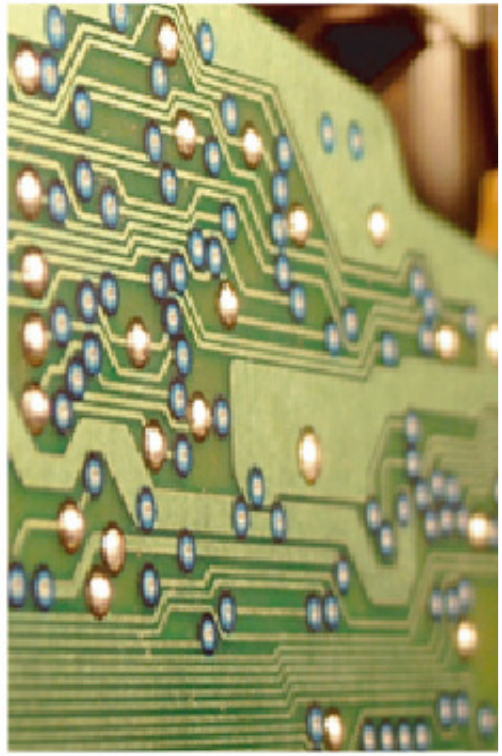
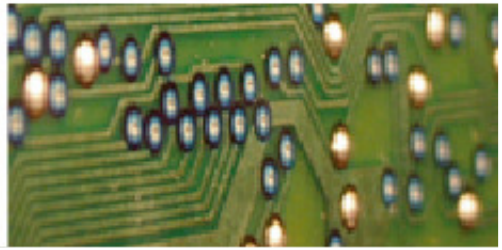
LSITEC

Laboratório de Sistemas Integravéis Tecnológico

# Soluções Inovadoras em Tecnologias Digitais Avançadas



**www.lsitec.org.br**



# Certificação Digital no Brasil: Programas, regulamentos e projetos

Edson Alonso

ealonso@lsitec.org.br

Laboratório de Sistemas Integráveis Tecnológico

**www.lsitec.org.br**

# Agenda

- Introdução a certificação digital
- A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)
- Certificações de equipamentos e sistemas aplicáveis no âmbito nacional (LEA)
- Regulamentações nacionais e internacionais
- Projetos envolvendo certificação digital no mundo.
- Ataques em smart cards

# Um pouco de história

- Uma breve história da criptografia
  - Algoritmos simétricos
  - Uso militar e restrito

Laboratório de Sistemas Integráveis Tecnológico


# Introdução a certificação digital

Conceitos básicos de criptografia

# Criptografia

- É a técnica de ocultar dados legíveis, por meio de algoritmos criptográficos, para envio a um destinatário específico

- As entidades que desejam se comunicar de forma segura fazem uso de algoritmos criptográficos, para proteger suas mensagens contra acesso não autorizado

# Criptografia

- Chaves criptográficas
  - São cadeias de bits que são utilizadas por um algoritmo para transformar dados legíveis (texto claro) em dados ilegíveis (texto cifrado)
  - A escolha dos bits da chave deve ser o mais aleatória possível

# Chaves e algoritmos

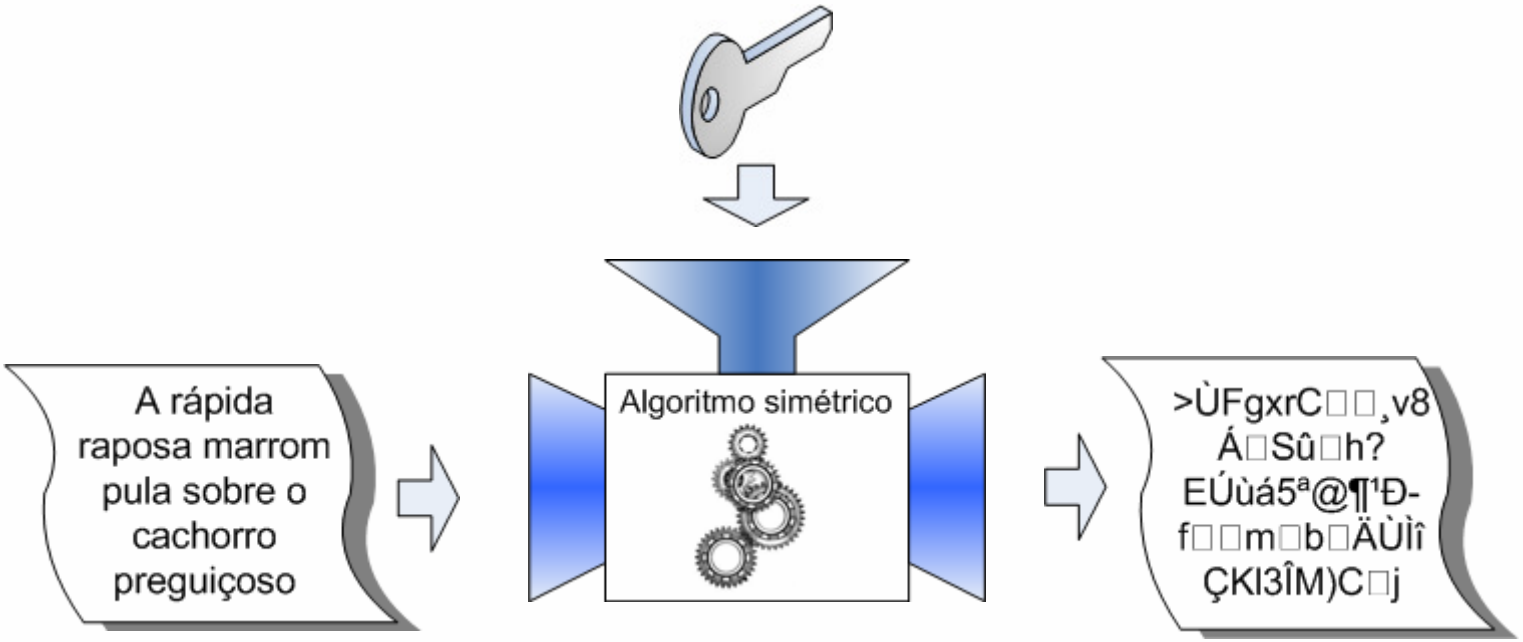
- Tamanho da chave
  - Cada algoritmo criptográfico utiliza um tamanho diferente de chave
- Remetente e destinatário
  - São aqueles que possuem uma chave previamente compartilhada entre eles para estabelecer uma comunicação segura

# Cifração / Decifração

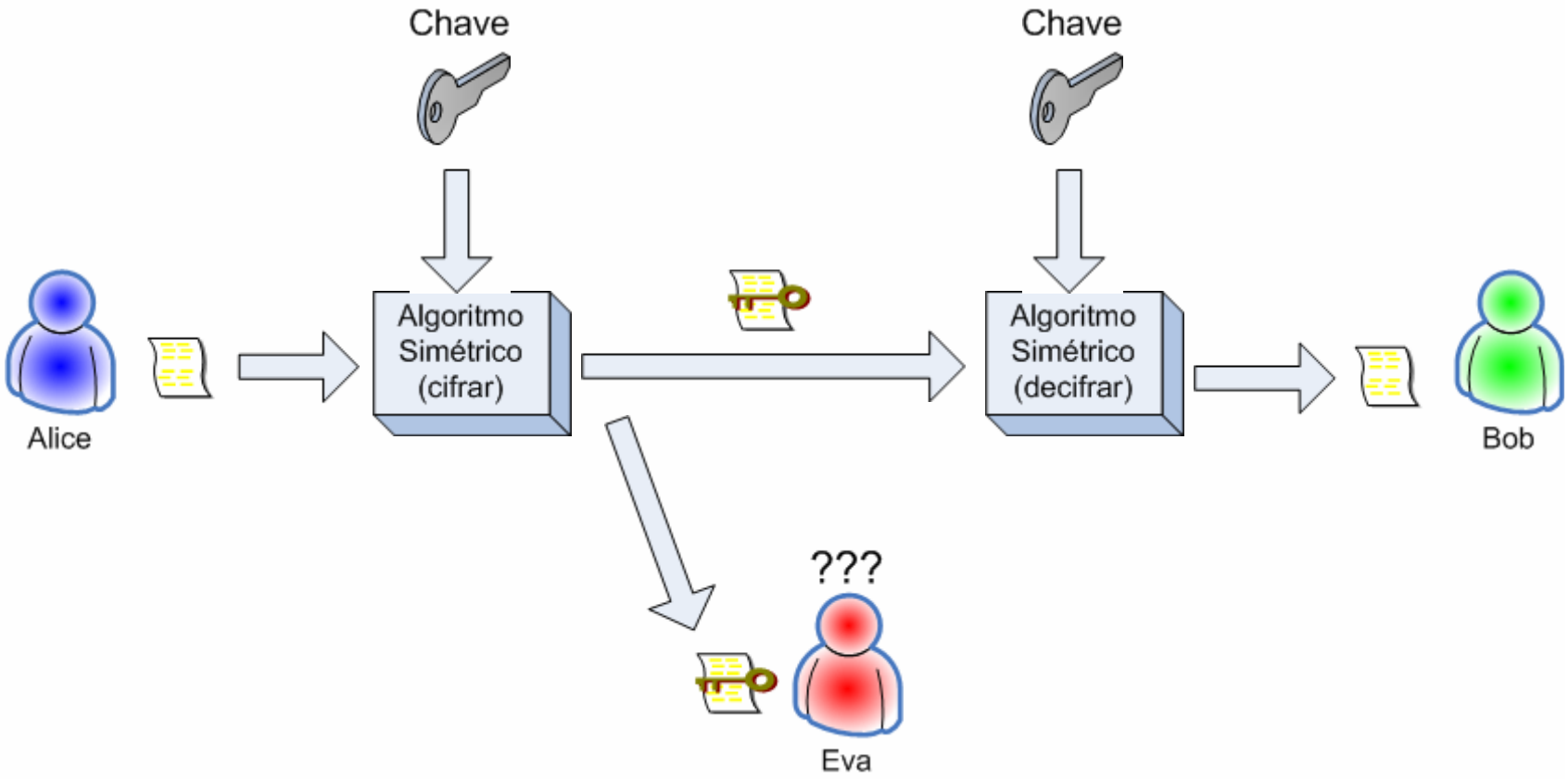
- Cifração: processo que transforma uma mensagem de texto legível em uma mensagem de texto cifrada ou ilegível

