Introdução à Segurança da Informação

Ameaças e Vulnerabilidades – Parte II

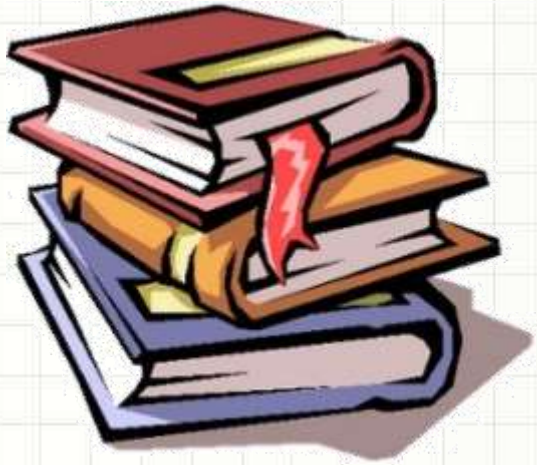
Prof. Dr. Daniel Caetano

2020 - 1

Objetivos

- Conhecer as principais vulnerabilidades
- Tomar contato com mecanismos de segurança das informações
- Conhecer os principais conceitos de Criptografia
- Compreender as assinaturas e os certificados digitais

Material de Estudo



Material	Acesso ao Material
Notas de Aula e Apresentação	http://www.caetano.eng.br/ (Segurança da Informação – Aula 6)
Material Didático	Gestão de Segurança da Informação, Cap 2.
Leitura Adicional	https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf (Cartilha do CERT, pra quem não leu ainda!)

VULNERABILIDADES

Vulnerabilidades

- O que são?
  - Pontos fracos existentes nos ativos

  - Quando explorados, afetam
    - Integridade, disponibilidade e confiabilidade.

Vulnerabilidades

- Não seriam um problema se...
  - Não houvesse ameaças que as explorem
  - Mas as ameaças existem!

  - E com a evolução...
    - As vulnerabilidades tendem a aumentar

Pontos fracos devem ser eliminados!

Vulnerabilidade dos Dados

- Segurança deve...
  - Cobrir clientes, fornecedores e parceiros
- Business 2 Consumer (B2C)
  - Na interação com os clientes
  - Sistemas, tráfego de dados...
- Business to Business (B2B)
  - Compartilhamento de dados
  - Parceiros devem implementar segurança
    - Igual ou maior

Identificando Vulnerabilidades

- Identificar falhas de segurança
- Ponto de partida?
  - Lista de ativos (soft, hard, processos, pessoas...)
  - Lista de ameaças

- Processos
  - Fontes de vulnerabilidades
  - Testes de segurança
  - Lista de verificação de requisitos
- Segundo ABNT
  - Testes e simulações (incluindo invasão)
  - Auditorias em códigos fonte

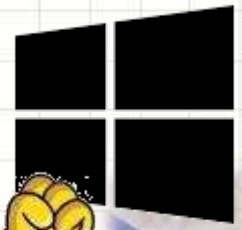
Terminologia Mais Completa

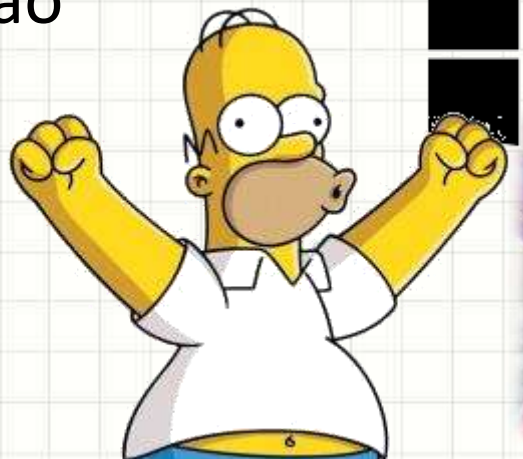
- Ameaças: Circunstância, ação ou evento que pode levar à quebra de segurança
- Vulnerabilidade: fragilidade nos ativos que o expõe a ameaças
- Risco: valor que resume a probabilidade de uma ameaça e seu impacto
- Incidente ou ataque: uma tentativa ou sucesso de uma ameaça em explorar uma vulnerabilidade
- Desastre: impacto de um ataque de sucesso
- Exploit: programa que explora uma vulnerabilidade

