Introdução à Segurança da Informação

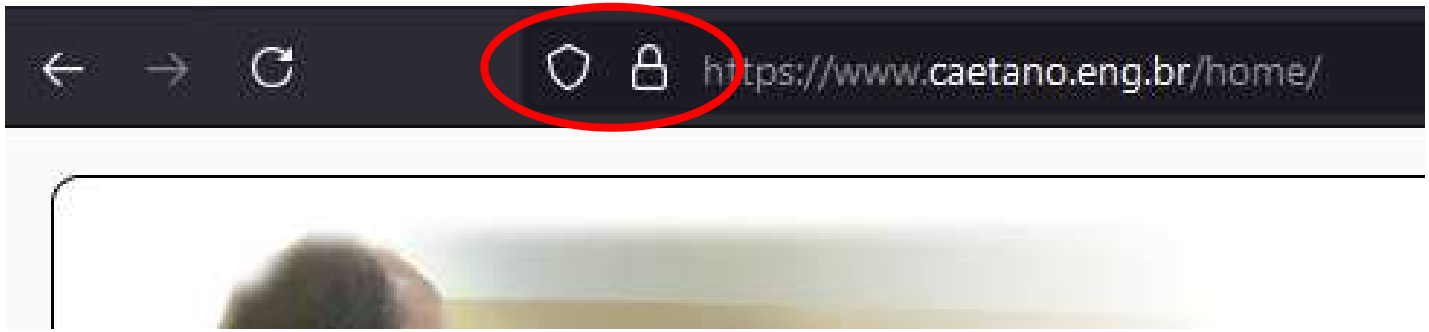
Certificados e Assinaturas Digitais

Prof. Dr. Daniel Caetano

2021 - 1

Compreendendo o problema

- **Situação:** Com o crescimento das transações virtuais, há também o crescimento das fraudes. Assim, certificar-se da identidade de pessoas e serviços é fundamental...

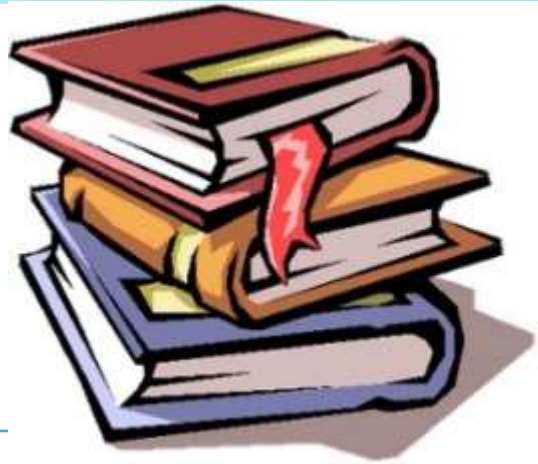


Você presta atenção no cadeado na barra de endereço de seu navegador?

Objetivos

- Compreender a diferença entre assinatura digital e eletrônica
- Compreender o processo de assinatura digital
- Compreender o papel do certificado digital e da autoridade certificadora

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 9)
Biblioteca Virtual	Trilhas em Segurança da Informação: caminhos e ideias para a proteção de dados. Págs 94 a 102. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002, Cap. 10. Criptografia e Segurança de Redes: princípios e práticas. Caps. 13 e 17.

Mecanismos de Segurança para os Dados

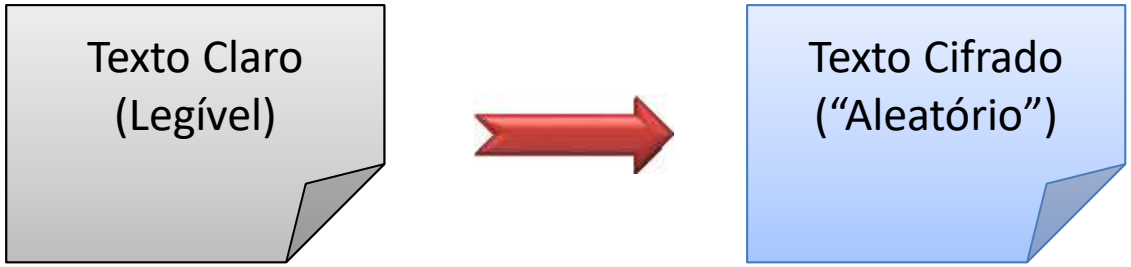
Mecanismos de Segurança

- Os mecanismos mais clássicos são:
  - Criptografia dos dados
  - Assinatura digital dos dados
    - **Foco de hoje!**

- Focam em garantir
  - Sigilo: só quem pode acessar, acessará
  - Integridade: conferir se dado permanece “original”
  - Autenticação: de usuário, remetente, destinatário
  - Atualidade: a mensagem é nova, não um reenvio.

