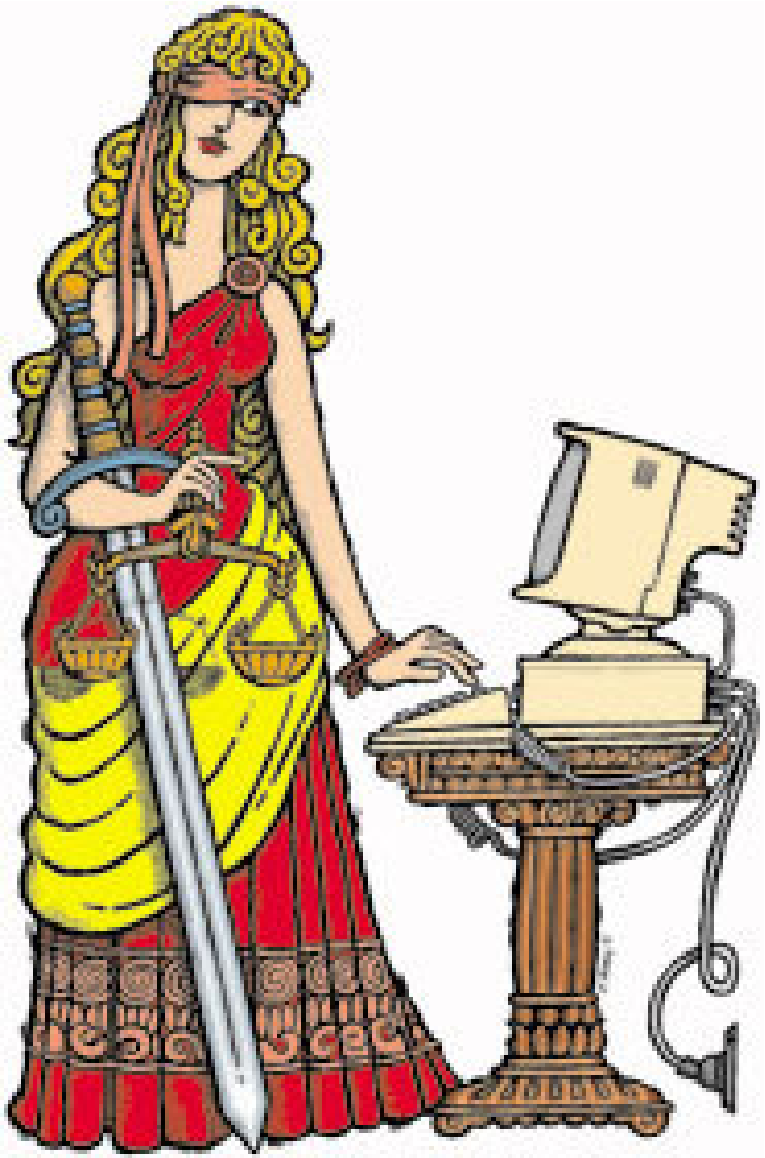
airesrover@linjur.ufsc.br



Aires José Rover

Doutor em direito

Universidade Federal de SC

- 1o dia: Internet, riscos e acidentes, formas de controle e métodos criptográficos de segurança
- 2o dia: Documentos digitais, contratos e comércio eletrônicos

Riscos e acidentes

Segurança

Insegurança

Incertezas da nova realidade

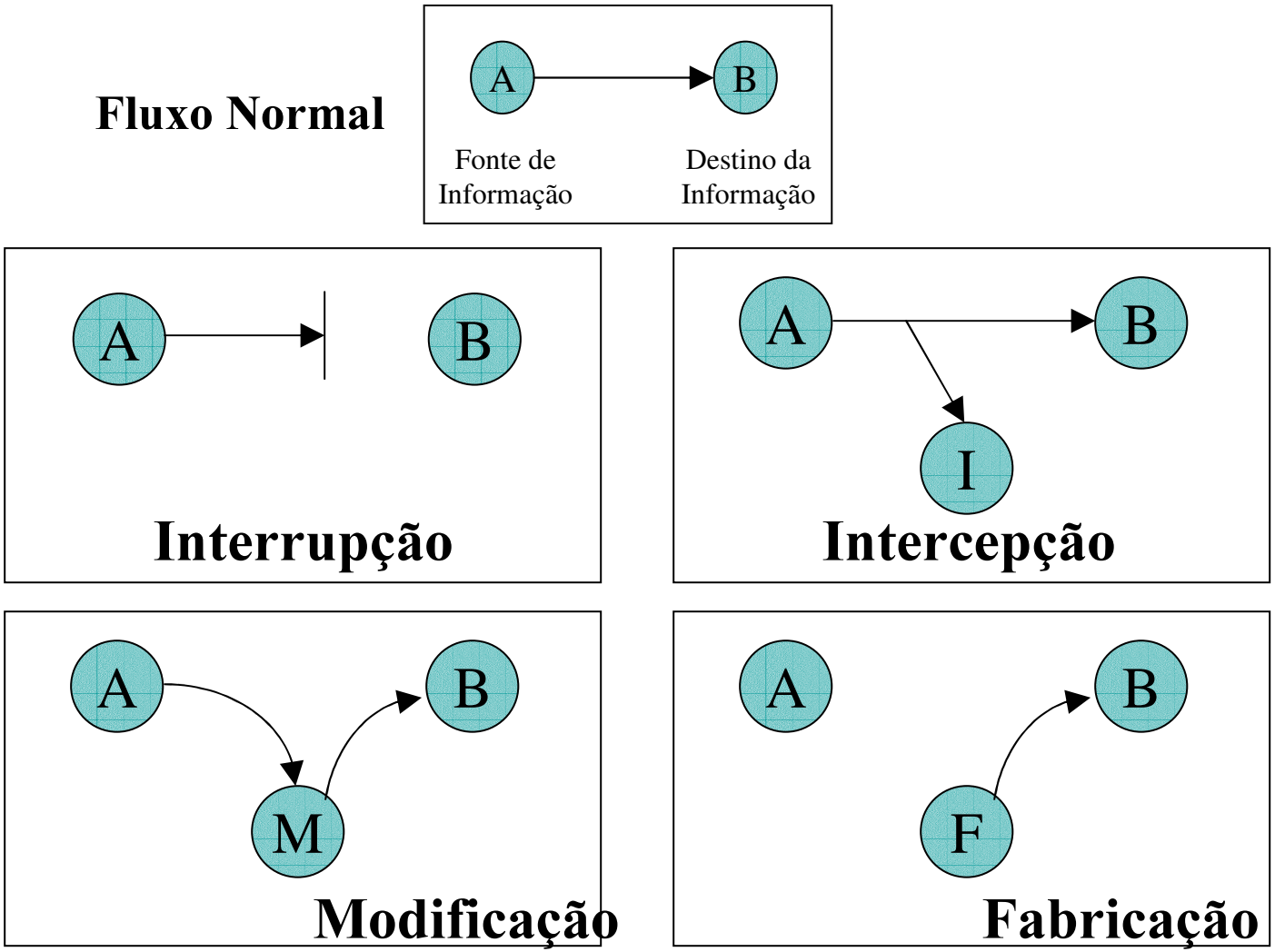
- A economia globalizada
- O fim do emprego
- Mais desemprego
- Blocos econômicos
- Guerras regionais
- Velhas e novas doenças
- Dois princípios: SDS e PSP (PETERS)

- Há perigo onde menos se espera

Riscos gerenciais

- Perda **financeira** direta resultado de fraude
- **Roubo de informação** confidencial
- Perda de **oportunidade** de negócio
- Uso desautorizado de **recursos**
- Perda do **respeito/confiança** do consumidor
- Custos associados às **incertezas**

Ameaças aos documentos



Ameaças de segurança

- Exemplos
  - Cartão de crédito - 5 bilhões de dólares por ano
  - Roubo de informação On-line - 10 bilhões
  - Comprometimento com a segurança da informação - 50% das organizações

Média nos anos 90 - EUA

Ameaças de segurança

Ex-empregado - vingar-se por ter sido despedido

Hacker - examinar a segurança do sistema; Roubar informação

Representante de vendas - dizer que representa todo o Brasil e não somente são Paulo

Estudante - alterar/mandar e-mail divertido em nome de outros

Contador - desviar dinheiro de uma empresa

Corretor - negar uma solicitação feita a um cliente por e-mail

Inimigo - aprender o poderio militar de um inimigo

Cybertroubles

- Excesso e irrelevância de informação
- Fadiga e angústia tecnológica
- Isolamento social
- Infowar, guerra da informação
- Ciberterrorismo
- Espionagem digital
- Insegurança nacional
- Insegurança dos sistemas **2a**
- Pirataria
- Vírus, invasão de sistemas, spam
- Invasão de privacidade
- TUDO é digital

Riscos e perigos

"se o jurista se recusar a aceitar o computador, que formula um novo modo de pensar, o mundo, que certamente não dispensará a máquina, dispensará o jurista" (BORRUSO, Renato. Computer e Diritto)

Advogado "mata" computador a bala

"Matei o computador". Foi o que disse o advogado Jahir Galvão de Lima, 77 anos, logo depois de dar cinco tiros no computador que estava sendo usado pelo escrivão Otacílio Santos, da Delegacia de Marituba, ontem de manhã. Essa foi a maneira encontrada por Jahir para denunciar a condução do inquérito instaurado para apurar a invasão de um condomínio evangélico, para cujos proprietários ele trabalha.

