UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia e Certificação Digital
Quarta Aula

Prof. Frederico Sauer, D.Sc.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Criptografia Assimétrica

- Diffie & Hellmann (1976)
- Assimetria → as chaves de encriptar e decifrar são diferentes, porém relacionadas (*public-key/private-key*)
- Não pretende substituir a simétrica
  - Distribuição de chaves sem KDC
  - Assinaturas digitais
- Fundamentos
  - É computacionalmente inviável descobrir a chave para decriptar (privada) conhecendo apenas o algoritmo e a chave usada para encriptar (pública);
  - É computacionalmente fácil cifrar/decifrar quando a chave necessária é conhecida; e
  - Apenas um determinado par de chaves pode ser usado para cifrar/decifrar

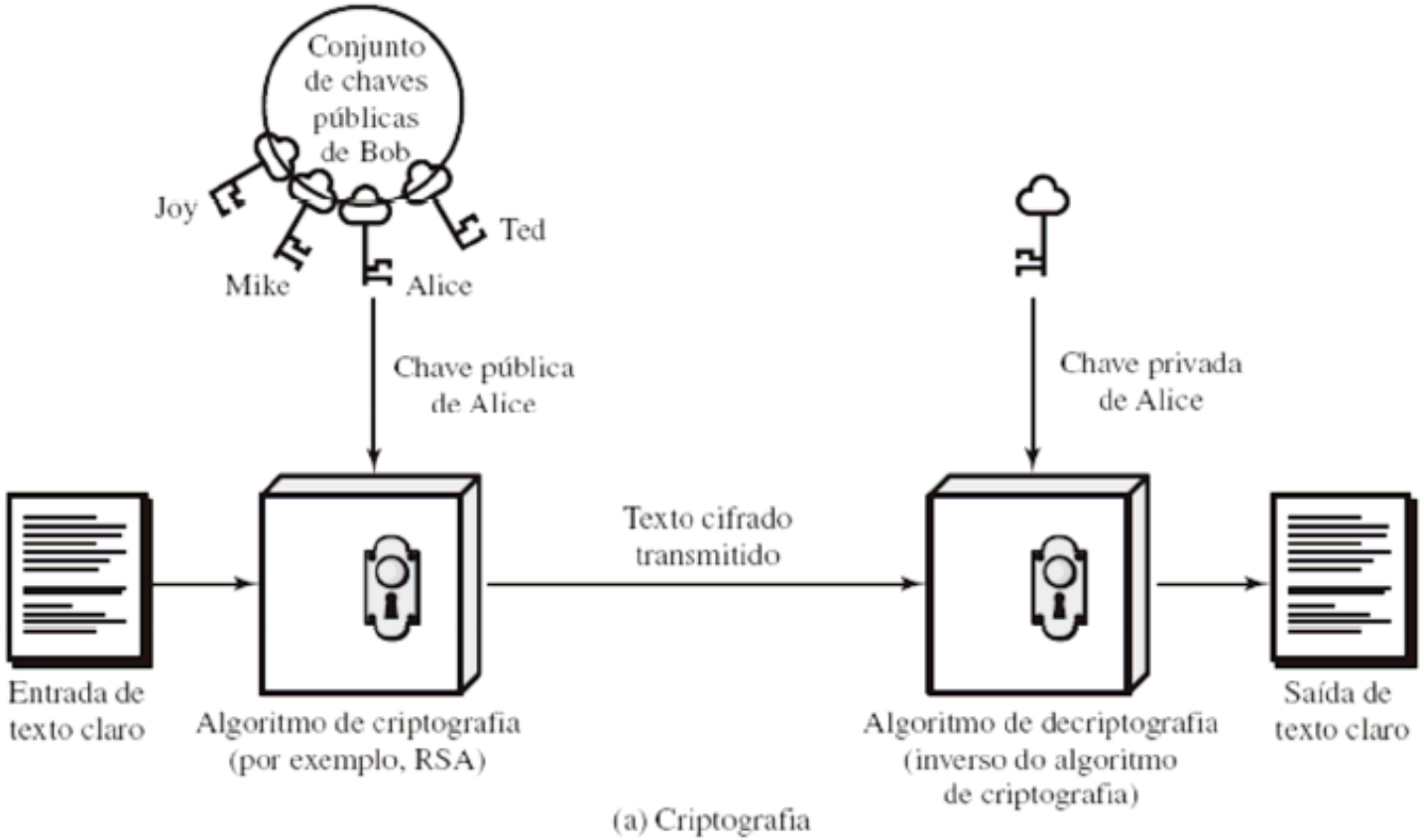
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Comparações com a Simétrica

