Prof. Wanderson Reis
professor@wanderson.pro.br

Gerenciamento e Segurança de Dados

04/03/2011

Informática - PDS

Tópicos principais

- Definições básicas de segurança da informação
- Políticas de segurança da informação
- ***Criptografia e certificação digital***
- Desenvolvimento seguro
- Segurança em banco de dados
- Segurança em sistemas operacionais
- Sistemas e políticas de backup
- Espelhamento de volumes e servidores
- Análise de ameaças e vulnerabilidades
- Técnicas de invasão e ataque
- Segurança em redes de computadores
- Segurança na Internet
- Segurança de serviços de rede

Criptografia

(kriptós = escondido, oculto; grápho = grafia)

Arte ou ciência de escrever em cifra ou em códigos, de forma a permitir que somente o destinatário a decifre e a compreenda.

Criptoanálise

Arte ou ciência de determinar a chave ou decifrar mensagens sem conhecer a chave. Uma tentativa de criptoanálise é chamada ataque.

Criptologia

Ciência que reúne a criptografia e a criptoanálise

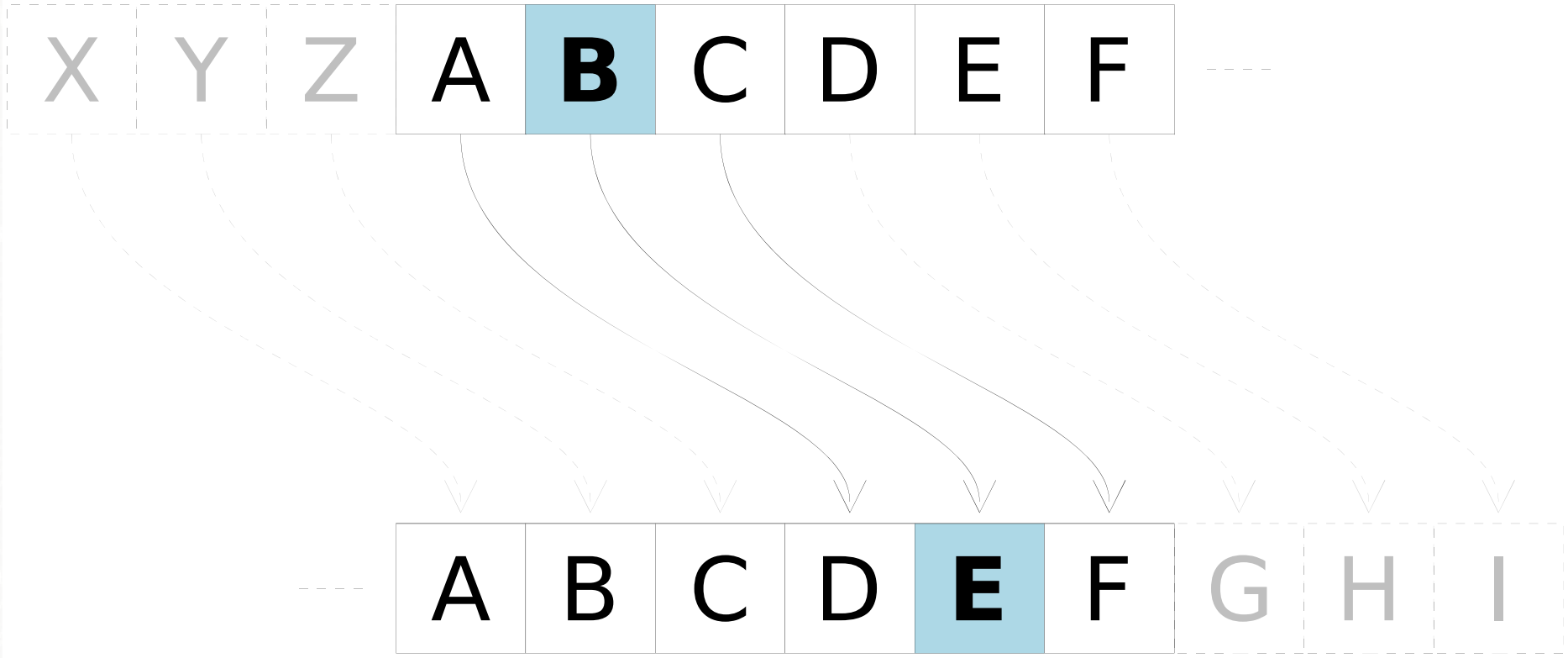
Esteganografia

Esteganografia é um ramo particular da criptologia que consiste em fazer com que uma forma escrita seja camuflada em outra a fim de mascarar o seu verdadeiro sentido.

Vantagens da criptografia

Confere a informação: integridade, autenticidade, privacidade e não-repúdio as informações transmitidas ou transportadas.

Criptografia por transposição



Uso prático da criptografia

- Comunicação GSM (celular)
- Transações em bancos e lojas utilizam SSL (HTTPS)
- Administradores de sistemas utilizam SSH
- Redes sem fio utilizam WEP, WAP, etc
- Redes Privadas Virtuais (VPN) utilizam IPSec
- Assinatura digital
- Certificação digital
- Verificação de integridade de arquivos e documentos

Funções criptográficas

- Unidirecional (hash) – somente encripta
- Bidirecional (usa chave) – encripta e decripta

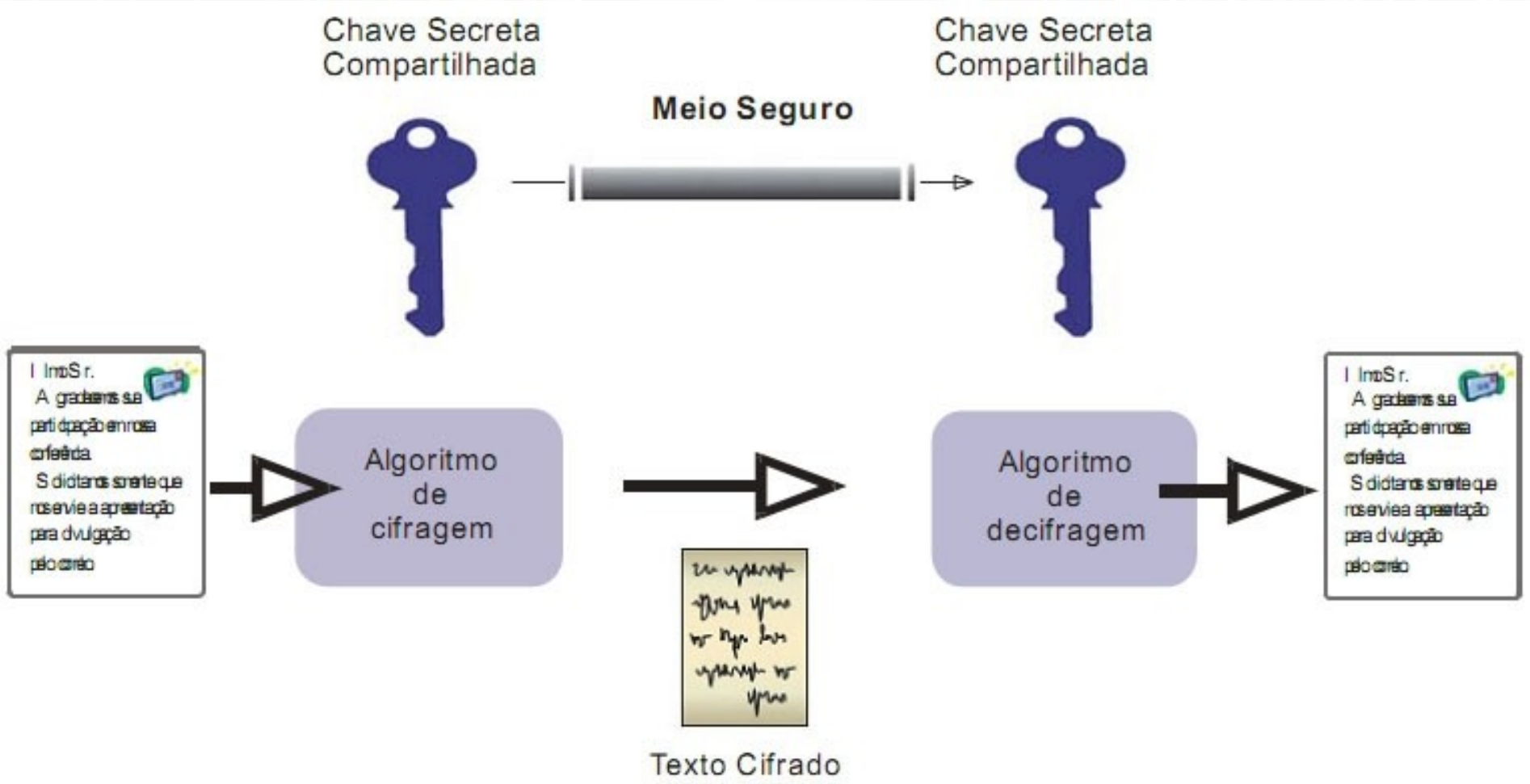
Resumo criptográfico (HASH)