Criptografia

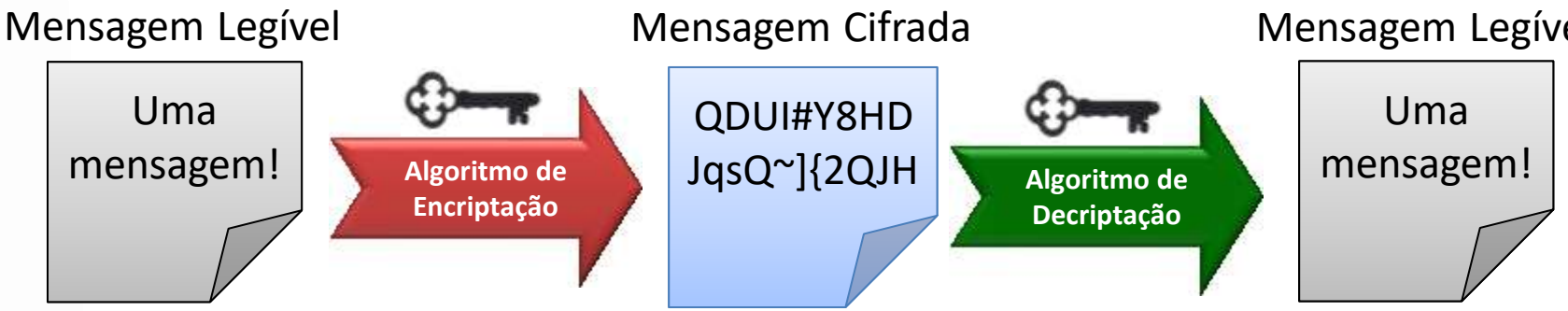
- Codificação dos dados
- Processo que transforma



- Algoritmo de criptografia
  - Cifragem: tornar o texto claro em cifrado
    - “Criptografar” ou “Encriptar”
  - Decifragem: tornar o texto cifrado em claro
    - “Decriptografar” ou “Decriptar”

Chave Criptográfica

- Chave permite “trancar” e “destrancar”
  - É o “segredo” de um criptografia
  - Similar a uma “senha”
- Tradicionalmente, remetente e destinatário...
  - Precisam ter uma cópia da chave

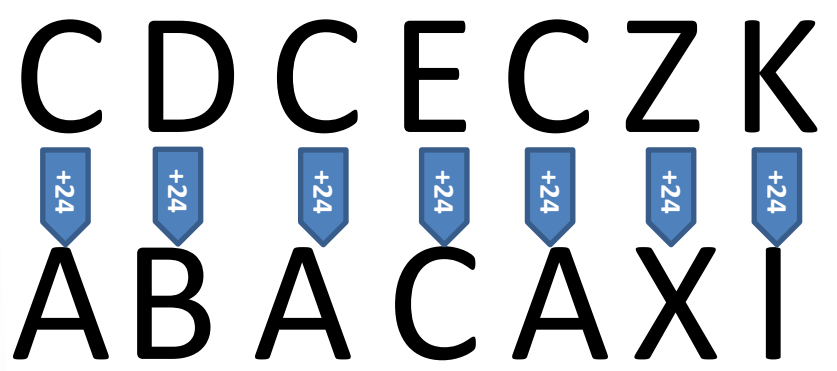


Criptografia de Chave Pública

- Codificar: “somar 2” a cada letra

Algoritmo: somar o valor da chave “α” à letra
Chave: 2 **Chave Privada**

- Decodificar: “somar 24” a cada letra



Algoritmo: somar o valor da chave “β” à letra
Chave: 24 **Chave Pública**

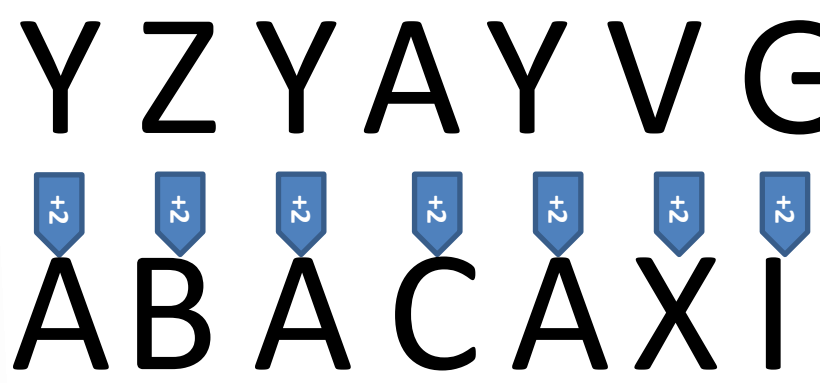
Criptografia Assimétrica ou de Chave Pública

Criptografia de Chave Pública

- E se codificar com a chave pública (Ex. 24)?

Algoritmo: somar o valor da chave pública
Chave: 24 **Chave Pública**

- Decodificar: "somar 2" a cada letra

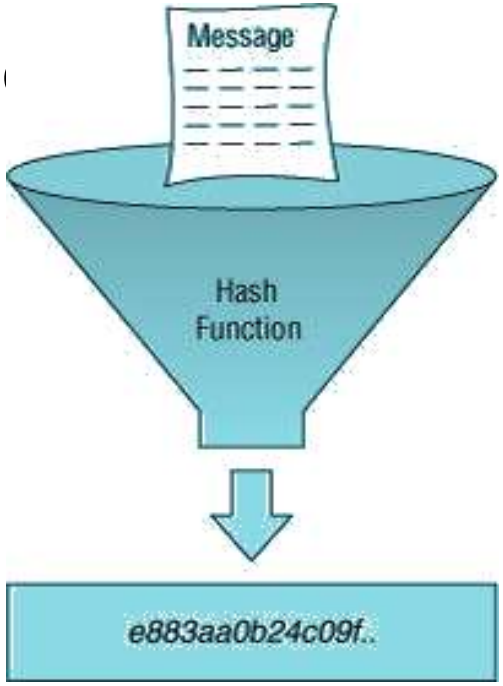


Algoritmo: somar o valor da chave privada
Chave: 2 **Chave Privada**

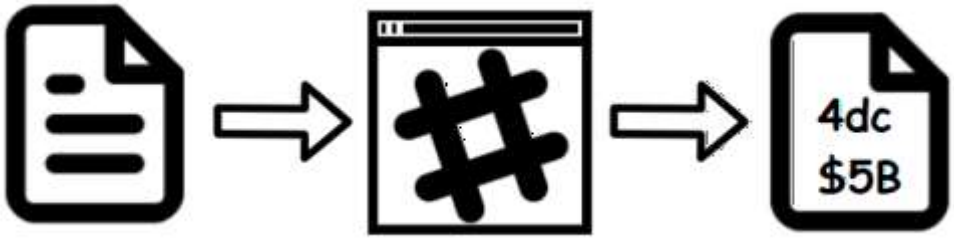
Funciona nas duas direções!

