Introdução à Economia e à Administração 2024

13ª Aula – Introdução à Tecnologia da Informação

Introdução à Economia e à Administração 2024

O que é Tecnologia para Você?

Sugestão para casa – “2001: Uma Odisseia no Espaço” (EUA, Reino Unido, 1968)

Cena do filme:
https://www.youtube.com/watch?v=9etefsYMm5o
(pular de 1’30” a 3’)

Trilha sonora da cena: “Also sprach Zarathustra, Op. 30 (1896)”, de Richard Strauss e “An der schönen, blauen Donau, Op. 314 (1866)“, de Johann Strauss II

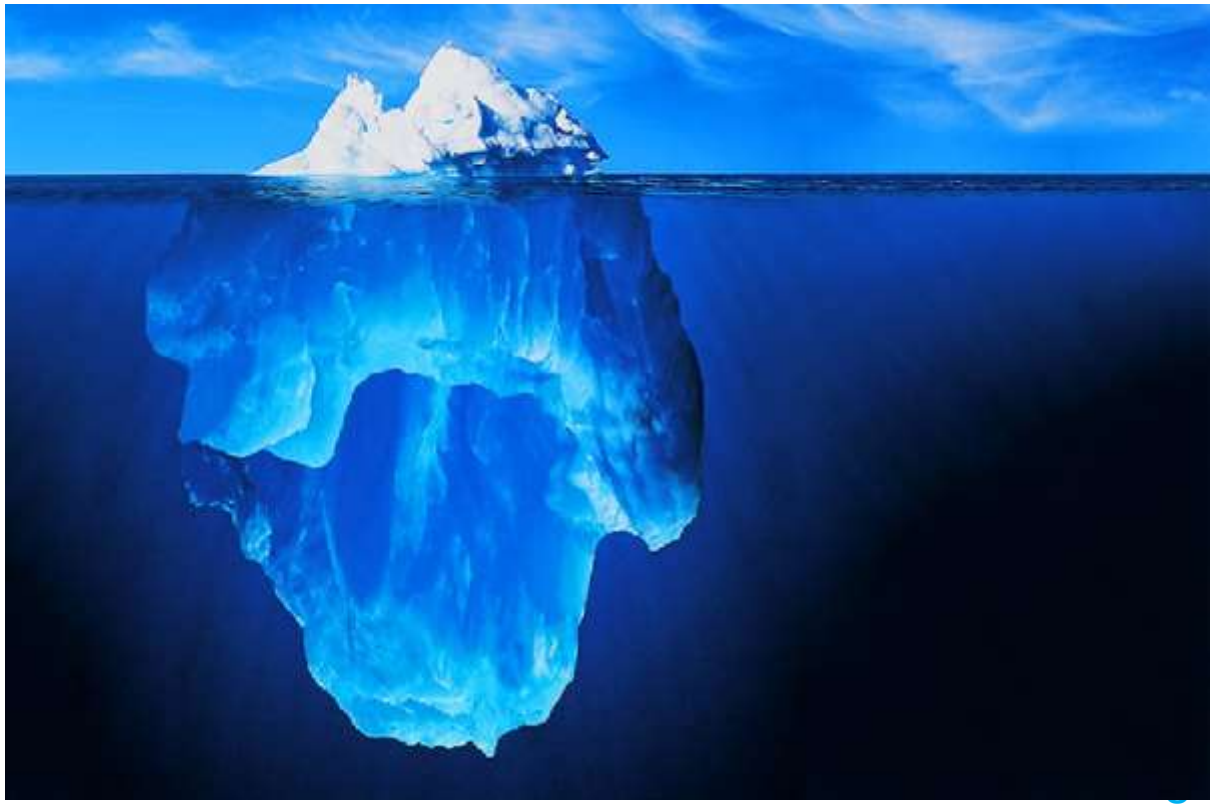
Pessoas + Ferramentas + Processos

Sugestão de leitura: A tecnologia sem nome no filme ‘2001’
http://innovatrix.com.br/a-tecnologia-sem-nome-no-filme-2001/

Sistemas de Informação

Conjunto de componentes inter-relacionados que coletam (ou recuperam), processam, armazenam e distribuem informação para o suporte à decisão, coordenação e controle. São compostos por:

- *Hardware*
- *Software*
  - Aplicativos
  - *Software* básico
  - Linguagens de programação
  - Bancos de dados
- Telecomunicações



Mas, o que é mesmo Informação?

É uma mensagem que é transmitida de um ponto para o outro.

Essa mensagem tem que produzir um efeito, senão não será Informação, mas Ruído. Portanto, a Informação requer uma seleção daquilo que será transmitido.

A Informação não é transmitida apenas por humanos e por meio de tecnologias por nós desenvolvidas. Exemplos: comportamento dos animais, funcionamento de células, etc.

Da mesma forma que o petróleo refinado vale mais do que o petróleo bruto, a Informação selecionada e formatada de acordo com nossas necessidades é o bem mais valioso dos dias de hoje.

Sugestões para casa:

Filmes:

"A Chegada"
(EUA, 2016)

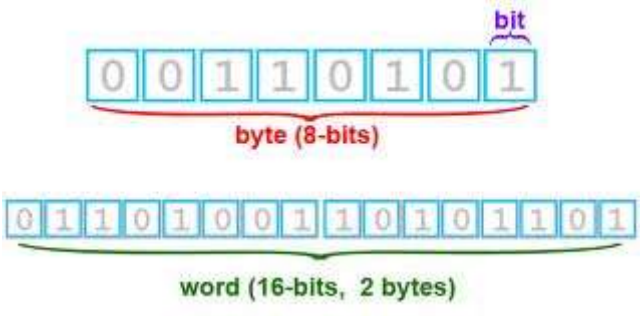
"E.T.: O Extraterrestre"
(EUA, 1982)

Medidas de Informação

1 Bit – menor informação possível, pode assumir valor 0 ou 1.
1 Byte – conjunto de 8 bits

Quantos valores possíveis um byte pode assumir?

Na Tecnologia da Informação (T)I, 1 KiloByte é 1.024 (2^{10}) Bytes e não 1.000 Bytes, e assim sucessivamente.