- MD5SUM – 128 bits
- SHA1SUM – 160 bits
- Outros utilizados para checagem

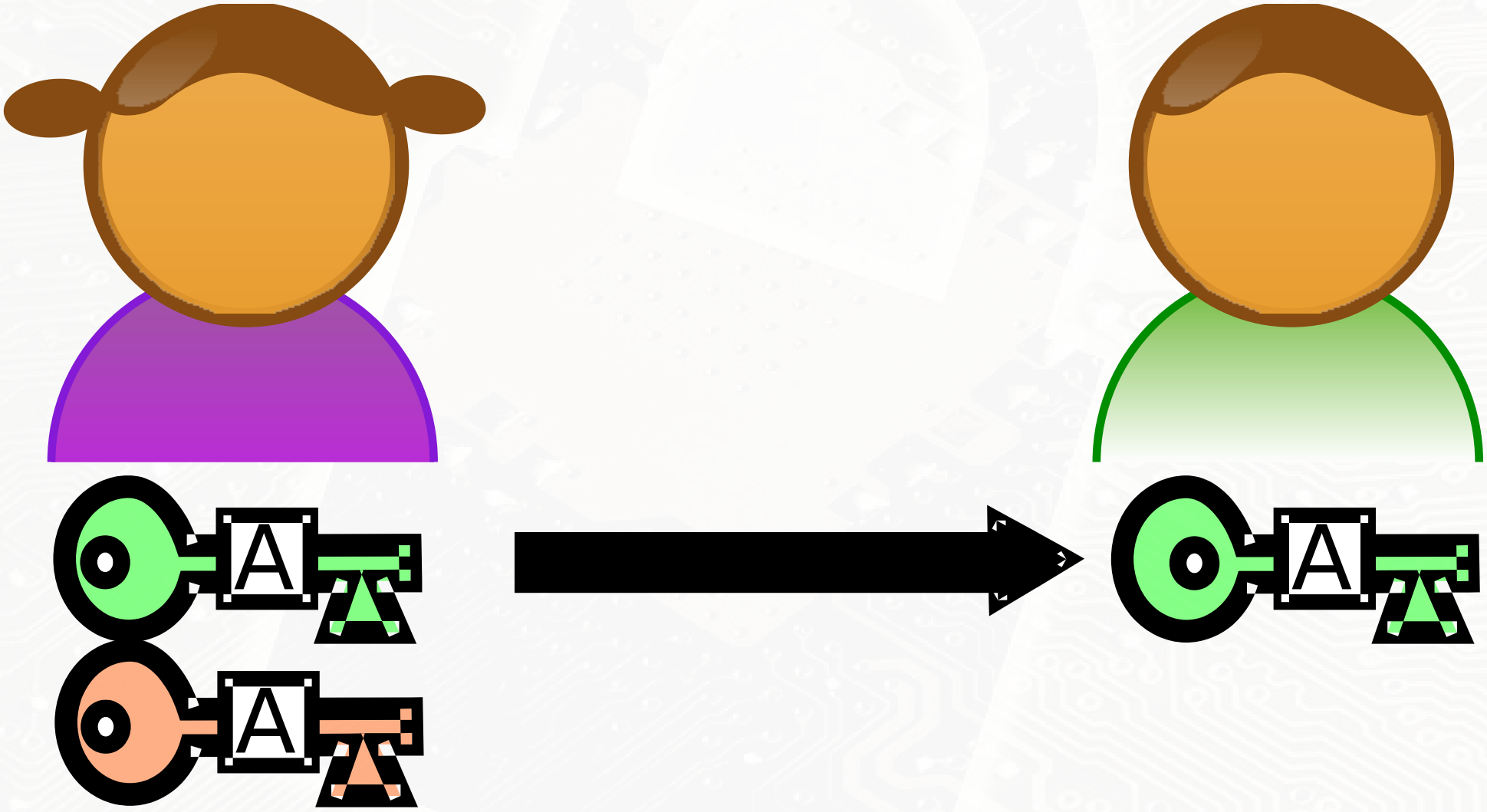
Chaves criptográficas

- Privada ou simétrica (rápida)
- Pública ou assimétrica (lenta)