- Decifração: processo que transforma uma mensagem de texto cifrado em uma mensagem de texto legível

# Cifração / Decifração



# Cifração / Decifração



# Algoritmos criptográficos

- Em criptografia, a chave deve ser secreta, mas o algoritmo não
- O algoritmo deve ser de preferência público

# Algoritmos criptográficos

- Algoritmos proprietários podem conter vulnerabilidades que seus criadores não detectaram
- Algoritmos públicos podem ser analisados por um número maior de especialistas do que apenas seus próprios criadores, apontando possíveis problemas

Laboratório de Sistemas Integráveis Tecnológico


# Introdução a certificação digital

Criptografia de chaves públicas

# Criptografia de chaves públicas

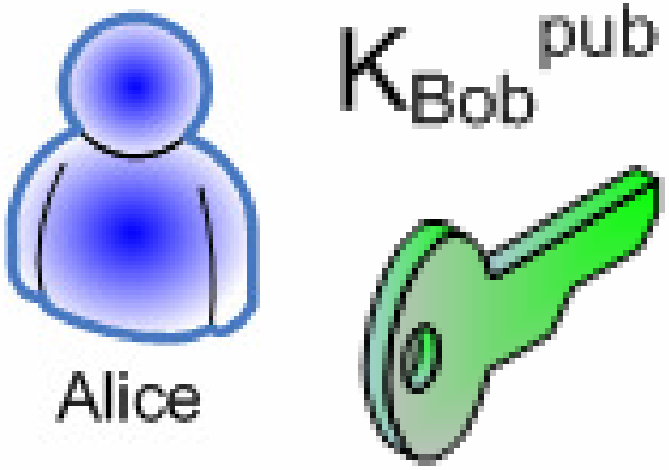
- Objetivos
  - Confidencialidade
  - Autenticidade
- A chave que cifra não pode ser utilizada para decifrar

# Criptografia de chaves públicas

- Baseado em pares de chaves
  - Chave pública ($K^{pub}$)
  - Chave privada ($K^{priv}$)
  - Conhecendo apenas uma destas, é computacionalmente inviável deduzir a outra
  - Cifração é feita com uma das chaves e a decifração é feita com a outra

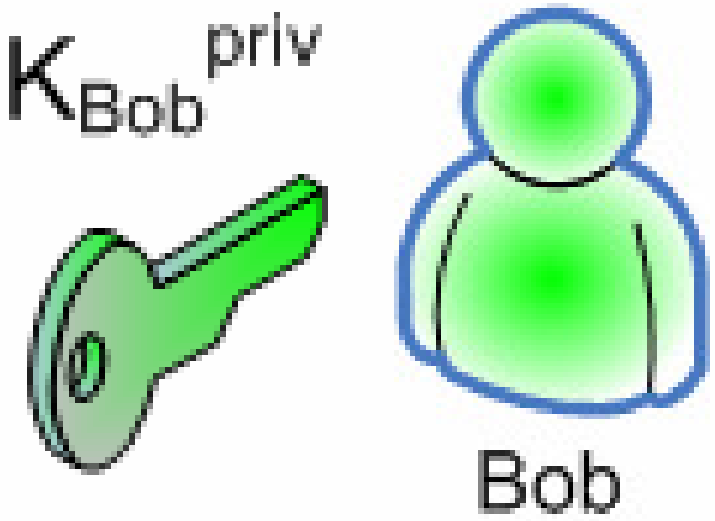
# Criptografia de chaves públicas

- Funcionamento da cifração e decifração
  - Remetente (Alice) cifra a mensagem com a chave pública do destinatário (Bob).

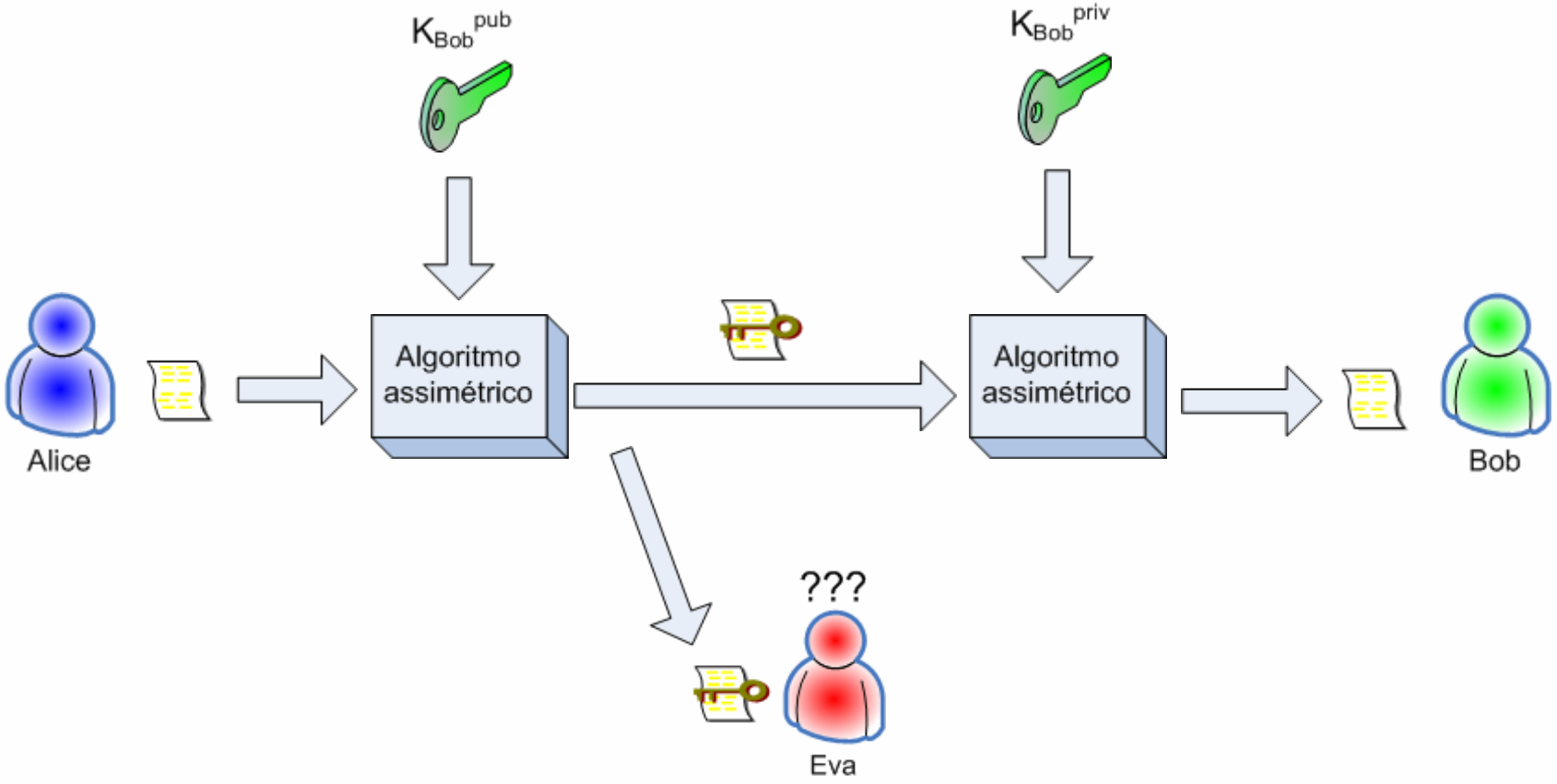


# Criptografia de chaves públicas

- Do outro lado, o destinatário (Bob) recebe a mensagem cifrada e utiliza sua chave privada para decifrar a mensagem

