Segurança
Sistemas Distribuídos

junho de 2017

Segurança

- confidencialidade
- autenticidade
- integridade
- não repudiação

} comunicação

processos se comunicam por rede ”pública”

PUC RIO

comunicação – ameaças

- interceptação
- interrupção
- modificação
- fabricação

PUC RIO

ataques a canais de comunicação

- escuta
  - obtenção de informação na rede
    - senhas, etc
- masquerading
  - uso de identidades falsas
- message tampering
  - alteração de mensagens trocadas
- replay
  - reenvio de mensagens obtidas por escuta
- negação de serviço
  - inundação de rede (ou servidor)

PUC RIO

mecanismos e políticas

PUC
RIO

mecanismos

- protocolos
- criptografia

- autenticação
- autorização
- auditoria

PUC RIO

e qualidade do software...

- http://xkcd.com/1354/

PUC RIO

projeto de segurança

- equilíbrio entre custos – política
  - risco X sobrecarga
- modelo do atacante
  - mecanismos devem atender política com esse modelo
- medidas de sobrecarga

PUC RIO

criptografia básica

- Alice
- Bob
- Carol
- Dave

} entidades ou usuários

- Eve, Trudy ou Mallory – malfeitores
- Sara – servidor

- chave K – seq. de bytes usada para criptografar/decriptar

PUC RIO

criptografia básica

- M + K -> mensagem codificada
  - criptografar
- mensagem codificada + K -> conteúdo original
  - decriptar

