Fundamentos de Segurança Informática (FSI)

2021/2022 - LEIC

Manuel Barbosa
mbb@fc.up.pt

Aula 17
Criptografia: Parte 4

O que vimos até agora

- Criptografia simétrica
  - canais seguros e eficientes
  - exigem chaves secretas iguais de ambos os lados
  - chaves secretas confidenciais e autenticas

O que vimos até agora

- Criptografia de chave pública
  - autenticação e não-repúdio com assinaturas digitais
  - confidencialidade com cifras de chave pública
    - usadas para transportar chaves simétricas
  - não exigem chaves partilhadas e confidenciais
  - ainda exigem chaves públicas autênticas (próxima aula)

Cenário Email Seguro

- Pressupostos
  - Alice conhece chave pública de Bob => permite cifrar
  - Bob conhece chave (pública) de verificação de Alice
- Objetivos:
  - mensagem a enviar deve ser confidencial
  - mensagem a enviar deve ser **autêntica** e não-repudiável
- Não objetivos:
  - Alice tem a certeza que Bob recebeu a mensagem e a aceitou

Cenário Email Seguro

- Solução Sign-then-Encrypt:
  - Alice assina mensagem
  - Alice cifra mensagem com chave pública do Bob (cifra híbrida)
- Garante não repúdio, confidencialidade e autenticidade?
  - se mensagem assinada incluir a informação de que Bob era o destinatário => sim!
  - caso contrário, Alice pode ter enviado para Carol que re-cifrou para Bob => não!
- Em geral: cuidado com meta-dados quando se combina cifras com assinaturas

https://theworld.com/~dtd/sign_encrypt/sign_encrypt7.html

Cenário Acordo de Chaves

- Pressupostos
  - Alice conhece chave(s) pública(s) de Bob => permite cifrar e/ou verificar assinaturas
  - Bob conhece chave(s) pública(s) de Alice => permite cifrar e/ou verificar assinaturas
- Objetivos:
  - chave a estabelecer deve ser confidencial
  - chave a estabelecer deve ser autêntica, confirmada
  - perfect forward secrecy: comprometer chaves de longa duração não compromete sessões passadas
- Não objetivos: não repúdio de mensagens

Cenário Acordo de Chaves

- A solução deste problema é crucial para aplicações tipo HTTPS/TLS
- Foram preciso décadas para convergir para uma solução segura e eficiente
- Essa solução:
  - não utiliza cifras de chave pública para transportar chaves simétricas
  - baseia-se no primeiro paper sobre criptografia de chave pública:
    - O protocolo **Diffie-Hellman**
  - Autenticação => assinaturas digitais