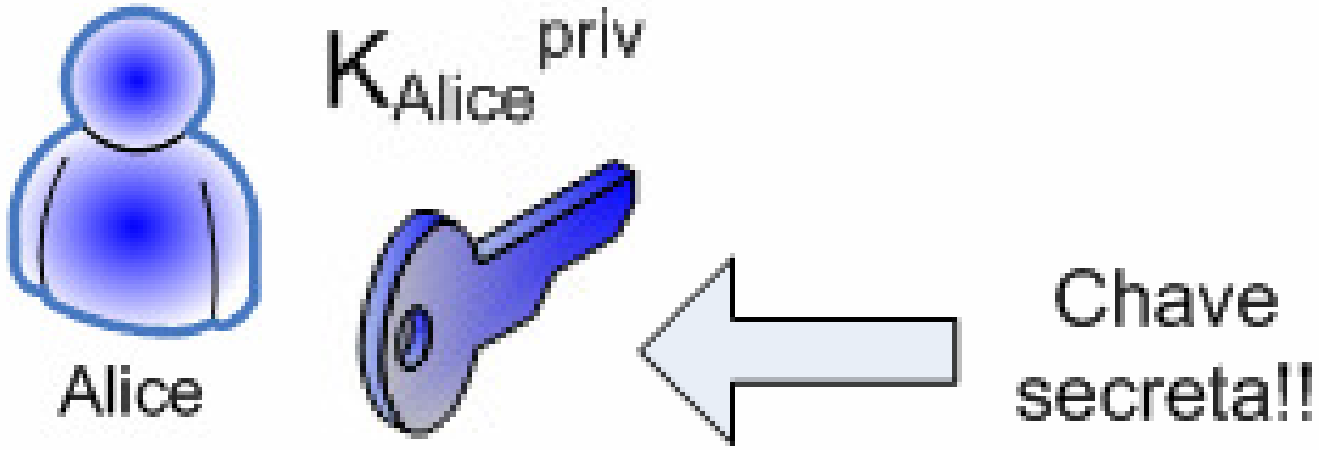


# Criptografia de chaves públicas



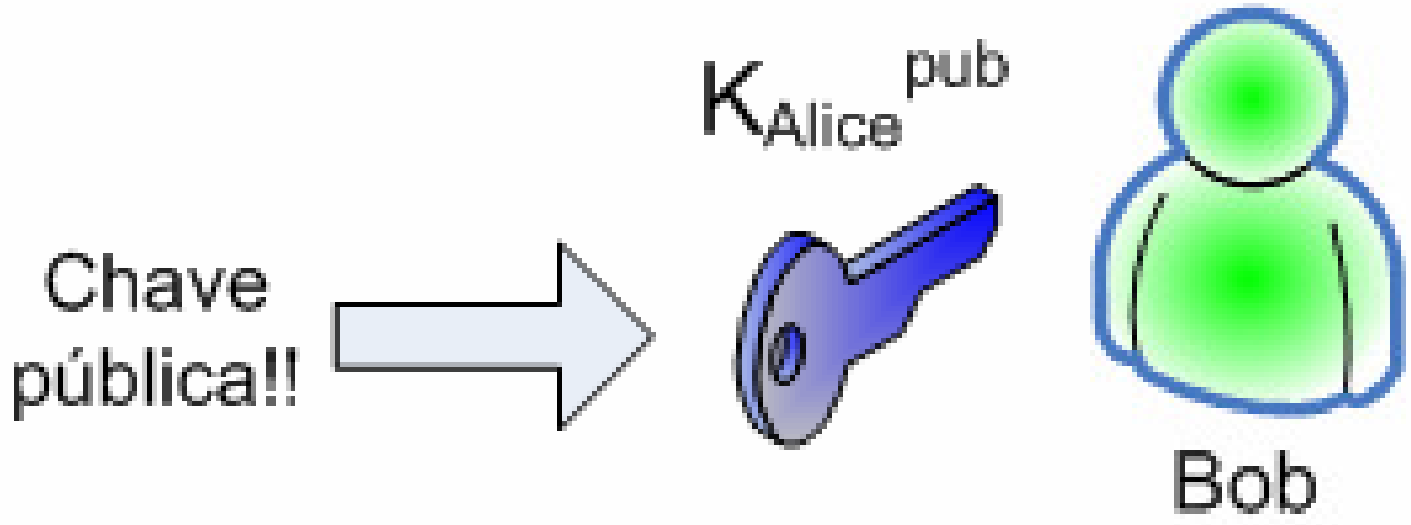
# Criptografia de chaves públicas

- Funcionamento da autenticação
  - Remetente (Alice) cifra mensagem com sua própria chave privada e envia ao destinatário (Bob)

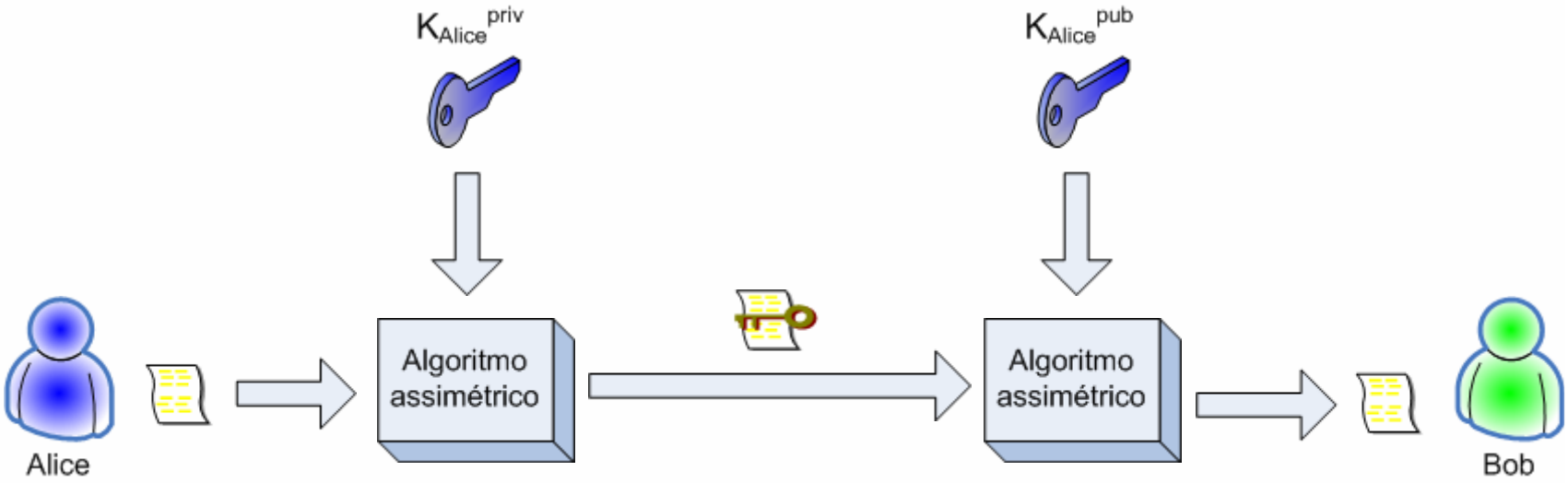


# Criptografia de chaves públicas

- De posse da chave pública do remetente (Alice), o destinatário (Bob) decifra a mensagem



# Criptografia de chaves públicas



# Criptografia de chaves públicas

- O destinatário (Bob) pode ter a certeza que aquela mensagem é de fato daquele remetente (Alice)
- Só Alice pode estar de posse de sua própria chave privada (secreta)

# Algoritmos

- RSA (Rivest Shamir Adelman)
  - Algoritmo publicado em 1978 e mais utilizado no mundo
  - Opera com chaves de 512, 1024, 2048, 3072 bits
  - Escolha do tamanho das chaves depende da aplicação
  - Pode ser utilizado para assinatura digital e sigilo de dados

# Algoritmos

- DSA (Digital Signature Algorithm)
  - Baseado no problema do logaritmo discreto
  - Utilizado somente para assinatura digital
- ECC (Eliptic Curve Cryptography)
  - Baseada na teoria matemática de curvas elípticas
  - Utilizado para assinatura digital e sigilo de dados
  - Opera com chaves de 160, 256, 384 e 512 bits