Hash ou Número Resumo

- Analisar arquivo ou mensagem:
  - Certificar-se de que não foi alterad
- Criptografia: “ida” e “volta”
  - Se eu codifiquei, eu decodifico
- Hash: só “ida”
  - Só codifico, nunca decodifico
  - Deve ser único para uma mensagem legível



Hash ou Número Resumo



- Exemplo: pegar apenas as letras de posições pares, somando 1 se a anterior for vogal

T R A B A L H O

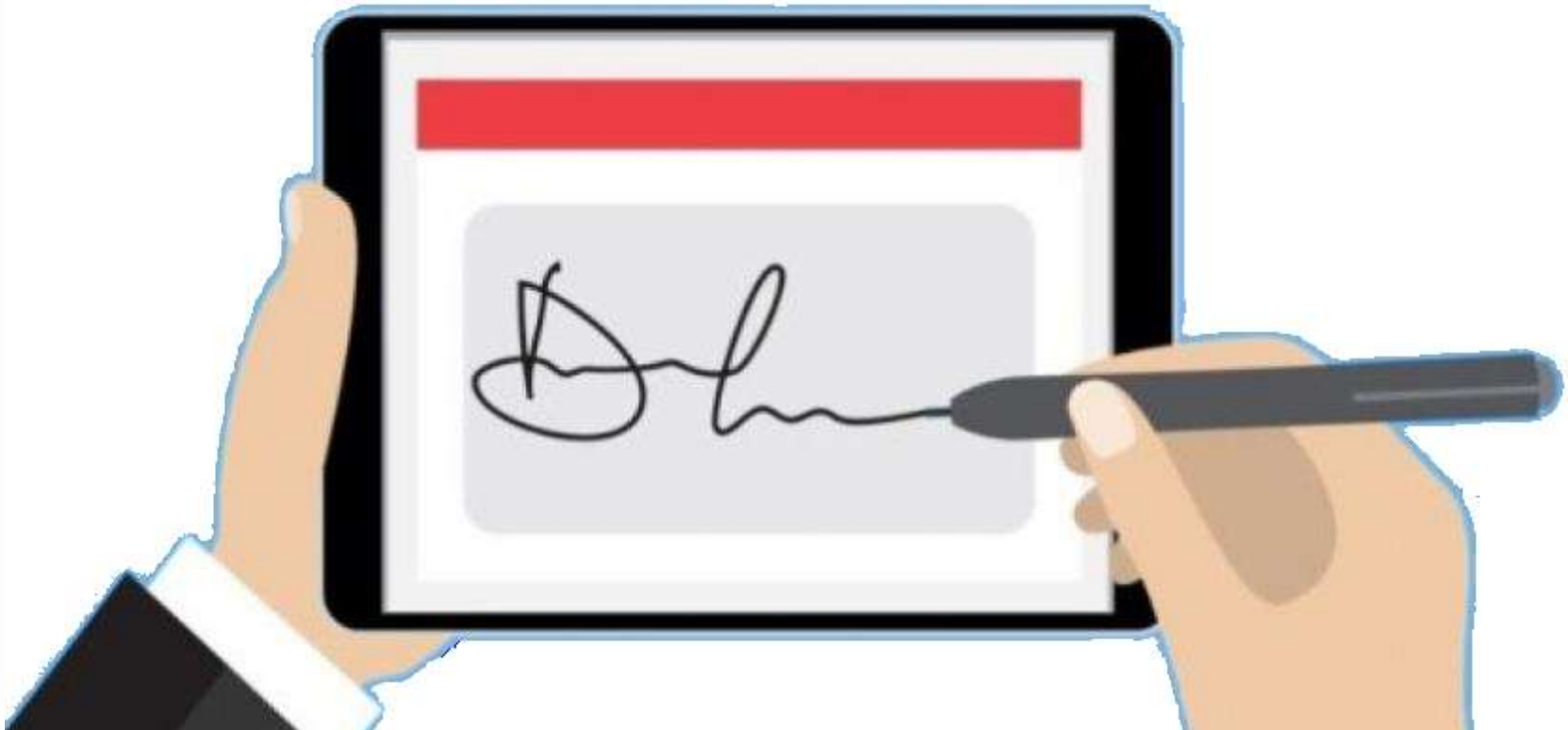
+0 +1 +1 +0

R C M O

Assinatura Eletrônica x Assinatura Digital

Assinaturas Eletrônicas

- Objetivo: mesmo da assinatura em papel
- Digitalização da assinatura manual
  - Facilmente reproduzida por cópia simples