Segundo Jahir, que já foi juiz e há sete anos, depois que se aposentou, tirou a carteira da OAB, "o computador está do lado da bandidagem", ao transformar, por exemplo, um acusado de estar envolvido na invasão daquele condomínio em mera testemunha dos fatos. Em entrevista à imprensa, ontem à tarde, Jahir Galvão não citou o nome de nenhum policial com o qual estaria descontente em relação ao inquérito, embora tenha revelado que há dez anos vem lutando para que essas investigações sejam realizadas.

O tempo todo, porém, o advogado fez questão de deixar claro que sua revolta era contra a máquina. "Saí de casa para matar o computador", afirmou ele, diante do delegado Bertolino Neto, diretor da Seccional do Paar, à qual a DP de Marituba está vinculada. Ele chegou na delegacia com um revólver calibre 38, da marca Taurus, com cinco balas, todas disparadas contra seu alvo. O advogado foi preso em flagrante pelo delegado Clóvis Oliveira, supervisor da unidade de Marituba.

Segundo Bertolino Neto, o acusado iria ser autuado em flagrante por dano contra o patrimônio do Estado, por colocar em risco a vida de terceiros, por usar uma arma num ambiente onde há outras pessoas e por porte ilegal de arma. Bertolino também disse que o advogado ia ser submetido a exame de pólvora combusta e de sanidade mental. Ele acrescentou que, em quase 30 anos de Polícia Civil, ainda não tinha visto uma situação como a de ontem. Depois das formalidades legais e de pagar a fiança, Jahir ia ser solto, para responder ao processo em liberdade.

O escrivão Otacílio observa o computador destruído, que levou cinco tiros do advogado

Tudo começou por volta das 10h30 de ontem. Jahir chegou à Delegacia de Marituba e foi à sala onde estava o escrivão Otacílio Santos, logo na entrada do prédio. Otacílio ouvia o depoimento de duas pessoas, num processo relacionado a um acidente de trânsito, cujos autos haviam retornado da Justiça. Segundo o escrivão, Jahir disse que queria conversar alguns minutos com ele e o policial saiu para comunicar ao delegado Clóvis Oliveira que o advogado encontrava-se na unidade.

Ao retornar à sala em que estava, Otacílio encontrou a porta fechada. E, em seguida, ouviu os disparos de arma de fogo. Às pressas, foi à sala do delegado Clóvis e, assustado, comentou: "O doutor Jahir se matou". Depois, os policiais entraram na sala e um dos investigadores apanhou a arma do advogado. Antes de fazer os disparos, Jahir disse ao casal que prestava depoimento que saísse da sala. Como, a princípio, os dois não lhe deram ouvidos, ele puxou a arma que carregava numa sacola e voltou a pedir ao casal que deixasse o local, porque iria "matar o computador".

Versão - Na Seccional do Paar, Jahir apresentou sua versão, mas fez questão de enfatizar que sua história era "longa" e iria revelar só a "ponta do iceberg". Ele disse que há dez anos luta para que seja instaurado inquérito para apurar o que, à época, era uma tentativa de invasão ao residencial "Absalão Piano", localizado em Marituba e fundado pela Assembléia de Deus. Depois de passar pela Divisão de Investigações e Operações Especiais (Dioe) e recorrer até mesmo à direção da Secretaria Executiva de Segurança Pública, Jahir afirmou que, finalmente, o inquérito foi instaurado na DP de Marituba, o que, segundo ele, ocorreu há dois meses.

Mas, há 70 dias, conta o advogado, o condomínio foi invadido. Ainda conforme Jahir, foram apontadas nove pessoas para serem ouvidas como acusadas de participação da invasão. Para sua surpresa, ele disse que uma das pessoas apontadas como envolvidas nesse episódio aparece, no computador, como testemunha. "Agora que o inquérito foi instaurado, o computador começa a fazer bandalheira", disse o advogado, para acrescentar que, agindo assim, a máquina "está trabalhando do lado da bandidagem e contra mim".

O advogado contou que, por volta das 9 horas de ontem, saiu de casa, no bairro de Nazaré, para, de ônibus, ir à DP de Marituba. Não foi em seu carro porque ele está batido. Antes de sair de seu apartamento, apanhou o revólver, adquirido há 20 anos e que não usava há muito tempo, e foi para a delegacia com a intenção de "matar o computador". Ao chegar lá, conversou rapidamente com o escrivão Otacílio, que já o conhecia, e que saiu da sala para falar com o delegado Clóvis. Em seguida, pediu às duas pessoas que também deixassem a sala, solicitação que fez pela segunda vez, já que na primeira não foi atendido. O advogado fechou a porta e, em seguida, deu quatro tiros na lateral do computador e um no visor da máquina. Segundo Jahir, tudo o que ele quer é que o inquérito esclareça todos os fatos relacionados à invasão do condomínio.

O delegado disse que o inquérito está sendo feito e que já foi ouvido um dos acusados, que já está indiciado. O outro homem apontado como cabeça da invasão também vai prestar depoimento. E, assim como o anterior, será indiciado em inquérito. Até as 17 horas, o computador ainda não havia sido submetido à perícia.

Riscos e perigos

Perigos no progresso tecnológico

Preocupação apenas **mercantil**

Medo das novidade

Essa turma é fogo!

Definindo a internet

- Interconnect Network
- Origem militar: projeto financiado pela DARPA (Defense Advance Research Projects Agency)

- Interligação das redes de computadores existentes
- Uso do TCP/IP
- Operação descentralizada
- Duplo caminho

Definindo a internet

- rede de redes
- rede global
- de uso geral

- “sem dono”
- sem personalidade jurídica

Correio eletrônico

- Forma assíncrona de comunicação
- correspondência eletrônica através da internet
- Recurso mais utilizado na internet
- Muito utilizado nos tribunais
  - Internamente
  - Iniciar processos

- Listas ou grupos de interesse
- Mensagem = cartão postal

- Fragilidade dos protocolos, da internet

"you've got mail!"

WWW – World Wide Web

Interface universal
Conteúdos e serviços em massa
Cada página = uma interpretação do mundo
milhões de editores (LIPMAN)

Forte interação
Forte participação em comunidades

Ser vivo
Mudanças contínuas e rápidas
Redefinição contínua de identidades e subjetividades

Questões problemas desafios

- desterritorialidade
- Soberania

Intolerância, crimes de ódio
Spam, censura
Privacidade, big brother
3a Pirataria
3b Pornografia
Hackers, virus

- Comércio eletrônico
- Confiabilidade e segurança

Formas de controle dos riscos e conflitos na sociedade

Porque mais controle

- A tecnologia avança fortemente
- O conhecimento
  - tem prazo de validade cada vez menor
  - cada vez mais abundante (quantidade)
- Os riscos e a complexidade dos sistemas aumentam
- Insegurança real e aparente
  - Na sociedade
  - No direito

+ controle + segurança
Conseqüências

+ custos

+ complexidade dos processos

-+ difusão da informação

-+ liberdade de informação

-+ investimento na cultura

-+ consumidores

-+ monopólios

-+ riqueza

Autocontrole pela comunidade

- Netiqueta - regras do “bom usuário” da internet
- Código de ética
- Definição de políticas pelos provedores
- Selos de qualidade
- Listas negras

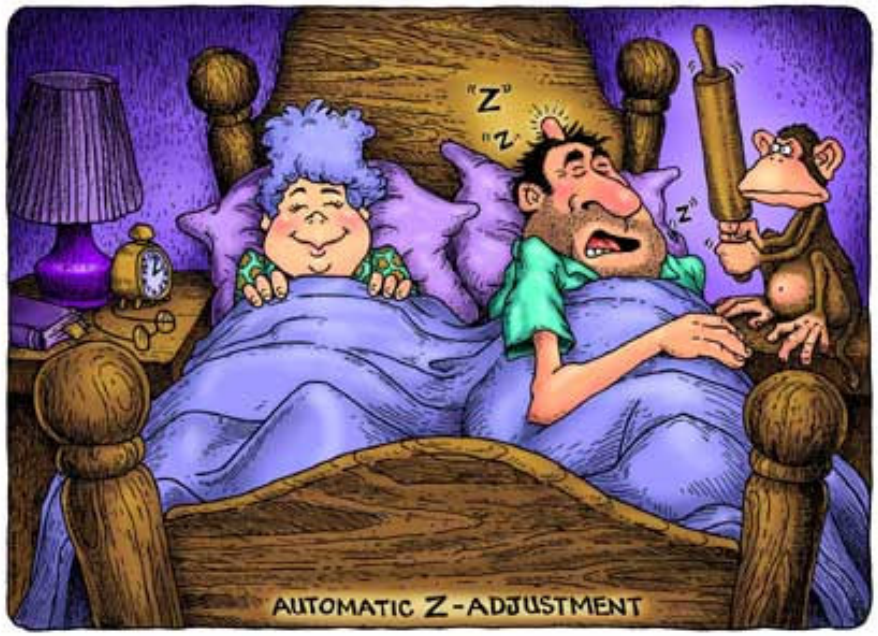
- Peopleware
  - Treinamento das pessoas envolvidas
  - Manter coesão sob a liderança de forte autoridade
  - Manter vigilância e atenção permanente
  - Assegurar boa informação sobre segurança

auto-organização
auto-regulamentação

- **isoc** - organização internacional de padronização e normalização tecnológica
- **Icann** - nomes de domínio
- comunidade do **código aberto**
- comunidade anti-spam