Principais Vulnerabilidades

Tipos de Vulnerabilidades

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





1. Vulnerabilidades Naturais

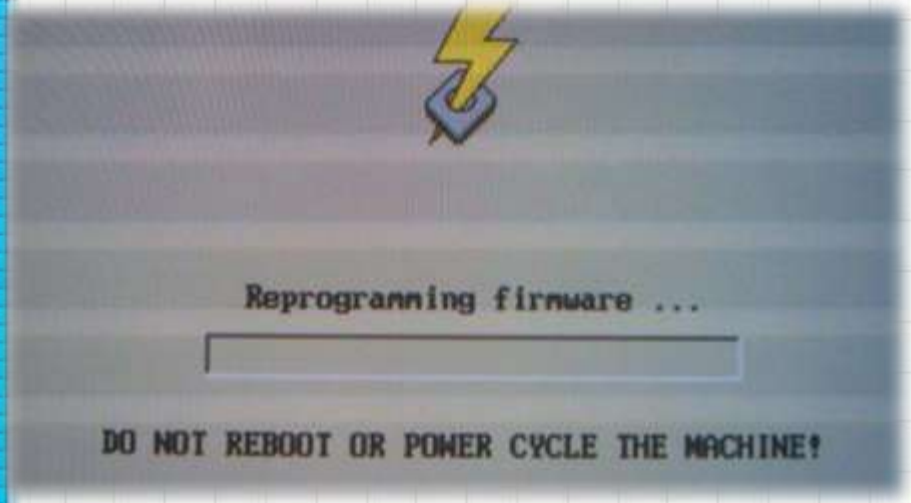
- São aquelas decorrentes de fenômenos naturais e que trazem riscos para equipamentos e informações
  - Ex. : inundações, terremotos, maremotos...

2. Vulnerabilidades Físicas

- São ambientes que possuem pontos fracos em nível de espaço físico, comprometendo a segurança dos equipamentos e informações
  - Ex.: espaço inadequado para trabalho, falta de extintores de incêndio, pessoas não autorizadas transitando no local...

3. Vulnerabilidades de Hardware

- São aquelas relacionadas à defeitos de fabricação ou configuração inadequada podendo permitir ataques
  - Ex.: falta de atualização de firmware, equipamentos mal dimensionados...



4. Vulnerabilidades de Software

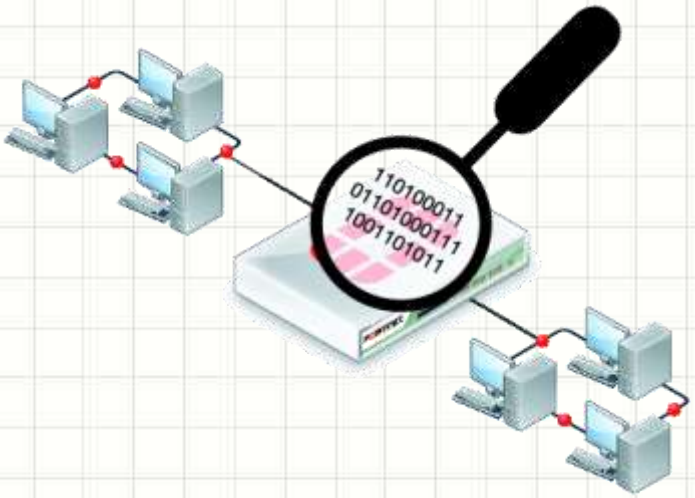
- Falhas em programas que permitam acesso não autorizado aos equipamentos.
  - Ex.: aplicativos mal configurados, programas de e-mail que permitem execução de código, programas desatualizados...