Name	Abbr.	Size
Kilo	K	2^10 = 1,024
Mega	M	2^20 = 1,048,576
Giga	G	2^30 = 1,073,741,824
Tera	T	2^40 = 1,099,511,627,776
Peta	P	2^50 = 1,125,899,906,842,624
Exa	E	2^60 = 1,152,921,504,606,846,976
Zetta	Z	2^70 = 1,180,591,620,717,411,303,424
Yotta	Y	2^80 = 1,208,925,819,614,629,174,706,176

Lei de Moore

Em 1965, Gordon Earl Moore (1929-2023), um dos fundadores da Intel, previu que o poder de processamento dos computadores dobraria a um ritmo constante.

Após alguns anos de observações, ele concluiu que essa duplicação ocorreria a cada 24 meses. Isto é, daqui a dois anos você vai poder comprar um chip com o dobro da capacidade de processamento pelo mesmo preço que você paga hoje.

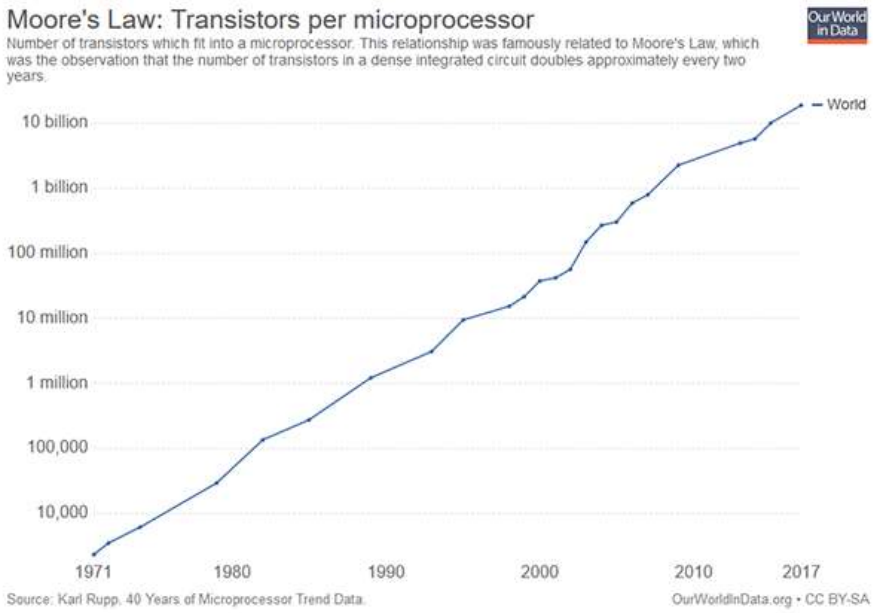
O crescimento do número de transistores nos processadores fabricados pela Intel praticamente seguiu à risca essa previsão ao longo de mais do que cinco décadas!

Lei de Moore

O efeito disso é gigantesco, uma vez que faz com que a potência de computação cresça exponencialmente.

Especula-se que a miniaturização dos processadores encontra-se próxima do nível atômico, e que, portanto, a Lei de Moore finalmente estaria próxima de chegar a seu limite.

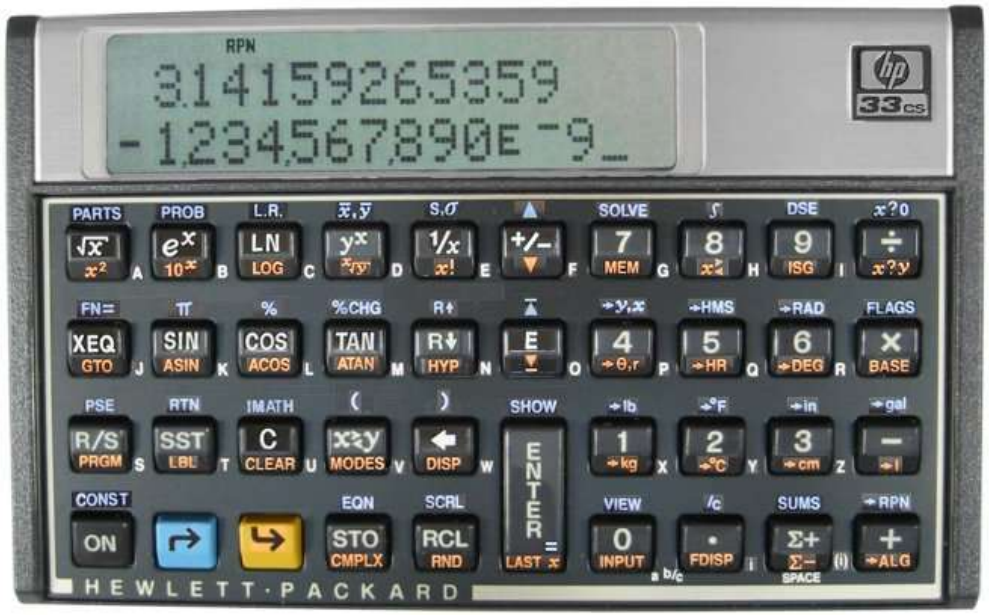
Para discussão em classe: quantas vezes o processador de um *desktop* doméstico comprado hoje é mais rápido que o de um desktop doméstico comprado 20 anos atrás pelo mesmo preço?