Controle através da tecnologia

- Utilizar a melhor tecnologia para tornar tecnicamente difícil
  - A realização do crime
  - A sua dissimulação
- Utilizando métodos de controle de acesso
  - Limitação do uso
  - Uso e mudança constante de senhas
  - Certificação e assinatura digital
  - Controles biométricos **4a**
- Proteção dos documentos **4b**
  - Criptografia
- Proteção dos dados
  - Cópias de segurança
  - Anti-vírus
  - Firewall: filtros e bloqueios de mensagens, controle de origem e conteúdo
- Construindo sistemas confiáveis



sistemas confiáveis

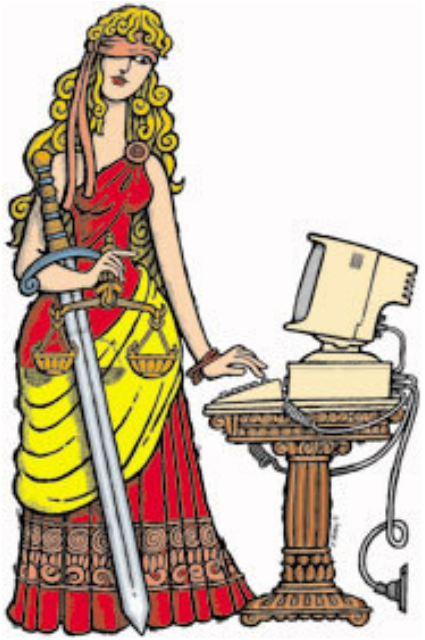
dependência

- Do conhecimento das regras, dos termos e condições
- Dos diferentes níveis de segurança
- Da tecnologia e do mercado

Ações sócio-políticas e culturais

- Investir na educação para um futuro de paz, autonomia e cooperação
- Pensar globalmente x agir localmente
- Investir em tecnologias
  - Abrangentes e não nas excludentes
  - Moleculares e não nas molares (LÉVY)
- Aumentar a transparência da produção e distribuição das informações
- Exigir o uso regulado das informações
  - Não permitir que a informação prestada para determinado objetivo seja utilizada para outro fim
- Facilitar a publicação de informações
- Proteger aquelas de caráter privado

Controle jurídico



- Promulgar leis
  - Realistas e longevas
  - Adequadas, específicas e rígidas
  - Devem ter em vista a rápida evolução da tecnologia
  - Que chamem a atenção do público
  - Com ampla divulgação
  - Que compatibilizem o controle penal, civil e administrativo
  - Adaptação legislativa de textos legais incompatíveis
- Aplicá-las
- Preparar a polícia, o ministério público (flagrante)
- Uniformização das normas de direito internacional privado
- Definir acordos internacionais
- Constituição de um juizado internacional
- Arbitragem e formas alternativas de resolução de conflitos
- Os usuários e a população devem ser preparados para as mudanças

esclarecimento

Contradições e desordem sistêmicas

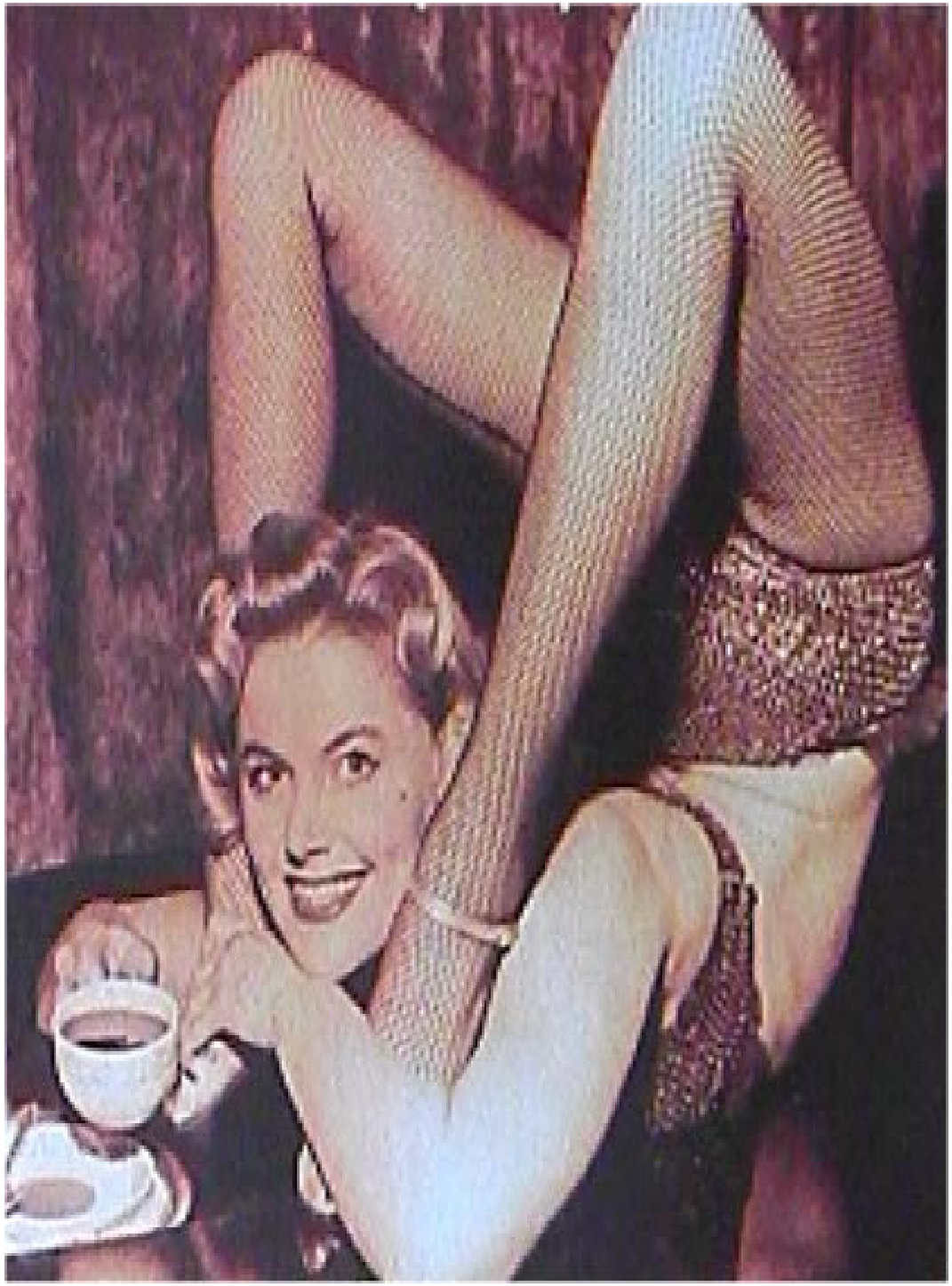
Função esclarecedora das **perturbações**

Aceleração das mudanças

Libertação dos velhos **paradigmas**

Novos meios que compensarão as perdas

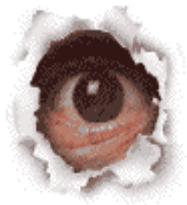
"you've got mail!"



