Introdução à criptografia Assimétrica

Auditoria e Segurança de SI

Prof. Roberto Cabral
rbcabral@ufc.br

Universidade Federal do Ceará

1º semestre/2023

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Introdução à criptografia assimétrica

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Criptografia de chave pública ou criptografia assimétrica?

Introdução à criptografia assimétrica

- Criptografia de chave pública ou criptografia assimétrica?
- A criptografia simétrica foi usada por pelo menos 4000 anos.

Introdução à criptografia assimétrica

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Criptografia de chave pública ou criptografia assimétrica?
- A criptografia simétrica foi usada por pelo menos 4000 anos.
- Criptografia assimétrica é bastante nova!

Introdução à criptografia assimétrica

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

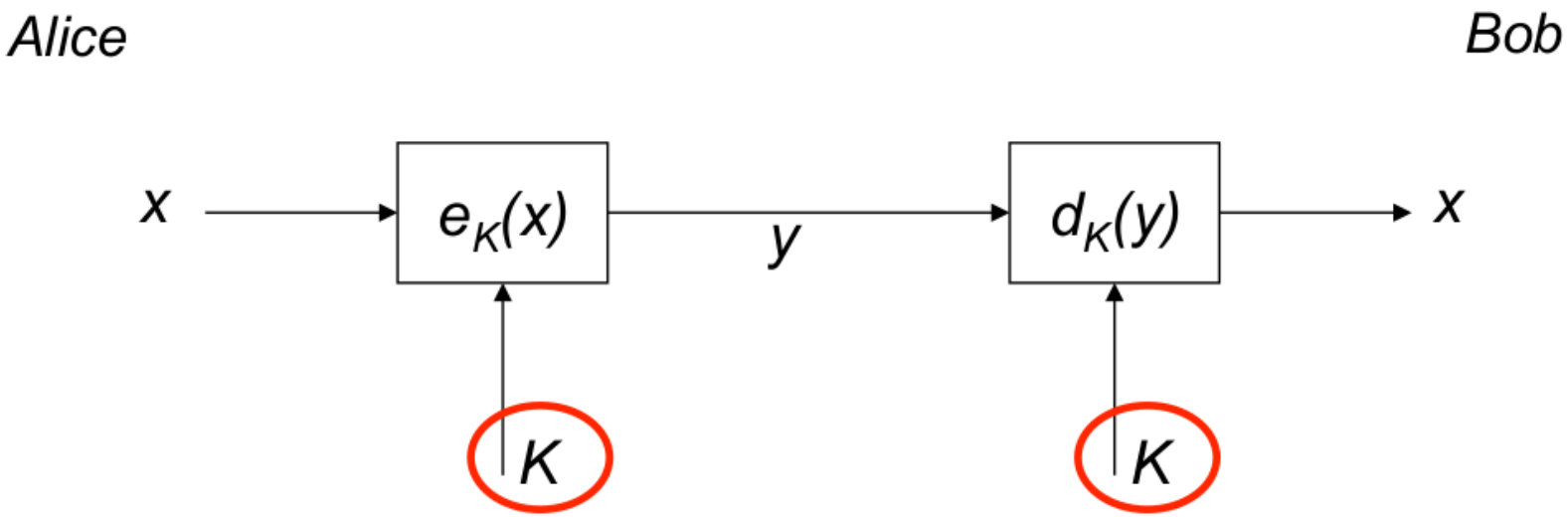
- Criptografia de chave pública ou criptografia assimétrica?
- A criptografia simétrica foi usada por pelo menos 4000 anos.
- Criptografia assimétrica é bastante nova!
  - Foi introduzida pela primeira vez em 1976 por Diffie, Hellman e Merkle.

Introdução à criptografia assimétrica

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

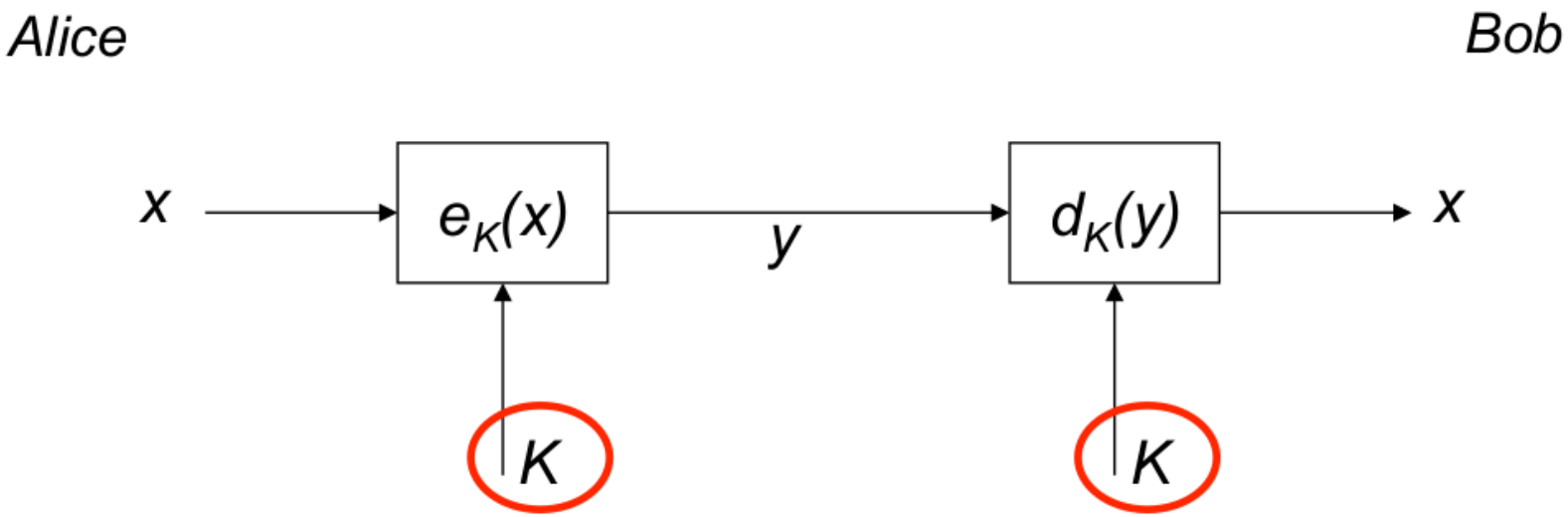
- Criptografia de chave pública ou criptografia assimétrica?
- A criptografia simétrica foi usada por pelo menos 4000 anos.
- Criptografia assimétrica é bastante nova!
  - Foi introduzida pela primeira vez em 1976 por Diffie, Hellman e Merkle.
- A maioria dos algoritmos assimétricos são baseados na teoria dos números!