Lei de Moore

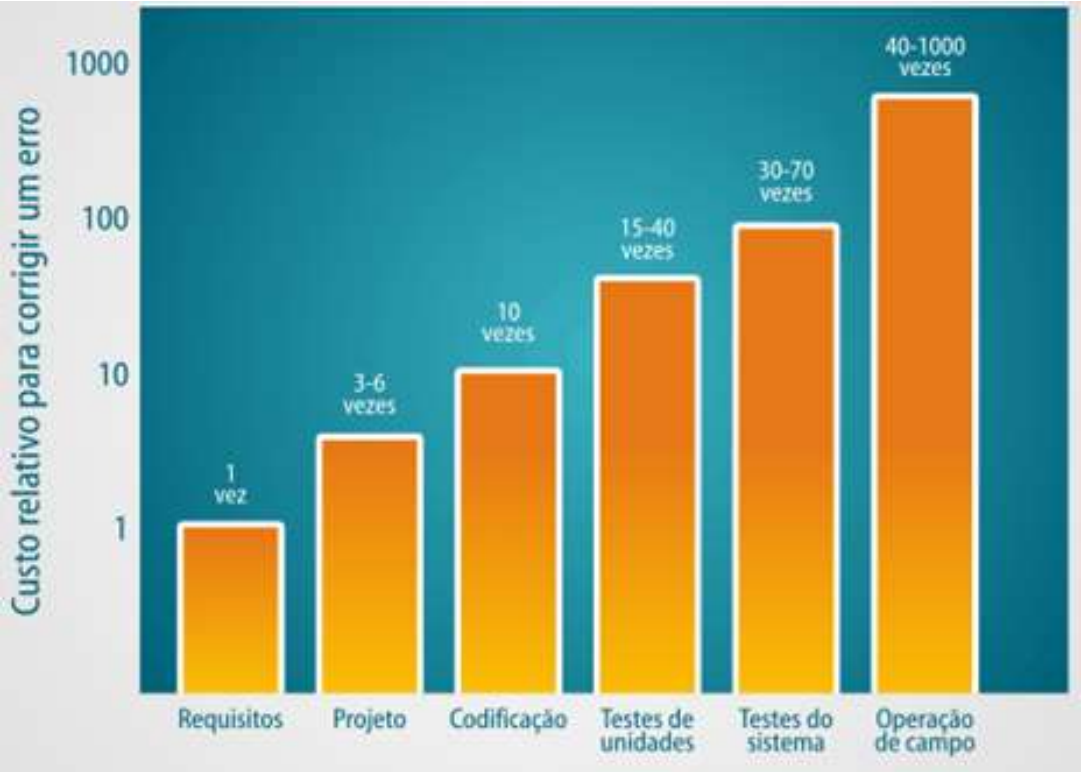
Por conta da Lei de Moore, praticamente todo o mundo eletrônico é renovado a cada 5 anos.

Mas existem exceções, que são temas de diversos estudos. Por exemplo, as calculadoras financeiras da HP.



Regra 10 de Myers

Em 1979, Glenford Myers, em seu livro 'The Art of Software Testing', apresentava o conceito no qual quanto mais cedo descobrimos e corrigimos um erro, menor é o seu custo para o projeto.



Esse custo em correção de *bugs* cresce 10 vezes para cada estágio em que o projeto do software avança.

Isso é coerente com o que foi visto no TPS (Toyota Production System).

Inteligência Artificial

Dentro de duas décadas, grande parte das profissões estará profundamente diferente do que são hoje em função da aplicação de Inteligência Artificial, que será capaz de ter autoaprendizagem e acessará um grande volume de dados.

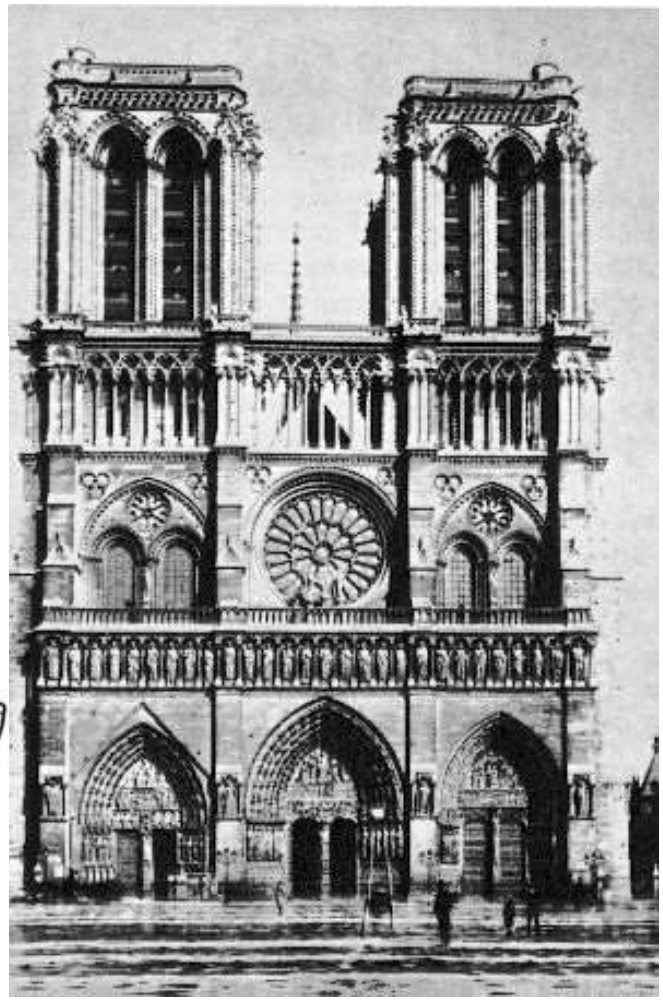
Impacto cada vez maior dos algoritmos nas nossas vidas.

Riscos e oportunidades

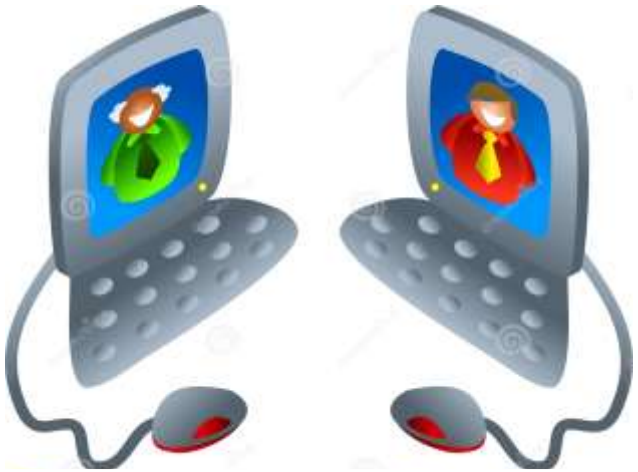
Vantagem para quem for capaz de programar.