é preciso flexibilizar

-leis
-sistemas
-mentalidade

O negócio é ficar de olho

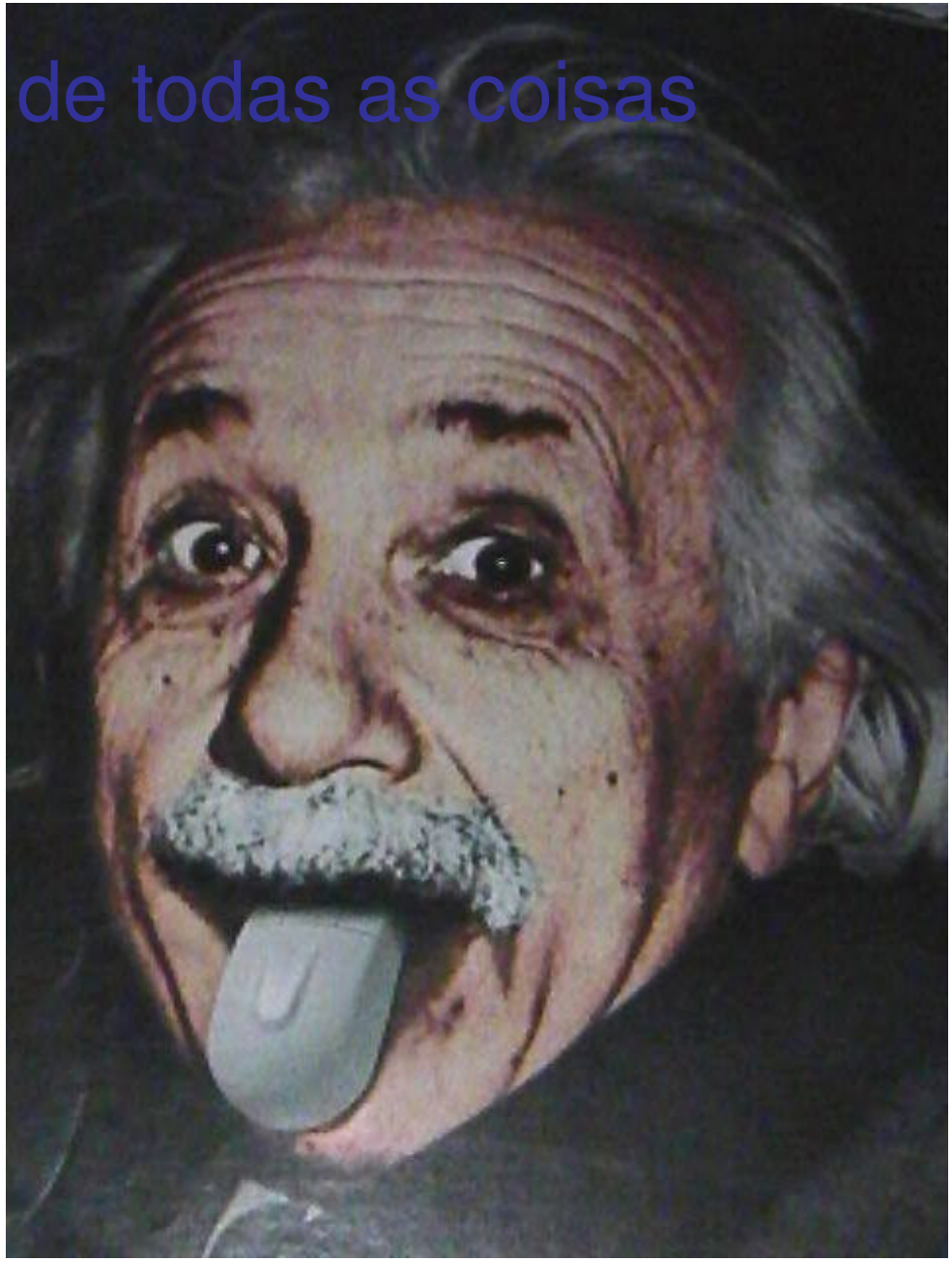


- O que distingue a "modernidade reflexiva" e a torna problemática é o fato de que devemos encontrar respostas radicais aos desafios e aos riscos produzidos pela própria modernidade. Os desafios poderão ser vencidos se conseguirmos produzir mais e melhores tecnologias, mais e melhor desenvolvimento econômico, mais e melhor diferenciação funcional (BECK)

bem aberto

Homem como medida de todas as coisas

A preocupação pelo homem e por seu destino deve constituir o interesse fundamental subjacente a todo o empenho técnico, a preocupação com os grandes e ainda não resolvidos problemas da organização do trabalho e da distribuição de bens, a fim de que criações da mente humana venham a se constituir em benção e não maldição para toda a humanidade
EINSTEIN, 1937



Segurança e autenticação digitais

aspectos técnicos

Documento tradicional

- Conhecimento, fixado materialmente em **algum meio**, que possa ser utilizado posteriormente
- Informação + suporte material
  - Pedra, madeira, papiro, pele de animais, cerâmica, papel
- Indissociável do suporte. Conteúdo e continente se integram como um todo
- Longa evolução através da história

Código de Hamurabi

Documento eletrônico

- Conhecimento, fixado em **meio eletrônico**, que possa ser utilizado posteriormente
- Informação + suporte
- Dissociável do suporte. Conteúdo e continente não se confundem
- É um conjunto de bits
- Rápida evolução

Documento eletrônico

Sistema decimal

Dígitos 0 a 9

1.000	100	10	1		
			1	=	1
		2	0	=	20
	1	1	0	=	110
3	4	0	0	=	3.400
6	4	3	2	=	6.432

Documento eletrônico

Sistema binário
Dígitos 0, 1

8	4	2	1		
			1	=	1
0	0	1	0	=	2
0	0	1	1	=	3
1	1	1	1	=	15
1	0	0	1	=	9

Documento eletrônico

00100001010111110100	= texto
00010111010001011110	= música
01000101000000011101	= voz
01100101000110101100	= imagem
00010100111010010010	= foto
10011101010010110010	= cinema
10110100101110100001	= programas

Documento eletrônico
características

- Mobilidade
  - Não está preso ao suporte físico
- Alterabilidade
  - Permite alterações, no conteúdo e em atributos, sem deixar vestígios
- Facilidade de manipulação
- Pouca ocupação de espaço físico

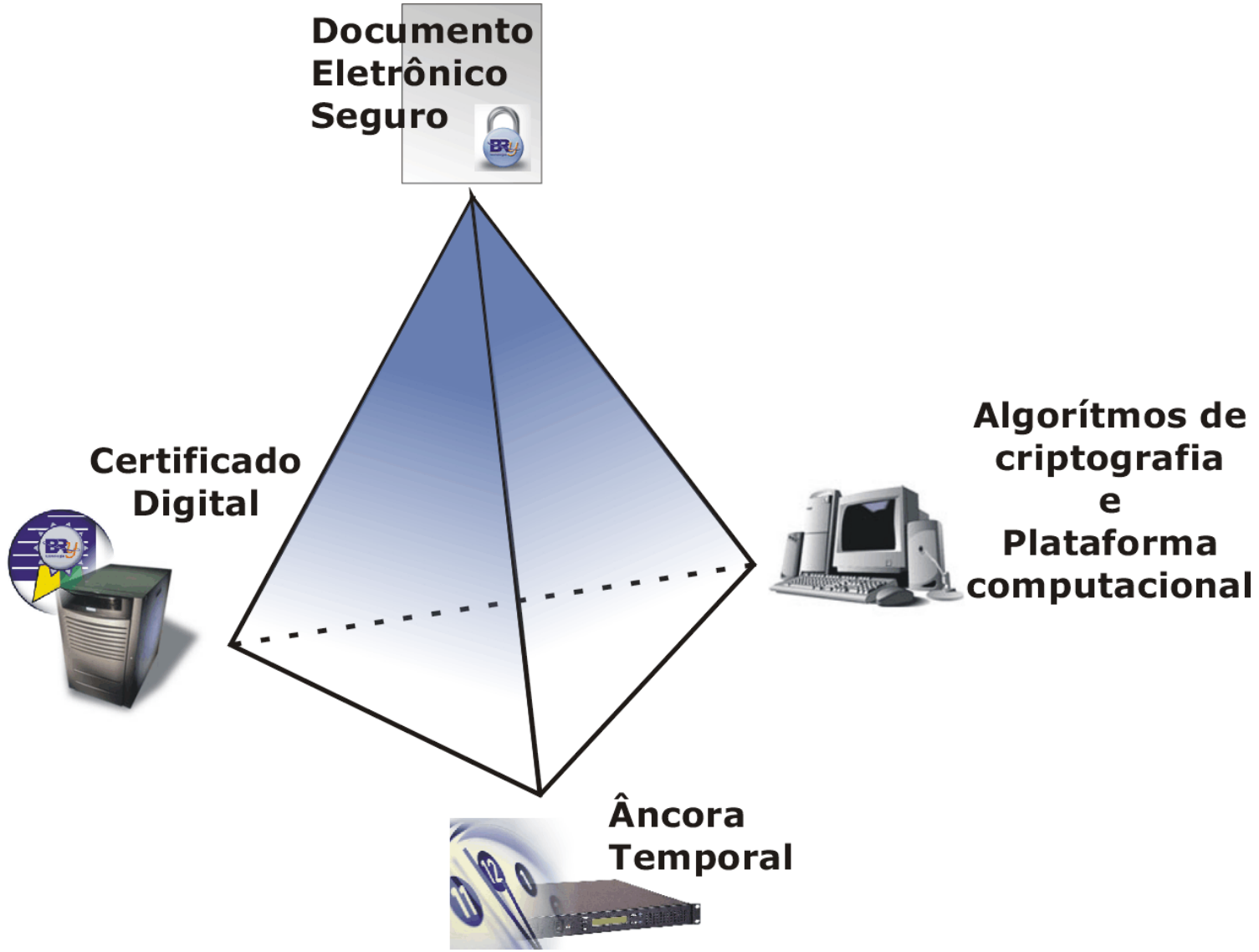
Documento eletrônico
validade / segurança

- Autenticidade
  - Bob sabe que Alice enviou a mensagem (autoria)
- Integridade
  - A mensagem que bob recebeu foi a que Alice enviou (conteúdo original)
- Não recusa, repúdio, rejeição
  - Alice não pode negar após bob ter recebido uma mensagem dela, que ela enviou a mensagem
- Tempestividade
  - Data certa e determinada da assinatura digital
- Verificabilidade
  - A assinatura deve poder ser verificável por terceiros (resolver disputas)

Requisitos de implementação dos sistemas

- Anonimato x identificação
- Facilidade de uso
- Flexibilidade
- Mobilidade
- Robustez não cair
- Escalabilidade para grandes massas
- Interoperabilidade entre sistemas **5a**
- Disponibilidade