5. Vulnerabilidades de Armazenamento

- Falha ou uso inadequado do suporte físico, podendo comprometendo a segurança dos dados
  - Ex.: equipamento além da vida útil, defeitos de fabricação, prazo de validade das mídias...

6. Vulnerabilidades de Comunicação

- São as relacionadas ao tráfego de informação, seja por cabo de cobre, fibra, ondas de rádio ou satélite, permitindo eventuais intervenções de terceiros.
  - Ex.: Sniffer na rede, interrupção da comunicação...



6. Vulnerabilidades Humanas

- São aquelas relacionadas à atitudes humanas inadequadas, intencionais ou não, que possam colocar em risco a segurança da informação
  - Ex.: Uso de senhas fracas, compartilhamento de credenciais, desconhecimento da política de segurança, funcionários descontentes...

Ferramentas para Análise de Vulnerabilidades

Por Que Usar Ferramentas?

- Não há como evitar 100% dos ataques
- Análise de Risco
  - Permitir identificar os maiores riscos
    - Probabilidade x Impacto
    - Associados à ameaças e **vulnerabilidades**
  - Base em vulnerabilidades conhecidas...
    - E as desconhecidas?

- Mapear as vulnerabilidades
  - Para mitigá-las ou eliminá-las
  - Sempre observando os custos

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 vulnerabilidades
    - Maneira automatizada

Exemplos de Ferramentas

- NMAP
  - Detecta portas abertas no equipamento
  - Base para teste de firewall e sistemas de intrusão
- LanGuard

GFI LanGuard™

  - Registra eventos de rede e pesquisa vulnerabilidades na rede
  - Indica correções para as vulnerabilidades
- NESSUS

Nessus® vulnerability scanner

  - Cliente-Servidor, analisa vulnerabilidades remotas
  - Plugins para testes de vulnerabilidades específicas

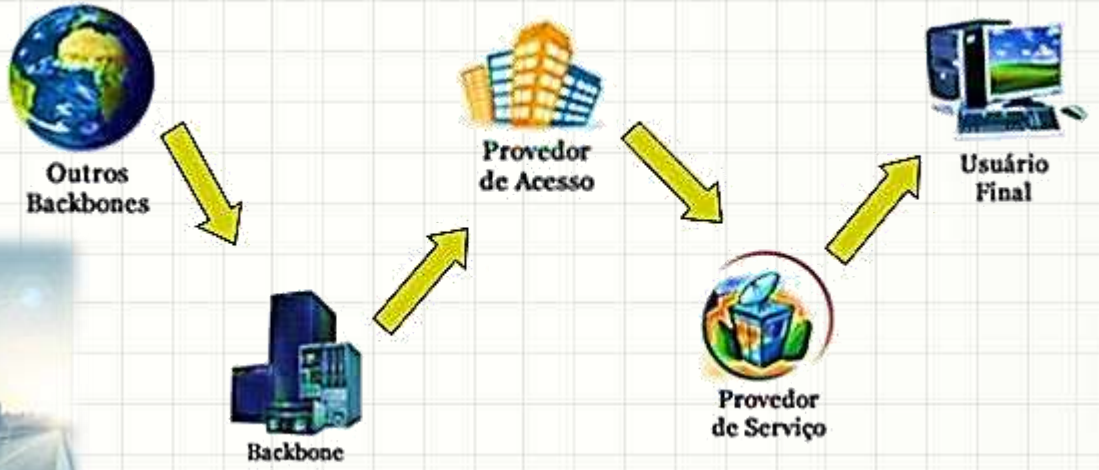
Exemplos de Ferramentas

- Lynis
  - Analisa vulnerabilidades em geral, gerando um relatório de ações para corrigí-las
- Chkrootkit / rkhunter
  - Verifica se arquivos do sistema estão comprometidos
- Tripwire
  - Registra mudanças em arquivos e gera relatórios periódicos sobre as mesmas

Mecanismos para Garantir a Segurança das Informações

Mecanismos de Segurança

- O que isso tem a ver com vulnerabilidades?
- Transmissão de informações: pela internet
  - Internet é pública e os dados são abertos
  - Isso, em si, é uma vulnerabilidade



Mecanismos de Segurança

- Mesmo que o dado não saia do computador
  - Pessoa com acesso físico...
  - Como dificultar o acesso aos dados?