tamanho de chave determina custo computacional de ataques de força bruta

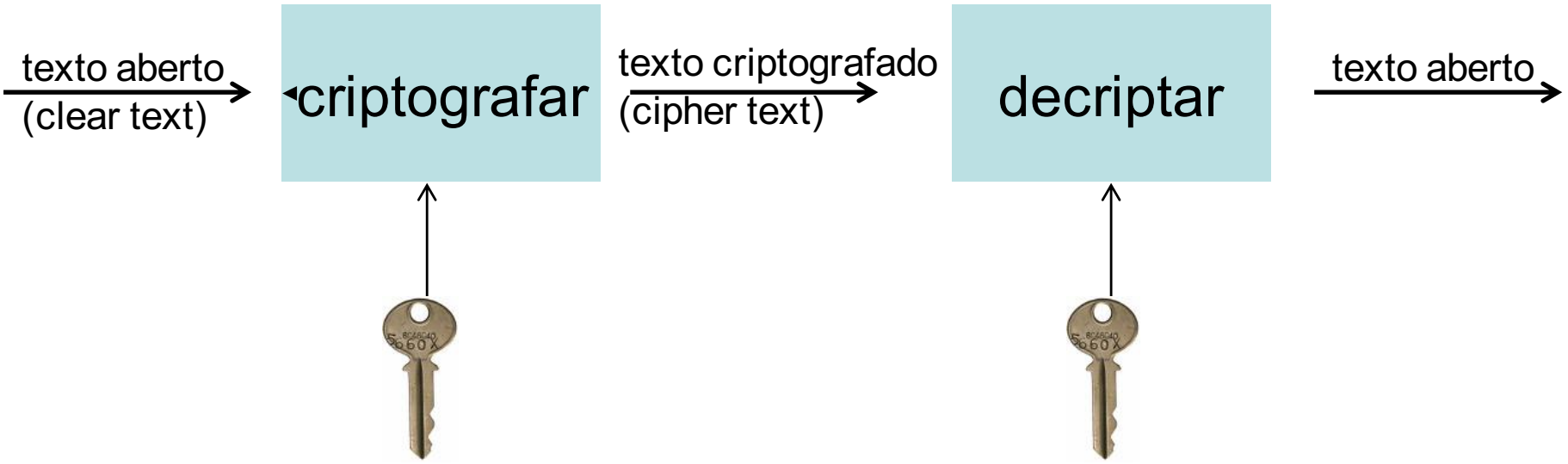
PUC RIO

criptografia simétrica

- K_{AB} chave compartilhada por A e B

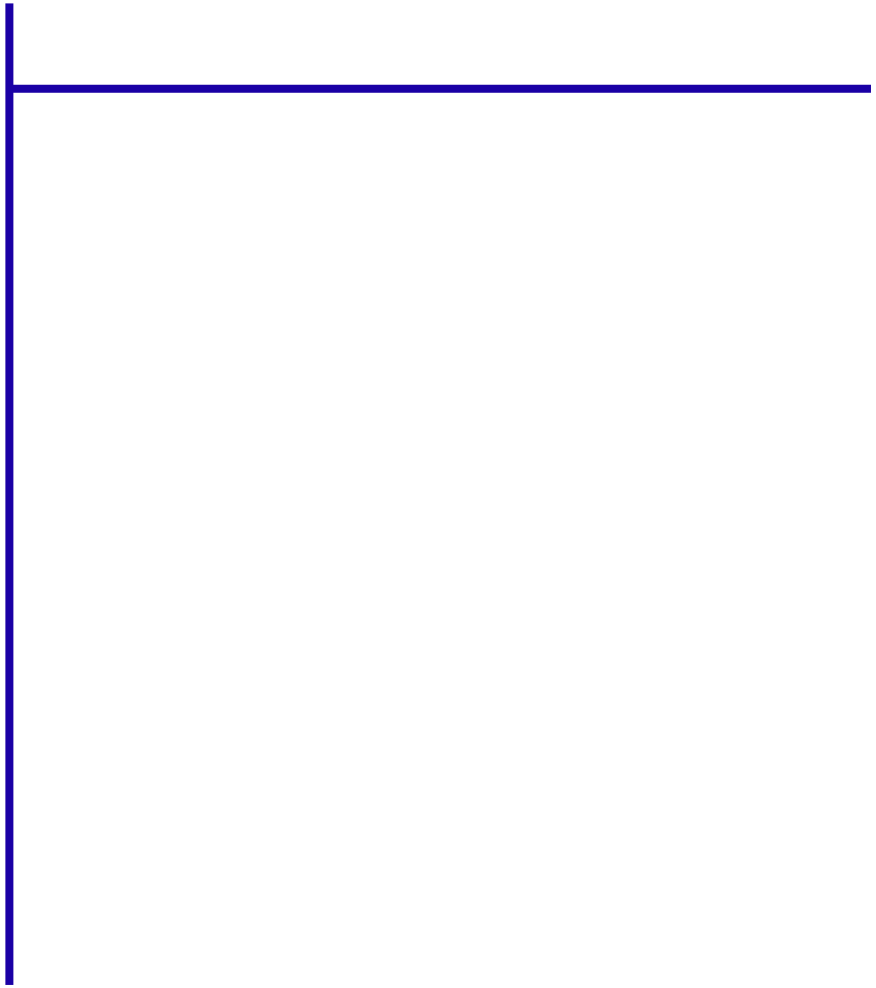
PUC RIO

Criptografia de chave secreta



- mesma chave nas duas direções
  - muitas vezes chamada de segredo compartilhado