Documento Eletrônico Confiável



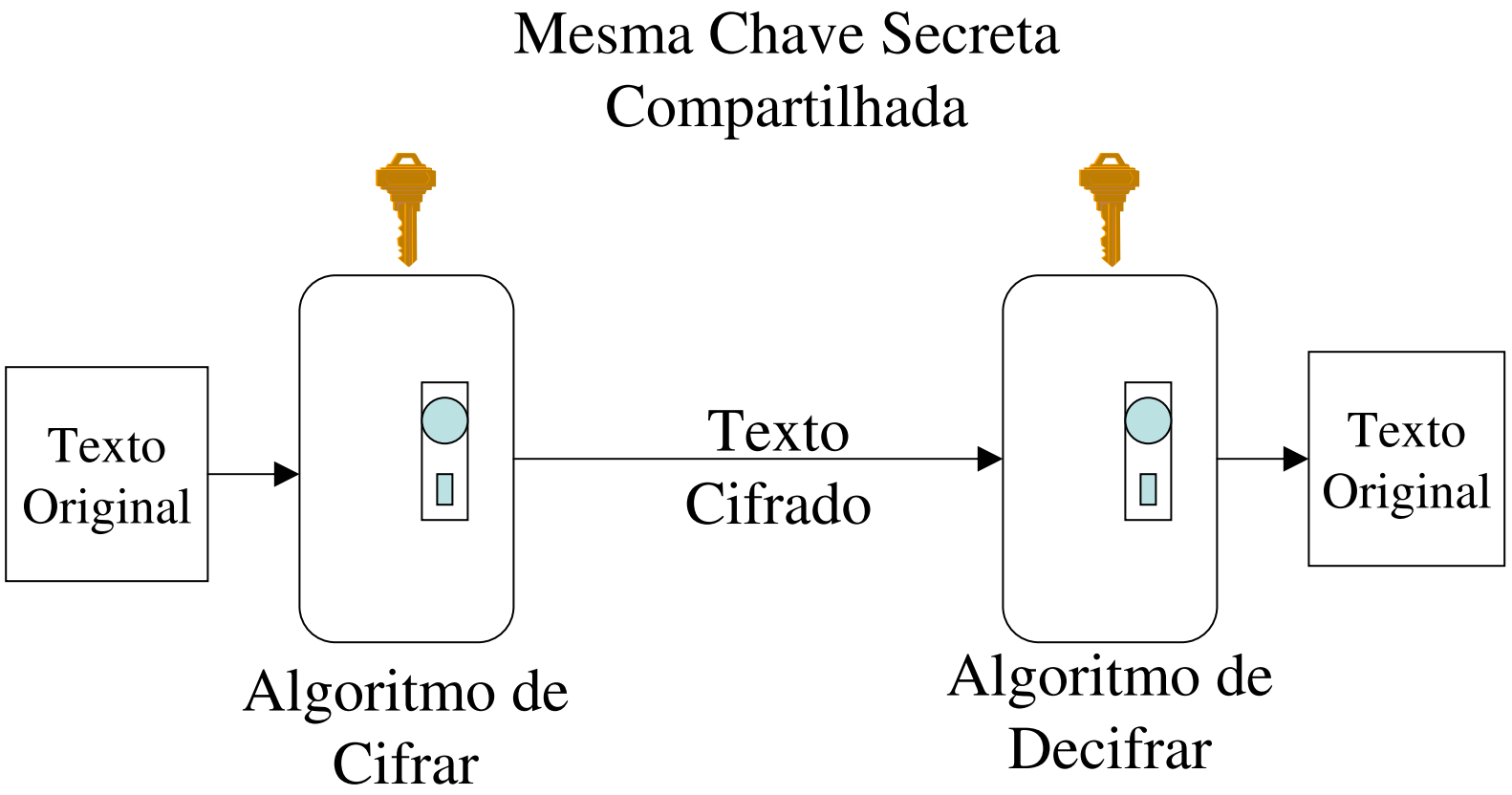
Criptografia

- Escrita (grafia) secreta (Cripto)
  - Esconder a informação de todos exceto
  - Verificar a exatidão de uma informação
  - Base tecnológica para problemas de segurança em comunicações e em computação

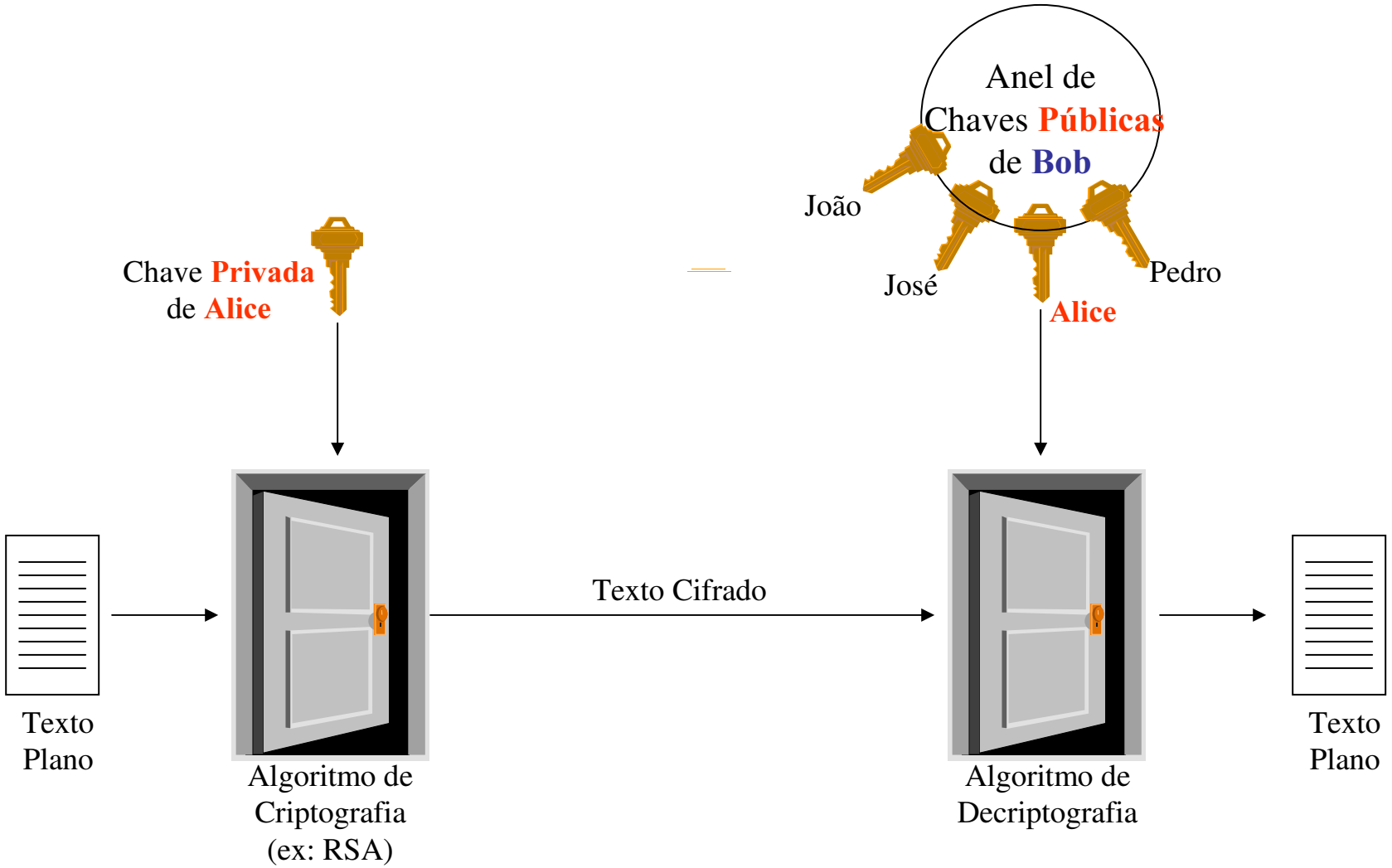
Tipos de criptografia

- Simétrica - 4.000 anos
  - Chave secreta
  - Garante o sigilo (com integridade)
- Assimétrica - 25 anos
  - Chave pública e chave privada
  - Garante a troca segura de chaves
  - Garante o sigilo e a autenticidade (com integridade)