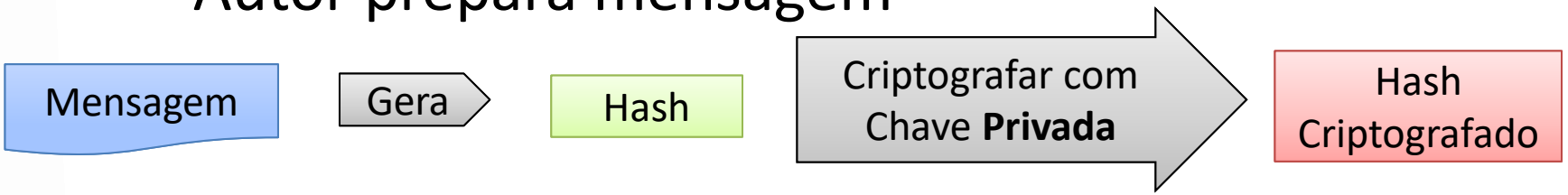


Assinaturas Digitais

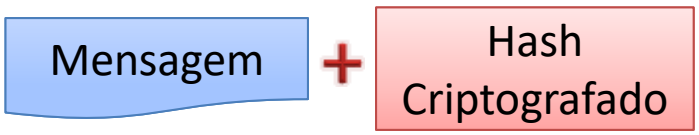
- Objetivo: garantir integridade e não-repúdio
- Requisitos
  - Receptor: verificar identidade do autor
  - Autor: não repudiar o conteúdo
  - Receptor/Intermediário: não alterar/forjar conteúdo.
- Meio comum:
  - Criptografia Assimétrica
  - Hash Criptográfico

Assinaturas Digitais

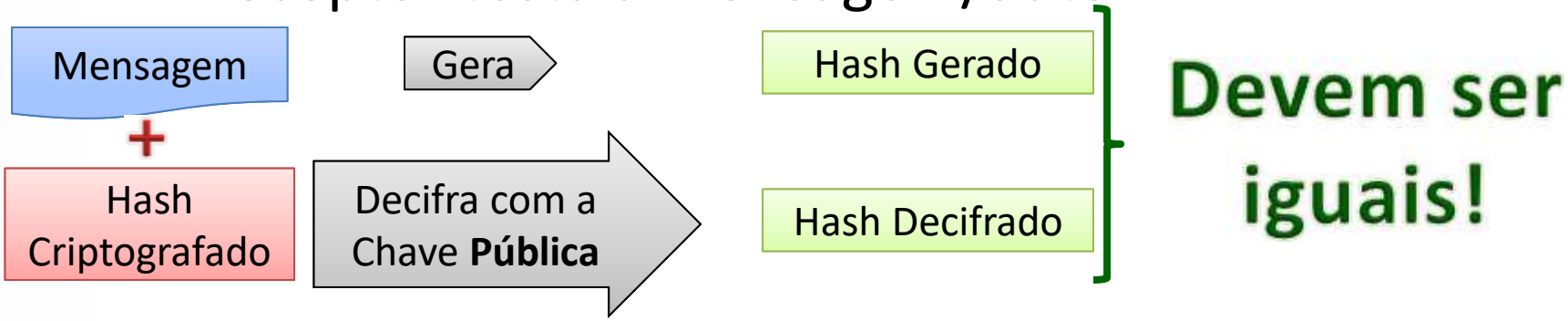
- Mecanismo
  - Autor prepara mensagem



  - Autor envia a mensagem



  - Receptor testa a mensagem/autor



Chave Pública: Como Obter?

- É importante, então, ter acesso confiável às chaves públicas das pessoas!
  - Para decifrar e verificar as mensagens delas
  - Para enviar mensagens secretas para elas

- Como saber se a chave pública é realmente a da pessoa, e não de um bisbilhoteiro qualquer?
  - "Terceiro Confiável": entidade certificadora
  - Certificados Digitais
    - Banco de chaves públicas
    - Domínios ou CPFs ou CNPJs

Autoridades Certificadoras

- Hierarquia de Certificação no Brasil
  - Infraestrutura de Chaves Públicas Brasileira
  - ICP-Brasil
- Instituto Nacional de Tec. Da Inf. (ITI)
  - Autoridade Certificadora Raiz (AC-Raiz)
  - Credencia/fiscaliza Autoridades Certificadoras (AC)
    - Emitem, renovam, revogam os Certificados Digitais
    - Exemplo: Certisign, Serasa, RFB...
    - https://www.gov.br/iti/pt-br/assuntos/icp-brasil/autoridades-certificadoras
  - Autoridades de Registro (AR)
    - Locais de atendimento: validam seu certificado

ITI
Instituto Nacional de Tecnologia da Informação

Negociação e Verificação de Chaves

- "Terceiro Confiável"
  - Fornece a chave pública de uma entidade
- Procedimento Simplificado (Navegador x Server)
  - Negociam algoritmos
  - Trocam chaves públicas
  - **Validam as chaves x domínios (autoridades)**
  - Geram chaves secretas de comunicação
  - Codificam com chave pública e enviam pra parte
  - Passam a trocar mensagens criptografadas

https://www.davidsonsilva.com.br/seguranca-com-o-protocolo-https/

Tipos de Certificado Digital

- Sempre possuem um par chaves (pub+priv)
- São dois tipos: A e S
  - A: Assinatura de documentos
  - S: Sigilo de dados

- Níveis de Segurança 1 a 4
  - A1 e S1: 1024 bits, arquivos em disco
  - A2 e S2: 1024 bits, arquivos em dispositivo
  - A3 e S3: 1024 bits, hardware dedicado
  - A4 e S4: 2048 bits, hardware dedicado

Tipos de Certificado Digital

- Detalhando os níveis de segurança 1 a 4
  - A1 e S1: chaves de 1024 bits geradas por software e armazenado no hardware do usuário (computador, laptop). Vale por 1 ano.
  - A2 e S2: chaves de 1024 bits geradas por software, armazenado em mídia própria (pendrive, por exemplo). Vale por 2 anos.
  - A3 e S3: chaves de 1024 bits geradas e armazenadas em hardware dedicado para o certificado (chip ou token). Parece pendrive, mas não é. Vale por 3 anos.
  - A4 e S4: chaves de, no mínimo, 2048 bits geradas e armazenadas em hardware dedicado para o certificado (chip ou token). Vale por 3 anos.