Mecanismos de Segurança

- Os mecanismos mais clássicos são:
  - Criptografia dos dados
  - Assinatura digital dos dados

- 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

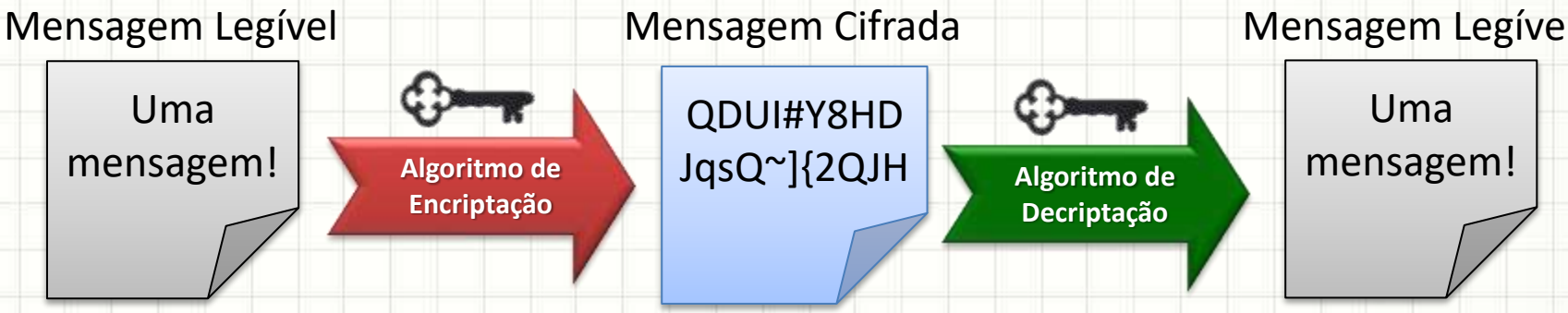
- Codificação dos dados
- Processo que transforma

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

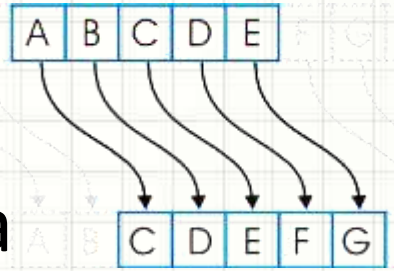
Criptologia

Chave Criptográfica

- Porta: basta ela existir?
  - Precisa haver uma chave
- 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



Exemplo: Substituição



- Codificar: “somar 2” a cada letra

A B A C A X I

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

C D C E C Z K

Algoritmo: somar 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

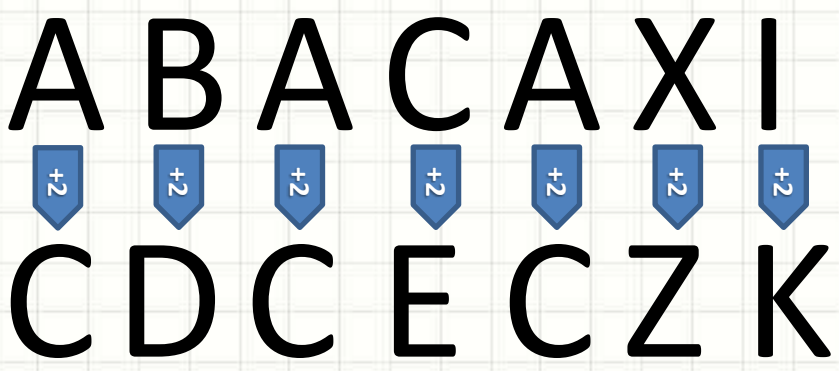
Algoritmo: subtrair o valor da chave da letra