Laboratório de Sistemas Integráveis Tecnológico


# Introdução a certificação digital

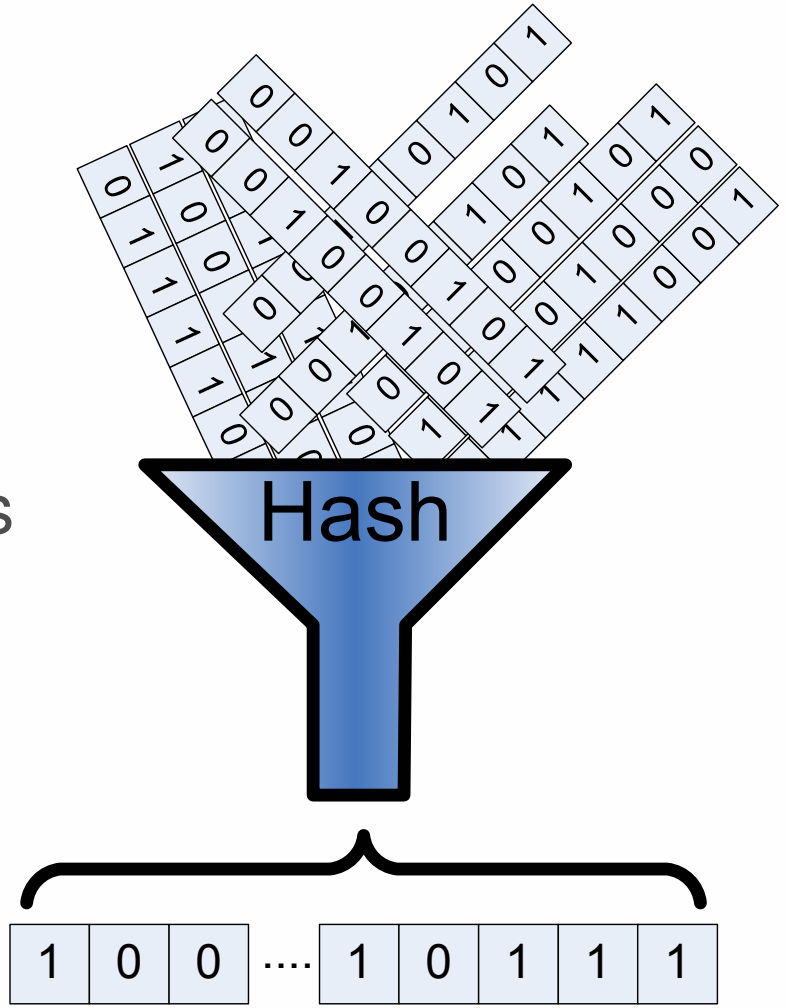
## Resumos criptográficos

# Resumos criptográficos

- Utilizados para assegurar que a mensagem transmitida está íntegra e não sofreu alterações no caminho
- São conhecidos como funções de Hash ou resumo criptográfico

# Resumos criptográficos

- A função de Hash consiste em transformar qualquer quantidade de dados em um conjunto limitado de caracteres



# Algoritmos

- Família de funções MD
  - MD2, MD4 e MD5
  - Já foram todas quebras!
  - Apesar disso, o MD5 ainda é utilizado em sistemas atuais

# Algoritmos

- Família de funções SHA
  - SHA-0, SHA-1
  - SHA-2 (composto por um conjunto de 4 funções: SHA-224, SHA-256, SHA-384 e SHA-512)
  - SHA-1 é a mais utilizada, porém existem diversas publicações acadêmicas se aproximando da quebra deste algoritmo

Laboratório de Sistemas Integráveis Tecnológico


# Introdução a certificação digital

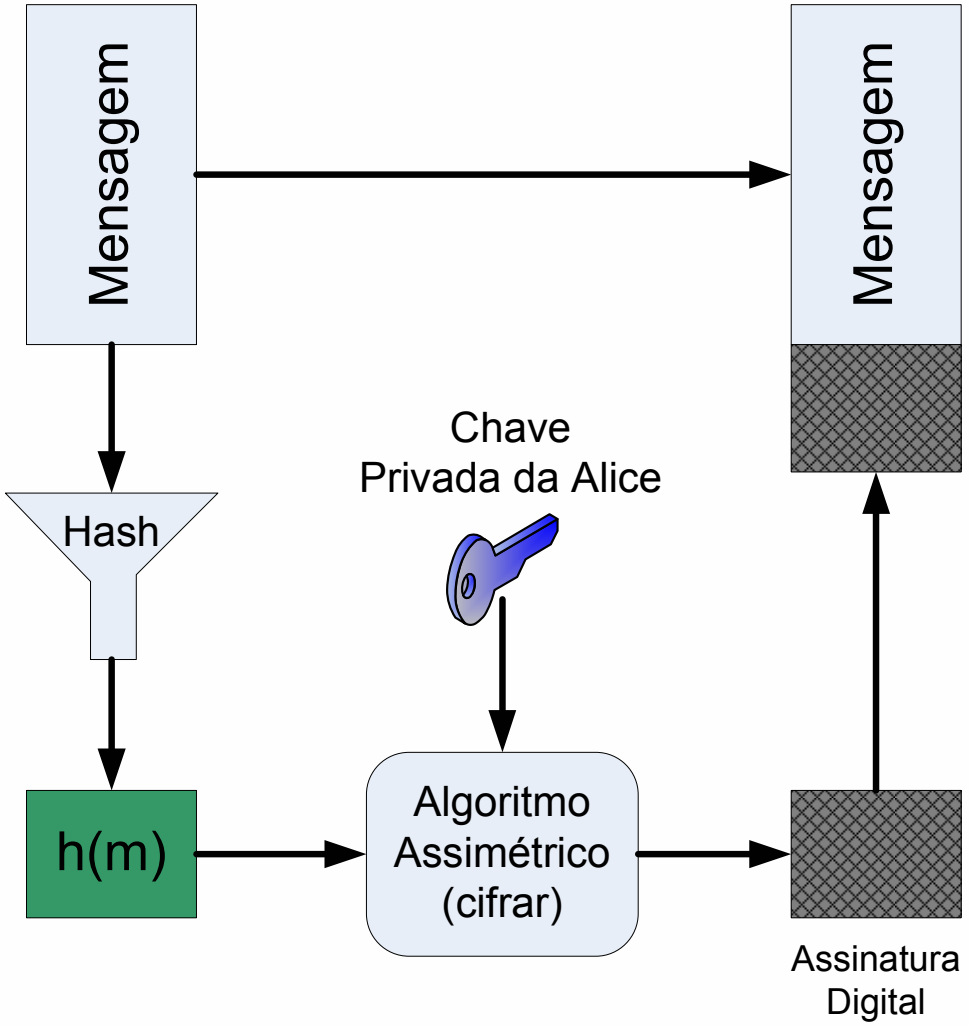
Assinatura digital

# Assinatura digital

- Para realizar uma assinatura digital, vamos precisar dos seguintes componentes
  - Mensagem a ser assinada
  - Algoritmo assimétrico
  - Par de chaves do remetente
  - Função de Hash