RESUMÃO

SEMANA 01

Importância da Informação

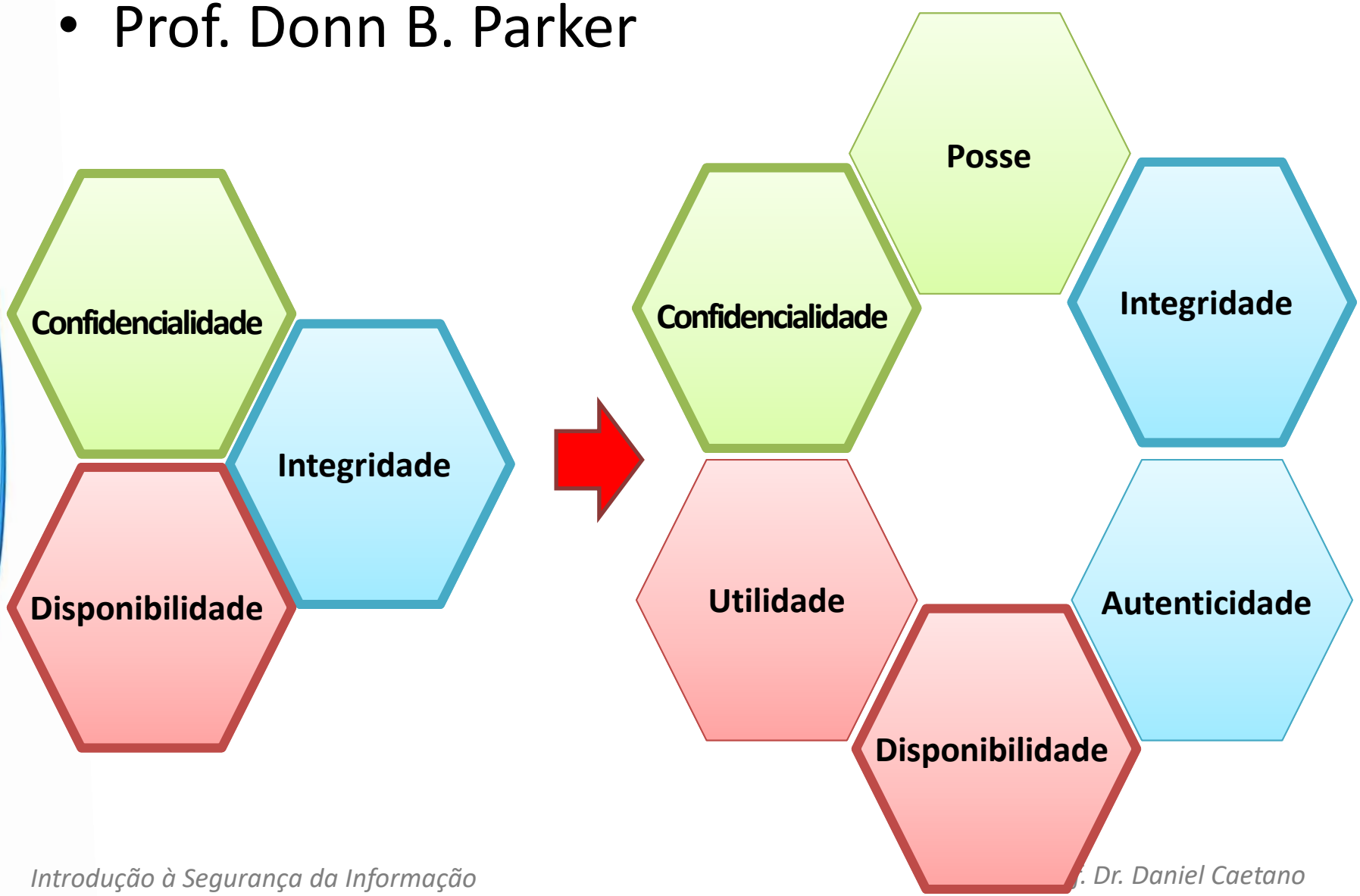
- Necessidades das empresas
  - Saber fazer
  - Aprimorar o que faz
  - Conhecer a quem vender
  - Satisfazer aos clientes.

- Tudo isso exige informações
  - São essenciais para os negócios!

Ciclo de Vida da Informação

Hexagrama Parkeriano

- Prof. Donn B. Parker



SEMANA 02

Norma ISO/IEC 27002

- Código de Prática para a GSI
  - Gestão de Segurança da Informação

- Objetivo
  - Estabelecer diretrizes e princípios iniciais para:
    - Iniciar, implementar e melhorar a GSI da organização
  - Ou seja: proteger informações importantes...
    - ...para a continuidade dos negócios.

