividades são feitas pelos computadores pessoais, como pagamento de contas e armazenamento de arquivos com informações pessoais. Diante disso, cada vez mais deve-se pensar na segurança da informação. A melhor maneira de um usuário proteger informações quando está longe de seu computador é:

a) bloquear o computador com uma senha.
b) deixar o computador em modo de baixa energia.
c) ativar a proteção de tela.
d) desligar a rede sem fio.
e) desligar o monitor.

13. **(IF-TO / IF-TO - 2016)** O suporte para as recomendações de segurança da informação pode ser encontrado em controles físicos e controles lógicos. Existem mecanismos de segurança que apoiam os controles físicos assim como os controles lógicos. Das alternativas abaixo qual não é um mecanismo de segurança que apoia os controles lógicos?
a) Assinatura digital. Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade do documento associado, mas não a sua confidencialidade.

b) Mecanismos de controle de acesso. Palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.

c) Sistema de controle de acesso eletrônico ao centro de processamento de dados, com senha de acesso ou identificações biométricas como digitais e íris.

d) Mecanismos de certificação. Atesta a validade de um documento.

e) Mecanismos de criptografia. Permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros.

14. **(ESAF / CASSE/MS – 2016)** Ao receber uma mensagem eletrônica, deve-se fazer a verificação da assinatura digital. Nas alternativas, assinale a que indica a resposta correta para se efetuar esse procedimento.

a) Ter acesso ao CPF e identidade do remetente.
b) Ter acesso ao certificado digital do remetente.
c) Ter acesso ao certificado digital do destinatário.
d) Ter acesso à chave criptográfica dupla do destinatário.

15. **(INAZ do Pará / CRO RJ - 2016)** Quando navegamos na internet, sempre nos preocupamos na segurança das informações. Marque a alternativa **correta** em que o browser demonstra que o site está seguro.

a) http
b) https
c) http://
d) Antivírus
e) Worm

16. **(ESAF / Ministério da Fazenda – 2014)** Assinale a opção correta relativa à Segurança da Informação.

a) Criptografia: técnica para converter uma mensagem de texto entre sistemas operacionais distintos.

b) Autenticação: sequência de símbolos destinada a permitir que o algoritmo cifre uma mensagem em texto claro ou decifre uma mensagem criptografada.
c) Autenticação: procedimento destinado a autorizar a sintaxe de determinada mensagem.
d) Autenticação: procedimento destinado a verificar a validade de determinada mensagem.
e) Inicializador: sequência de símbolos destinada a permitir que o algoritmo inicie uma mensagem em texto claro para decifrar uma mensagem criptografada.

17. **(INAZ do Pará / Prefeitura de Curuçá – 2014)** Em função de muitos ataques de hacker em diversos dados sigilosos, atualmente a maioria das empresas estão utilizando a certificação digital como uma forma de envio mais seguro das informações a diversos órgãos governamentais e privados. Qual a técnica que garante a veracidade do envio da informação pelo real remetente?

a) VPN.
b) Senha.
c) Não repúdio.
d) Integridade.
e) Confidencialidade.

18. **(INAZ do Pará / BANPARÁ – 2014)** Segundo os padrões internacionais, o tripé da segurança da informação são:

a) Antivírus, Firewall e Certificação Digital
b) Senha, Antivírus e AntiSpam
c) Consistência, Autenticidade, Integridade
d) Confidencialidade, Disponibilidade e Integridade
e) Navegabilidade, Acessibilidade e Usabilidade

19. **(IDECAN / AGU – 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.

20. **(FUNDATEC / SEFAZ-RS – 2014)** Considerando os aspectos da segurança da informação, a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, prejudicando a organização, é chamada de:

a) Eventos de segurança da informação.
b) Incidentes de segurança da informação.

c) Riscos de segurança da informação.
d) Impacto organizacional.
e) Criticidade de ativo.

21. (TJ-SC / TJ-SC – 2011) Em segurança da informação, "assinatura digital" diz respeito a:

a) Ação de digitalizar uma assinatura em papel e incluí-la em documentos eletrônicos.

b) Uma tecnologia que permite dar garantia de integridade a autenticidade a arquivos eletrônicos, através da aplicação de operações criptográficas e da utilização de chaves.

c) Ação de escrever sobre a tela de um computador com uma caneta especial.

d) Uma tecnologia que permite a digitalização das impressões digitais do usuário.

e) Ação de digitar o nome completo do usuário no momento de escrever uma mensagem de e-mail.

22. (FUNDATEC / SEFAZ RS – 2009) O Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), em seu artigo 313-A, incluído pela Lei no 9.983, de 2000, diz o seguinte: "Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa.". Esse artigo do Código Penal auxilia na preservação das informações existentes nas entidades e órgãos públicos, através da fixação de pena de reclusão, caso seja violado, nas condições desse artigo, o(s) seguinte(s) princípio(s) fundamental(ais) da Segurança da Informação:

I. Integridade.
I. Disponibilidade.
III. Confidencialidade.

Quais estão corretas?

a) Apenas I.
b) Apenas II.
c) Apenas III.
d) Apenas I e II.
e) I, II e III.

23. (COPESE-UFPI / Prefeitura de Bom Jesus/PI – 2008) Com relação à segurança da informação, o evento decorrente da exploração de uma vulnerabilidade por uma ameaça é um:

a) impacto.

b) risco.
c) antispyware.
d) repúdio.
e) ataque.

GABARITO – DIVERSAS BANCAS

1. LETRA A
2. LETRA B
3. LETRA B
4. LETRA A
5. LETRA B
6. LETRA C
7. LETRA D
8. LETRA A
9. LETRA A
10. LETRA B
11. LETRA D
12. LETRA A
13. LETRA C
14. LETRA B
15. LETRA B
16. LETRA D
17. LETRA C
18. LETRA D
19. LETRA C
20. LETRA C
21. LETRA B
22. LETRA D
23. LETRA E

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.