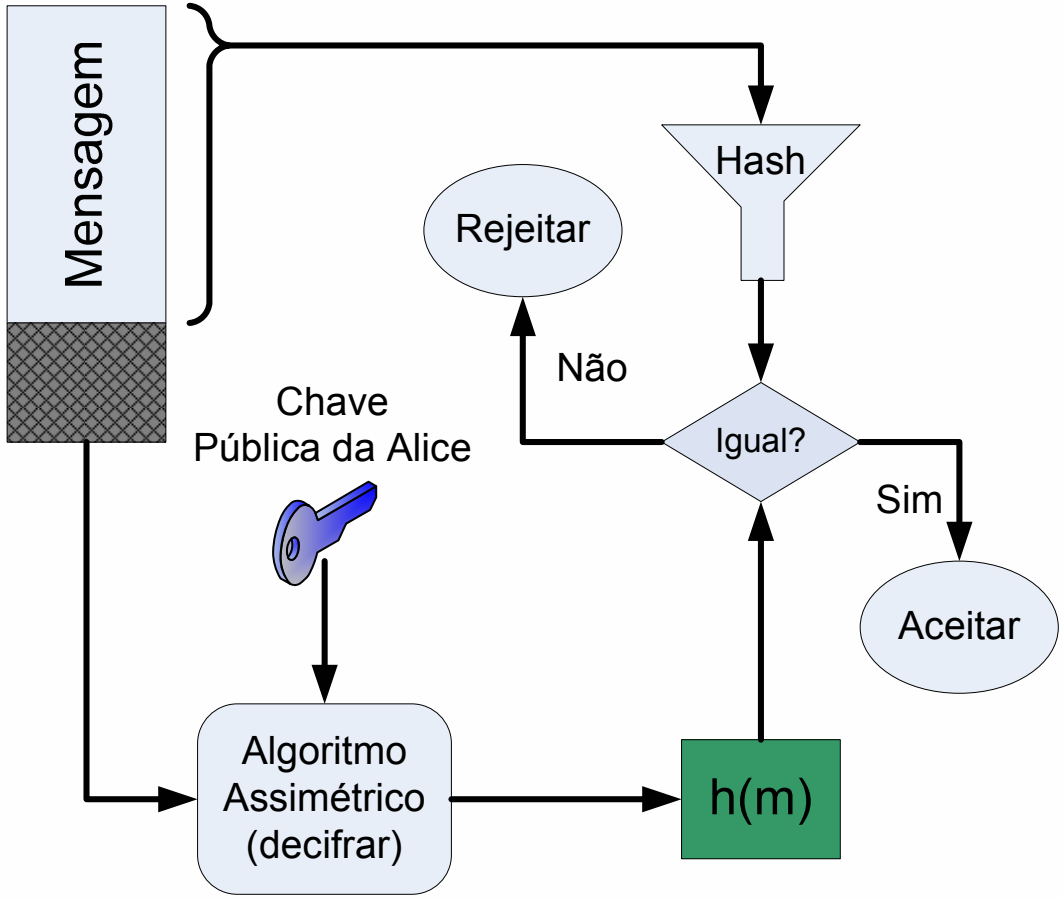
# Assinatura digital

- Alice envia uma mensagem assinada para o Bob



# Assinatura digital

- Bob verifica a assinatura digital da Alice

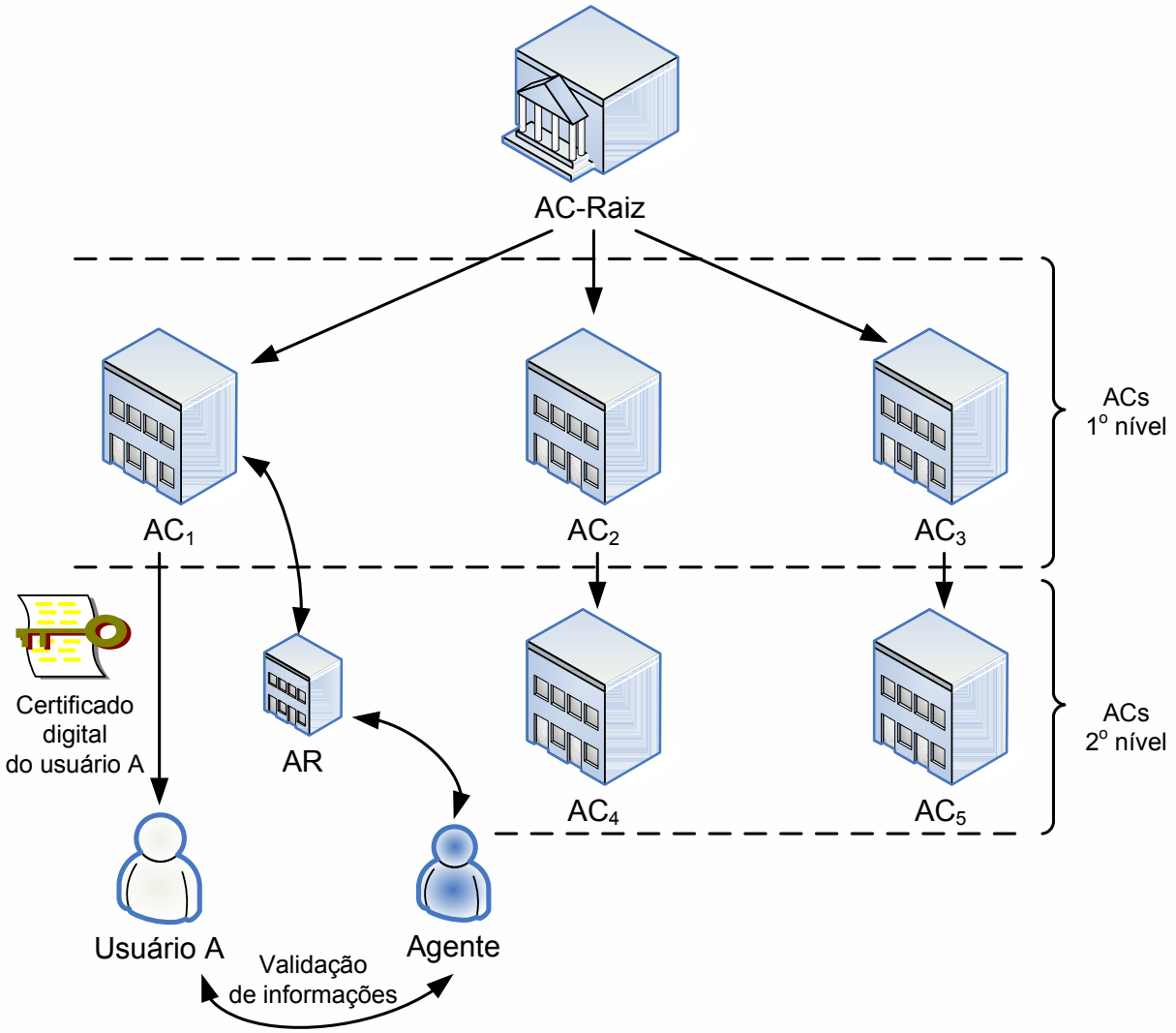


Laboratório de Sistemas Integráveis Tecnológico


# Introdução a certificação digital

Infraestrutura de chaves públicas

# Hierarquia



# Autoridade Certificadora Raiz (AC-Raiz)

- Orgão central da cadeia de certificação
- Responsável pela emissão dos certificados digitais das ACs de 1º nível somente.
- Seu próprio certificado tem uma validade longa
- O atual da ICP-Brasil possui 13 anos

# Autoridade Certificadora (AC)

- Responsável pela gestão do ciclo de vida dos certificados digitais. Isto envolve:
  - Emitir certificados
  - Renovar certificados
  - Revogar certificados
- Um certificado emitido por uma AC é assinado digitalmente com sua chave privada.

# Autoridade de Registro (AR)

- Responsabilidades da AR
  - Receber requisições de certificados digitais
  - Confirmação da identidade de entidades finais por meio de Agentes de Registro
  - Tornar disponíveis informações sobre certificados digitais emitidos
- Subordinada à AC
- AR não emite certificados!!

# Certificados digitais

- Documento eletrônico utilizado para troca confiável de chaves públicas entre os participantes de uma comunicação
- O certificado digital deve ser assinado por uma autoridade certificadora (AC)
- Somente uma AC pode emitir certificados digitais

# Certificados digitais

- O que um certificado digital contém?
  - Identificação do portador do certificado
  - Chave pública do portador do certificado
  - Prazo de validade do certificado
  - Identificação da AC
  - Número de série
  - Outros campos
  - Assinatura do certificado pela AC

# Certificados digitais

- Como é solicitado?
  - O usuário gera um par de chaves (por exemplo, RSA) e envia uma requisição a AC
  - Esta requisição contém um vínculo com a chave pública do usuário e seus dados pessoais

# Certificados digitais

- E após a solicitação?
  - É realizada a verificação  presencial dos dados do usuário por intervenção de um Agente de Registro (AR), a AC gera e assina o certificado digital para o usuário solicitante
  - Este certificado digital pode ser tornado público