- também chamada de criptografia simétrica

confidencialidade



PUC
RIO

integridade/autenticidade

- assinaturas digitais

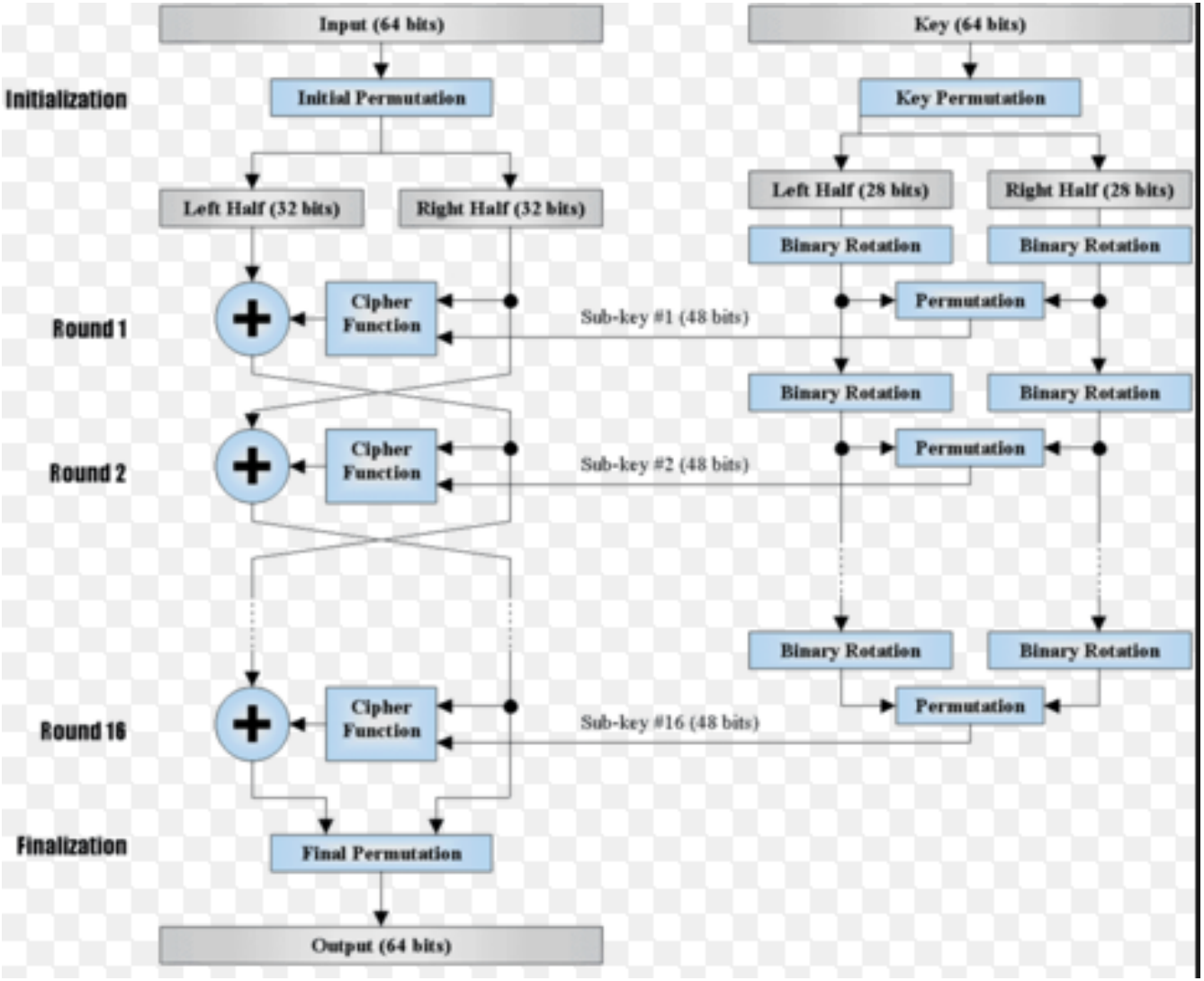
PUC RIO

algoritmos de chave secreta

- técnicas de embaralhamento
- muitas vezes pensados para implementação em hardware

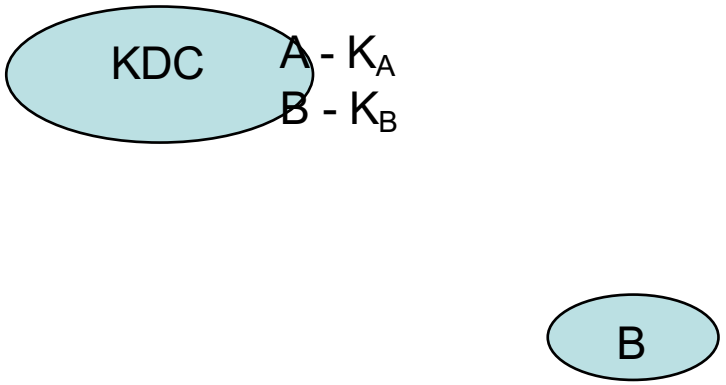
PUC RIO

DES ("deprecated")