Chave: 2

Criptografia Simétrica ou de Chave Secreta

Criptografia de Chave Pública

- Codificar: “somar 2” a cada letra



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

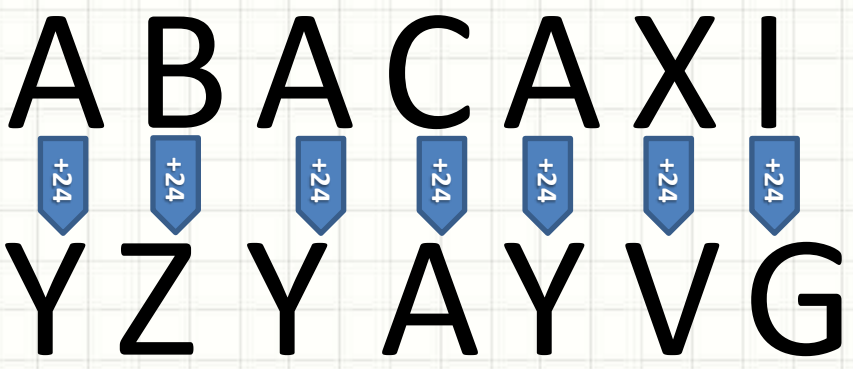
- Decodificar: “somar 24” a cada letra

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

Criptografia Assimétrica ou de Chave Pública

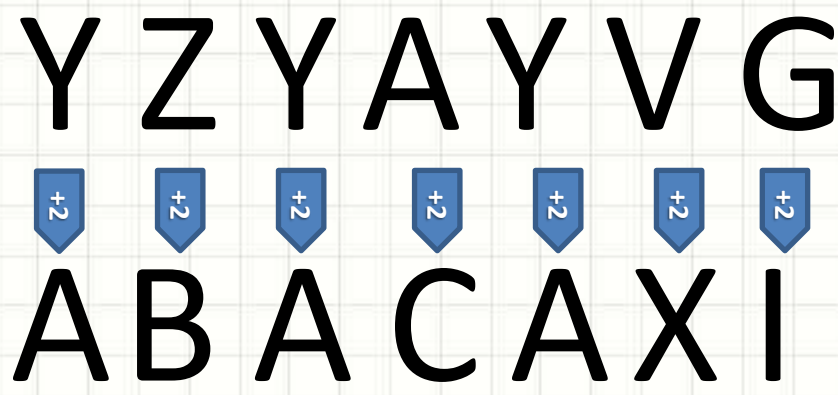
Criptografia de Chave Pública

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



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