Norma ISO/IEC 27001

- Objetivo: requisitos para quê?
  - Estabelecimento, implementação, operação, monitoração, análise crítica, manutenção e melhoria de um SGSI
- Se aplicam a que tipo de empresas?
  - Quaisquer, independente de tipo, tamanho ou natureza
- Ajuda a proteger ativos de informação
- Única norma auditável para esse fim

Leis Envolvendo Redes e Segurança

- Três são especificamente relevantes:
  - Lei Carolina Dieckman
    - Lei Federal 12.737 de 30 de Novembro de 2012
    - Tipificação criminal

    http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm
  - Marco Civil da Internet
  - Lei Geral de Proteção de Dados (LGPD)

CERT.BR

- Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
  - Mantido pelo NIC.Br
    - Do Comitê Gestor da Internet no Brasil (CGI.Br)

https://cert.br/

- Missão
  - Aumentar os níveis de segurança...
  - E de capacidade de tratamento de incidentes...
  - Das redes conectadas à internet no Brasil.

Terminologia

- Ameaça
  - Circunstância, ação ou evento que pode levar à quebra de segurança

- Vulnerabilidade
  - Fragilidade nos ativos que os expõem a ameaças
- Incidente ou ataque
  - Uma tentativa ou sucesso de uma ameaça em explorar uma vulnerabilidade

- Desastre
  - Resultado do sucesso de um ataque
- E risco?

Abordagens de Segurança

- Há dois tipos principais de abordagem:
  - Reativa
  - Proativa

SEMANA 03

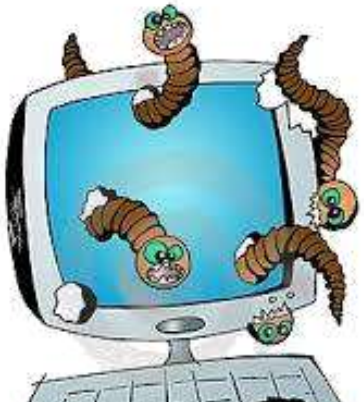
Principais Tipos de Ameaças

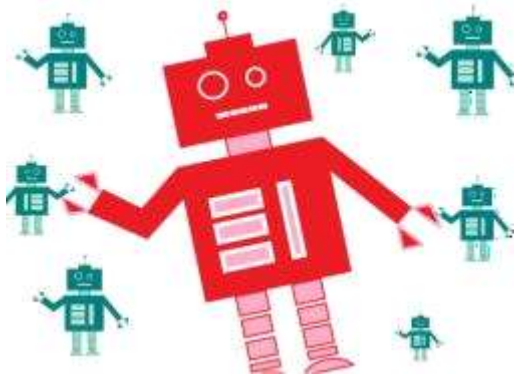
- Pessoas mal intencionadas!
  - E seus ataques...

- Golpes diversos (mais na aula que vem)
- Softwares do tipo "*malware*"
  - **Mal**icious Soft**ware**
  - Software que se infiltra na máquina de forma ilícita
    - Causa danos, alterações ou roubo de informações

Principais Tipos de Ameaças

- Principais tipos de *malware*
  - Vírus
  - *Worms*
  - *Trojans*
  - *Bots* e *Botnets*
  - *Spywares*
  - *Rootkits*





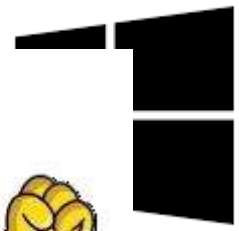
Proteção Básica

- Qual é o mínimo que devo fazer
  - Antivírus
  - Firewall
  - Configuração Segura da Rede
  - Configuração Segura de Softwar
  - Rotinas de segurança

SEMANA 04

Tipos de Vulnerabilidades

- São 7 os tipos de vulnerabilidades:
  1. Naturais
  2. Físicas
  3. Hardware
  4. Software
  5. Armazenamento
  6. Comunicação
  7. Humanas

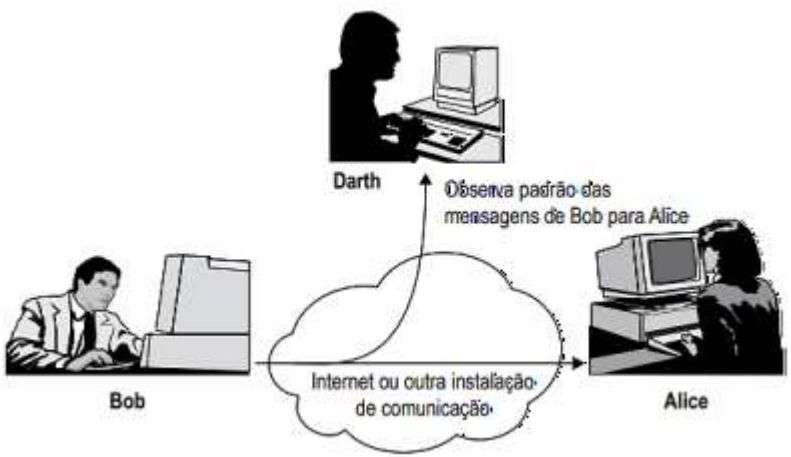


Quais Ferramentas?