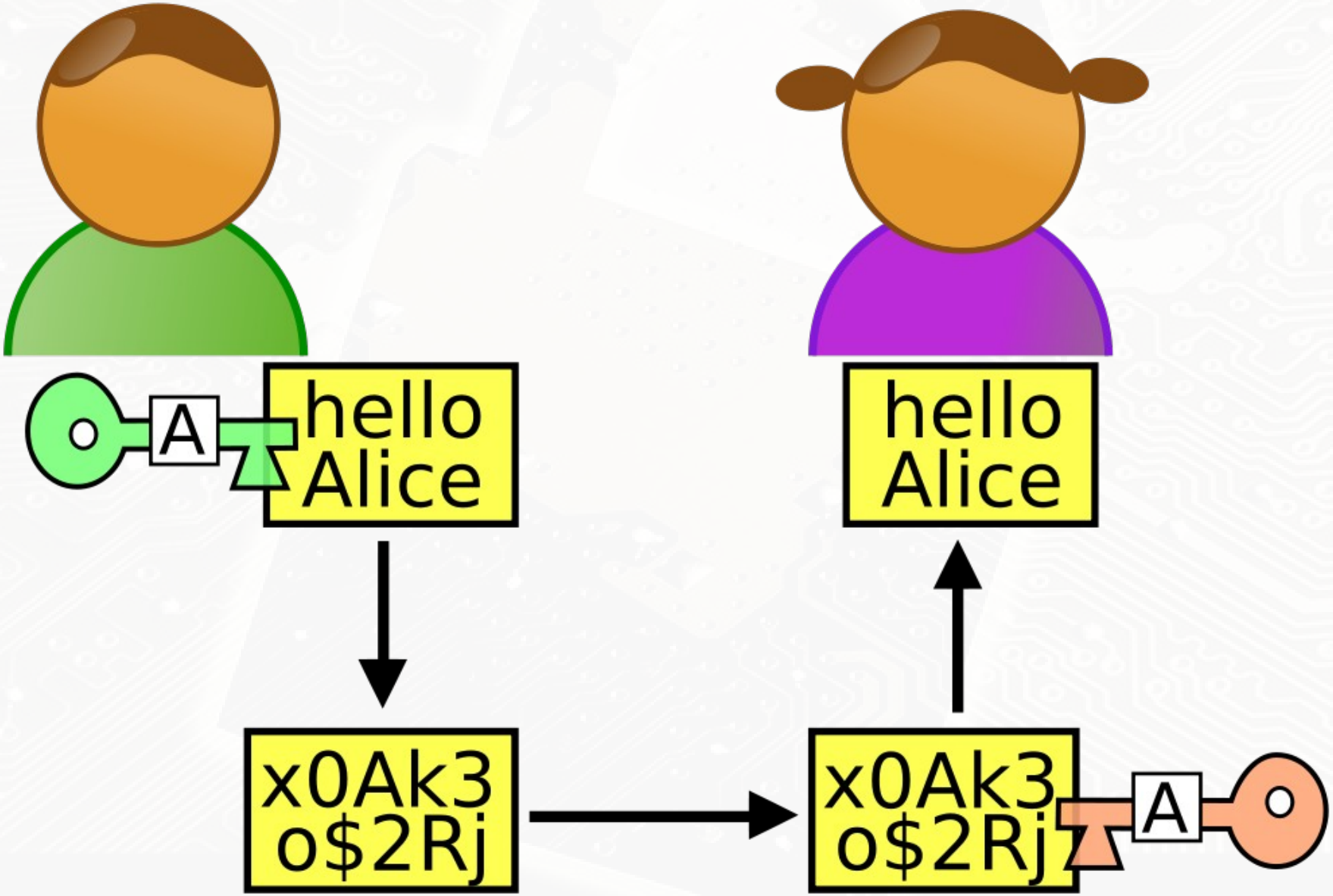
Criptografia simétrica



Criptografia assimétrica

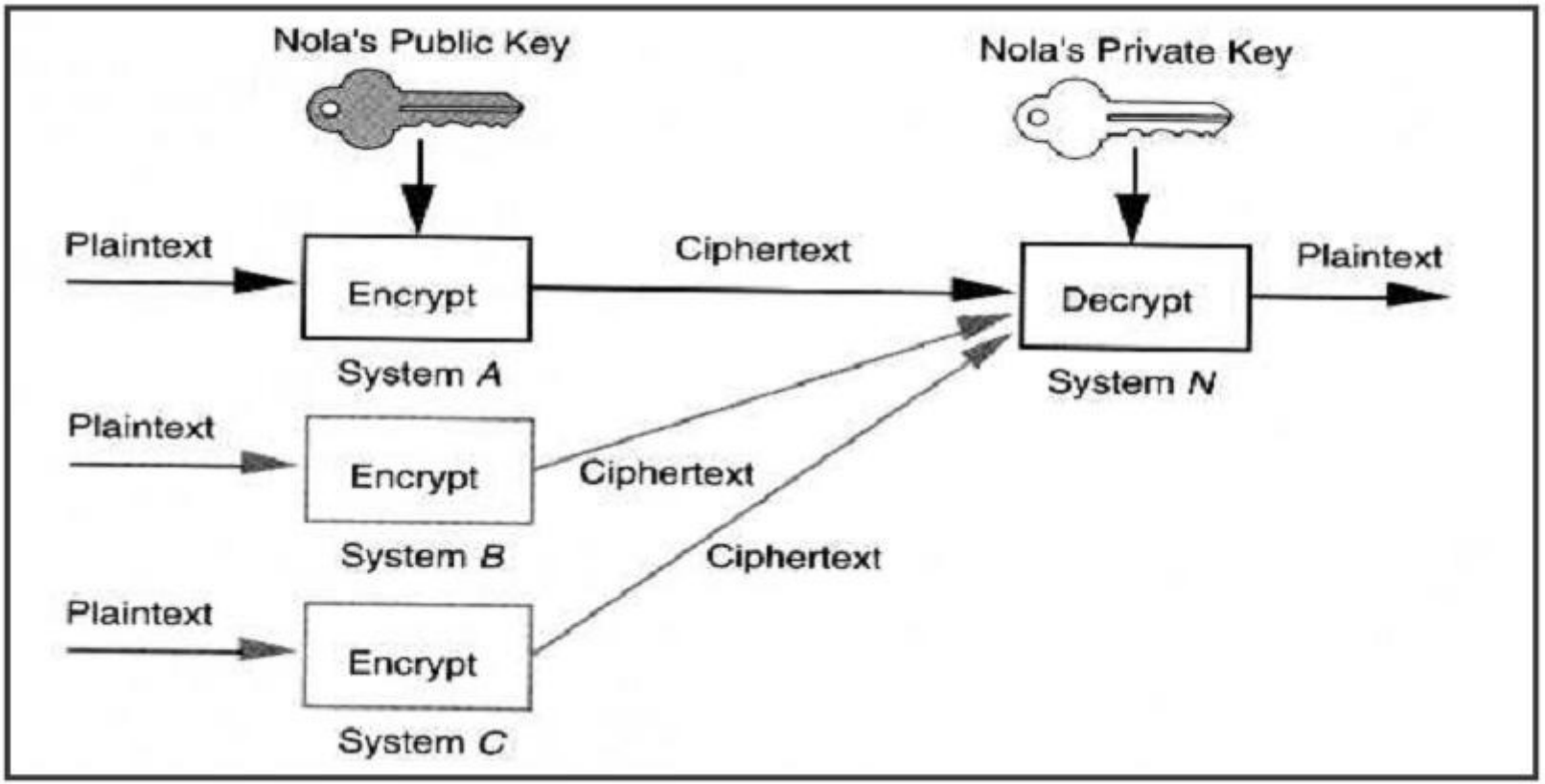