- Decodificar: "somar 24" a cada letra

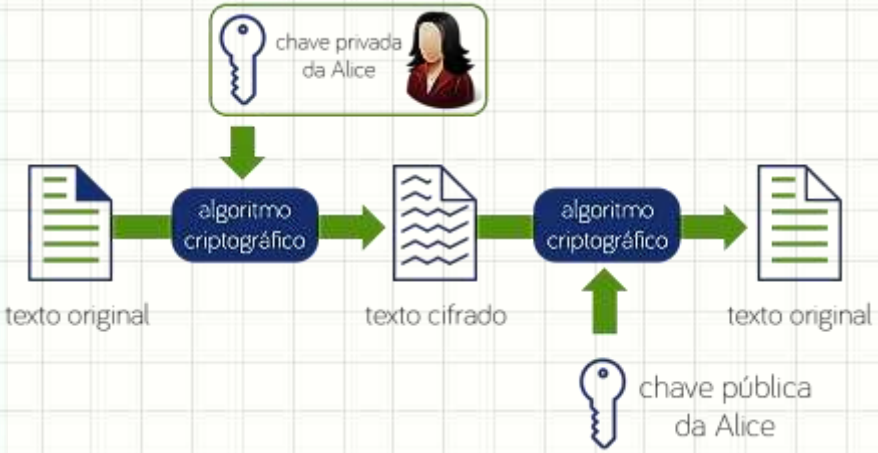


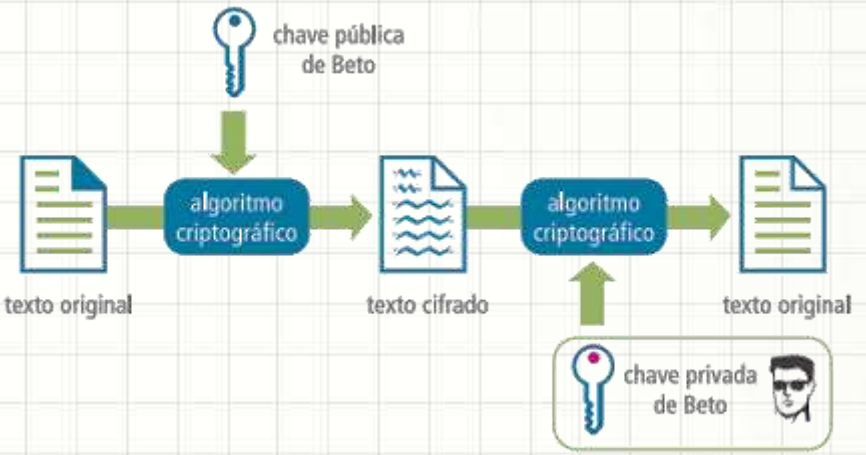
Algoritmo: somar o valor da chave privada
Chave: 2 **Chave Privada**

Funciona nas duas direções!

Criptografia de Chave Pública

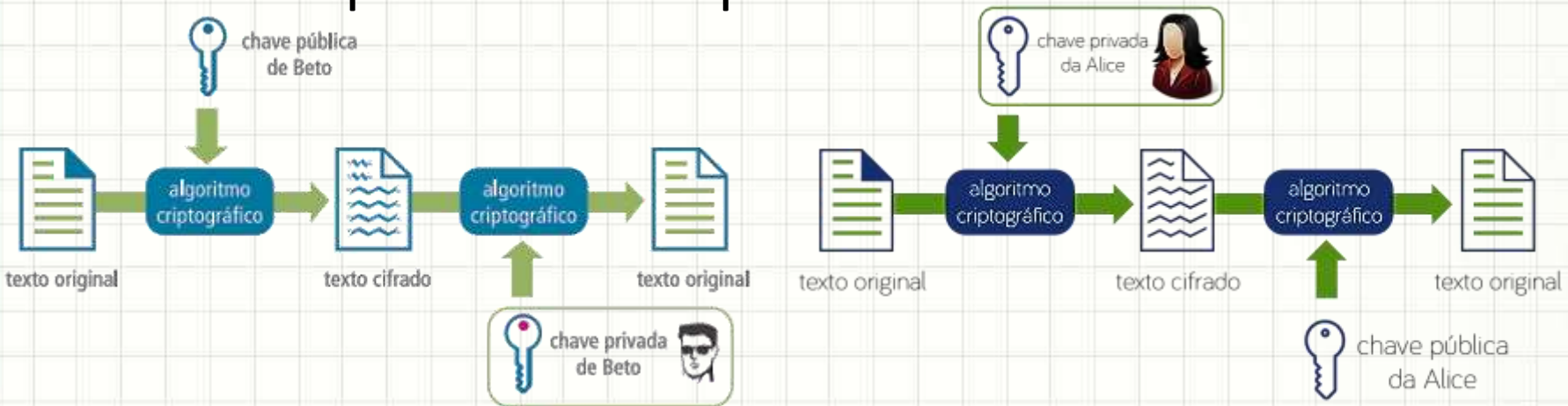
- Se eu codifico com minha chave privada
  - As pessoas podem decifrar com minha chave pública e verificar que a mensagem é minha
- Se alguém codifica com minha chave pública
  - Apenas eu posso decifrar com minha chave privada