Sugestão: Blade Runner (EUA, 1982)

O Avanço da Tecnologia mata o que existia antes?



Internet das Coisas (IoT)



Conexão de dispositivos eletrônicos utilizados no dia-a-dia (aparelhos eletrodomésticos, eletroportáteis, máquinas industriais, meios de transporte etc.) à Internet. IoT ocupará uma proporção cada vez maior do tráfego global na nuvem.

Ex: ao chegar em casa de automóvel, isso é automaticamente detectado e dá início a vários processos, desde abrir a garagem e ligar o ar condicionado até iniciar o preparo de alguma refeição.

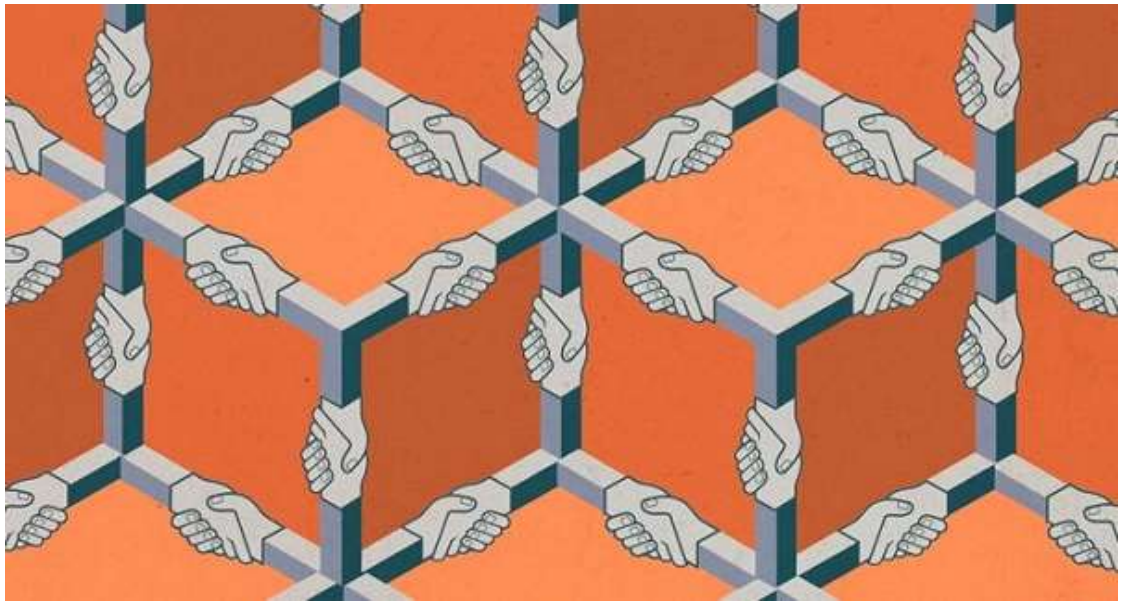
Tecnologias utilizadas: Internet, RFID, bancos de dados, nuvem, inteligência artificial, sensores, drones...

Video

TED (Technology, Entertainment, Design) Talks
Colaboração online em Larga Escala (legendas em Português)
http://www.ted.com/talks/luis_von_ahn_massive_scale_online_collaboration?language=pt-br

Sugestão para casa: assistir a partir dos 5’20”

Blockchain – Tecnologia criada para o Bitcoin



Visa a descentralização como medida de segurança. Rede *peer-to-peer* e banco de dados distribuído e descentralizado.

Funciona como uma coleção de informações contábeis, guardadas em forma de blocos. Novos blocos completos são continuamente criados e adicionados à *blockchain* de modo linear e cronológico por um novo conjunto de registros.

O que se procura obter com a tecnologia *Blockchain*

Clareza e transparência totais nas transações de compra e venda de qualquer coisa.

Segurança: ausência de fraudes e veracidade na transação.

No lugar qualquer autoridade governamental, financeira ou tecnológica, há uma rede que valida, atesta e dá posse de qualquer coisa a que se tenha realmente direito (dinheiro, bem, propriedade intelectual, acesso a alguma coisa, execução de um contrato, permissão a ser dada a alguém).

Tudo acontece entre as partes diretamente, sem intermediário. Não há nenhuma parte para avaliar ou arbitrar os direitos de cada um.

Segurança de Informação e seus 3 Níveis Básicos

- Evitar que uma criança pequena acesse um conteúdo.
- Proteger uma informação de uma grande empresa concorrente.
- Proteger uma informação de uma grande potência estrangeira.

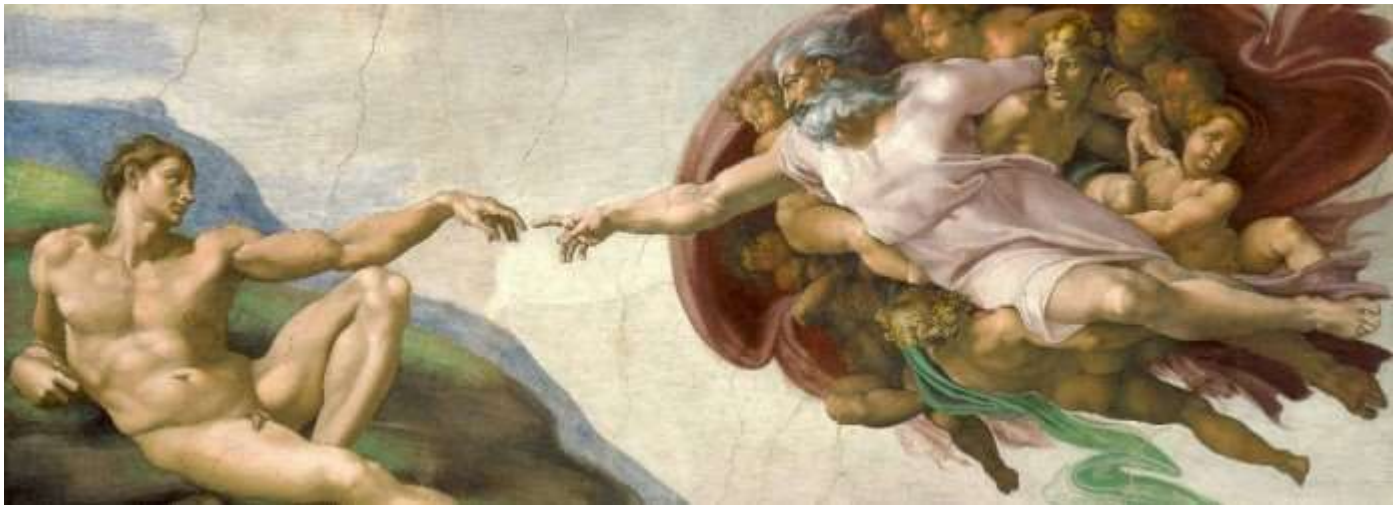
Segurança é normalmente composta de dois destes componentes:

- Posse de um objeto.
- Informação que só você possui (senha).
- Características biométricas.