Distribuição de chaves secretas

- como fazer para as duas partes compartilharem um segredo?
- uso de *intermediários confiáveis* ou Key Distribution Centers



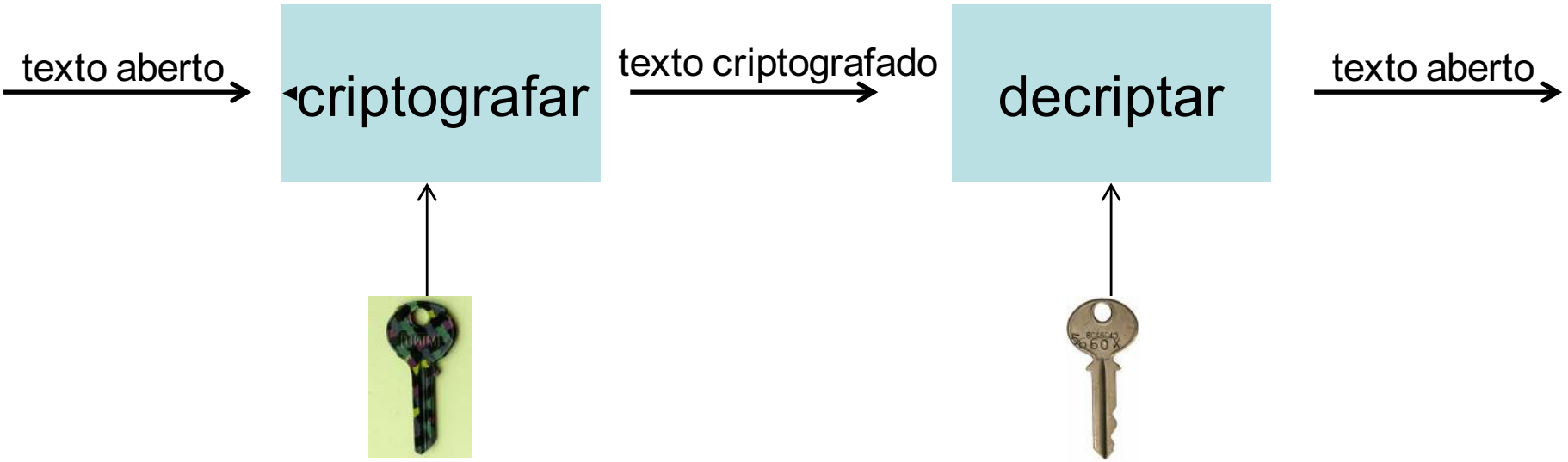
PUC RIO

criptografia assimétrica

- K_{Apriv} chave privada de A
- K_{Apub} chave pública de A

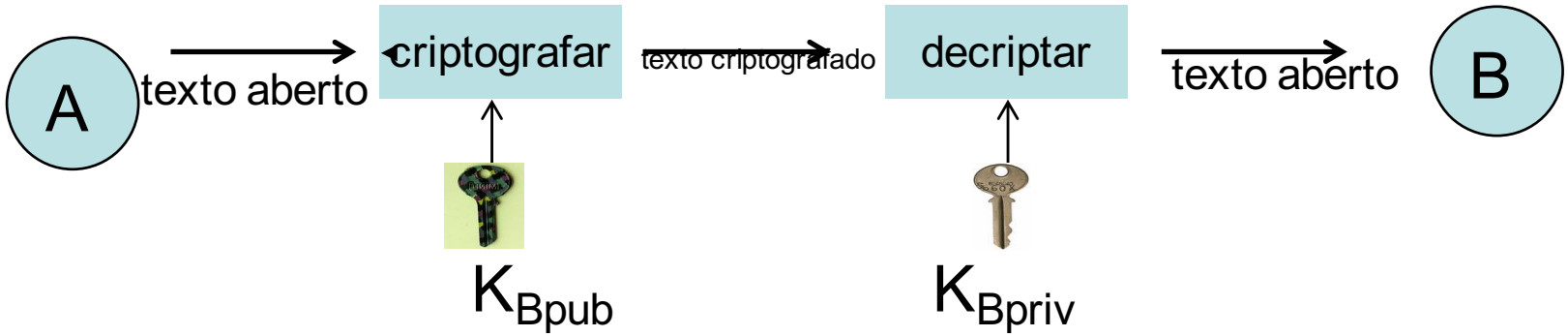
PUC RIO

Criptografia de chave pública e privada



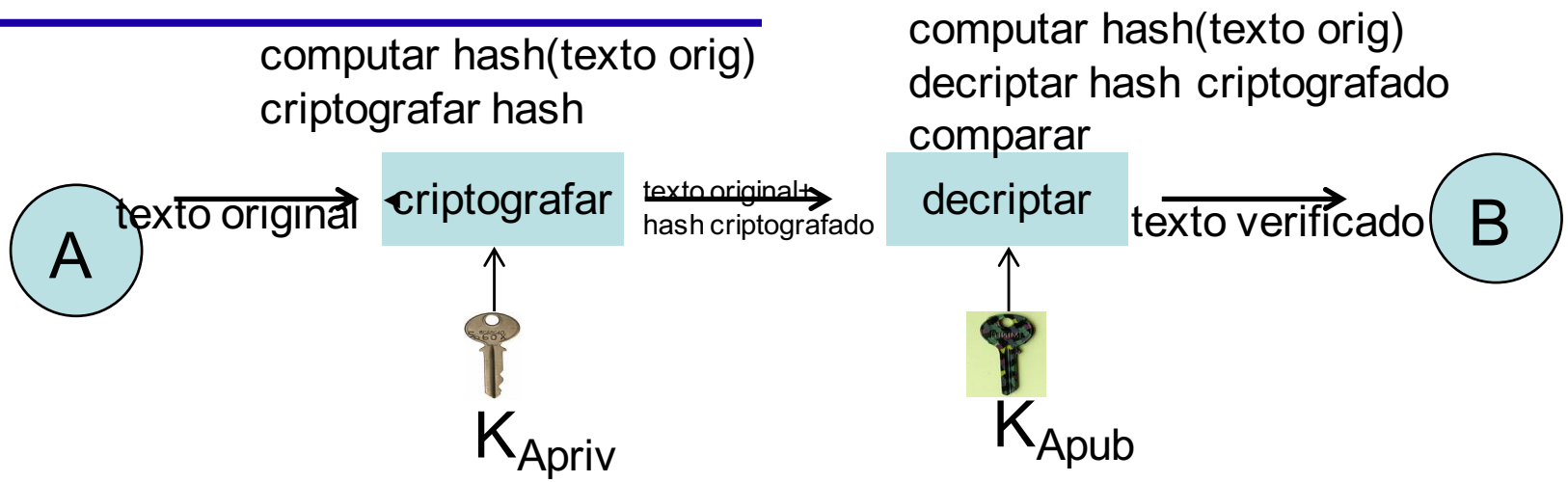
- chaves diferentes em cada direção
  - também chamada de criptografia assimétrica
- uma das chaves pode ser pública sem problemas