Criptografia simétrica



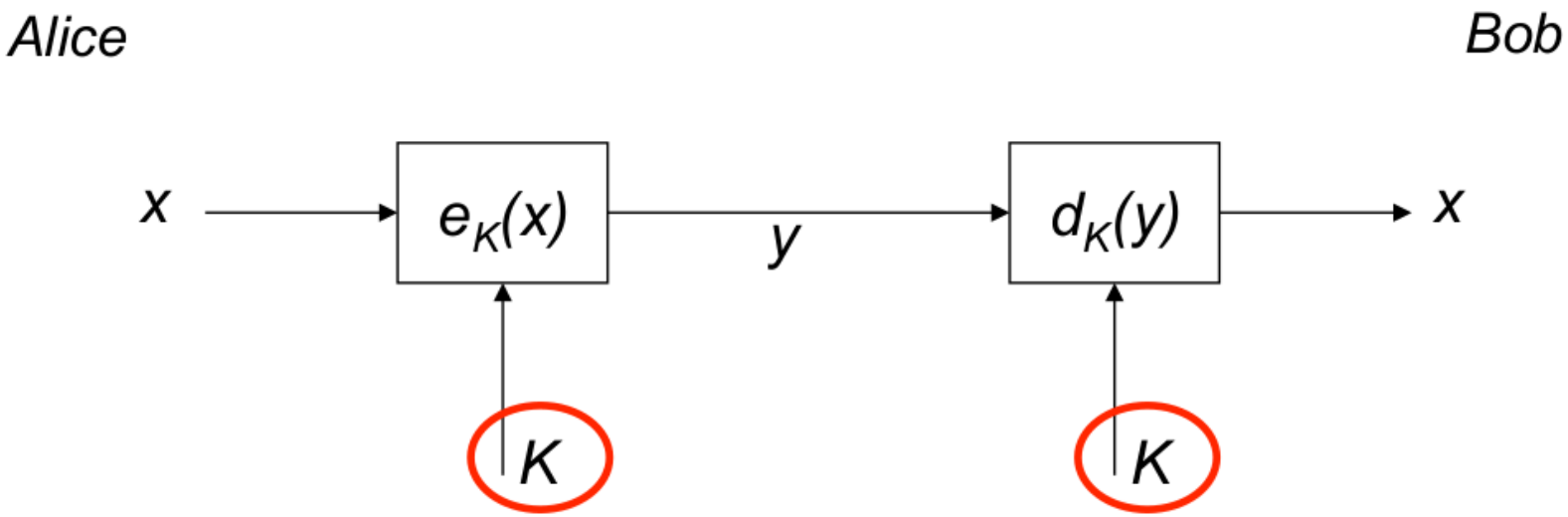
Criptografia simétrica

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ



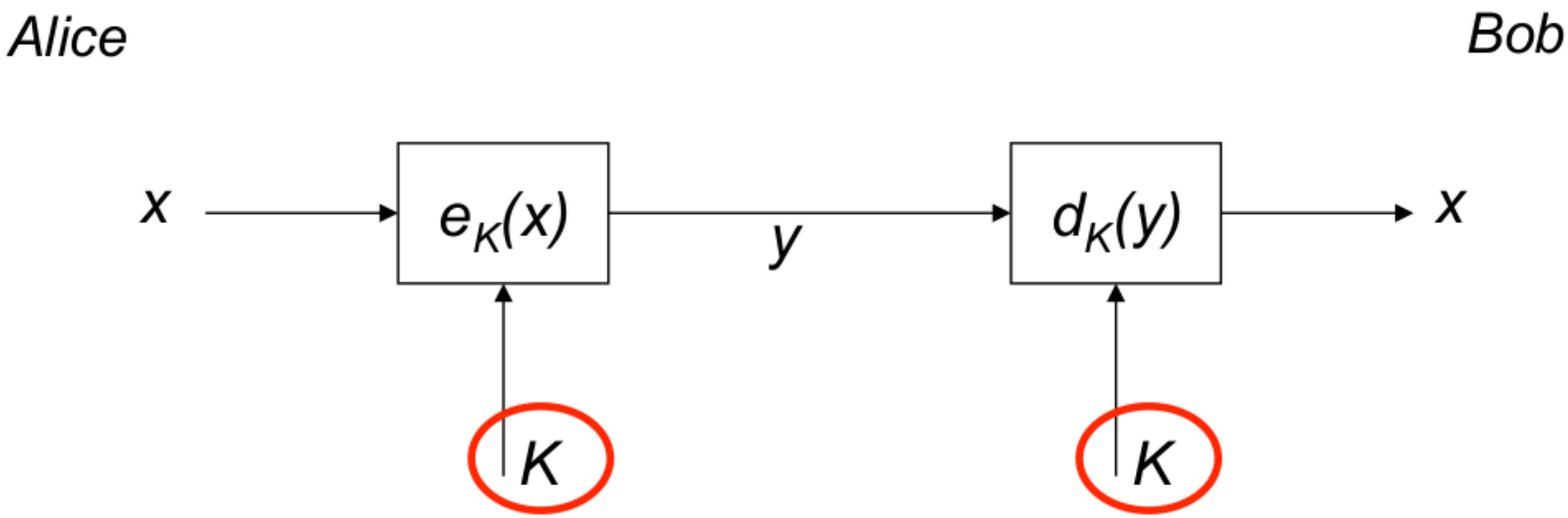
- Duas propriedades de criptossistemas simétricos:

Criptografia simétrica



- Duas propriedades de criptossistemas simétricos:
  - A mesma chave é usada na encriptação e decriptação.