Segurança da Informação e Criptografia

Criptografia = “escrita secreta”

“Primeiro veio a Palavra...



... depois muitas palavras apareceram, e o homem percebeu que algumas palavras precisavam ser escondidas. Aí nascia a criptografia.” (Anatoly Nicolaenko – “Máquinas Inteligentes”)

A Criptografia na Antiguidade

Egito antigo:

- Cabeças de escravos raspadas.
- Conceito de chaves – papiro embrulhado ao redor de um bastão de diâmetro fixo.

Império Romano:

- Bastões de diâmetros variáveis.
- Escrita fonética permite troca de letras, de acordo com uma chave.

Hoje tem festa nas termas!

Jqlg vgo hguvc pcu vgtocu!

A Criptografia na Idade Média

Durante grande parte foi banida, considerada heresia.

No Renascimento começaram a ser introduzidos fundamentos matemáticos na Criptografia.

A Criptografia na Idade Moderna

Grande impulso com o fortalecimento das monarquias, especialmente na França, incentivada pelo Cardeal Richelieu.

A Criptografia na Idade Contemporânea

A Criptografia torna-se uma Ciência em meados do séc. XIX.

No início do Século XX, a utilização em larga escala de telégrafo e rádio provocam o aumento do tráfego e da vulnerabilidade.

Criação de agências especializadas após a “Grande Guerra”.

II Guerra Mundial:

- Enigma x “Bomba” de Turing.
- Batalha de Midway: “AF is short of water.”
- Utilização da língua navajo.

Sugestão: The Imitation Game (EUA, Reino Unido, 2014)

A Criptografia na Guerra Fria

Investimentos maciços em segurança nos EUA e URSS.
Parceria NSA-IBM faz a criptoanálise chegar aos computadores.

A Criptografia no Mundo Atual

Criptografia deixa de ser domínio exclusivo da área militar.

Uso corriqueiro (dinheiro, TV paga, Internet, etc..).

Novos algoritmos (simétricos e assimétricos).