criptografia assimétrica



- confidencialidade:
  - A criptografa com chave pública de B

criptografia assimétrica



- autenticação e integridade:
  - A criptografa hash de texto com chave privada de A
    - assinaturas digitais
    - integridade
    - não repudiação

PUC RIO

algoritmos de chave pública e privada

- técnicas aritméticas
  - manipulação de números primos muito grandes
- surgimento do conceito com Diffie-Hellman, em 1976
  - D-H apenas para estabelecimento de segredo compartilhado
- processamento mais custoso que o de algoritmos de chave secreta
  - uso combinado

PUC RIO

Distribuição de chave pública

- intruso ainda pode fazer crer que sua chave pública é a de outra entidade
  - man in the middle

- infraestutrura de distribuição
  - certificados
  - autoridades de certificação
  - infraestruturas de chaves públicas

PUC RIO

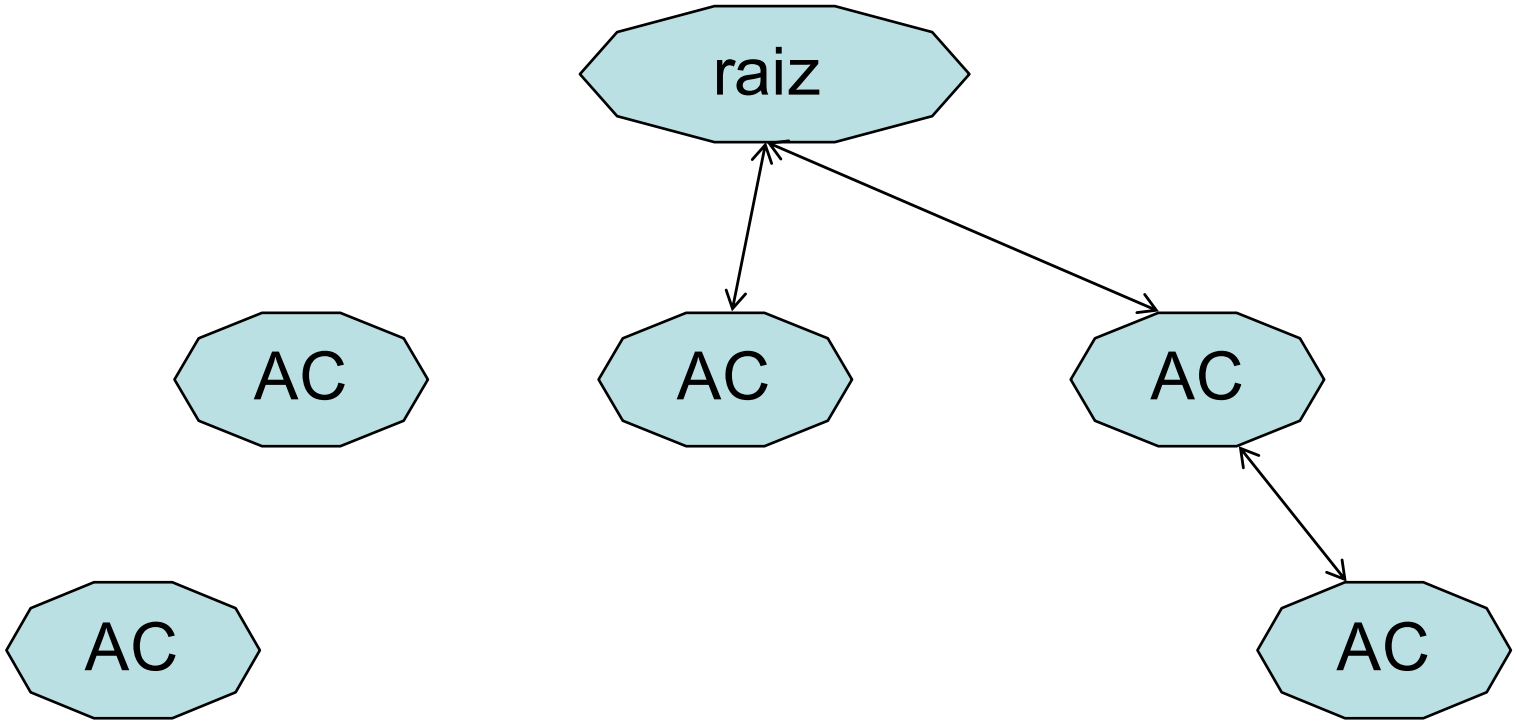
Certificados

issuer
validity
subject
public key info

- padronização X.509

PUC RIO

ICPs – infraestruturas de chaves públicas



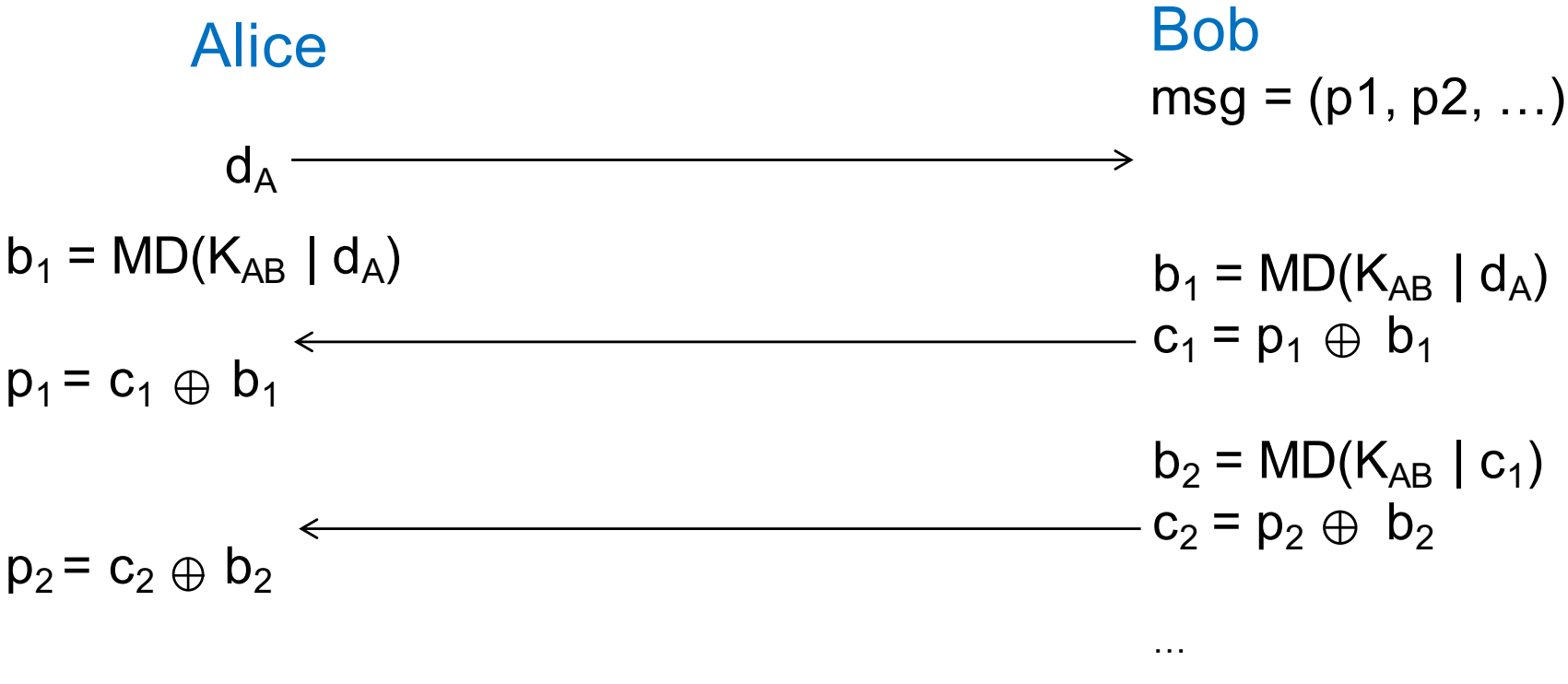
algoritmos de hash

- funções de hash:
  - dado um bloco de dados de tamanho arbitrário, retornam um string de bytes de tamanho fixo
    - entrada: mensagem
    - saída: hash ou digest
  - pequenas alterações nos dados de entrada devem alterar o valor do hash
  - não é possível descobrir a mensagem a partir do hash
  - duas mensagens diferentes dificilmente levam ao mesmo hash

PUC RIO

hash como técnica criptográfica

– em conjunto com segredo compartilhado K_{AB}



PUC RIO

ataques para descoberta de chaves

- Diferentes níveis de dificuldade se atacante dispõe de:
  - apenas texto criptografado
  - pares (texto aberto, texto criptografado)
  - pares escolhidos
- ataques de "força bruta"
  - tentativa de quebra com cada chave possível
  - tamanho de chaves e o "computacionalmente difícil"