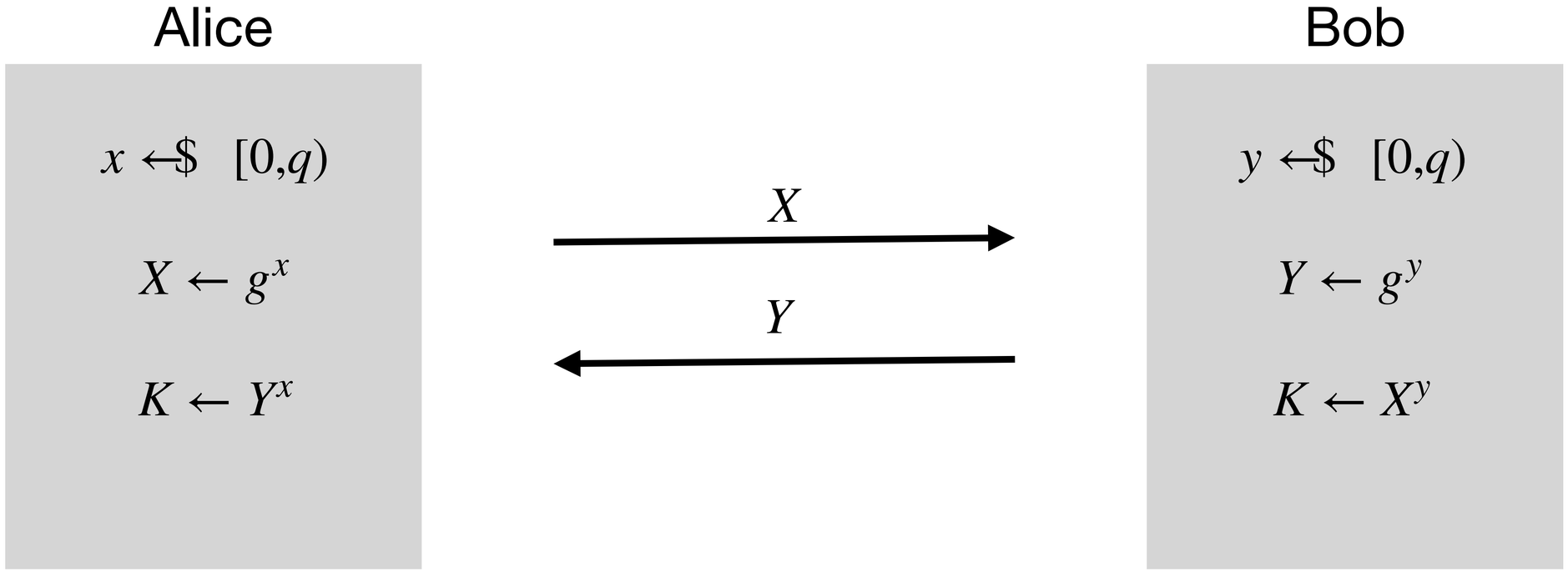
Protocolo Diffie-Hellman

Parâmetros públicos: um grupo finito $(G, g, \circ)$

- Conjunto G:
  - podem ser valores em [0,p), para p um primo grande
  - podem ser pontos núma curva elíptica => utilizado hoje em dia por razões de eficiência
- Operação $\circ$:
  - mapeia dois elementos do conjunto num terceiro, comutativa, associativa, elemento neutro, etc.
- Gerador g => permite codificar um inteiro grande gerado aleatoriamente, de forma irreversível
  - para *e* na gama *0..q-1* (para *q* primo grande), $g^e = g \circ g \ldots \circ g$ produz *q* elementos de *G* diferentes
- Temos $(g^x)^y = g^{xy} = g^{yx} = (g^y)^x$