Segurança X Conveniência X Privacidade X Custos

Conceitos Modernos de Segurança de Informação

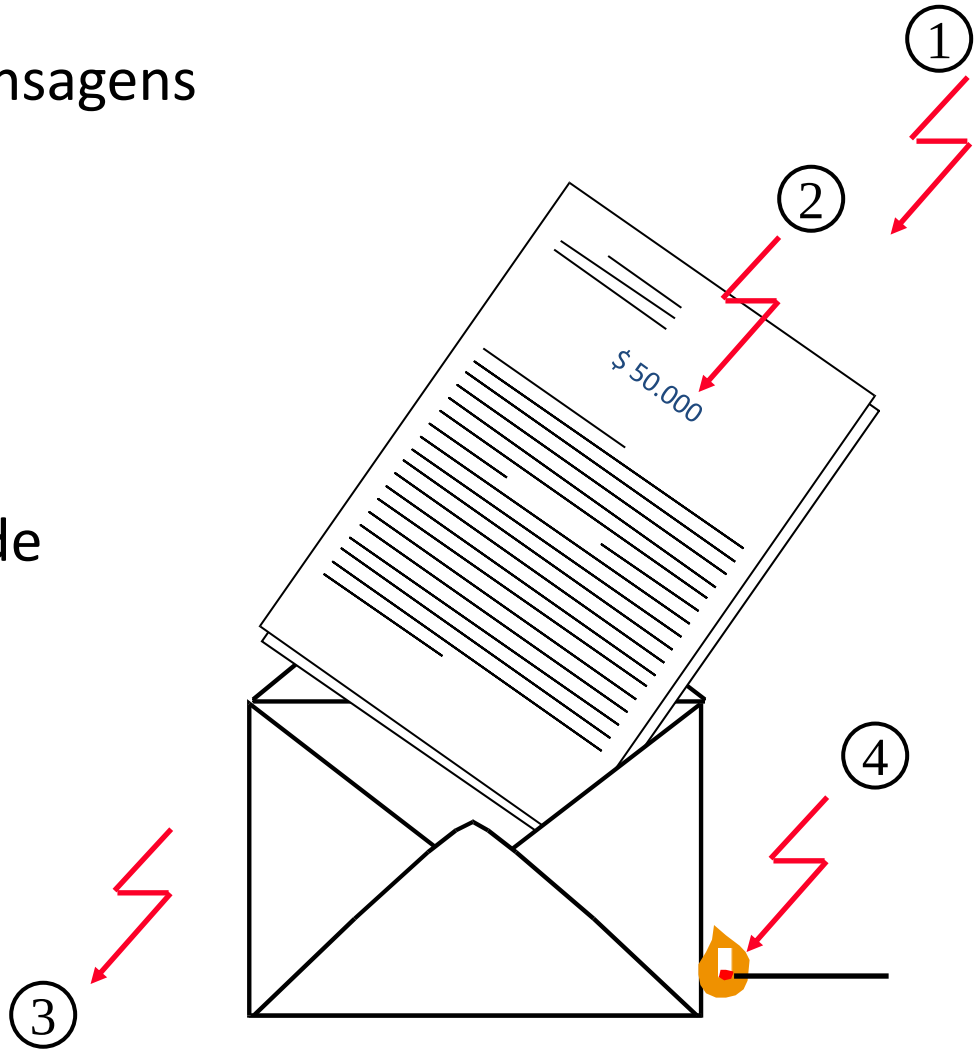
Riscos na Transmissão de Mensagens

1) Perda de Autenticidade

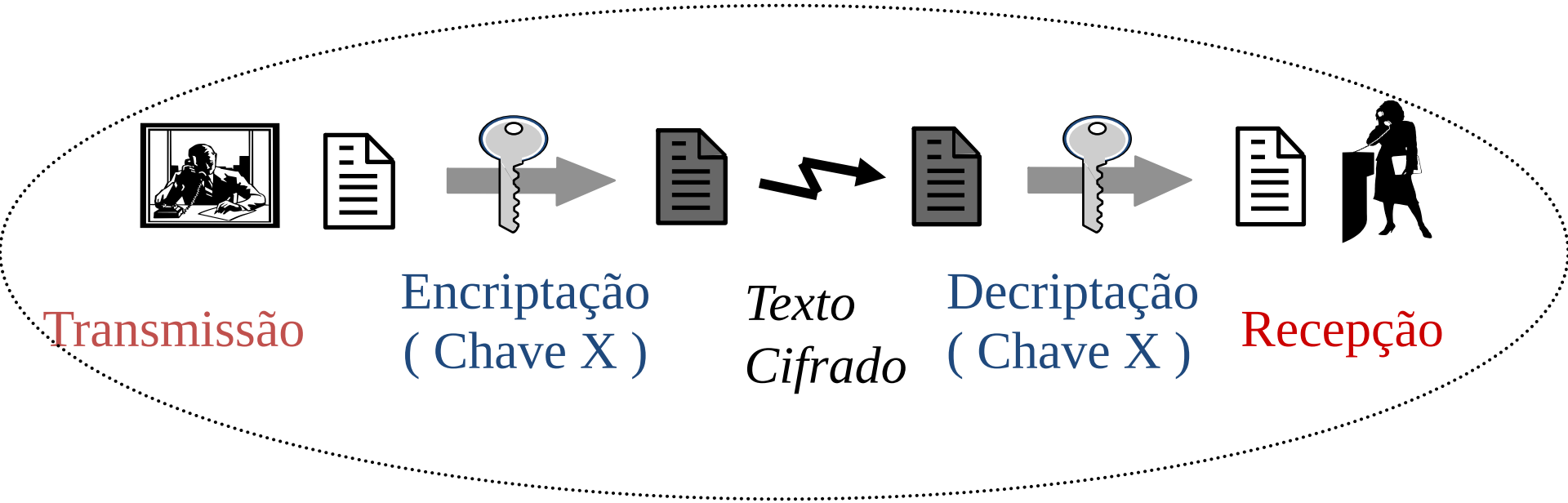
2) Perda de Integridade

3) Perda de Confidencialidade

4) Perda de Disponibilidade



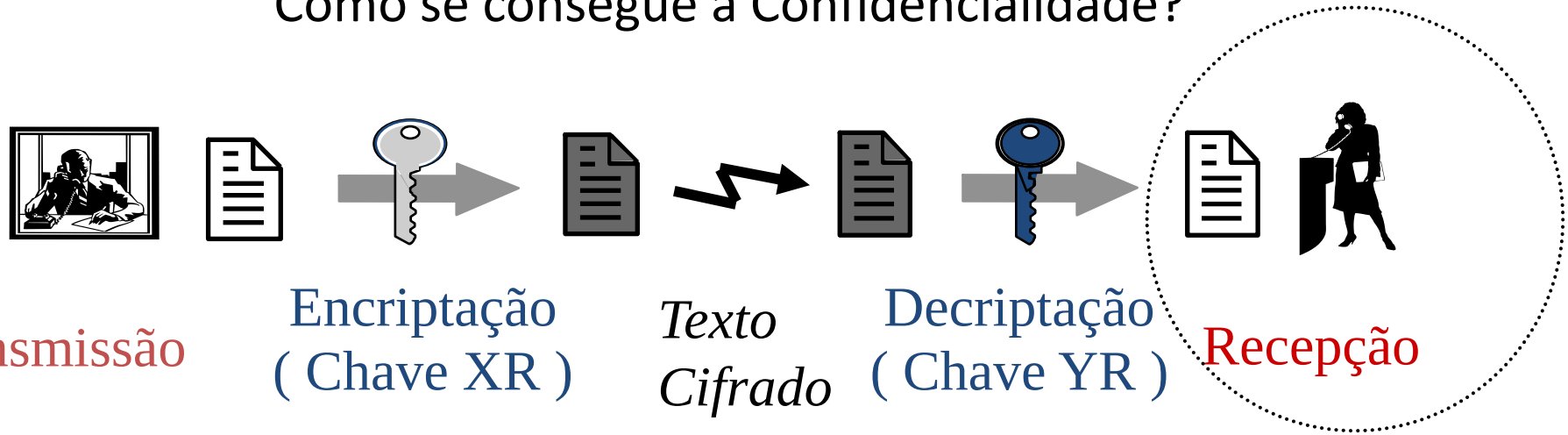
Como se consegue a Confidencialidade?



Algoritmos Simétricos:

- Chave da Encriptação = Chave da Decriptação.
- Apropriados para sistemas fechados.
- Segurança baseada só no segredo da chave.
- Exemplos: DES, 3-DES, AES…

Como se consegue a Confidencialidade?