Criptografia simétrica



- Duas propriedades de criptossistemas simétricos:
  - A mesma chave é usada na encriptação e decriptação.
  - As funções de encriptação e decriptação são muito similares (ou até mesmo idênticas).

Criptografia simétrica

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Criptografia simétrica

- Seguro como um cofre, só Alice e Bob têm uma cópia da chave

Criptografia simétrica

- Seguro como um cofre, só Alice e Bob têm uma cópia da chave
  - Encriptação da Alice: “bloqueia” a mensagem no cofre com sua chave.

Criptografia simétrica

- Seguro como um cofre, só Alice e Bob têm uma cópia da chave
  - Encriptação da Alice: "bloqueia" a mensagem no cofre com sua chave.
  - Decriptação de Bob: usa sua chave para abrir o cobre.

Criptografia simétrica: falhas

- Algoritmos simétricos, como AES ou 3DES, são muito seguros e rápidos, **mas**.

Criptografia simétrica: falhas

- Algoritmos simétricos, como AES ou 3DES, são muito seguros e rápidos, **mas**.
- Problema da distribuição de chaves: a chave secreta deve ser transportada de forma segura.

Criptografia simétrica: falhas

- Algoritmos simétricos, como AES ou 3DES, são muito seguros e rápidos, **mas**.
- Problema da distribuição de chaves: a chave secreta deve ser transportada de forma segura.
- Número de chaves: em uma rede, cada par de usuários deve possuir uma chave individual.

Criptografia simétrica: falhas

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Algoritmos simétricos, como AES ou 3DES, são muito seguros e rápidos, **mas**.
- Problema da distribuição de chaves: a chave secreta deve ser transportada de forma segura.
- Número de chaves: em uma rede, cada par de usuários deve possuir uma chave individual.
  - Seja n o número de usuários da rede, são necessárias $\frac{n*(n-1)}{2}$ chaves, cada usuário deve manter $n-1$ chaves.

Criptografia simétrica: falhas

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Algoritmos simétricos, como AES ou 3DES, são muito seguros e rápidos, **mas**.
- Problema da distribuição de chaves: a chave secreta deve ser transportada de forma segura.
- Número de chaves: em uma rede, cada par de usuários deve possuir uma chave individual.
  - Seja n o número de usuários da rede, são necessárias $\frac{n*(n-1)}{2}$ chaves, cada usuário deve manter $n-1$ chaves.
- Alice ou Bob podem trapacear o outro, pois eles possuem a mesma chave.

Criptografia simétrica: falhas

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Algoritmos simétricos, como AES ou 3DES, são muito seguros e rápidos, **mas**.
- Problema da distribuição de chaves: a chave secreta deve ser transportada de forma segura.
- Número de chaves: em uma rede, cada par de usuários deve possuir uma chave individual.
  - Seja n o número de usuários da rede, são necessárias $\frac{n*(n-1)}{2}$ chaves, cada usuário deve manter $n-1$ chaves.
- Alice ou Bob podem trapacear o outro, pois eles possuem a mesma chave.
  - Exemplo: Alice pode afirmar que nunca pediu uma TV online de Bob (ele poderia ter fabricado seu pedido). Para evitar isso: "não repúdio".

Exemplo

Ideia por trás da criptografia assimétrica

New Idea:

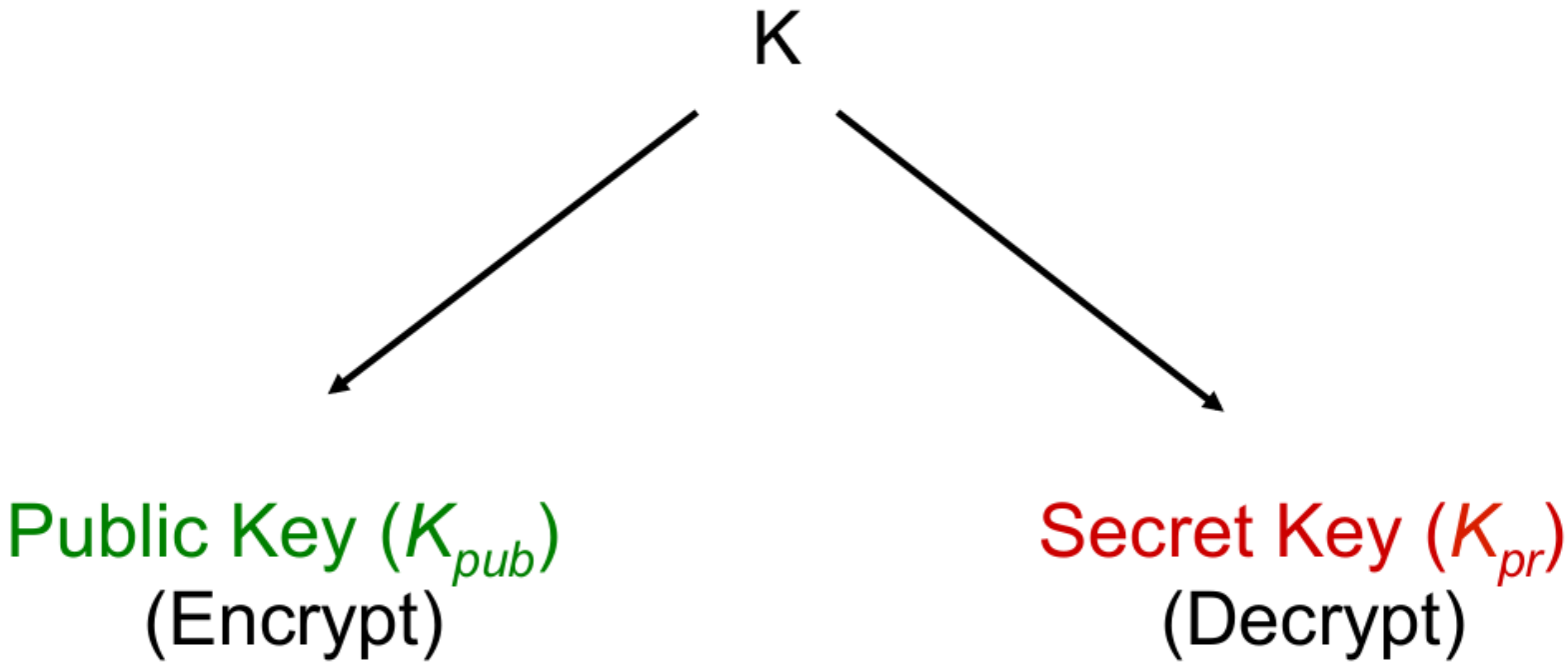
Use the "good old mailbox" principle:

Everyone can drop a letter

But: Only the owner has the correct key to open the box

Criptografia assimétrica

- Principio: "dividir" a chave



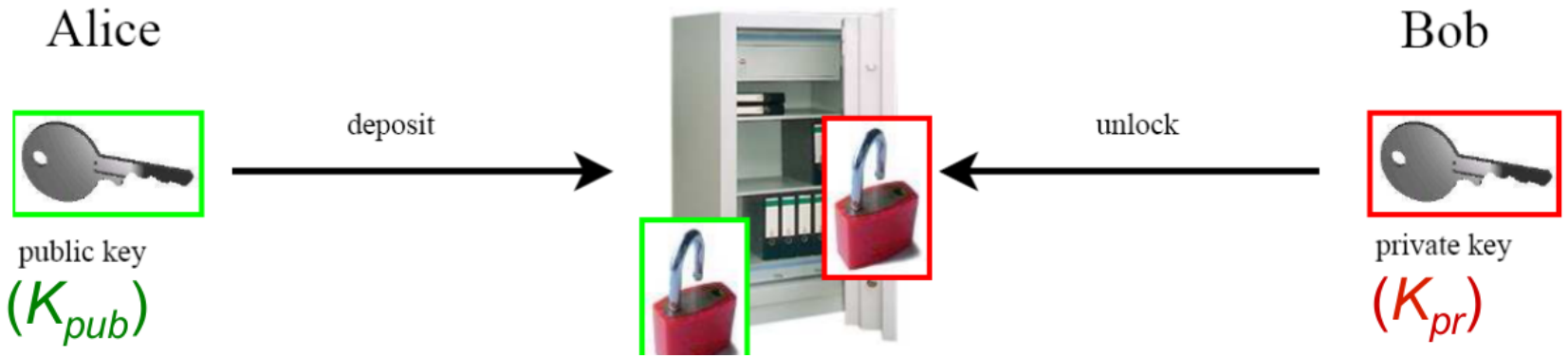
- Durante a geração de chaves, um par k_{pub} e k_{pr} é computado.

Criptografia assimétrica: analogia

- Um cofre que possui uma chave pública (para depositar) e uma privada (para resgatar).

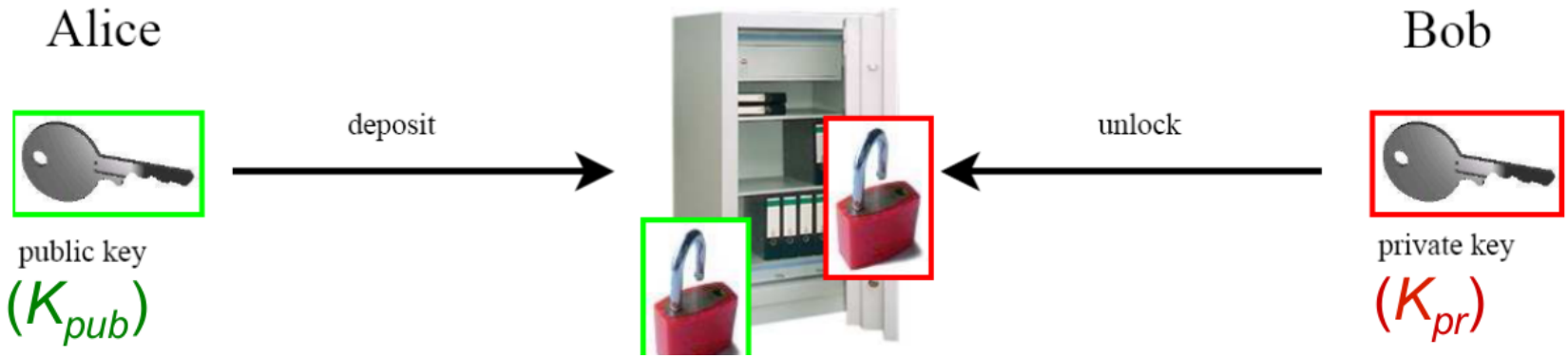
Criptografia assimétrica: analogia

- Um cofre que possui uma chave pública (para depositar) e uma privada (para resgatar).