Protocolo Diffie-Hellman

Parâmetros públicos: um grupo finito $(G, g, \circ)$



$$K = (g^y)^x = g^{yx} = g^{xy} = (g^x)^y = K$$

Protocolo Diffie-Hellman

Parâmetros públicos: um grupo finito $(G, g, \circ)$

Alice

$x \leftarrow\$ [0,q)$

$X \leftarrow g^x$

$K \leftarrow Y^x$

Bob

$y \leftarrow\$ [0,q)$

$Y \leftarrow g^y$

$K \leftarrow X^y$

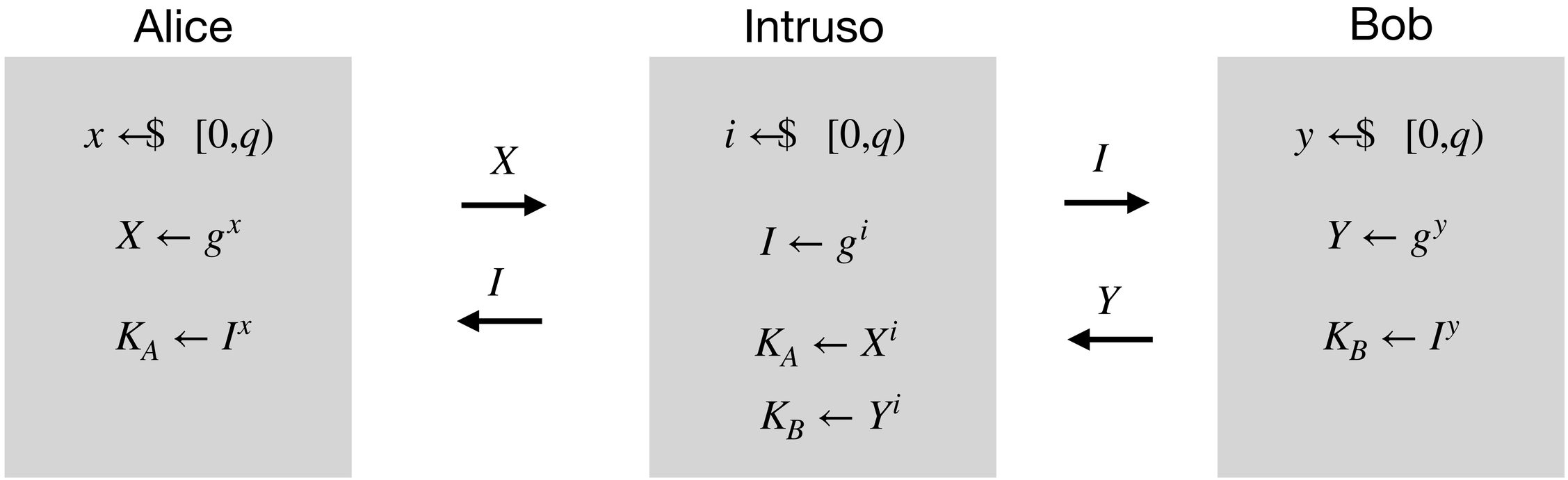
X

Y

Anónimo

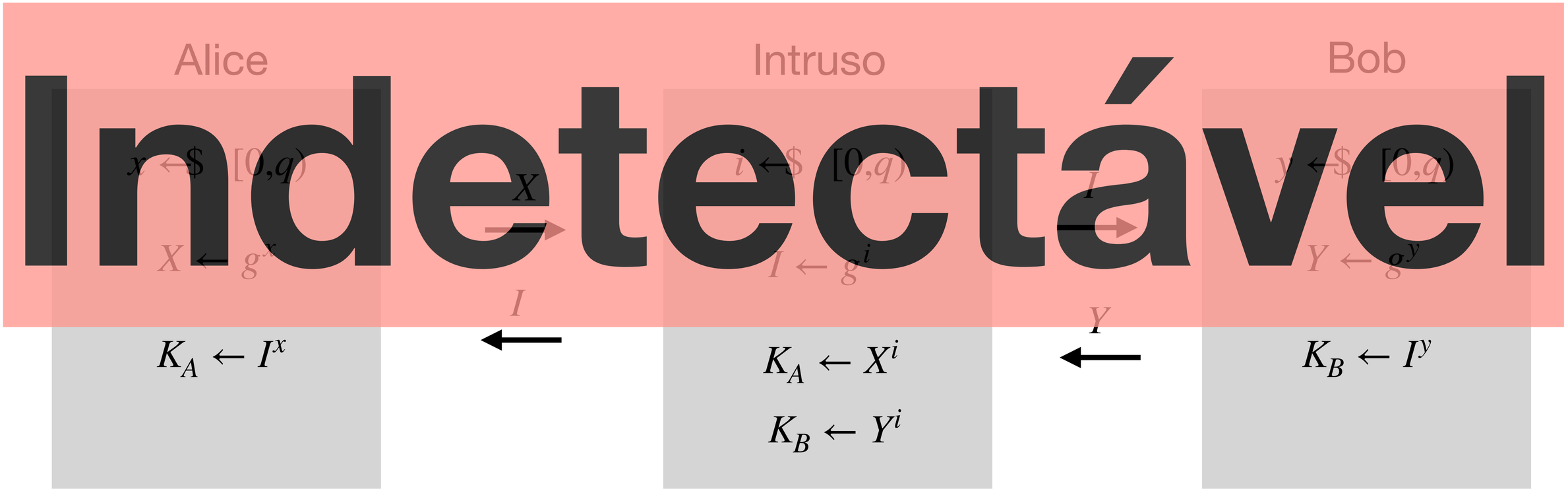
Man-in-the-Middle Attack

Parâmetros públicos: um grupo finito $(G, g, \circ)$



Man-in-the-Middle Attack

Parâmetros públicos: um grupo finito $(G, g, \circ)$



Indetectável

Man-in-the-Middle Attack

- Os ataques Man-in-the-Middle são possíveis sempre que:
  - utilizamos parâmetros públicos trocados na rede
  - sem sabermos a sua origem
- Isto aplica-se a:
  - chaves públicas de assinatura e/ou cifras
  - parâmetros públicos Diffie-Hellman
  - qualquer mensagem

Protocolo Diffie-Hellman Autenticado

Parâmetros públicos: um grupo finito $(G, g, \circ)$

Alice (sk_A, vk_B)

$x \leftarrow\$ \quad [0,q)$

$X \leftarrow g^x$

$K \leftarrow Y^x$

Bob (sk_B, vk_A)