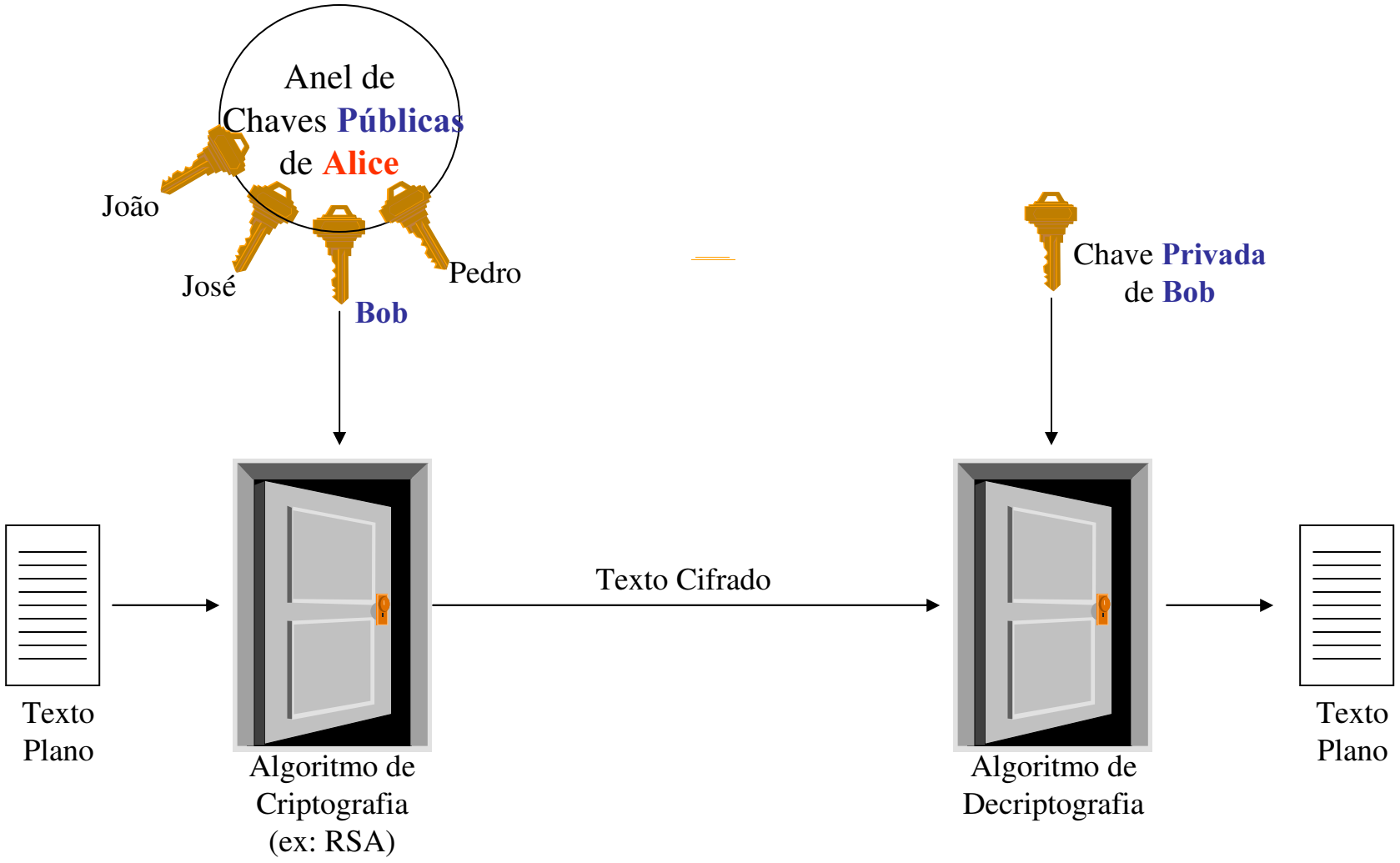
Criptografia **simétrica**



Criptografia **assimétrica** autenticação



Criptografia **assimétrica**
sigilo



Tempo médio de busca exaustiva

Tamanho da Chave	**Número de Chaves**	**Tempo Requerido (1 cripto/μs)**
32	$2^{32} = 4{,}3 \times 10^{9}$	35,8 minutos
56	$2^{56} = 7{,}2 \times 10^{16}$	1.142 anos
128	$2^{128} = 3{,}4 \times 10^{38}$	$5{,}4 \times 10^{24}$ anos
26 Caracteres (permutação)	$26! = 4 \times 10^{26}$	$6{,}4 \times 10^{12}$ anos

Assinatura Digital

- Uso da criptografia assimétrica
- Permite verificar
  - autor
  - data/hora
  - integridade do conteúdo
- Verificável por terceiros (resolver disputas)

Requisitos da assinatura digital

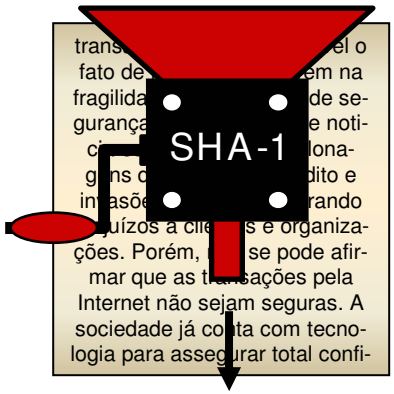
- Depender do conteúdo
- Fácil de reconhecer e verificar
- Usar informação única do originador
- Fácil de produzir
- Inviável de forjar
- Deve ser prático manter uma cópia da assinatura

O resumo é quase tudo

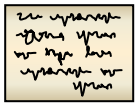
Documento original

transações, é compreensível o fato de muitos acreditarem na fragilidade dos sistemas de segurança. Freqüentemente notícia-se sobre *hackers*, clonagens de cartões de crédito e invasões a *websites*, gerando prejuízos a clientes e organizações. Porém, não se pode afirmar que as transações pela Internet não sejam seguras. A sociedade já conta com tecnologia para assegurar total confi-

Algoritmo



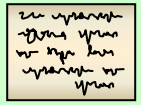
HASH



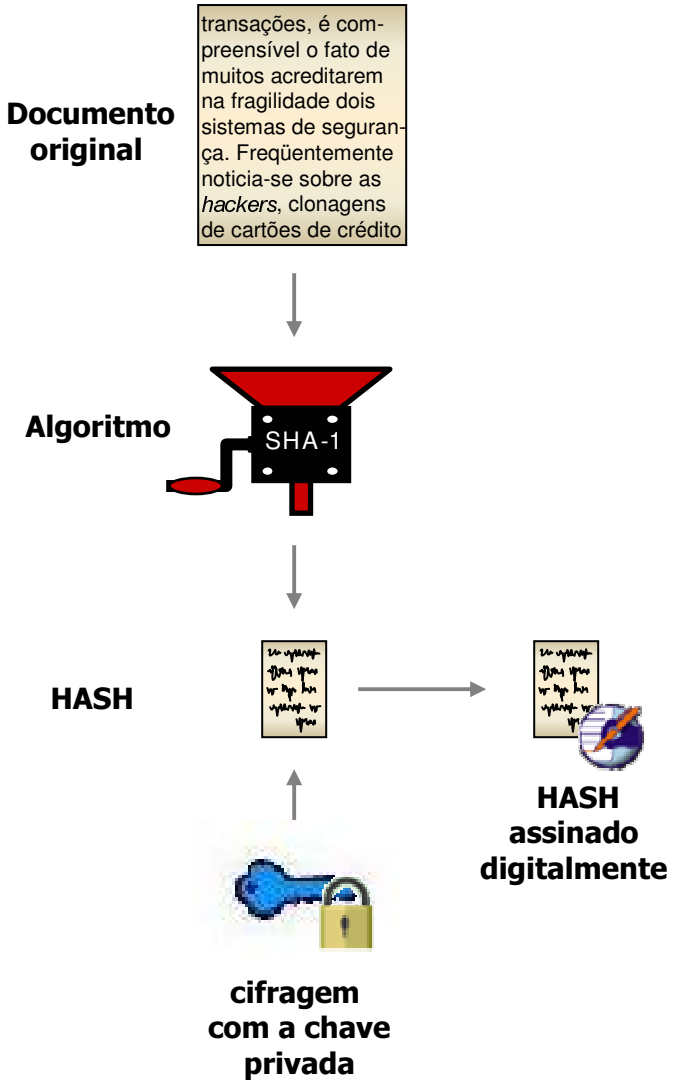
Assinando o HASH pode-se garantir estar assinando o próprio documento original pois cada HASH é único

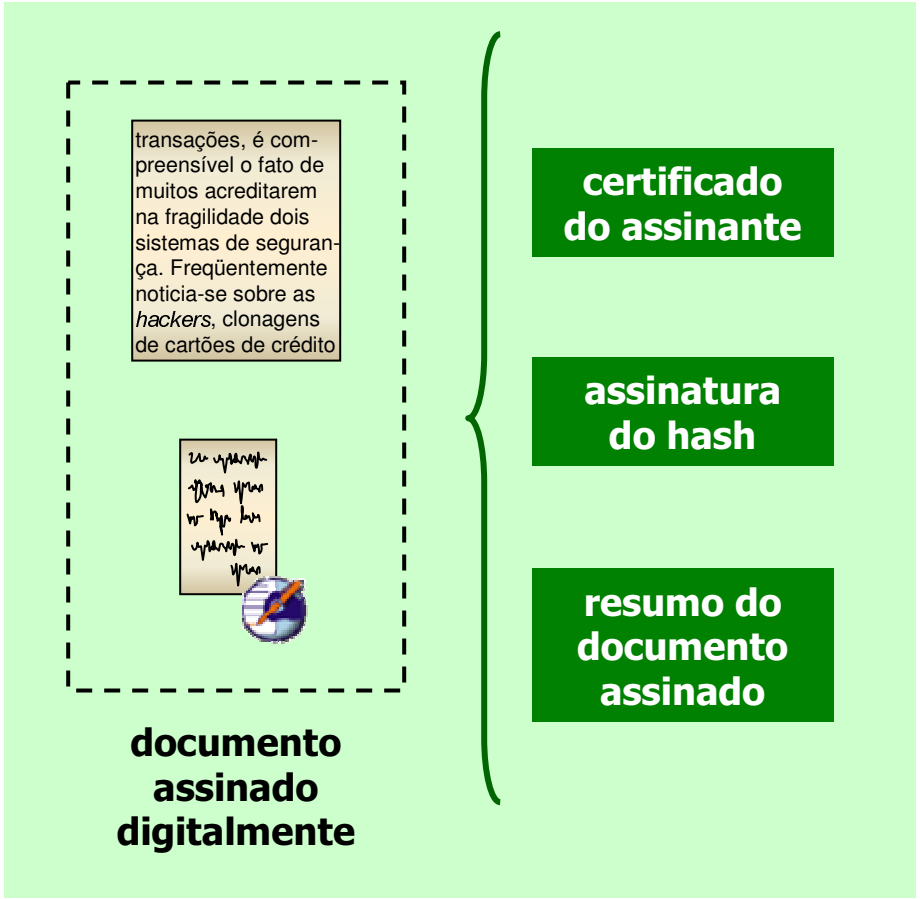
transações, é compreensível o fato de muitos acreditarem na fragilidade dos sistemas de segurança. Freqüentemente notícia-se sobre *hackers*, clonagens de cartões de crédito e invasões a *websites*, gerando prejuízos a clientes e organizações. Porém, não se pode afirmar que as transações pela Internet não sejam seguras. A sociedade já conta com tecnologia para assegurar total confi-