PUC RIO

Autenticação

- login e senha
- biometria
- algoritmos de autenticação

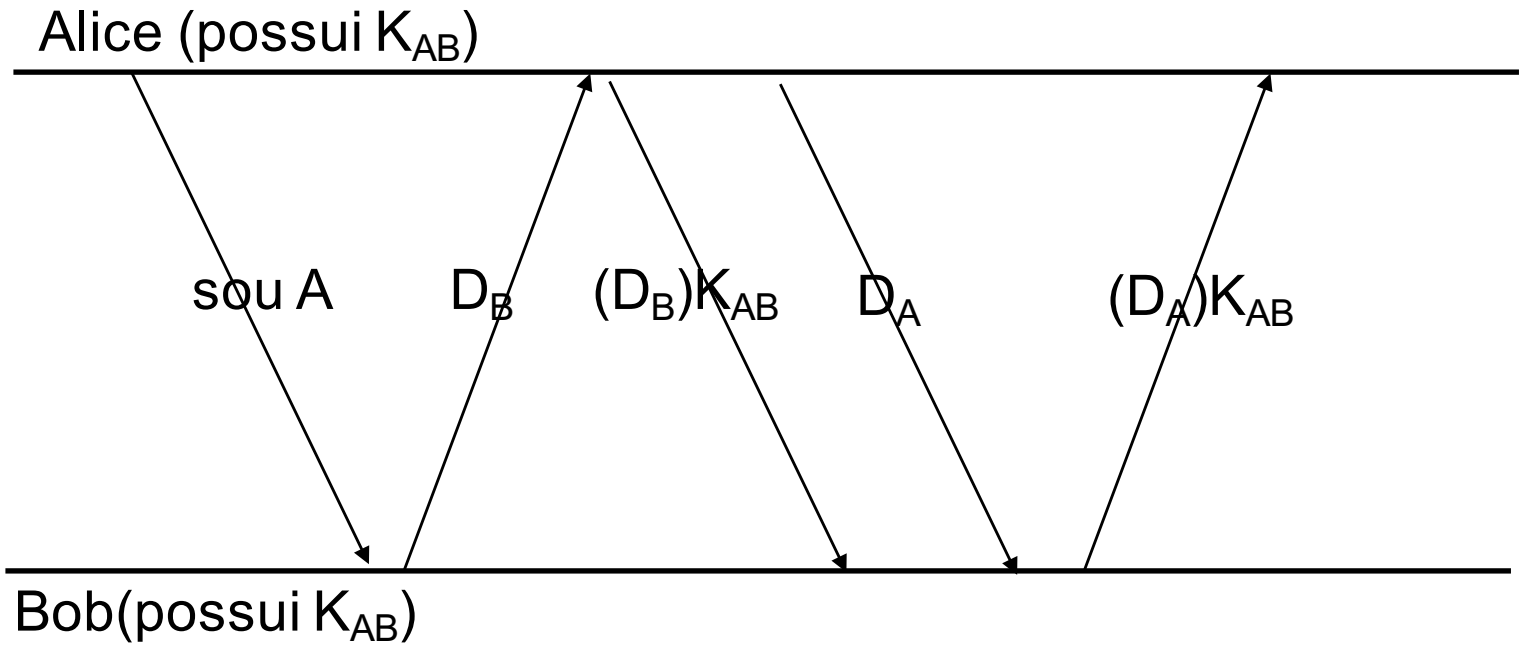
PUC RIO

protocolos de autenticação

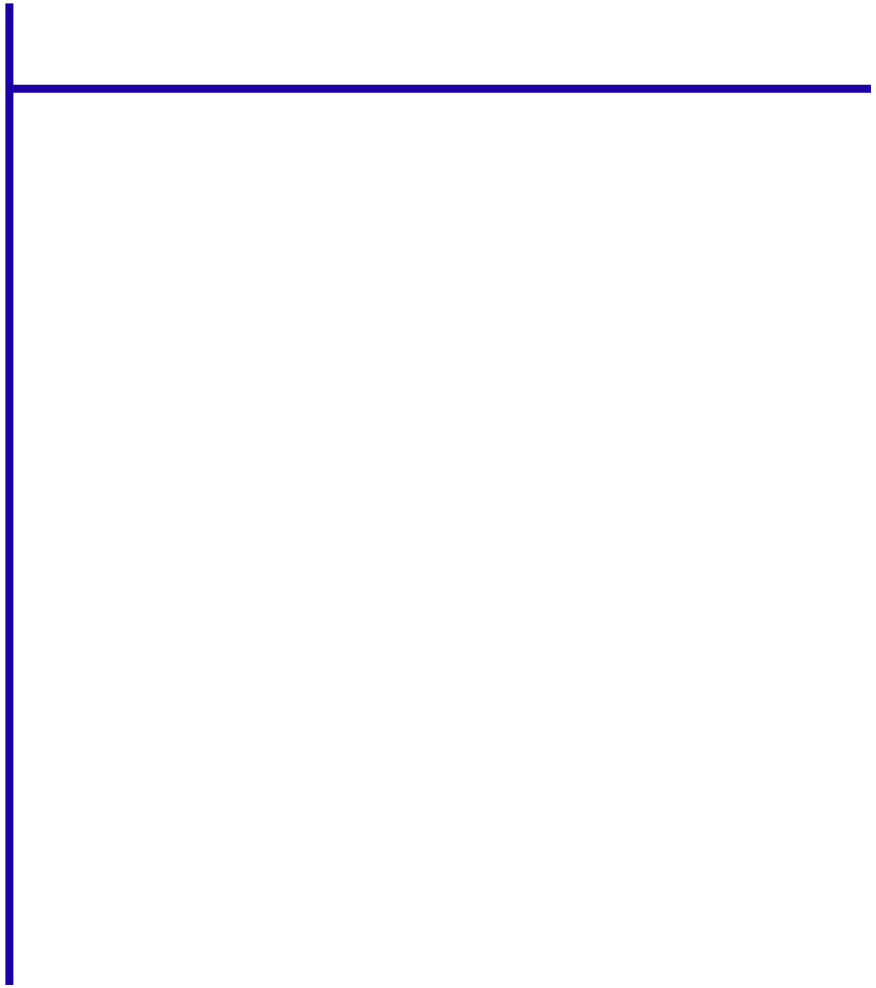
- uso de desafios e criptografia
  - simétrica e assimétrica