- Prevenção Básica
  - Antivírus/Antimalware: identifica, desativa ou elimina esses tipos de ameaças. Atua no lado da “ameaça”
  - Firewall: controla o que entra e sai em um equipamento ou uma rede. Atua no lado da “vulnerabilidade”
  - Comunicação segura (SSL/HTTPS): codifica os dados ponta a ponta. Atua no lado da “vulnerabilidade”
- Ferramentas de busca
  - Scanners: identificam vulnerabilidade
    - Maneira automatizada

Tipos de Ataques

- Passivos
  - Observação das informações
  - Sem interferência no tráfego
- Ativos
  - Manipulação doas informações
  - Conseguências diretas no tráfego



Golpes e Fraudes

- Ludibriar o usuário
  - Usuário fornece dados sens
- Tipos comuns
  - Scam/Phishing
  - *Pharming*
  - Sequestro
  - Aluguel de Conta
  - Falso Pagamento
  - *Hoax*

SEMANA 05

Componentes da Segurança

- Segurança, na prática: 3 aspectos
  - Físicos
  - Lógicos
  - Administrativos

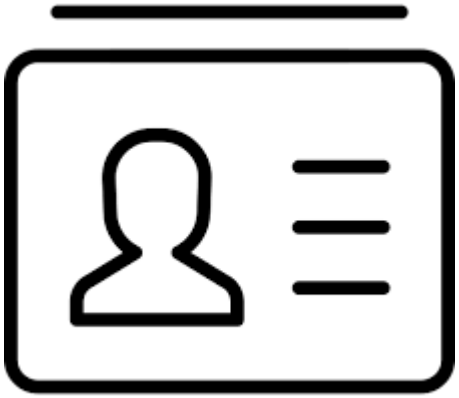
Aspectos Lógicos x Físicos

Não existe segurança lógica

sem segurança física

Controle de Acesso: Procedimento

- **Logon/Login**: dois processos básicos
  - Identificação**:** qual é o usuário e suas permissões
  - Autenticação**:** comprovar a identidade
- Resumindo
  - **Identificacão** + **Algo que usuário sabe ou tem**



Auditoria de Logs e Vídeos

- Reconstruir eventos
  - “Seguir as migalhas de pão”
- Monitoramento...
  - Proativo x Reativo
- Auditoria frequente
  - Tanto quanto o sistema for crítico
  - Qualquer evento estranho deve ser investigado.

SEMANA 06

Garantia de Autenticidade

- Requisitos da autenticidade:
  - Autenticação da origem
  - Autenticação do destino
  - Integridade da informação.

- Consequência: **não-repúdio**
  - Garantir a responsabilização dos envolvidos
- Para isso, é fundamental <u>controle de acesso</u>!

Mecanismos de Identificação

- Identificação
  - Objetivo: saber quem quer acessar
  - **Identificador** único para cada usuário (daí o nome!)
- Mecanismos comuns
  - Auto-declarado (username ou us
  - Uso de cartões de identificação
    - Cartões com código de barras / QR
    - Cartões Inteligentes SmartCards / F
      - Certificados Digitais **(em breve!**

Mecanismos de Autenticação

- Autenticação
  - Objetivo: provar que o usuário é quem ele diz ser
  - Comprovar **autenticidade/autoria d**
- Mecanismos comuns
  - Senhas
  - Cartões
  - *Tokens*
  - Biometria

Mecanismos Adicionais

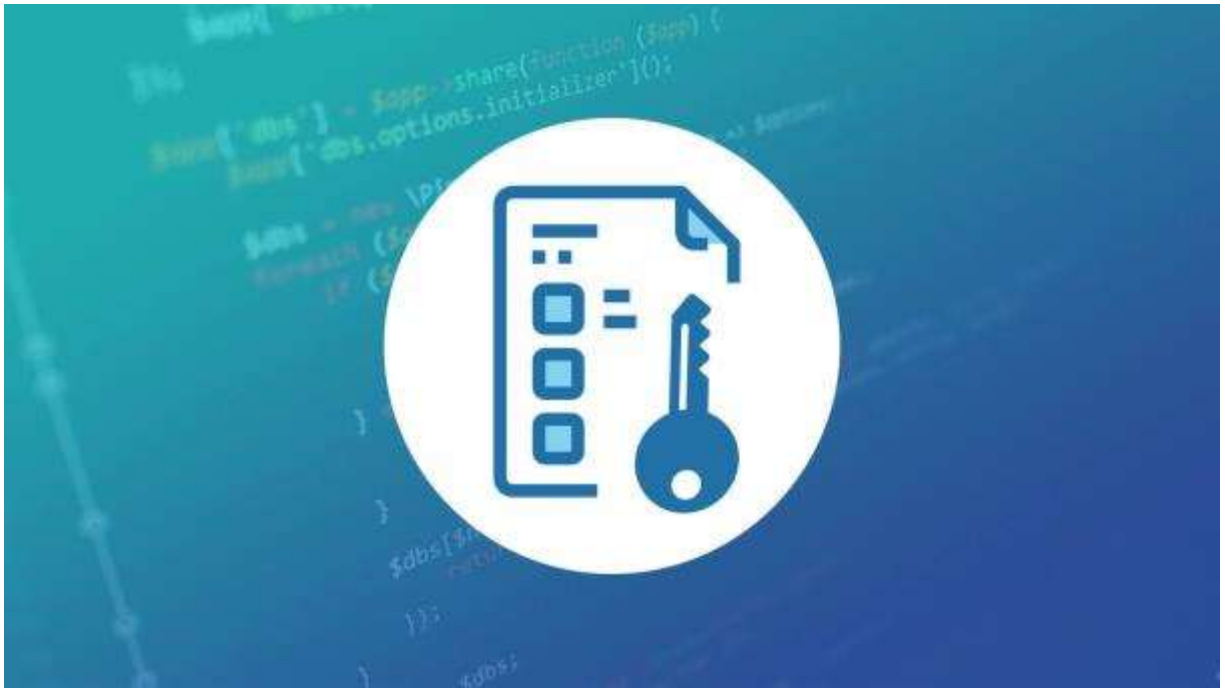
- Adições à Identificação e Autenticação
  - Objetivo: ampliar a segurança
  - Mecanismos de **naturezas diferentes** e...
  - Fatores adicionais
    - Identificador **+** algo sabido **+** algo possuído

- Mecanismos comuns
  - Restrição de Equipamentos
  - Autenticação em 2 Fatores.