Laboratório de Sistemas Integráveis Tecnológico

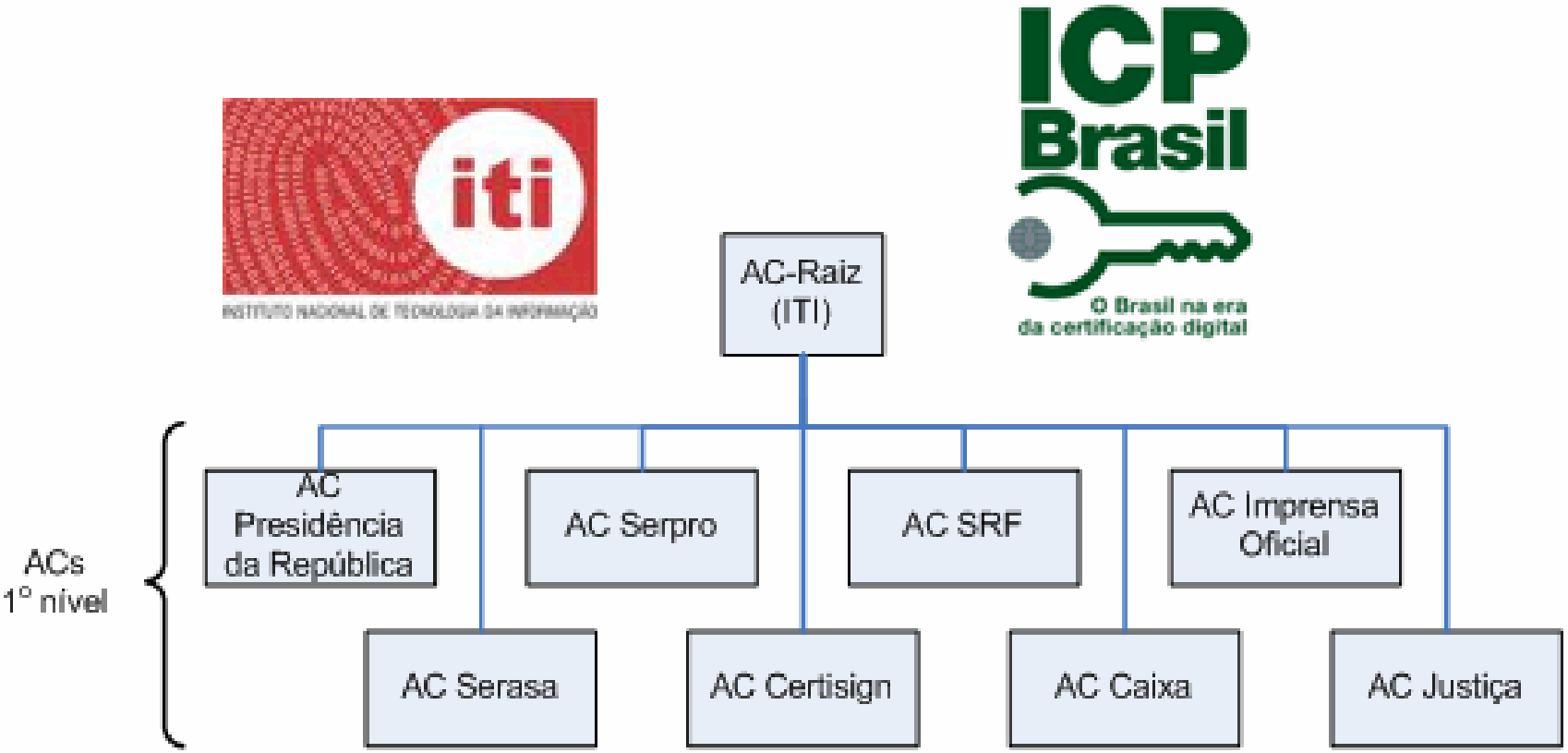
# A Infraestrutura de Chaves Públicas Brasileira ICP-Brasil

A estrutura da cadeia de certificação no Brasil

# A estrutura da cadeia de certificação no Brasil

- A AC-Raiz é representada pelo Instituto Nacional de Tecnologia da Informação (ITI)
- Abaixo da AC-Raiz estão as ACs de 1º nível
- Para cada AC de 1º nível podem haver diversas outras ACs de 2º nível

# A estrutura da cadeia de certificação no Brasil

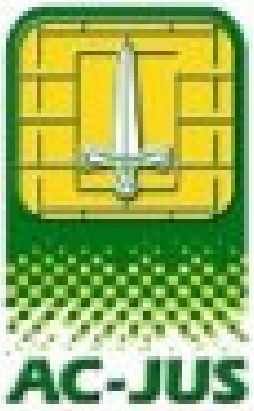


# A estrutura da cadeia de certificação no Brasil








# A estrutura da cadeia de certificação no Brasil

- Para maiores informações sobre a estrutura da ICP-Brasil, consulte: http://www.iti.gov.br/twiki/bin/view/Certificacao/EstruturaIcp
- Os seguintes documentos descrevem a estrutura completa da ICP-Brasil
  - http://www.iti.gov.br/twiki/pub/Certificacao/EstruturaIcp/Estrutura_da_ICP-Brasil_-_site.pdf
  - http://www.iti.gov.br/twiki/pub/Certificacao/EstruturaIcp/Estrutura_completa.pdf

# Certificados digitais ICP-Brasil

- Tipos de certificados digitais na ICP-Brasil
  - Certificados diferem quanto ao tamanho das chaves, mecanismo de geração das chaves, validade do certificado e propósito de uso


# Certificados digitais ICP-Brasil

- São definidos os seguintes perfis de certificados digitais
  - A1, A2, A3 e A4
    - Propósito de assinatura digital para pessoa física, júridica ou equipamento
  - S1, S2, S3 e S4
    - Propósito de sigilo de dados para pessoa física, jurídica ou equipamento

Laboratório de Sistemas Integráveis Tecnológico

# Certificações de equipamentos e sistemas aplicáveis no âmbito nacional (LEA)

Processo de homologação da ICP-Brasil

# A criação da ICP-Brasil

- Medida Provisória nº 2.200-2, de 24 de Agosto de 2001
  - Instituiu a ICP-Brasil

Laboratório de Sistemas Integráveis Tecnológico

# Regulamentação para laboratórios

- Resolução n° 36, de 21 de Outubro de 2004
  - Regulamenta a homologação de sistemas e equipamentos de certificação digital na ICP-Brasil
  - Pode-se então ser criado o primeiro LEA
  - O LSI-TEC passa pelos critérios adotados pelo ITI na seleção do primeiro Laboratório de Ensaios e Auditoria

# Algoritmos para ICP-Brasil

- Resolução n° 65, de 9 de Junho de 2009
  - Versão atual do documento que estabelece padrões e algoritmos criptográficos para uso na ICP-Brasil

# Regulamentação ICP-Brasil

- Para acessar outras regulamentações acesse os sites:

- http://www.iti.gov.br/twiki/bin/view/Certificacao/Resolucoes
- http://www.iti.gov.br/twiki/bin/view/Certificacao/DocIcp

# Objetos de homologação

- Antes de criar um processo para homologar dispositivo ou sistemas, é necessária a criação de normativos técnicos
- Estes normativos são denominados Manuais de Condutas Técnicas (MCT)
- É desenvolvido um MCT para cada objetivo de homologação, seja ele um dispositivo ou sistema

# Objetos de homologação

- O que pode ser homologado hoje?
  - Cartão criptográfico (smart card)
  - Leitora de cartão criptográfico
  - Token criptográfico
  - Softwares de assinatura digital, autenticação e sigilo
  - Bibliotecas criptográficas e provedores de serviços criptográficos (CSP)
  - -Módulos de segurança criptográficos (HSM – Hardware Security Module)



# Objetos de homologação

- Ainda em processo de elaboração de normativos técnicos
  - Equipamento de carimbo do tempo
  - Software de Autoridade Certificadora e Autoridade de Registro
- O site a seguir apresenta documentos sobre o processo de homologação http://www.iti.gov.br/twiki/bin/view/Homologacao/Documentos

Laboratório de Sistemas Integráveis Tecnológico

# O processo de homologação da ICP-Brasil

- A Parte Interessada inicia o processo formal no ITI em Brasília
- O depósito dos materiais é feito em São Paulo no LSI-TEC
- São conduzidas as análises de conformidade
- Um laudo é emitido para a Parte Interessada

# Limitações das certificações internacionais existentes

- Regulamentações como FIPS e Common Criteria já possuem programas de certificação de equipamentos
- Porém estes programas não são reconhecidos mutuamente entre o Brasil e outros países
- Outros padrões necessitam ser agregados para homologar por completo um sistema criptográfico

Laboratório de Sistemas Integráveis Tecnológico

# Regulamentações nacionais e internacionais

## Regulamentações internacionais para infraestruturas de chaves públicas

# Regulamentações internacionais

- FIPS 140
  - Criado e mantido pelo NIST
  - Certifica a segurança de módulos criptográficos (hardware ou software!)
  - Deficiente nas questões de interoperabilidade entre hardware e sistema
  - Sistemas criptográficos multi-aplicação não fazem parte do escopo

# Regulamentações internacionais

- Common Criteria
  - Pode ser considerado um conjunto de requisitos para garantir a segurança das funcionalidades de dispositivos
  - O mercado consumidor estipula as funcionalidades de segurança esperadas de um sistema (Protection Profile)
  - Os fabricantes apresentam as metas de segurança alcançadas por seus produtos (Security Targets)
  - O resultado da certificação com base nos Security Targets é denominado de Evaluation Assurance Level (EAL)

# Regulamentações internacionais

- ISO/IEC 7816 – Smart Cards com contato
  - Parte 1 – Características Físicas
  - Parte 2 – Dimensões e localização dos contatos elétricos
  - Parte 3 – Sinais eletrônicos e protocolos de transmissão
  - Parte 4 – Comandos interindustriais de interação
  - Parte 5 – Procedimento de sistema de numeração e registro para identificadores de aplicação