Criptografia convencional	Criptografia de chave pública
Necessário para funcionar: 1. O mesmo algoritmo com a mesma chave é usado para criptografia e decriptografia. 2. O emissor e o receptor precisam compartilhar o algoritmo e a chave. **Necessário para a segurança:** 1. A chave precisa permanecer secreta. 2. Deverá ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível. 3. O conhecimento do algoritmo mais amostras do texto cifrado precisam ser insuficientes para determinar a chave.	**Necessário para funcionar:** 1. Um algoritmo é usado para criptografia e decriptografia com um par de chaves, uma para criptografia e outra para decriptografia. 2. O emissor e o receptor precisam ter uma das chaves do par casado de chaves (não a mesma chave). **Necessário para a segurança:** 1. Uma das duas chaves precisa permanecer secreta. 2. Deverá ser impossível ou pelo menos impraticável decifrar uma mensagem se nenhuma outra informação estiver disponível. 3. O conhecimento do algoritmo mais uma das chaves mais amostras do texto cifrado precisam ser insuficientes para determinar a outra chave.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

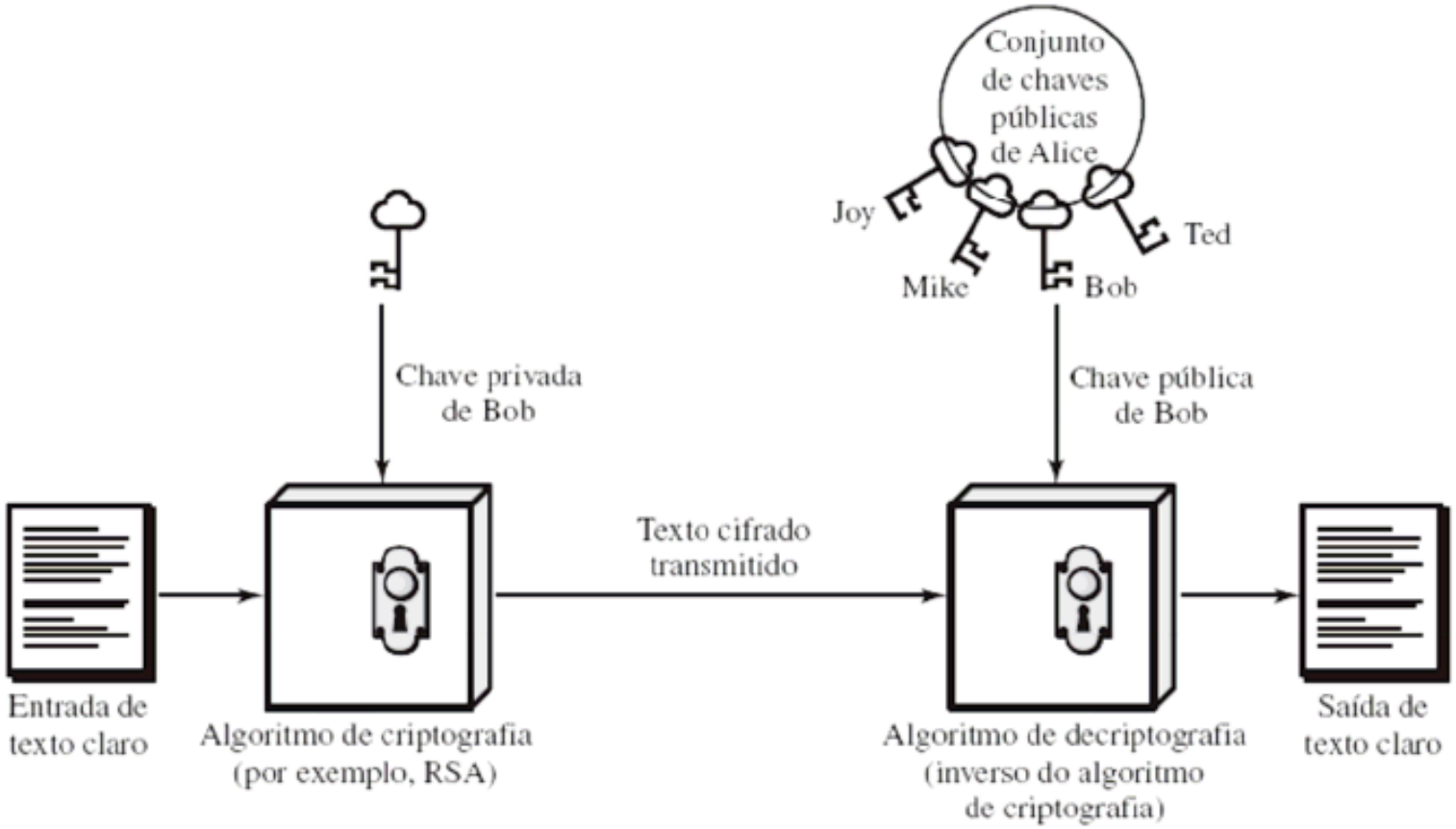
Criptografia



(a) Criptografia

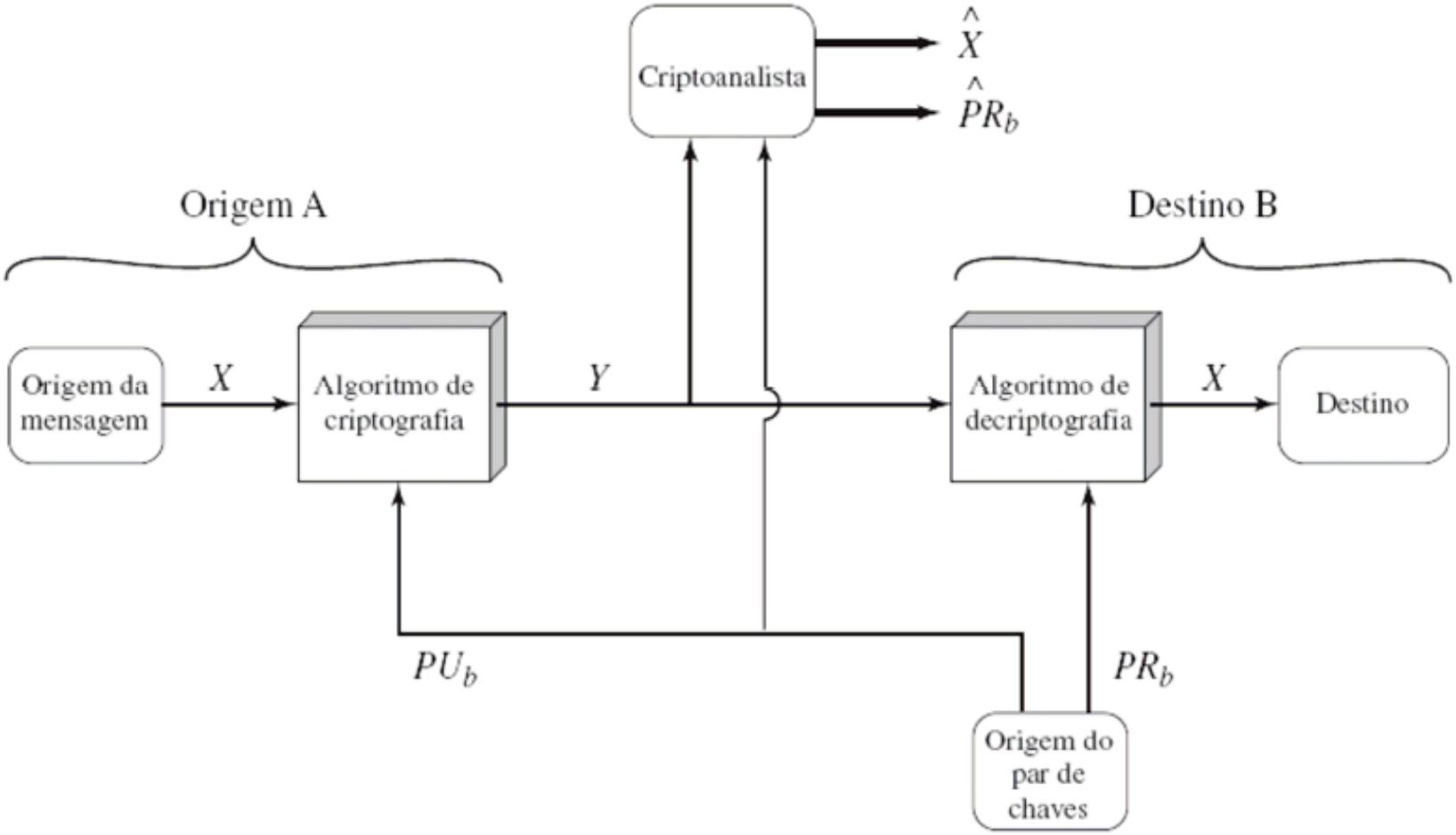
UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Autenticação