SEMANA 07

Controle de Acesso de Arquivos

- Além do *login*... existe outro aspecto
  - Proteção de acesso no nível do sistema de arquivos



- Unix/Linux x Windows

Política de Acesso Lógico

- Em geral, as permissões de acesso
  - Associadas à função do funcionário
    - Papel do funcionário dentro da empresa
  - Permissões devem ser atribuídas minuciosamente
    - Apenas o necessário...!
    - Revisões periódicas!
      - Remover excessos
    - Ex.: Estagiário

Senhas Seguras

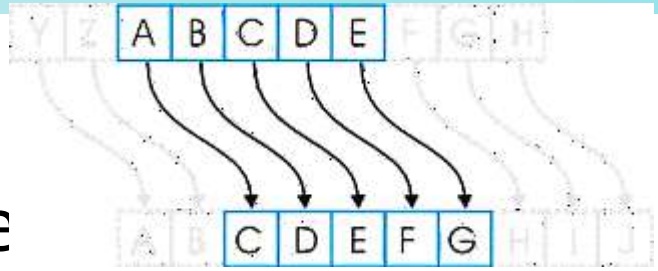
- São a forma mais tradicional de autenticacão
  - Solução de menor curso
  - Segurança tão grande quanto:
    - Qualidade da senha
    - Política de troca de senhas
    - Cuidados e atenção do usuário
      - "Senha é pessoal e intransferível"

Cópias de Segurança

- O que é isso?
  - Cópias de dados e programas relevantes...
  - ...para recuperação em caso de desastres
  - E para proteção legal
- Tamb

SEMANA 08

Exemplo: Substituição



- Codificar: “somar 2” a cada le

A B A C A X I

+2 +2 +2 +2 +2 +2 +2

C D C E C Z K

Algoritmo: <u>somar</u> o valor da chave à letra

Chave: 2

Tamanho da Chave?

- Decodificar: “subtrair 2” de cada letra

C D C E C Z K

-2 -2 -2 -2 -2 -2 -2

A B A C A X I

Algoritmo: <u>subtrair</u> o valor da chave da letra

Chave: 2

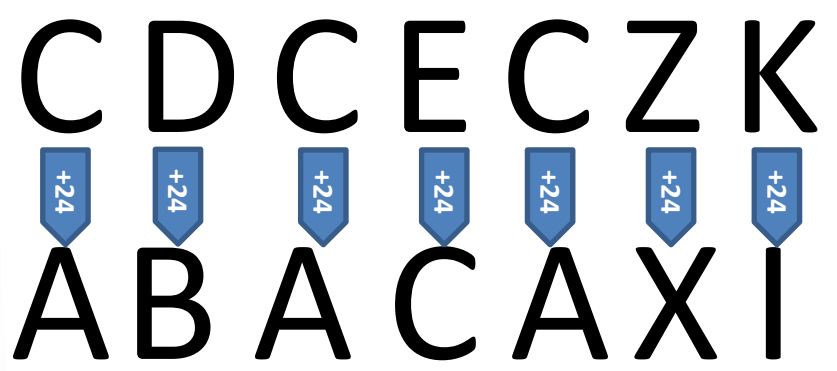
Criptografia <u>Simétrica</u> ou de <u>Chave Secreta</u>

Criptografia de Chave Pública

- Codificar: “somar 2” a cada letra

Algoritmo: somar o valor da chave “α” à letra
Chave: 2 **Chave Privada**

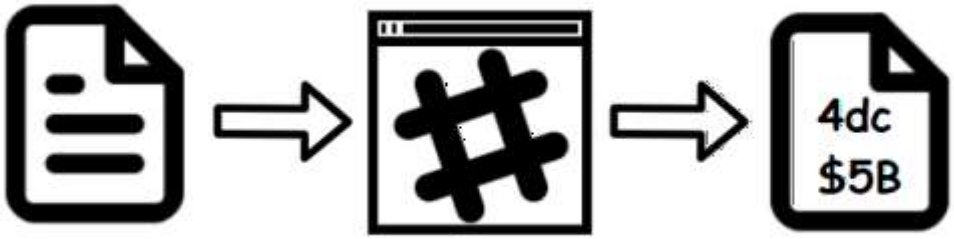
- Decodificar: “somar 24” a cada letra



Algoritmo: somar o valor da chave “β” à letra
Chave: 24 **Chave Pública**

Criptografia Assimétrica ou de Chave Pública

Hash ou Número Resumo



- Exemplo: pegar apenas as letras de posições pares, somando 1 se a anterior for vogal

T R A B A L H O

+0 +1 +1 +0

R C M O

ATIVIDADE

Atividade

- Ajude o professor a aprimorar a disciplina!
  - Preencha a nossa avaliação da disciplina!

https://tinyurl.com/si2021a

ENCERRAMENTO

Resumo e Próximos Passos

- Assinaturas Eletrônicas x Digitais
  - Busca pelo não-repúdio!
- Autoridades Certificadoras
- Tipos de Certificação Digital
- **Pós Aula**: Aprenda Mais, Pós Aula e Desafio!
  - No padlet: https://padlet.com/djcaetano/seguranca

- Estudar para a prova!

PERGUNTAS?