Criptografia assimétrica



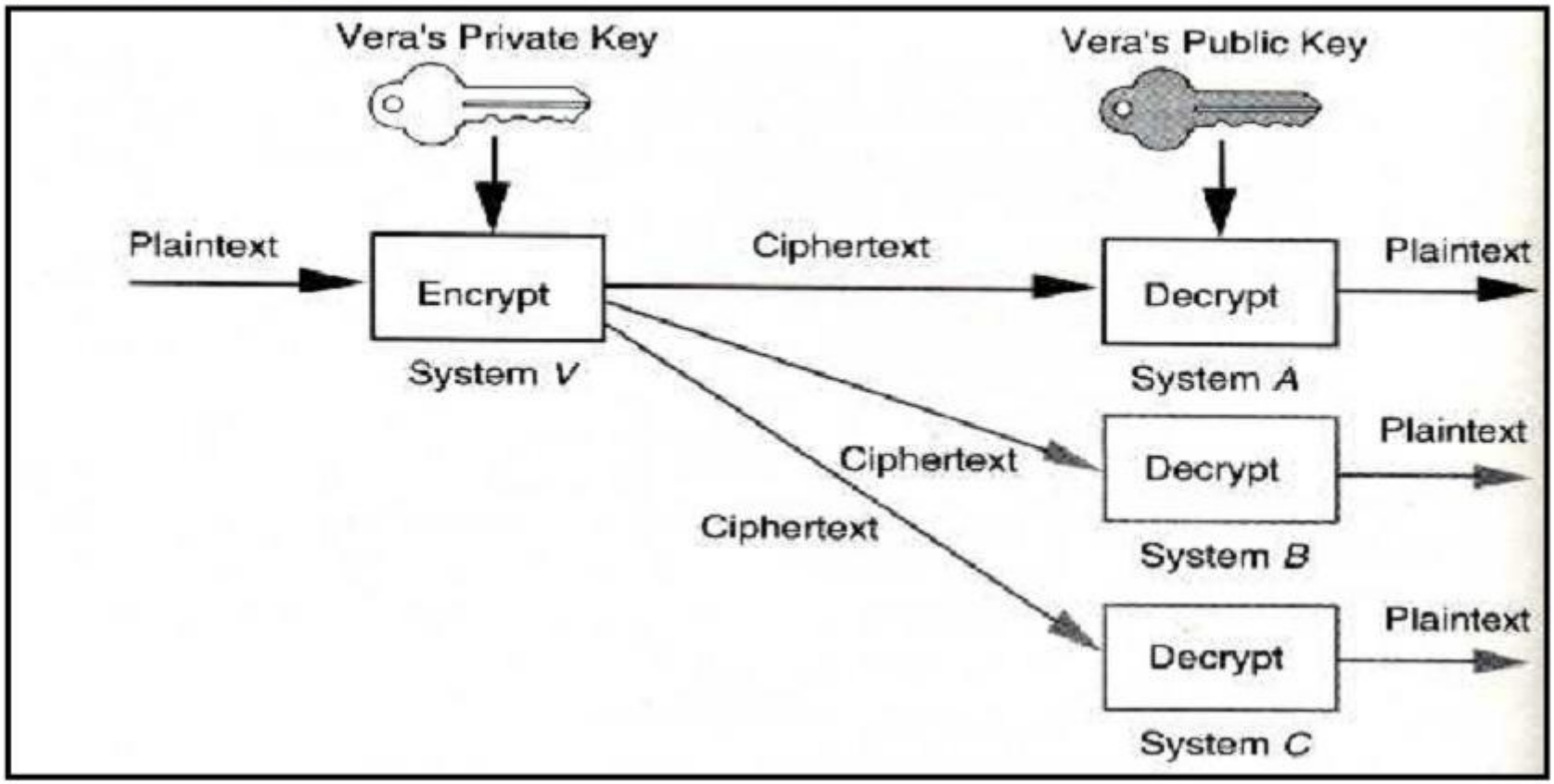
Criptografia assimétrica

Confidencialidade



Criptografia assimétrica

Autenticação



Segurança dos métodos criptográficos

- Geração de chaves
- Mecanismo de troca de chaves
- Taxa de troca de chaves
- Tamanho da chave