Criptografia de Chave Pública

- Se eu quero mandar uma mensagem secreta
  - Eu codifico essa mensagem com a chave pública do receptor e só ele poderá abrir
- Se receber uma mensagem codificada com a chave privada de alguém
  - Eu me certifico do autor decodificando com a chave pública dessa pessoa

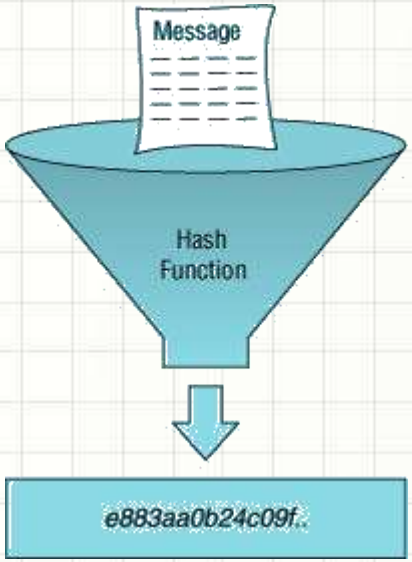


Criptografia de Chave Pública

- 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

Hash ou Número Resumo



- Criptografia: “ida” e “volta”
  - Se eu codifiquei, eu decodifico
- Hash: só “ida”
  - Só codifico, nunca decodifico
  - Deve ser único para uma mensagem legível
- 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

Hash ou Número Resumo

- Usado, por exemplo, para armazenar senha

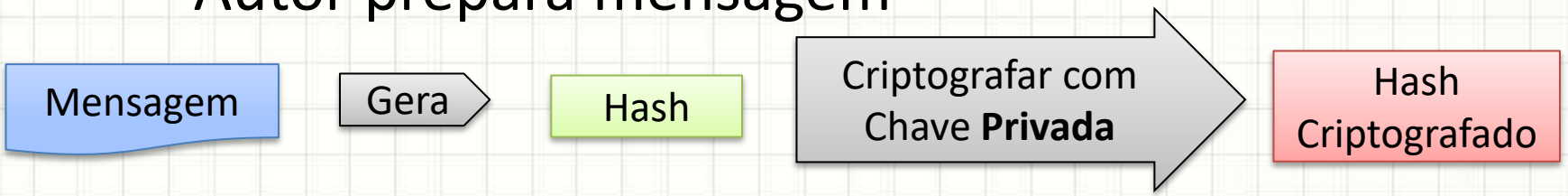
- Quando for ocorrer um *login*?
  - Usuário digita a senha
  - Geramos o hash da senha
  - Comparamos com o banco de dados
- Vantagem?
  - Se roubarem o BD, não terão as senhas!

Assinaturas Digitais – Retomando!

- 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

QUESTÕES

Questão

Sobre os tipos de vulnerabilidades, leia as asserções e assinale a alternativa correta.

I. Vulnerabilidades Naturais são, por exemplo: pessoas não autorizadas transitando no local;

II. Vulnerabilidades de Hardware englobam, por exemplo: a falta de atualizações dos programas e equipamentos não dimensionados corretamente;

III. Vulnerabilidades de Software englobam, por exemplo: aplicativos com configurações ou instalações inadequadas.

a) Somente a asserção I está correta.
b) Somente a asserção II está correta.
c) Somente a asserção III está correta.
d) As asserções I e II estão corretas.
e) As asserções II e III estão corretas.

Conclusões

Resumo e Próximos Passos

- Principais vulnerabilidades
- Ferramentas para detecção
  - Prevenção e scanners
- Mecanismos para proteger a informação
  - Criptografia e assinaturas digitais

- Boas práticas em segurança da informação
  - Políticas de senhas
  - Treinamento de usuários
  - Mecanismos de proteção

PERGUNTAS?