# Regulamentações internacionais

- ISO/IEC 7816 – Smart Cards com contato (continuação)
  - Parte 6 – Elementos de dados interindustriais
  - Parte 7 – Comandos interindustriais para linguagem estruturada de solicitações ao cartão (SCQL)
  - Parte 8 – Comandos interindustriais relacionados a segurança
  - Parte 9 – Comandos para gerenciamento do cartão
  - Parte 10 – Sinais eletrônicos e resposta de ativação para cartões síncronos

# Regulamentações internacionais

- ISO/IEC 7816 – Smart Cards com contato (continuação)
  - Parte 12 – Interface USB direto no chip
  - Parte 13 – Comandos para ambientes multi-aplicação
  - Parte 11 – Verificação pessoal por meio de métodos biométricos
  - Parte 15 – Aplicações de informações criptográficas

# Regulamentações internacionais

- PC/SC – Personal Computer / Smart Card
  - Especifica um conjunto mínimo de funcionalidades necessárias para smart cards e leitoras, que proporcionam interoperabilidade entre dipositivos
  - Mantém a consistência com os padrões já existentes e aplicáveis para PCs, smart cards e outros dispositivos relacionados
  - Permite interoperabilidade entre os componentes executados em diferentes plataformas

# Regulamentações internacionais

- USB – CCID (Integrated Circuit(s) Cards Interface Device)
  - Define uma classe de dispositivos para interações com smart cards
  - Descreve um protocolo padrão para interação com leitoras USB
  - Este protocolo permite transportar comandos para o Smart Card (comandos APDU)
  - Promove a interoperabilidade de diferentes leitoras com sistemas operacionais

# Regulamentações internacionais

- USB – ICCD (Specification for USB Integrated Circuit(s) Card Devices)
  - Define uma classe específica de tokens USB com capacidade criptográfica
  - Protocolo padrão para interação com tokens criptográficos USB
  - Transporta os comandos para o token e invoca suas funcionalidades criptográficas
  - Windows XP possui driver genérico aderente a este padrão

# Regulamentações internacionais

- Outros padrões e especificações
  - RSA PKCS#1, 2, 3…15
  - Javacard
  - Globalplatform
  - ETSI
  - IETF

# Regulamentações internacionais

- Estes componentes são a base da certificação digital
- A evolução dos padrões e especificações é constante e rápida
- As especificações de algoritmos criptográficos são as que evoluem mais rapidamente

Laboratório de Sistemas Integráveis Tecnológico

# Projetos envolvendo certificação digital no mundo

Assinatura digital, sigilo, identificação e outros serviços

# Projetos em certificação digital

- Assinatura digital
  - Declaração do imposto de renda e obtenção de documentos perante a Receita Federal
  - Cartório virtual (CRSEC): Registro Civil, Registro de Imóveis e Registro de Títulos
  - Nota fiscal eletrônica (NF-e)
  - Sistema de Pagamentos Brasileiro (SPB)

# Projetos em certificação digital

- Identificação eletrônica
  - Registro de Identidade Civil (RIC) unificando a base de identificação da população brasileira em smart card
  - Países como Bélgica e França criaram documentos de identificação eletrônica integrando com outros documentos já existentes
  - No total 21 países já adotaram um documento de identificação eletrônica

# Projetos em certificação digital

- Sigilo de dados
  - Sistemas garantem o sigilo de documentos eletrônicos em rede
  - Utiliza-se pares de chaves assimétricas e certificados digitais para cifrar a informação do usuário na rede
  - A estrutura permite a recuperação de arquivos do funcionário mesmo que este seja desligado da empresa

# Projetos em certificação digital

- Passaporte eletrônico
  - 54 países já adotaram o passaporte eletrônico(*)
  - 100 milhões de passaportes eletrônicos emitidos(*)


(*) Dados ICAO – Montreal outubro/2008

Fonte: Eurosmart

Laboratório de Sistemas Integráveis Tecnológico


# Ataques em smart cards

O lado negro da força…

# Introdução

- Em uma comunicação entre duas partes, é necessário o uso de equipamentos ou dispositivos
- Cada dispositivo utilizado, sendo ele criptográfico ou não, possui características intrínsecas que conforme a informação manipulada pode:
  - Emitir diferentes quantidades de ondas eletromagnéticas
  - Gastar diferentes quantidades de tempo de processamento
  - Consumir diferentes quantidades de corrente elétrica
  - Emitir diferentes ruídos sonoros

# Introdução

- Todas as características mencionadas são fontes de vazamento de informações
- Definição de ataque de *side-channel*:
  - Ataque que explora um vazamento não intencional de informação.

# Introdução

- O primeiro ataque de *side-channel* que se tem registro na história está relacionado a um agente da agência de inteligência britânica, o MI5
- O ataque foi feito em 1956 por Peter Wright durante espionagem da embaixada Egípcia em Londres

# Introdução

- O objetivo do ataque era a máquina criptográfica baseda em rotores conhecida como Hagelin
- Um pequeno microfone foi instalado dentro de um telefone que estava ao lado da máquina
- O sons emitidos pela máquina permitiram que a configuração de seus rotores fosse deduzida e portanto as mensagens poderiam ser decifradas

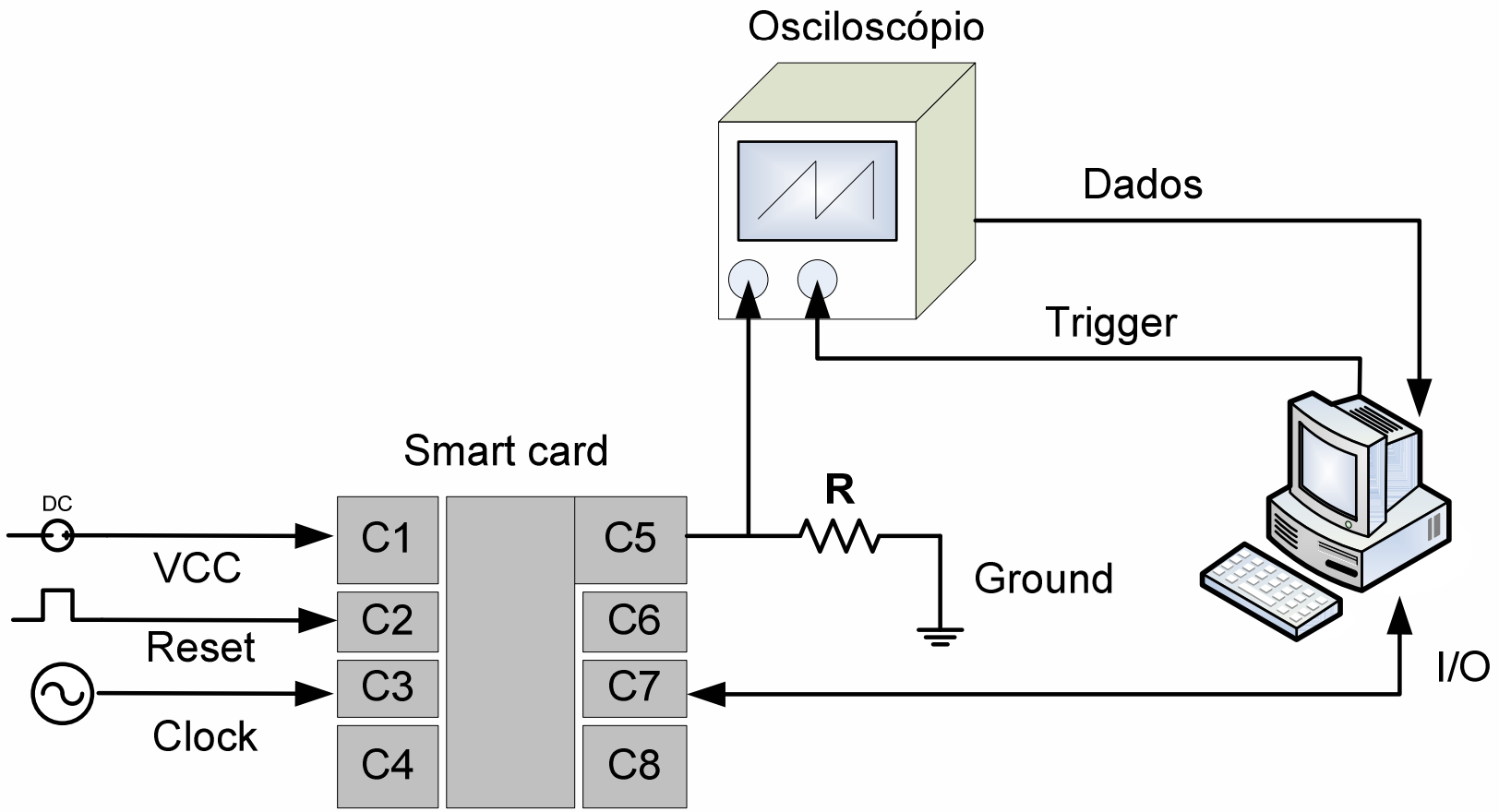
# Ataques em smart cards

- Conforme o tipo de informação que vaza do dispositivo, temos as seguintes classes de ataques de *side-channel*
  - *Simple Power Analysis (SPA)*
  - *Differential Power Analysis (DPA)*
  - *Electromagnetic Analysis (EMA)*
  - *Timming Analysis (TA)*