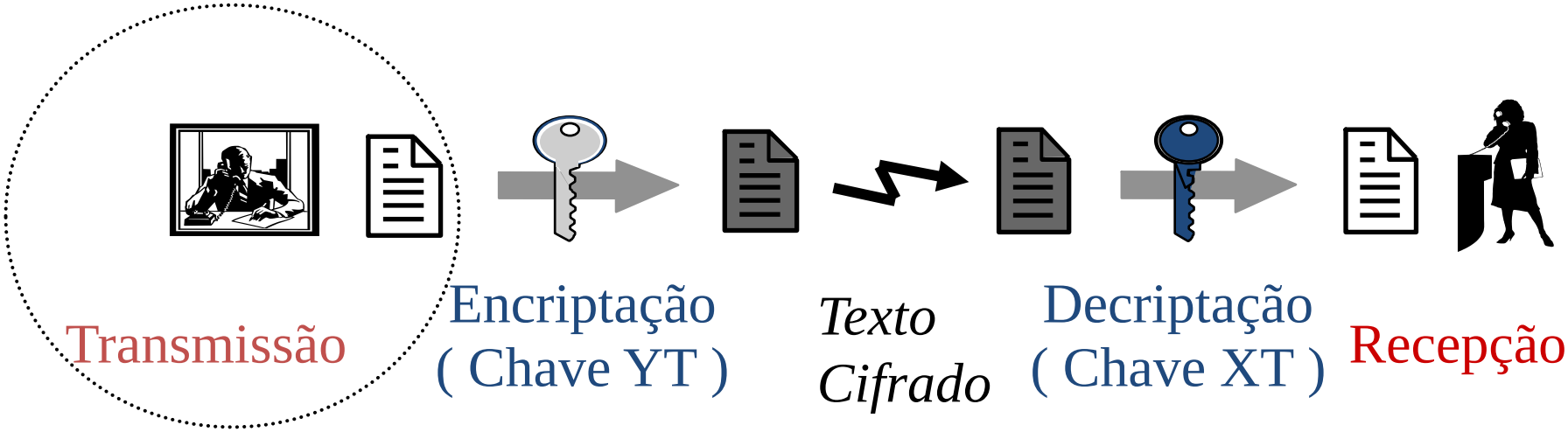
Par de chaves do receptor:
X: pública
Y: privada

Algoritmos Assimétricos (Chave Pública):

- Chaves opostas – o que é criptografado por uma somente pode ser descriptografado pela outra.
- Par de chaves calculadas por função sem retorno.
- Chaves muito maiores que as de algoritmos simétricos.
- Apropriados para sistemas abertos.
- Exemplos: RSA, curvas elípticas, …

Como se consegue a Autenticidade e o Não-Repúdio?

Princípio da Assinatura Digital



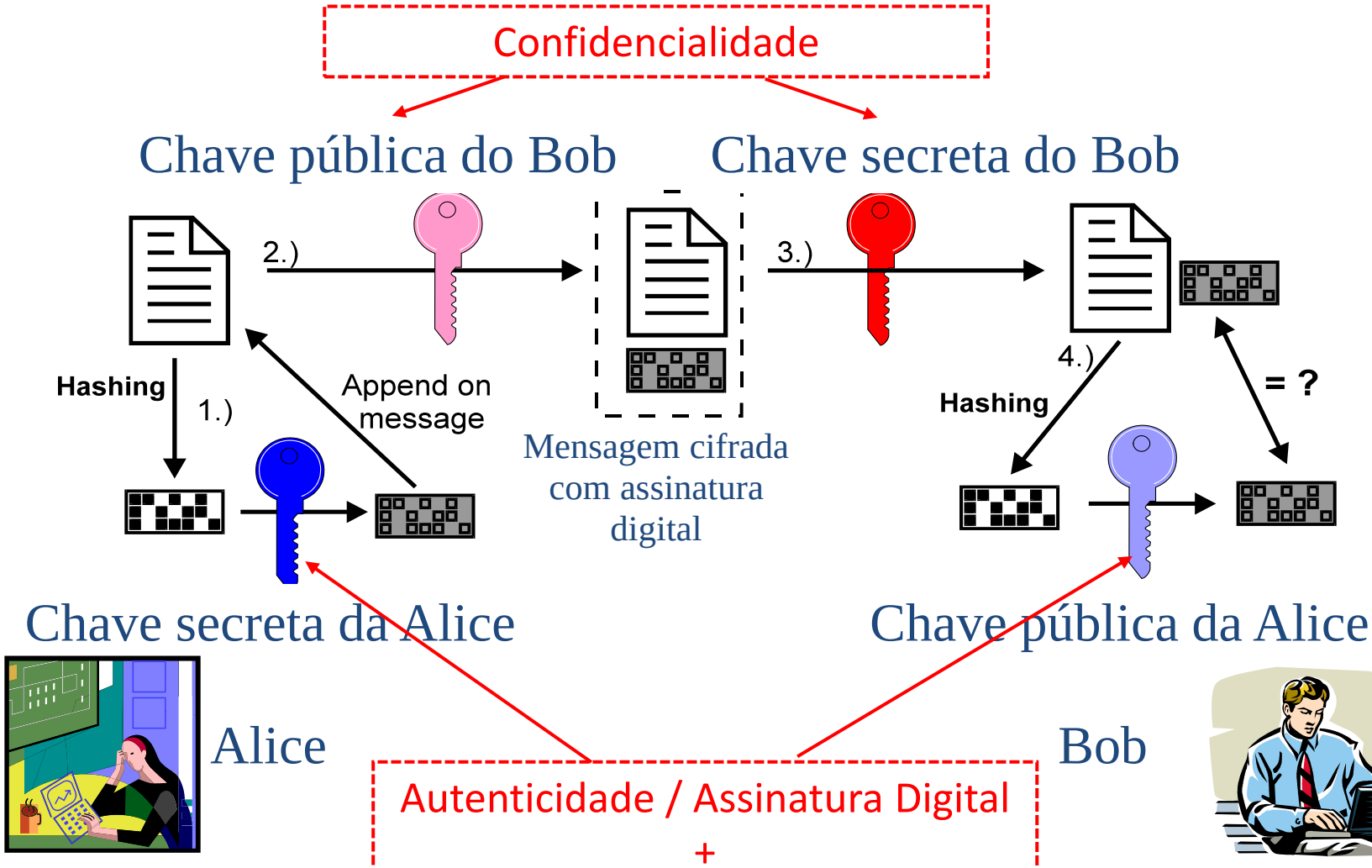
Par de chaves do transmissor:
x: pública
y: privada

Como se consegue a Integridade?