PUC RIO

protocolos de autenticação com chave compartilhada

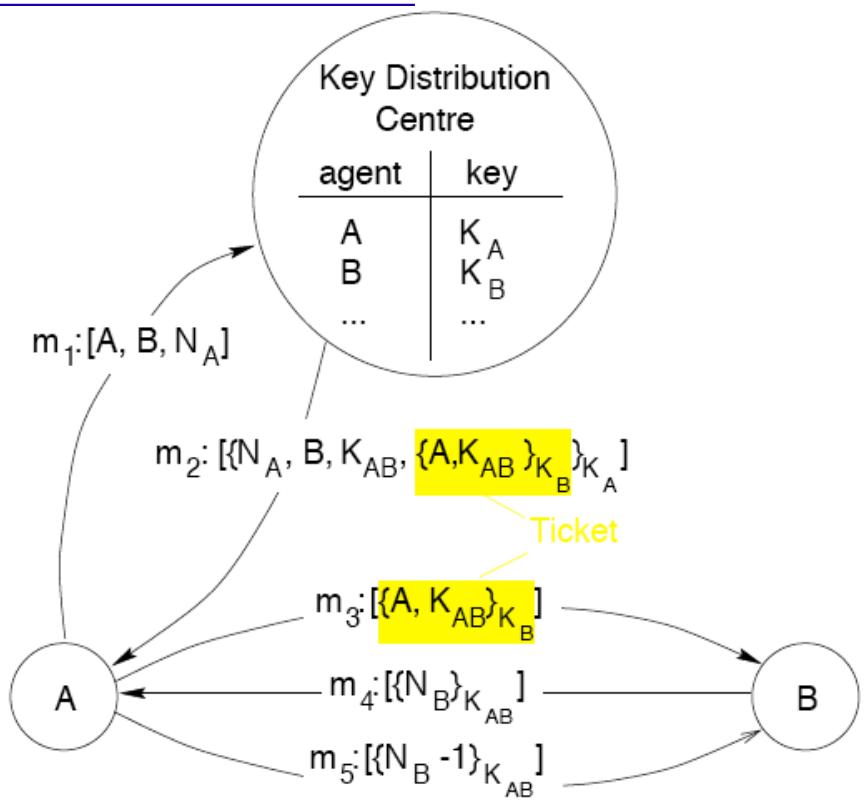


ataques possíveis



PUC RIO

Kerberos



- uso de nonces para evitar ataques de playback

PUC RIO

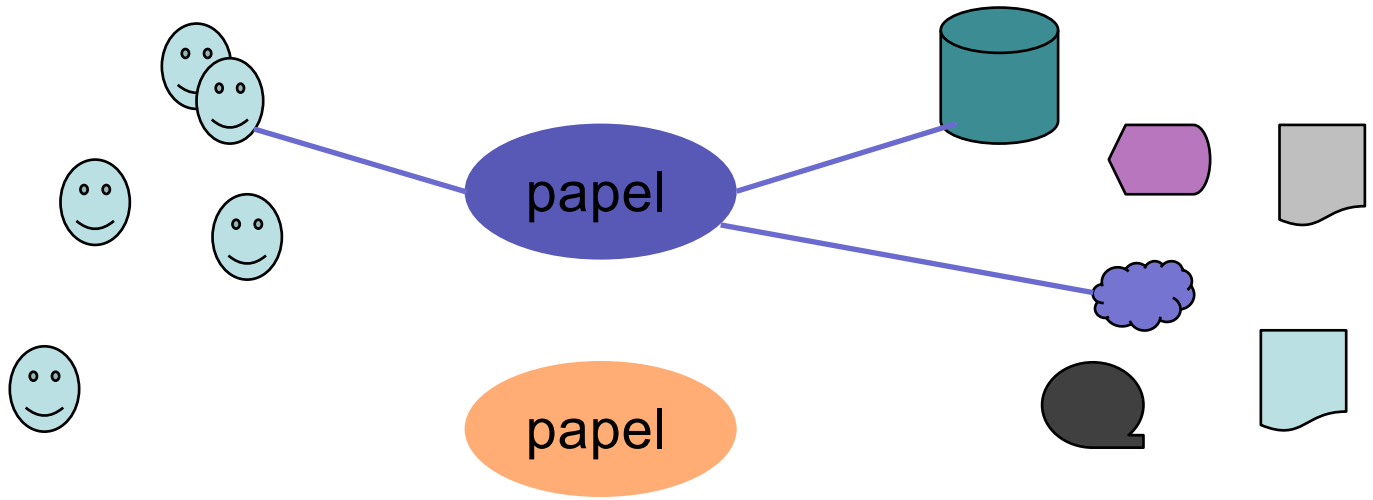
Controle de acesso

- matrizes de acesso
  - usuários X recursos
- normalmente esparsas
- opções:
  - lista de recursos para cada usuário/grupo
  - lista de usuários/grupos para cada recurso

PUC RIO

RBAC

- direitos nem sempre associados a usuários individuais
  - papel do usuário na organização
  - um mesmo usuário pode desempenhar diferentes papéis
    - dinamismo



ABAC

- simplificação de RBAC
  - atributos de usuário utilizados para definir autorizações

PUC RIO

autenticação em sistemas de larga escala

- acesso a serviços em diferentes pontos
  - (administrativos e geográficos)
  - escalabilidade
- cada um deles deve identificar o usuário individualmente?
  - cenários como grades, bibliotecas digitais, etc
  - autenticação e controle de acesso

PUC RIO

soluções clássicas

- cadastro individual de cada usuário em cada serviço
  - ônus para administrador de serviço
    - cadastro de cada usuário e de seus direitos
  - ônus para usuário:
    - senha (ou outra coisa) para cada serviço?
- conta única para todos os usuários de certa instituição
  - ônus para administrador de serviço:
    - não há como fazer auditoria
  - ônus para usuário
    - não há como diferenciar direitos

PUC RIO

delegação

- certificados temporários com atribuição de direitos
- uso frequente em cooperação científica

PUC RIO

sistemas de identidade web

- institucionais – federações
- centrados em usuários

PUC RIO

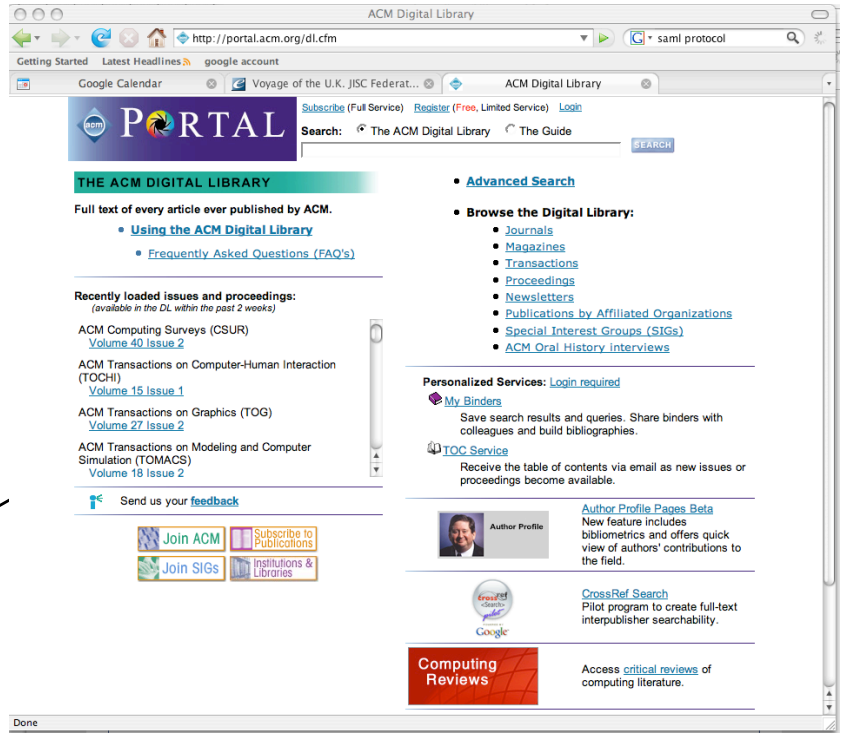
arquiteturas distribuídas

- provedor de serviço:
  - responsável por serviço controlado
- provedor de identidade
  - responsável por autenticação de usuários
- provedor de atributos
  - fornece informações que podem ser usadas pelo controle de acesso

  - rede de confiança entre provedores
  - mtas propostas para aplicações web
  - privacidade!