=

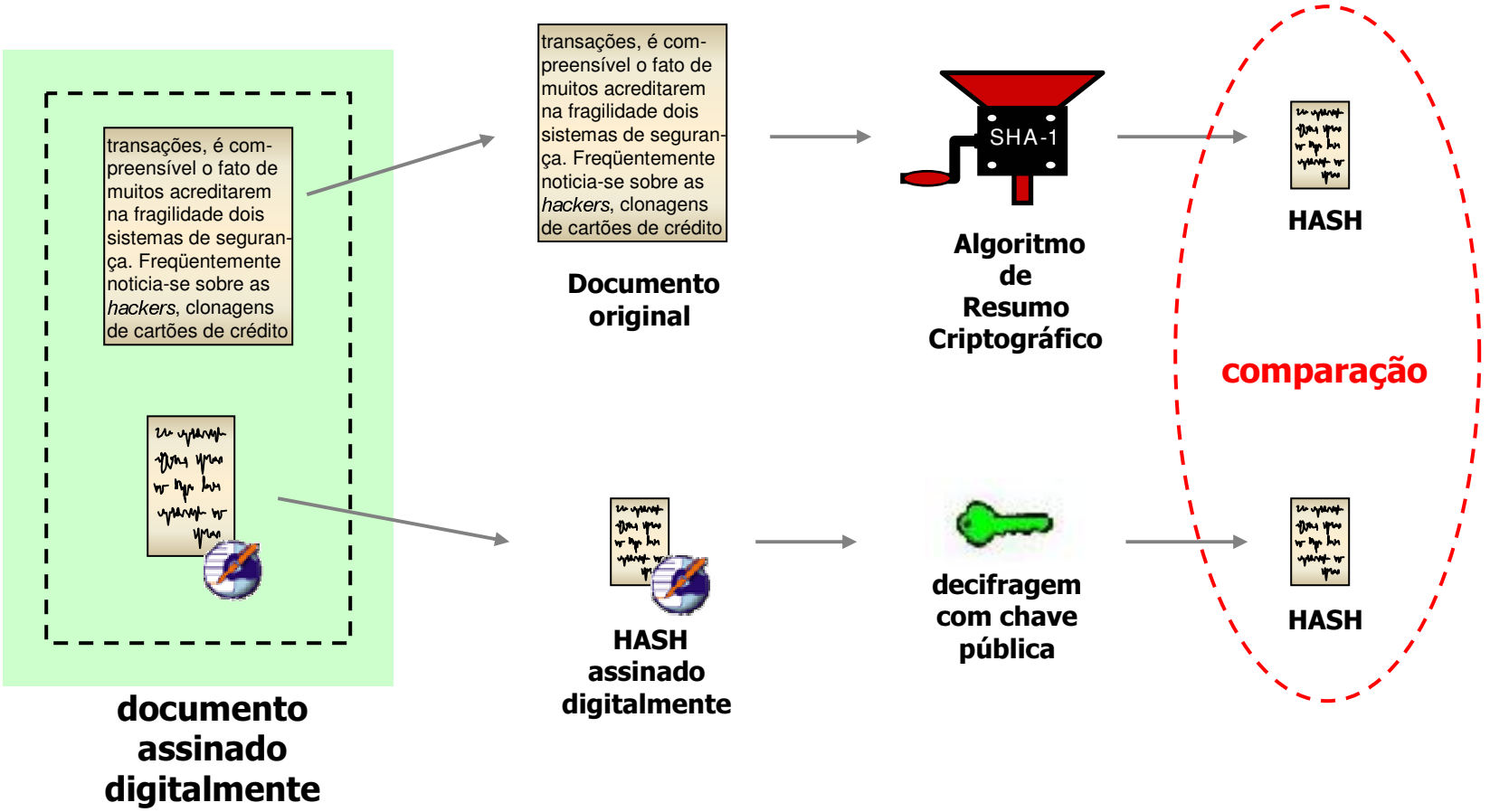


Assinando digitalmente





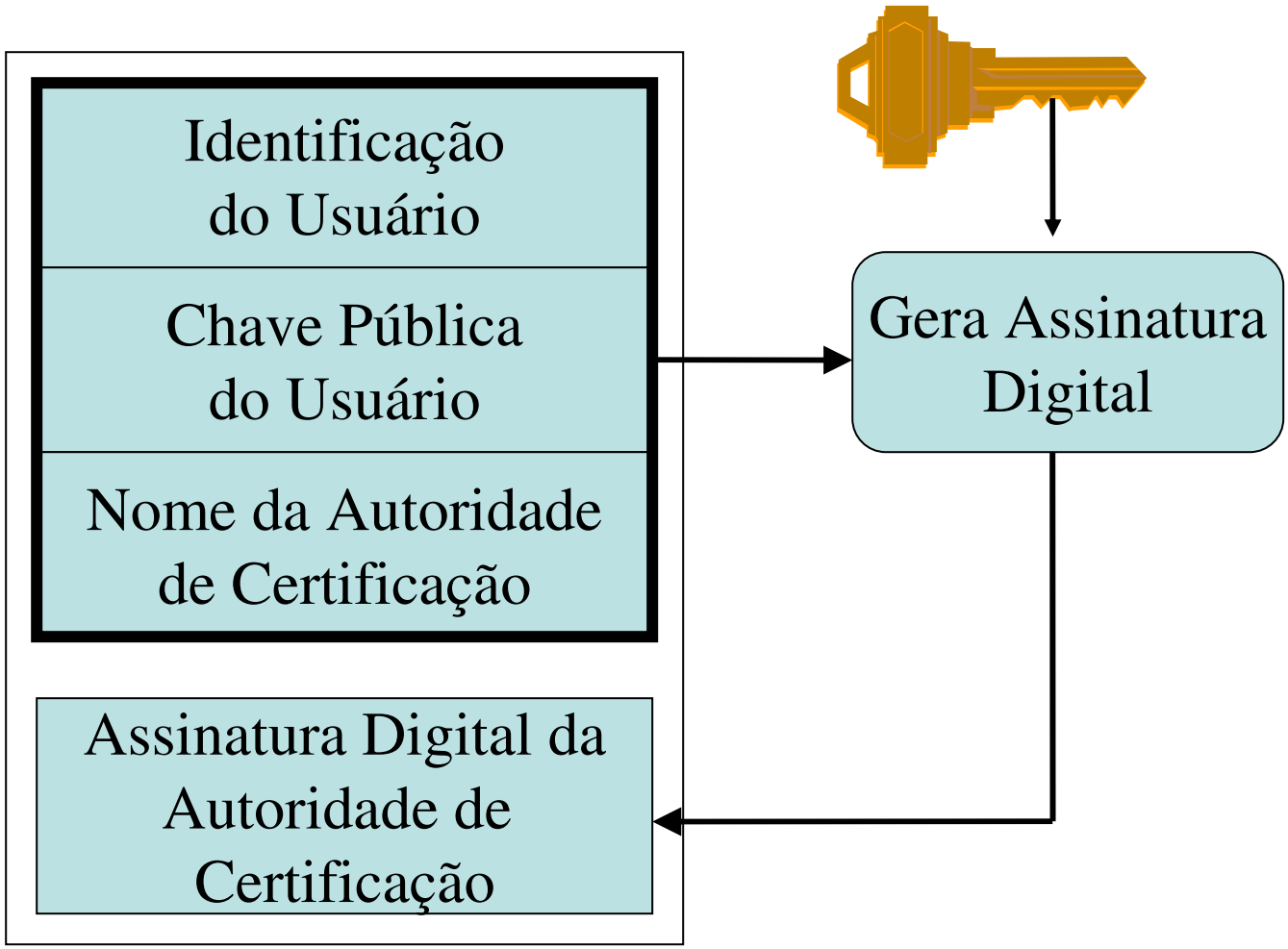
Verificando a assinatura digital



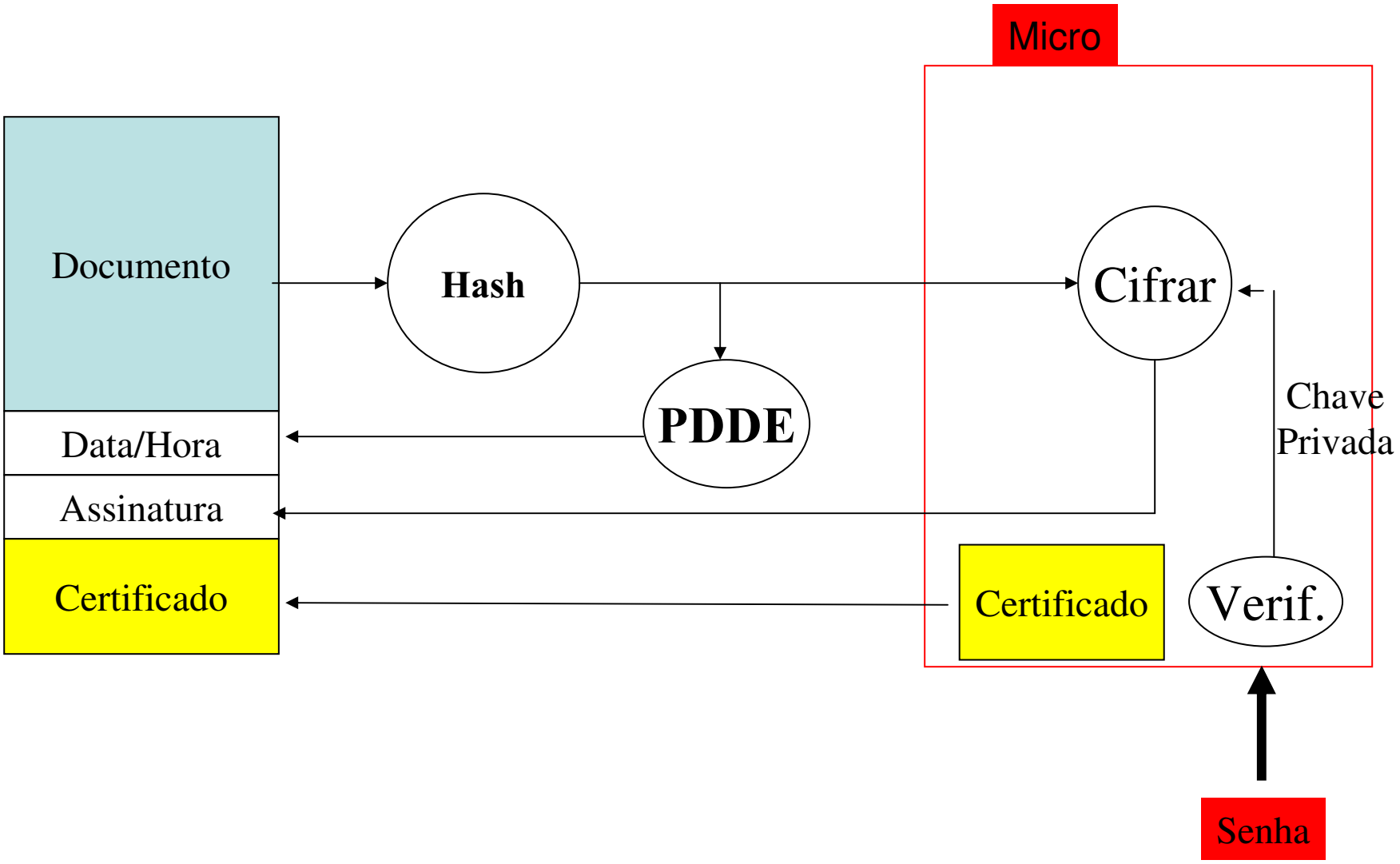
Principal crítica

- A assinatura é feita sobre informação e não sobre a mídia (papel), usando-se o micro
  - **Solução**: substituir a assinatura feita pelo micro por processamento feito em cartões inteligentes
- A autenticação é feita eletronicamente (software) e não há ligação física com a pessoa