Criptografia assimétrica: analogia

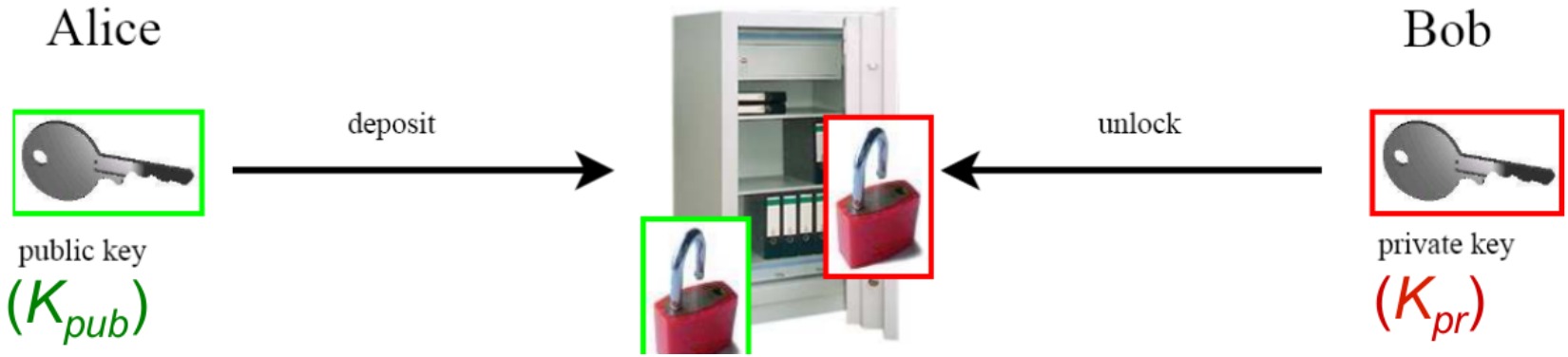
- Um cofre que possui uma chave pública (para depositar) e uma privada (para resgatar).



  - Alice deposita (encripta) uma mensagem usando a - não secreta - chave pública k_{pub}.

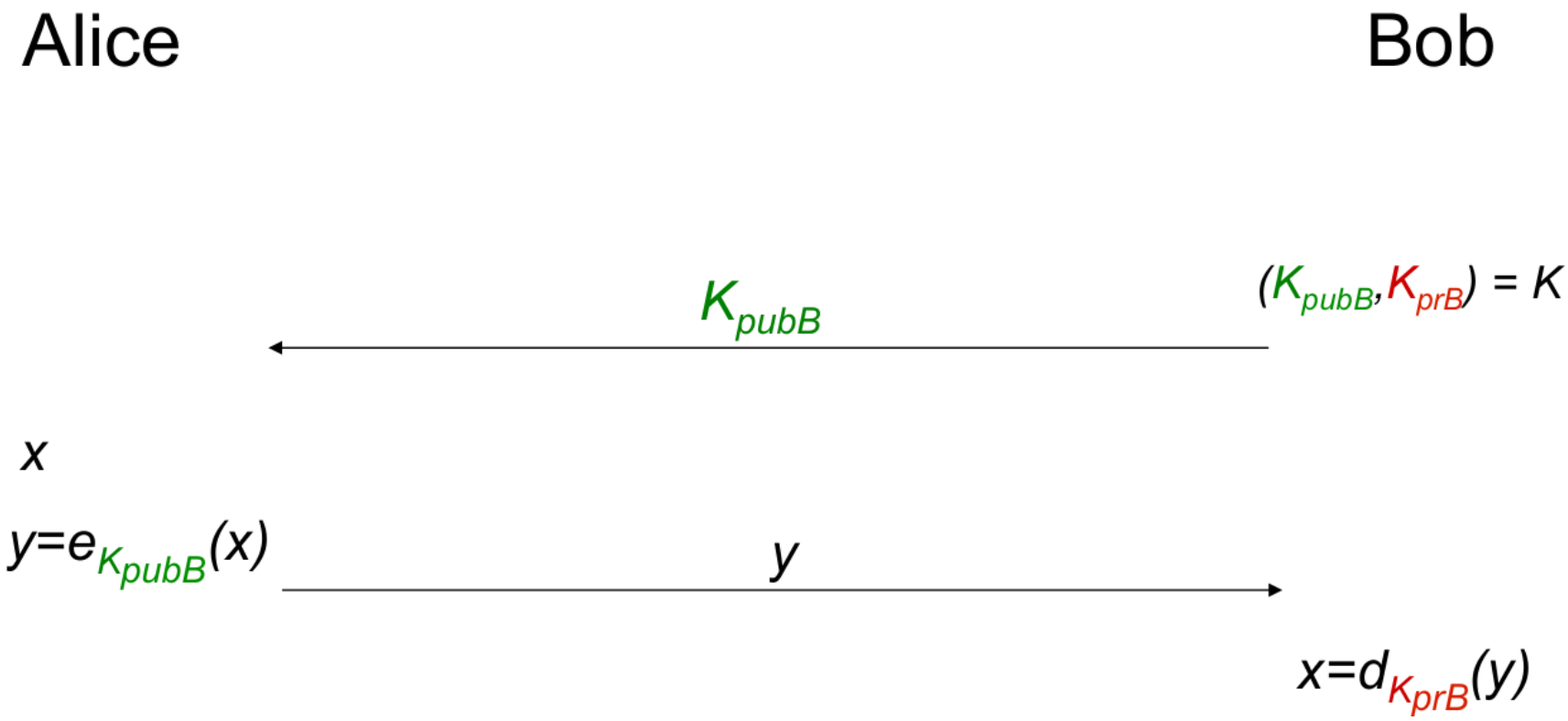
Criptografia assimétrica: analogia

- Um cofre que possui uma chave pública (para depositar) e uma privada (para resgatar).