PUC RIO

exemplos



acesso a editoras online

- reconhecimento de usuários de instituições cadastradas

PUC RIO

exemplos

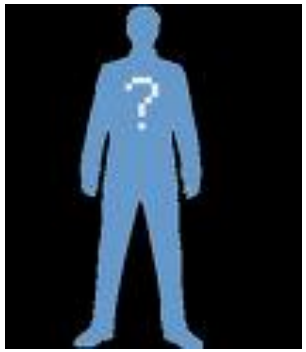
vendas com descontos p/ estudantes

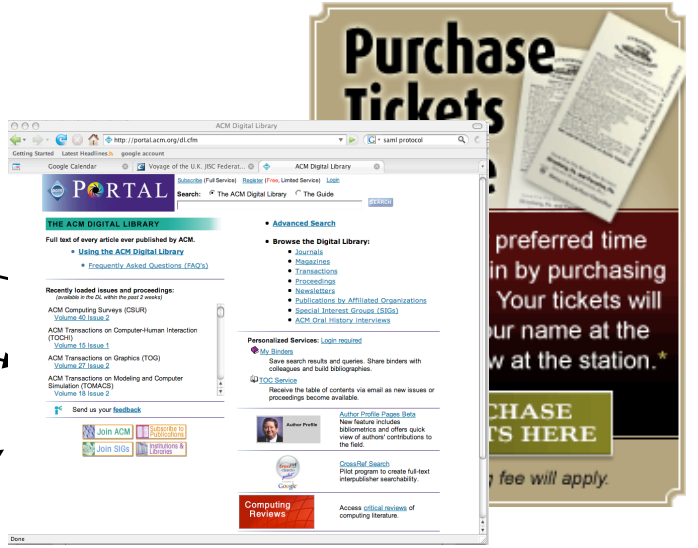
- como saber que usuário é estudante?
- certificado? mas serviço tem que conhecer cada usuário?
  - cert. de atributos

uso de provedores de identidade

- provedores de serviços confiam em algumas fontes de identidade

provedor de identidade

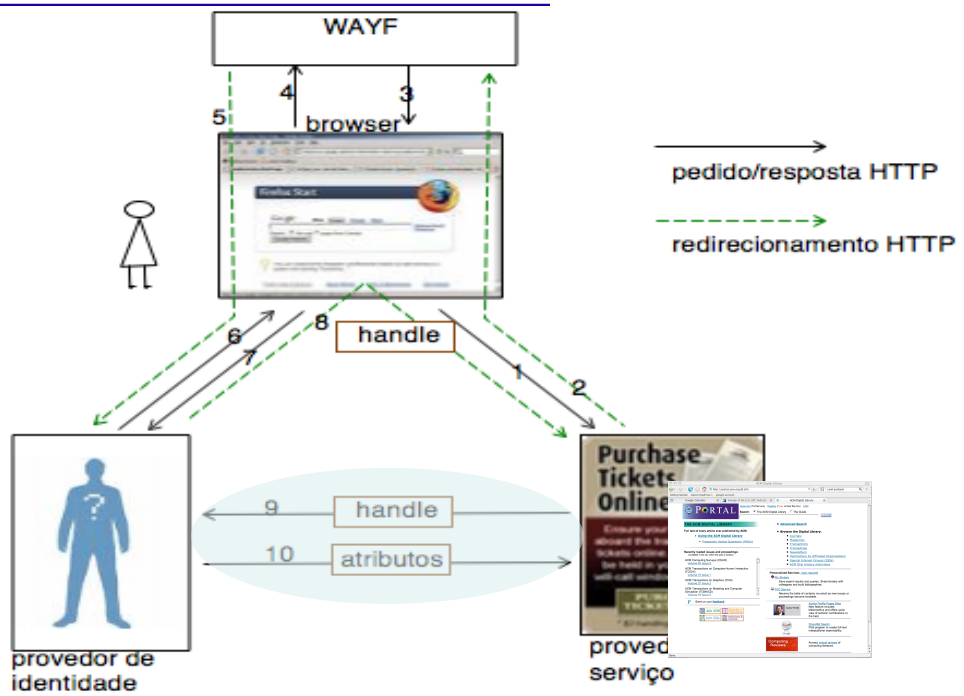




serviço em qualquer lugar

PUC RIO

exemplo: uso de SAML



- assertivas XML com assinatura digital
- conceito de servidor de metadados
- shibboleth: implementação de domínio público bastante difundida

PUC RIO

federações

- privacidade: fornecimento do conjunto mínimo de atributos necessários
- foco em aplicações web
- servidores de metadados mantêm a rede de confiança entre provedores de identidade e de serviço
- acoplamento com projetos de infraestruturas de chaves públicas
- conceito de *single sign-on*

PUC RIO

outros sistemas

- OpenId Connect: OpenId + oauth
  - idéia geral parecida com SAML
  - token JSON assinado por servidor OpenId
  - *back-channel* sempre usado para atributos

PUC RIO

outras questões

- segurança com código móvel
- segurança em dispositivos limitados
- … e muitas outras

PUC RIO

segurança em redes de sensores e atuadores

- tipicamente ignorada
- criptografia
  - pesada computacionalmente
    - uso de chave secreta única?
      - fácil invasão
    - conjunto de chaves S com distribuição aleatória de subconjuntos
- ataques Sybil
  - nó assume diversas ”identidades”
- falsas informações
  - roteamento: anúncios falsos

PUC RIO