Hashing:

- Um processo mais sofisticado do que aquele que chamamos de "Número de Verificação".
- Agrega um conteúdo a mais na mensagem que permite verificar se nada foi perdido, agregado ou modificado indevidamente.
- Calcula a Identidade Digital de um documento.
- Recebe uma entrada com tamanho variável e retorna uma saída com tamanho fixo.
- Resultados de *Hashing* são de direção única.
- A partir de um *Hashing* específico, não é possível encontrar a mensagem que o gerou.
- É possível, mas improvável que duas mensagens diferentes gerem o mesmo *Hashing*.
- Algoritmos mais usados – MD2, MD4, MD5, SHA-1.

Sistema Básico de Criptografia



Certificação Digital

Serve como prova de identidade eletrônica em qualquer situação.

Associa a identidade da pessoa ou de um servidor a uma chave pública.

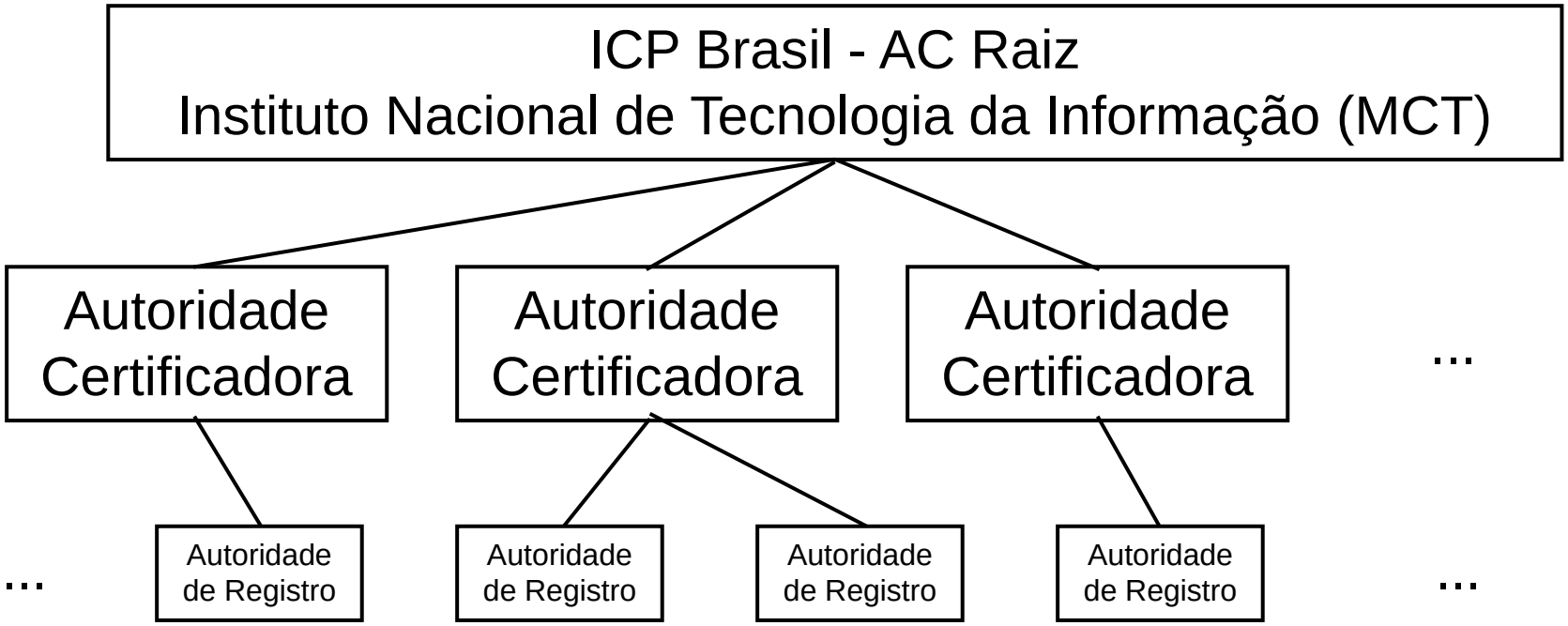
O Certificado é emitido por uma Autoridade Certificadora Digital, que o assina com a sua Chave Privada.

Vários certificados podem ser anexados a uma mensagem – um certificado autentica o certificado anterior.

Há uma Lista de Revogação de Certificados.

Certificação Digital

A Infraestrutura de Chave Pública ICP-Brasil foi criada pela Medida Provisória Nº 2200 (27/6/2001).



Conclusões referentes à Segurança da Informação

Segurança é um eterno jogo de gato e rato, no qual não basta ser competente, é preciso ser melhor do que o outro lado permanentemente.

Sempre podem surgir novas soluções de segurança e novos algoritmos. Do ponto de vista comercial, considera-se que as soluções mais confiáveis são aquelas que são testadas à exaustão pela comunidade científica e que têm a melhor referência no Mercado.

A credibilidade das entidades geradoras e certificadoras de chaves públicas é um aspecto essencial para nossas atividades.

Conclusões referentes à Segurança da Informação

A encriptação deve ser efetuada em uma plataforma que tenha uma segurança compatível com o algoritmo utilizado. O nível de segurança é determinado pelo elo mais fraco dentre todos os elementos de uma solução de segurança.

Normalmente o elo mais fraco corresponde a uma pessoa despreparada, desmotivada ou mal-intencionada.

Obsolescência ocorre à mesma velocidade que os avanços tecnológicos. Computação Quântica é um exemplo de tecnologia que, caso seja bem-sucedida, pulverizará a maior parte de proteção baseada em criptografia atualmente existente. Esse efeito será potencializado pela Inteligência Artificial.

Conclusões referentes à Segurança da Informação

Nada é 100% Seguro. Devemos nos preparar para reduzir nossas perdas caso a segurança seja quebrada. É melhor não ter um dispositivo de segurança e saber que está inseguro do que confiar em um dispositivo fraco de segurança.

O nível de segurança obtido por Criptografia é tema de grande controvérsia entre governos e sociedades civis.

Quando o assunto é Segurança, os governos das principais potências detêm recursos que são desconhecidos, e que certamente são mais sofisticados do que os produtos oferecidos no Mercado pelas melhores empresas de Tecnologia.

Introdução à Economia e à Administração 2024

Próxima aula: 7 de junho!

Obrigado pela atenção!