$y \leftarrow\$ \quad [0,q)$

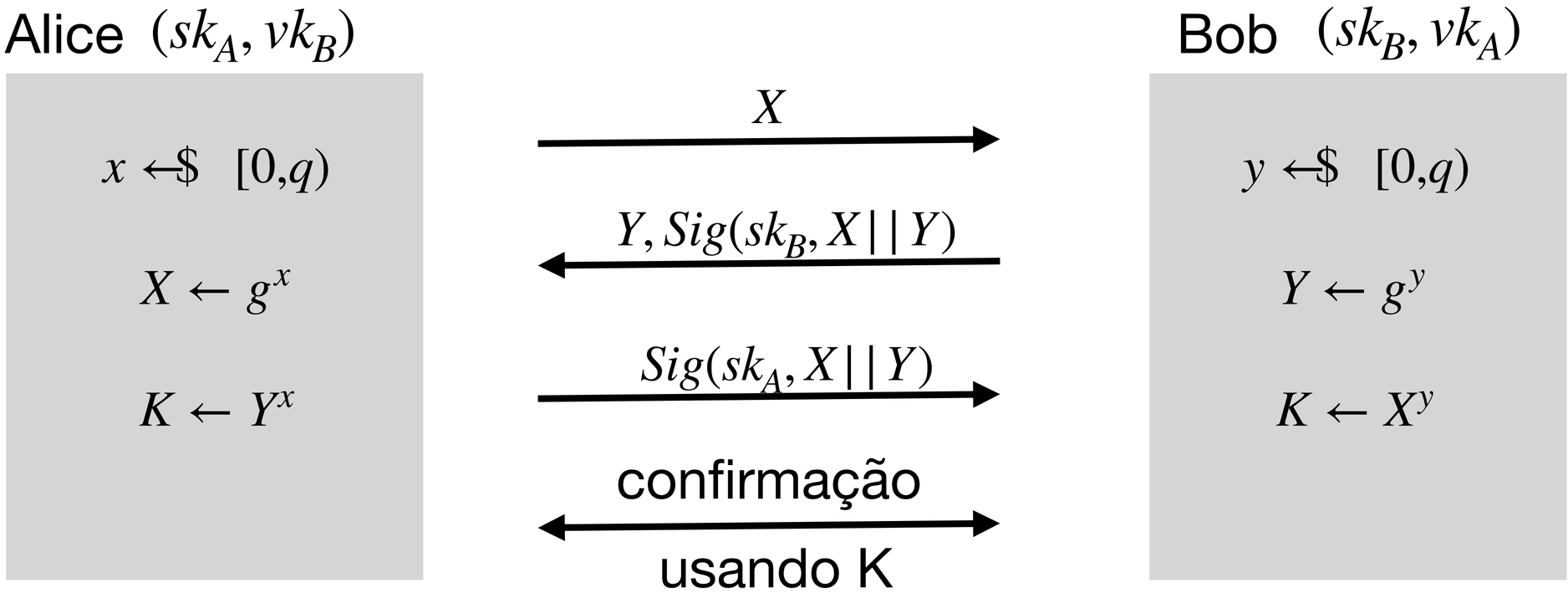
$Y \leftarrow g^y$

$K \leftarrow X^y$

Parâmetros públicos adicionais: chaves autenticadas de verificação de assinaturas

Protocolo Diffie-Hellman Autenticado

Parâmetros públicos: um grupo finito $(G, g, \circ)$



Parâmetros públicos adicionais: chaves autenticadas de verificação de assinaturas

Estabelecimento de Canais Seguros

- O estabelecimento de canais seguros na prática obriga a:
  - autenticação de chaves públicas => protegem acordo de chaves
  - protocolo de acordo de chaves
    - propaga autenticidade de chaves públicas para chave simétrica
    - protege chave simétrica quanto a confidencialidade
    - mesmo que chaves de assinatura sejam comprometidas no futuro!
  - tecnologia simétrica (AEAD) para troca eficiente de informação com garantias de confidencialidade e autenticidade

Estabelecimento de Canais Seguros

- Desenhar um protocolo completo é extremamente difícil
  - mesmo que os componentes individuais sejam seguros
  - a forma como são compostos pode não o ser
- O TLS 1.3 resulta de 30 anos de evolução (e ainda não é perfeito)
- Ainda estão por resolver desafios importantes:
  - por exemplo: anonimato

Autenticação de chaves públicas

- Problema
  - Alice envia mensagem assinada digitalmente a Bob
  - Como é que o Bob obtém a chave de verificação da Alice? Ou …
  - Dado *vk*, como é que o Bob tem a certeza que *vk* corresponde a uma chave privada que é apenas conhecida pela Alice?
- Veremos a solução mais utilizada:
  - Public Key Infrastructure