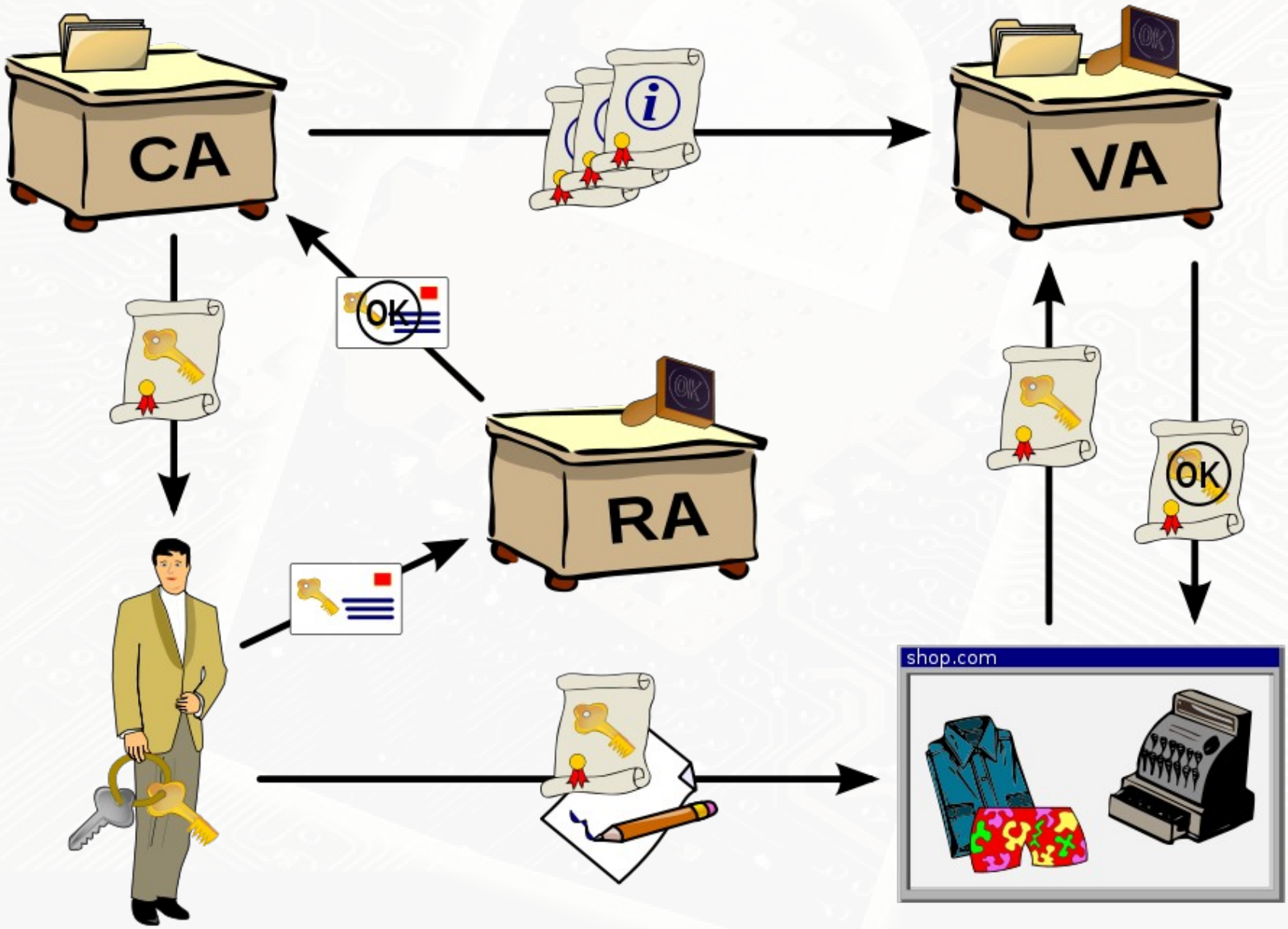
Segurança pelo tamanho da chave

- Algoritmo simétrico (US$ 1 mi)
  - 64 bits ~ 4 dias
  - 112 bits ~ 10^{12} anos
- Algoritmo assimétrico (300Mhz)
  - 512 bits ~ 8 meses
  - 768 bits ~ 300 anos

Infraestrutura de chaves públicas

- Servidor de chaves
- Autoridade Certificadora (AC)
- Rede de confiança

Infraestrutura de chaves públicas



Criptografia: mão na massa

Individualmente ou em duplas escrever um relatório com base nas seguintes tarefas:

1. Verificar a integridade de um arquivo com SHA1SUM
3. Esconder e recuperar uma mensagem em uma imagem usando esteganografia
2. Criar e utilizar um par de chaves (pública e privada) para assinatura e criptografia de mensagens

Mão na massa: objetivos

- Conhecer de forma prática como a criptografia pode ser aplicada para garantir a integridade, autenticidade, privacidade e não-repúdio as informações.

Mão na massa: ferramentas

Disponíveis em http://wanderson.pro.br

1. HashCalc e Marxio FCV

2. SteganoG e OpenPUFF

3. https://www.igolder.com/PGP/generate-key
   + PortablePGP

Mão na massa: Desenvolvimento

- **Verificar o HASH de arquivos** (resumo criptográfico)
  - Usando o programa HashCalc ou Maxio FCV verificar os arquivos **modelo_relatorio_atividade.odf e PDS_criptografia.rar**

- **Esteganografia**
  - Usando o programa **StegnoG revelar** a mensagem escondida no arquivo **mensagens/cadeado.bmp** (senha 123456)
  - Usando o programa OpenPUFF **revelar** a mensagem escondida no arquivo **mensagens/cadeado1.jpg** (senha 12345678)
  - Usuando um programa a sua escolha **esconder** uma mensagem em um arquivo qualquer

Mão na massa: Desenvolvimento

- **Utilizando par de chaves pública e privada**
  - Criar um par de chaves usando a ferramenta online em https://www.igolder.com/PGP/generate-key e salvar as chaves em arquivos textos com as extensões .pub e .priv
  - Usando a ferramenta PortablePGP importar as chaves geradas no passo anterior
  - Encriptar e descriptar um arquivo qualquer
  - Assinar um arquivo qualquer e verificar a assinatura

Mão na massa: entrega do relatório

- Converter o **arquivo do relatório** para PDF e **assinar o relatório** com a chave privada criada na atividade;
- Enviar para **professor@*wanderson.pro.br*** os seguintes arquivos:
    1. Arquivo texto contendo a **chave pública** correspondente da chave usada para assinar o relatório
    2. O **relatório** em formato PDF
    3. O **arquivo de assinatura** do relatório PDF