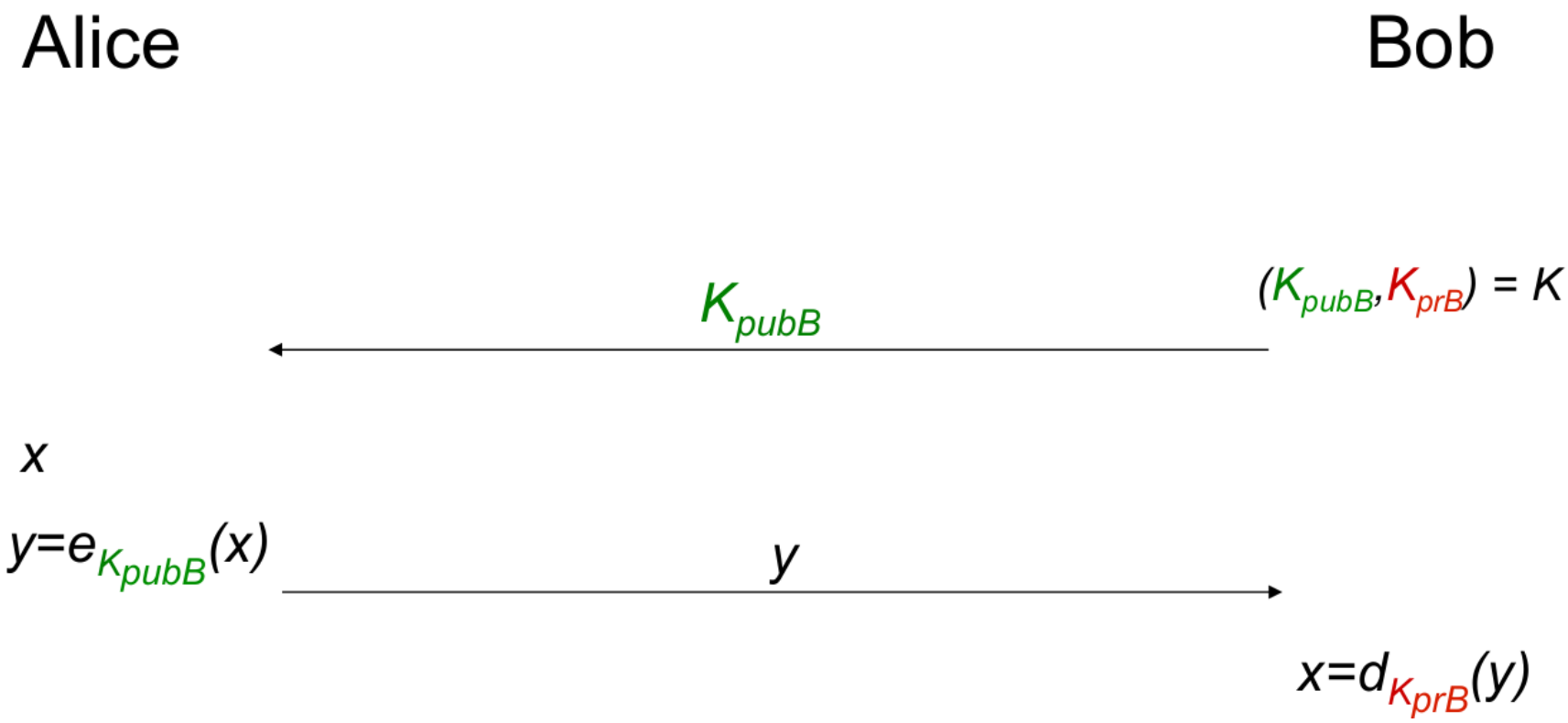


  - Alice deposita (encripta) uma mensagem usando a - não secreta - chave pública k_{pub}.
  - Apenas Bob possui a - secreta - chave privada k_{pr} para reaver (decriptar) a mensagem.

Protocolo básico para encriptação usando criptografia assimétrica



Protocolo básico para encriptação usando criptografia assimétrica



- Problema de distribuição de chaves resolvido*

Mecanismos de segurança com criptografia assimétrica

- O que pode ser realizado usando criptografia assimétrica?

Mecanismos de segurança com criptografia assimétrica

- O que pode ser realizado usando criptografia assimétrica?
  - **Distribuição de chaves:** distribuição das chaves sem segredo pré-compartilhado (Diffie-Helman key exchange, RSA).

Mecanismos de segurança com criptografia assimétrica

- O que pode ser realizado usando criptografia assimétrica?
  - **Distribuição de chaves:** distribuição das chaves sem segredo pré-compartilhado (Diffie-Helman key exchange, RSA).
  - **Não repúdio e assinatura digital:** prover a integridade das mensagens (RSA, DSA, ECDSA).

Mecanismos de segurança com criptografia assimétrica

- O que pode ser realizado usando criptografia assimétrica?
  - **Distribuição de chaves:** distribuição das chaves sem segredo pré-compartilhado (Diffie-Helman key exchange, RSA).
  - **Não repúdio e assinatura digital:** prover a integridade das mensagens (RSA, DSA, ECDSA).
  - **Identificação,** usando protocolos de resposta de desafio com assinaturas digitais.

Mecanismos de segurança com criptografia assimétrica

- O que pode ser realizado usando criptografia assimétrica?
  - **Distribuição de chaves:** distribuição das chaves sem segredo pré-compartilhado (Diffie-Helman key exchange, RSA).
  - **Não repúdio e assinatura digital:** prover a integridade das mensagens (RSA, DSA, ECDSA).
  - **Identificação,** usando protocolos de resposta de desafio com assinaturas digitais.
  - **Encriptação** (RSA, Elgamal).

Mecanismos de segurança com criptografia assimétrica

- O que pode ser realizado usando criptografia assimétrica?
  - **Distribuição de chaves:** distribuição das chaves sem segredo pré-compartilhado (Diffie-Helman key exchange, RSA).
  - **Não repúdio e assinatura digital:** prover a integridade das mensagens (RSA, DSA, ECDSA).
  - **Identificação,** usando protocolos de resposta de desafio com assinaturas digitais.
  - **Encriptação** (RSA, Elgamal).
    - Desvantagem: ineficiente computacionalmente! (1000 vezes mais lento que algoritmos simétricos.)