- Há apenas um contrato de responsabilidade com a certificadora
  - **Solução**: substituir as senhas lógicas por senhas biométricas
- FATOs
  - Nos documentos em papel o software está na cabeça das pessoas
  - Inevitável a angústia da mediação tecnológica

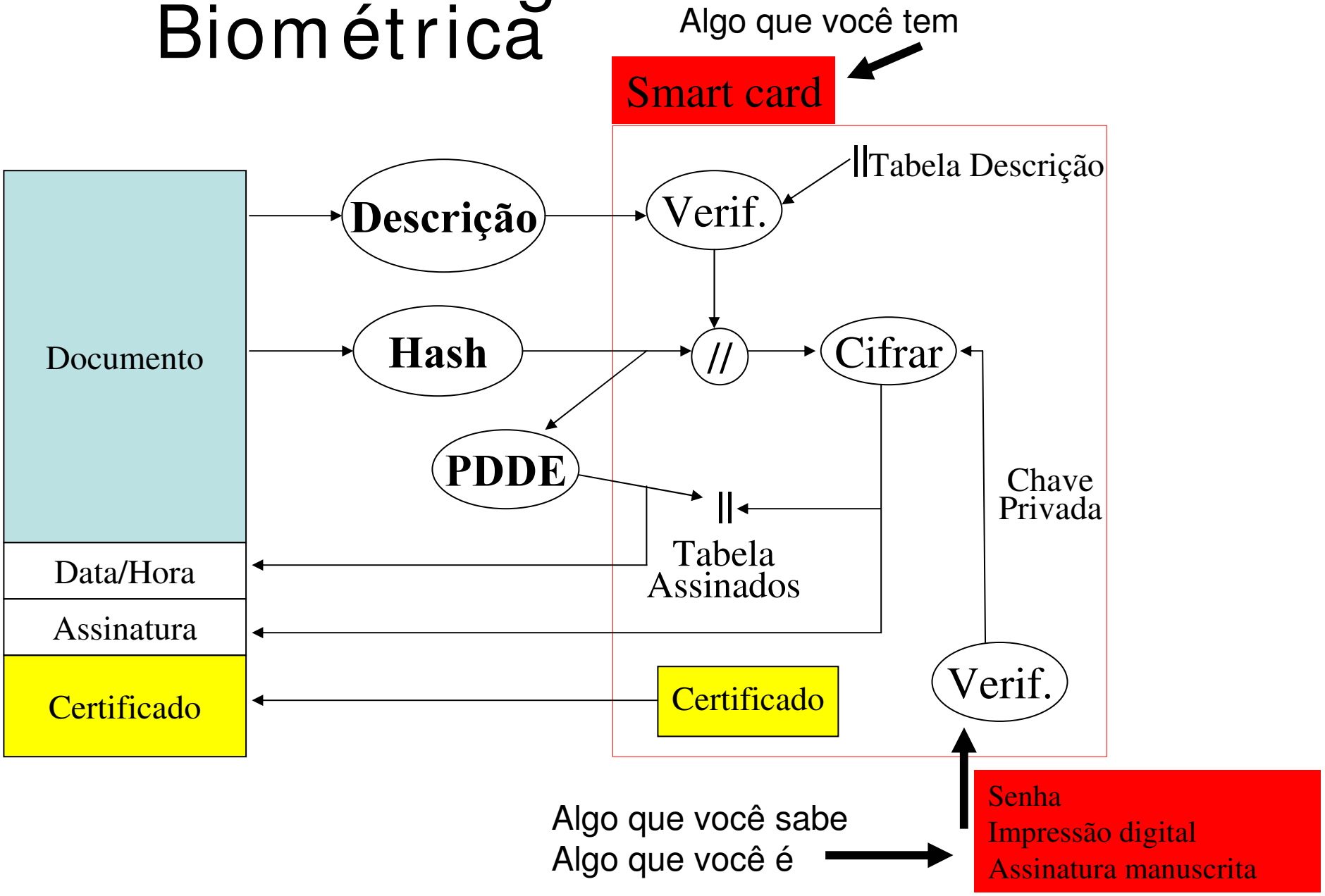
Certificado digital



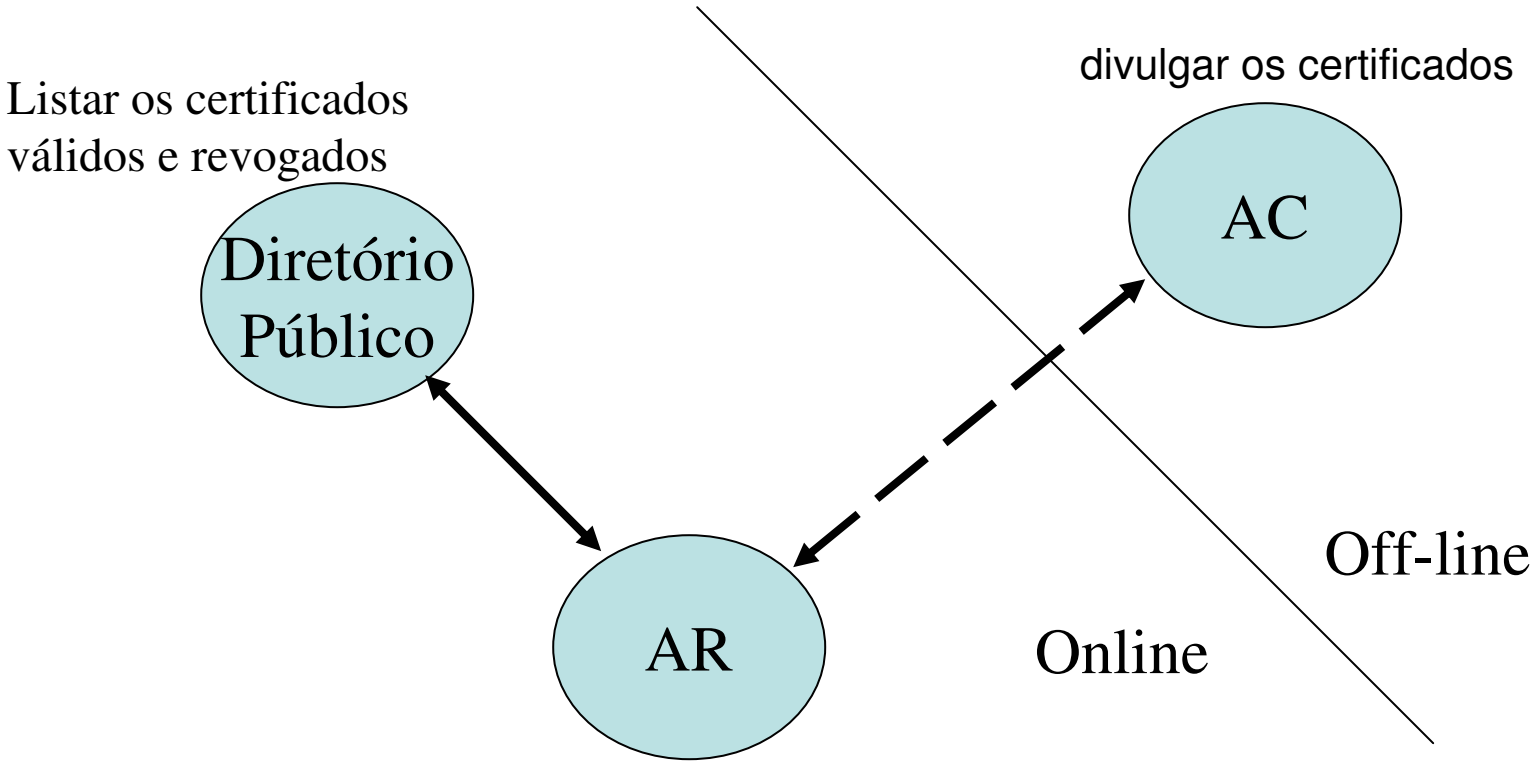
Assinatura Digital



Assinatura Digital Biométrica



Modelo Geral de uma ICP



Modelo ICP-Brasil

MP 2.200-2