# Ataques em smart cards

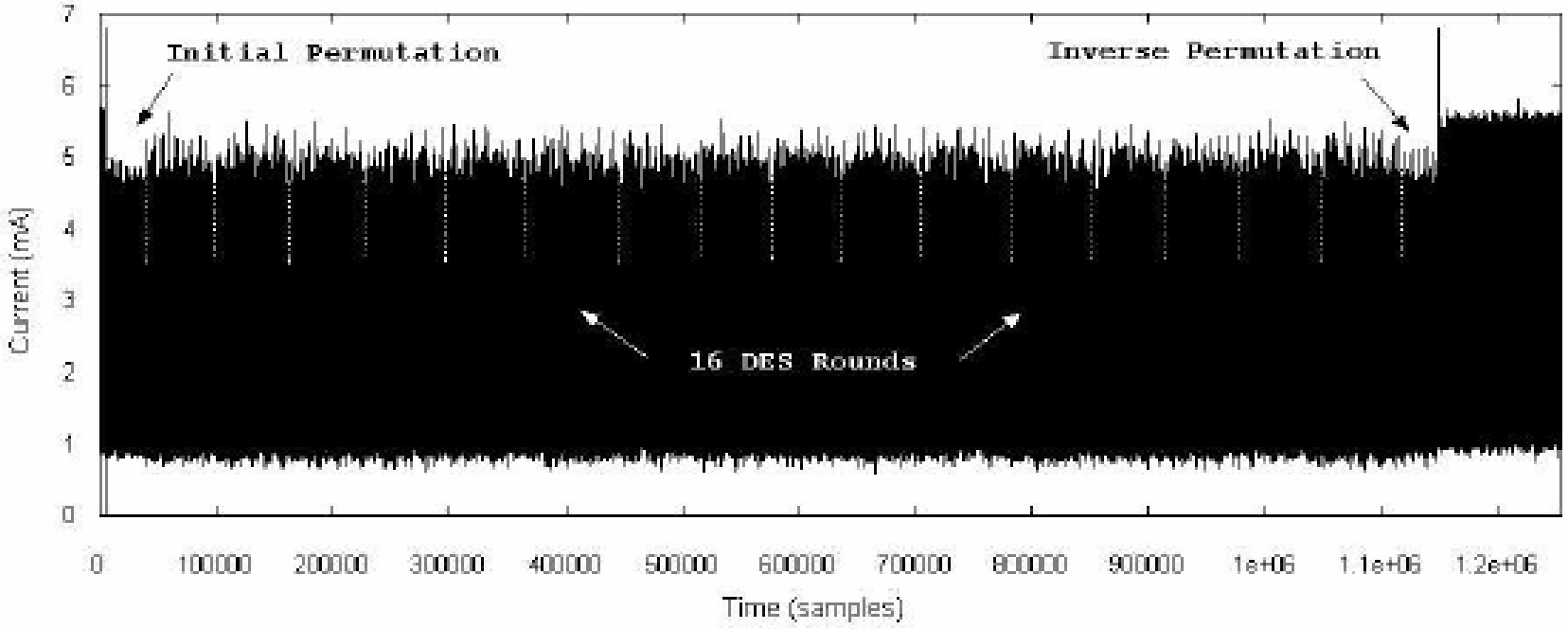
- Outros tipos de ataques necessitam de intrusão física no smart card, tais como os denominados *Fault Attacks*
- Neste caso é realizado uma intrusão de tal forma a induzir um comportamento anormal do smart card
- Este comportamento anormal pode acarretar no vazamento de informações críticas

# Setup de medições para DPA



# Exemplo de medição

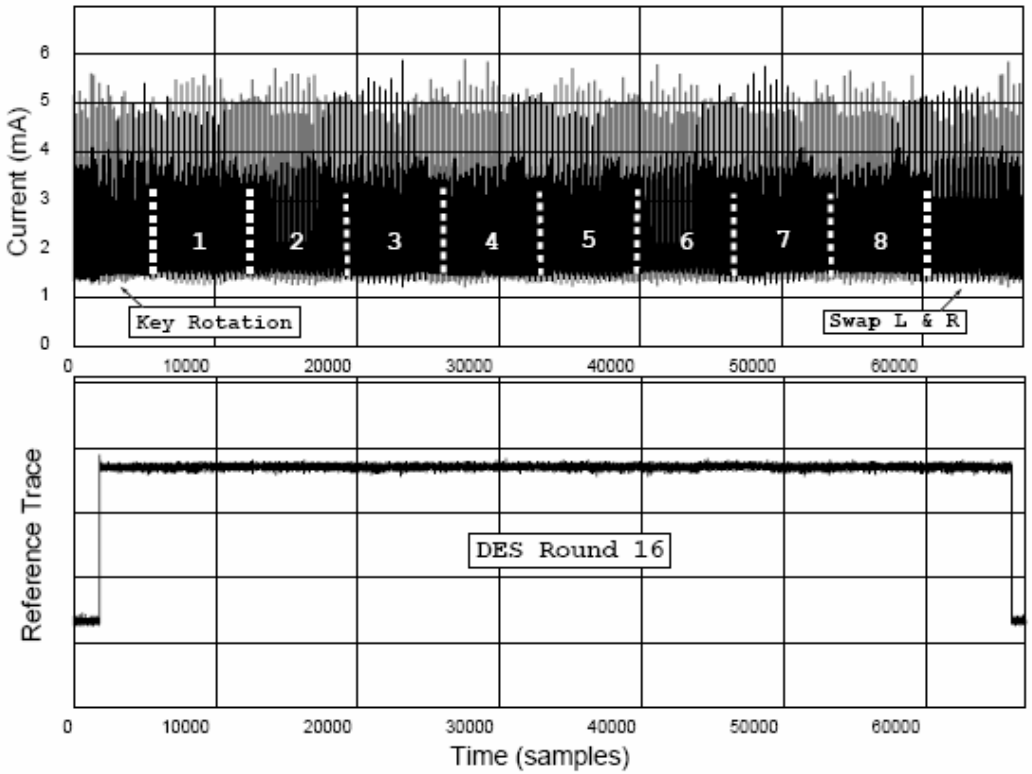
- Execução do algoritmo DES




Fonte: Junee, R. Power Analysis Attacks: A weakness in Cryptographic Smart Cards and Microprocessors. MSc Thesis.

# Exemplo de medição

- Expandindo o *Round* 16 do DES




Fonte: Junee, R. Power Analysis Attacks: A weakness in Cryptographic Smart Cards and Microprocessors. MSc Thesis.

# Proteções em smart cards

- Existem laboratórios especializados em testar chips de smart cards contra diversas classes de ataques existentes
- O laboratório testa e informa o fabricante para providenciar novas proteções se necessárias

CRYPTOGRAPHY RESEARCH

# Proteções em smart cards

- Algumas proteções para smart cards chegam a ser patenteadas por laboratórios que avaliam a segurança dos chips
- Existem empresas especializadas na pesquisa e no desenvolvimento de produtos para estudo de técnicas de ataques em smart cards

# Estamos seguros?

- Os chips de smart cards comercializados atualmente estão protegidos contra uma série de ataques invasivos e não invasivos
- Até o momento não se tem informação a respeito de clonagem de smart cards

# Onde isso vai parar?

- A pesquisa nesta área avança rápido
- Novas técnicas de ataques ultrapassam as proteções mais complexas
- Ataques em smart cards exigem um grau de sofisticação muito além daquele disponível ao fraudador
- Um fraudador tem como buscar alternativas mais fáceis no momento

# Conclusão

Laboratório de Sistemas Integráveis Tecnológico

# Muito obrigado!

Edson Emilio Alonso

ealonso@lsitec.org.br

# Literatura sugerida


- William Stallings, “Cryptography and Network Security – Principles and Practice”, 4th Edition, PrenticeHall, 2006.
- Douglas R. Stinson, “Cryptography – Theory and Practice”, 3rd Edition, CRC Press, 2005.
- Alfred Menezes, Paulo C. vanOorschot, Scott Vanstone, “Handbook of Applied Cryptography” CRC Press, 1997.