Protocolo básico de transporte de chaves

- Na prática, usa-se sistemas híbridos. Isto é, uma junção entre a algoritmos simétricos e assimétricos.

Protocolo básico de transporte de chaves

- Na prática, usa-se sistemas híbridos. Isto é, uma junção entre a algoritmos simétricos e assimétricos.
  - **Estabelecimento de chaves** (para esquemas simétricos) e **assinatura digital** são computados com algoritmos assimétricos (lentos).

Protocolo básico de transporte de chaves

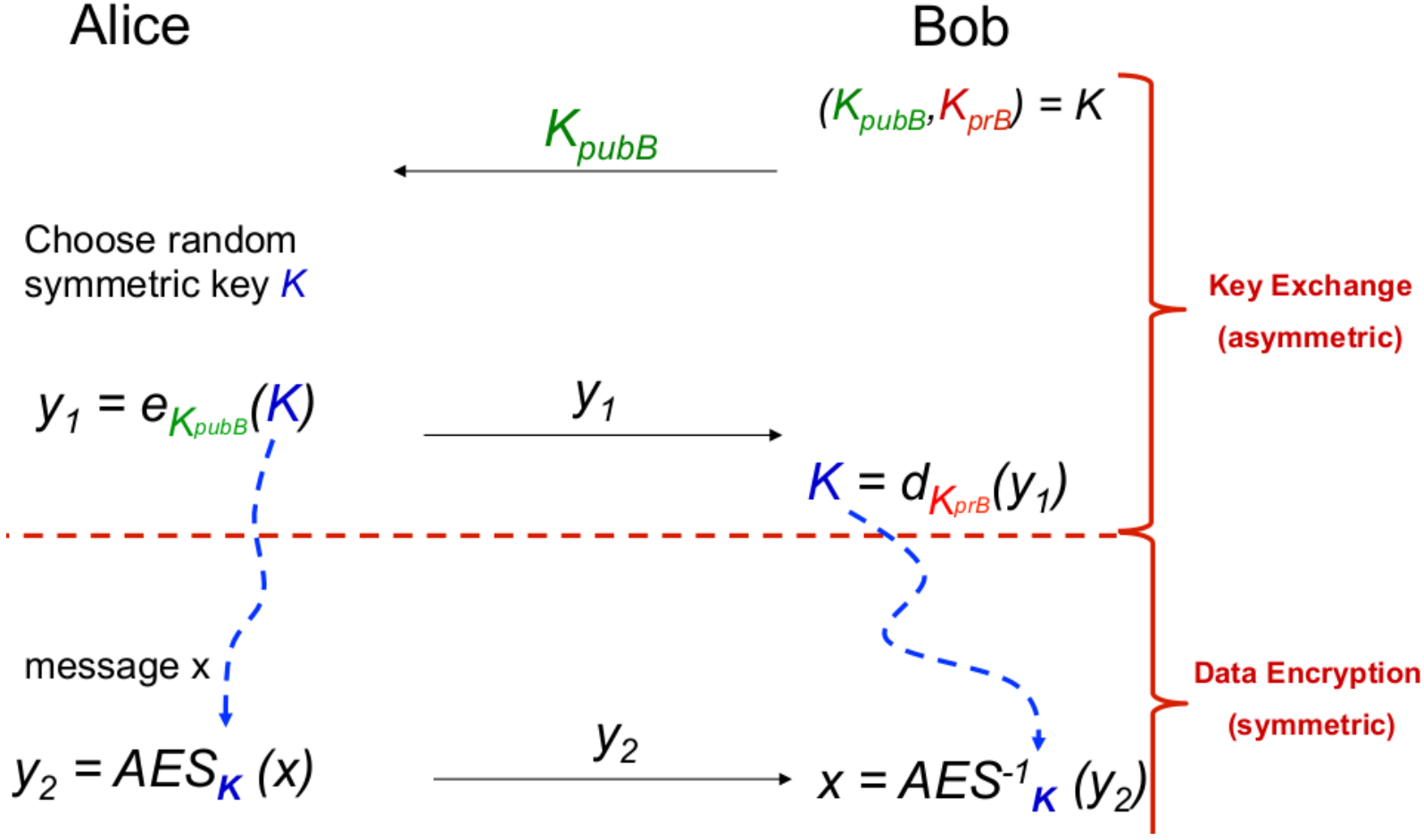
- Na prática, usa-se sistemas híbridos. Isto é, uma junção entre a algoritmos simétricos e assimétricos.
  - **Estabelecimento de chaves** (para esquemas simétricos) e **assinatura digital** são computados com algoritmos assimétricos (lentos).
  - **Encriptação** de dados é feita (rápida) com algoritmos simétricos, por exemplo, cifras de bloco e cifras de fluxo.

Protocolo básico de transporte de chaves - Exemplo

- Exemplo de protocolo híbrido que usa o AES como cifra simétrica.

Protocolo básico de transporte de chaves - Exemplo

- Exemplo de protocolo híbrido que usa o AES como cifra simétrica.



Autenticidade das chaves públicas

- Como saber se a chave pública pertence a quem diz pertencer?

Autenticidade das chaves públicas

- Como saber se a chave pública pertence a quem diz pertencer?
- Uma forma de resolver esse problema é por meio de certificados.

Autenticidade das chaves públicas

- Como saber se a chave pública pertence a quem diz pertencer?
- Uma forma de resolver esse problema é por meio de certificados.
  - Grosseiramente falando, os certificados vinculam uma chave pública a uma determinada identidade

Autenticidade das chaves públicas

- Como saber se a chave pública pertence a quem diz pertencer?
- Uma forma de resolver esse problema é por meio de certificados.
  - Grosseiramente falando, os certificados vinculam uma chave pública a uma determinada identidade
- Um outro problema nas chaves públicas são os tamanhos da chaves públicas e o desempenho computacional.

Como construir algoritmos assimétricos?

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.

Como construir algoritmos assimétricos?

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.
  - Calcular $y = f(x)$ é computacionalmente fácil.

Como construir algoritmos assimétricos?

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.
  - Calcular $y = f(x)$ é computacionalmente fácil.
  - Calcular $x = f^{-1}(y)$ é computacionalmente inviável.

Como construir algoritmos assimétricos?

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.
  - Calcular $y = f(x)$ é computacionalmente fácil.
  - Calcular $x = f^{-1}(y)$ é computacionalmente inviável.
- Funções de caminho único são baseadas em problemas difícil da matemática.

Como construir algoritmos assimétricos?

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.
  - Calcular $y = f(x)$ é computacionalmente fácil.
  - Calcular $x = f^{-1}(y)$ é computacionalmente inviável.
- Funções de caminho único são baseadas em problemas difícil da matemática.
- Três principais famílias:

Como construir algoritmos assimétricos?

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.
  - Calcular $y = f(x)$ é computacionalmente fácil.
  - Calcular $x = f^{-1}(y)$ é computacionalmente inviável.
- Funções de caminho único são baseadas em problemas difícil da matemática.
- Três principais famílias:
  - **Fatoração de inteiros:** (RSA...)

Como construir algoritmos assimétricos?

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.
  - Calcular $y = f(x)$ é computacionalmente fácil.
  - Calcular $x = f^{-1}(y)$ é computacionalmente inviável.
- Funções de caminho único são baseadas em problemas difícil da matemática.
- Três principais famílias:
  - **Fatoração de inteiros:** (RSA...)
    - Dado um inteiro composto n, encontre seus fatores primos.

Como construir algoritmos assimétricos?

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.
  - Calcular $y = f(x)$ é computacionalmente fácil.
  - Calcular $x = f^{-1}(y)$ é computacionalmente inviável.
- Funções de caminho único são baseadas em problemas difícil da matemática.
- Três principais famílias:
  - **Fatoração de inteiros:** (RSA...)
    - Dado um inteiro composto n, encontre seus fatores primos.
    - Multiplicar dois primos é fácil!

Como construir algoritmos assimétricos?

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.
  - Calcular $y = f(x)$ é computacionalmente fácil.
  - Calcular $x = f^{-1}(y)$ é computacionalmente inviável.
- Funções de caminho único são baseadas em problemas difícil da matemática.
- Três principais famílias:
  - **Fatoração de inteiros:** (RSA...)
    - Dado um inteiro composto n, encontre seus fatores primos.
    - Multiplicar dois primos é fácil!
  - **Logaritmo discreto:** (Diffie-Hellman, Elgamal, DSA,...)

Como construir algoritmos assimétricos?

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.
  - Calcular $y = f(x)$ é computacionalmente fácil.
  - Calcular $x = f^{-1}(y)$ é computacionalmente inviável.
- Funções de caminho único são baseadas em problemas difícil da matemática.
- Três principais famílias:
  - **Fatoração de inteiros:** (RSA...)
    - Dado um inteiro composto n, encontre seus fatores primos.
    - Multiplicar dois primos é fácil!
  - **Logaritmo discreto:** (Diffie-Hellman, Elgamal, DSA,...)
    - Dado um y e um m, encontre x tal que $a^x = y \bmod m$

Como construir algoritmos assimétricos?

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.
  - Calcular $y = f(x)$ é computacionalmente fácil.
  - Calcular $x = f^{-1}(y)$ é computacionalmente inviável.
- Funções de caminho único são baseadas em problemas difícil da matemática.
- Três principais famílias:
  - **Fatoração de inteiros:** (RSA...)
    - Dado um inteiro composto n, encontre seus fatores primos.
    - Multiplicar dois primos é fácil!
  - **Logaritmo discreto:** (Diffie-Hellman, Elgamal, DSA,...)
    - Dado um y e um m, encontre x tal que $a^x = y \bmod m$
    - Exponenciação a^x é fácil.

Como construir algoritmos assimétricos?

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.
  - Calcular $y = f(x)$ é computacionalmente fácil.
  - Calcular $x = f^{-1}(y)$ é computacionalmente inviável.
- Funções de caminho único são baseadas em problemas difícil da matemática.
- Três principais famílias:
  - **Fatoração de inteiros:** (RSA...)
    - Dado um inteiro composto n, encontre seus fatores primos.
    - Multiplicar dois primos é fácil!
  - **Logaritmo discreto:** (Diffie-Hellman, Elgamal, DSA,...)
    - Dado um y e um m, encontre x tal que $a^x = y \bmod m$
    - Exponenciação a^x é fácil.
  - **Curvas Elípticas:** (ECDH, ECDSA)

Como construir algoritmos assimétricos?

- Esquemas assimétricos são baseados em uma função de caminho único $f()$.
  - Calcular $y = f(x)$ é computacionalmente fácil.
  - Calcular $x = f^{-1}(y)$ é computacionalmente inviável.
- Funções de caminho único são baseadas em problemas difícil da matemática.
- Três principais famílias:
  - **Fatoração de inteiros:** (RSA...)
    - Dado um inteiro composto n, encontre seus fatores primos.
    - Multiplicar dois primos é fácil!
  - **Logaritmo discreto:** (Diffie-Hellman, Elgamal, DSA,...)
    - Dado um y e um m, encontre x tal que $a^x = y \bmod m$
    - Exponenciação a^x é fácil.
  - **Curvas Elípticas:** (ECDH, ECDSA)
    - Generalização do logaritmo discreto.

Tamanho de chaves e nível de segurança

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

Date	Minimum of Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ

FIM