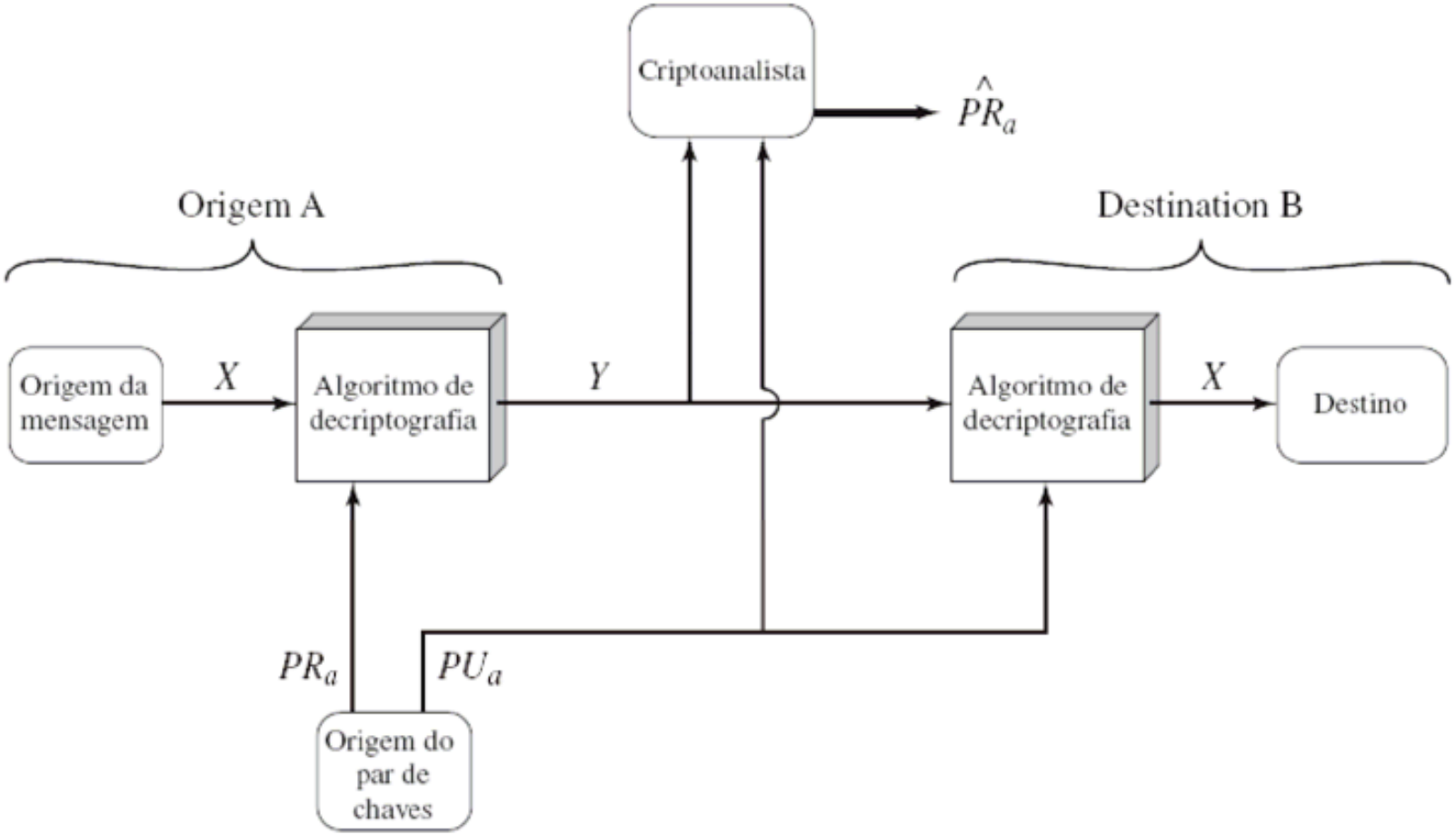


(b) Autenticação

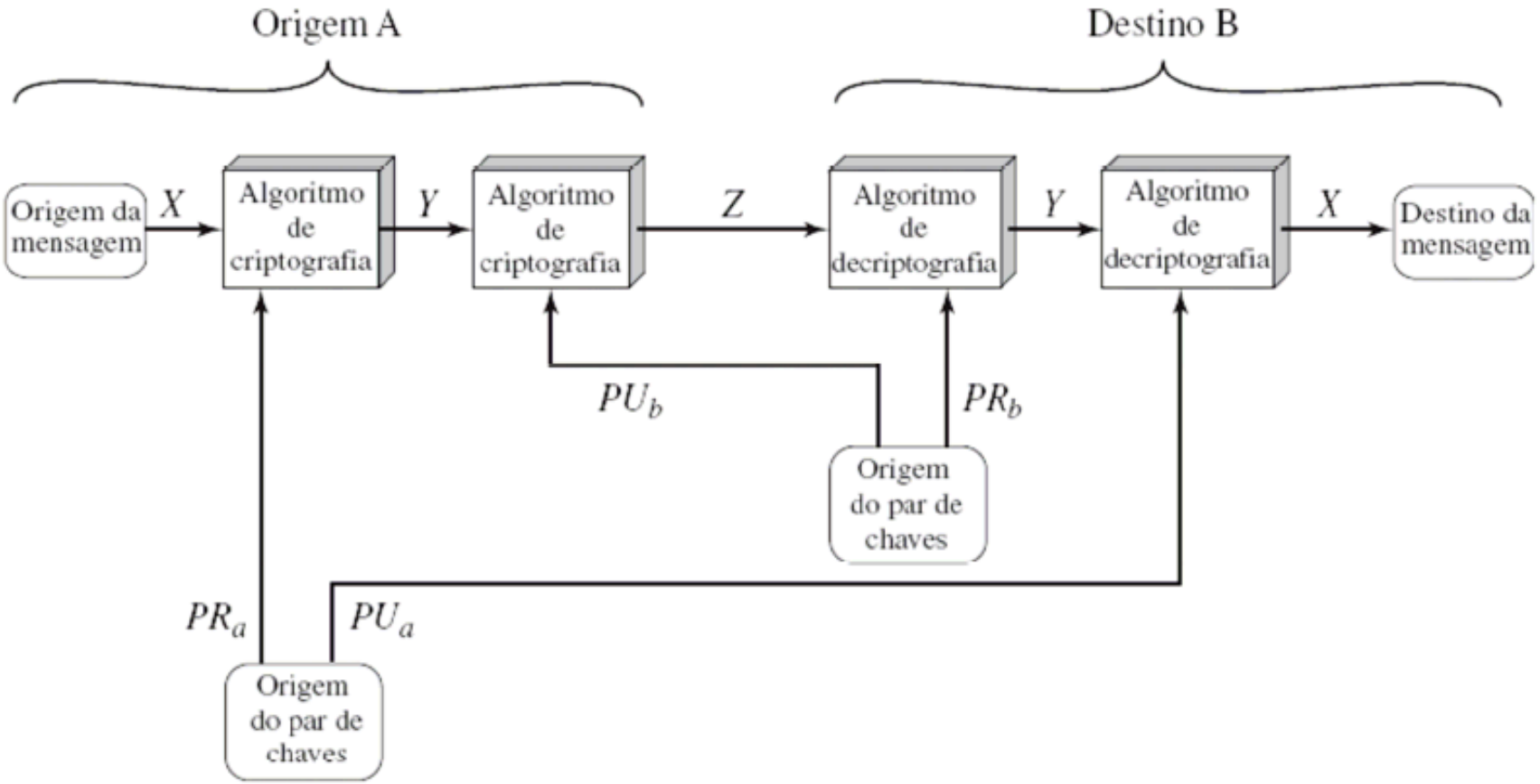
Confidencialidade



Autenticidade



Operações Combinadas



UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Questões de Robustez/Desempenho

- Ataques por força-bruta sempre são possíveis
- Chaves usadas são sempre grandes (>512 bits, típico mínimo 1024 bits)
- Números correspondentes grandes → execução lenta

RSA

- Proposta de Rivest, Shamir e Adleman (MIT-1977)

Geração de chaves

Selecione p, q — p e q são primos, $p \neq q$

Calcule $n = p \times q$

Calcule $\phi(n) = (p - 1)(q - 1)$

mdc $(\phi(n), e) = 1; 1 < e < \phi(n)$

$d \equiv e^{-1} \pmod{\phi(n)}$

$PU = \{e, n\}$

$PR = \{d, n\}$

Criptografia

Texto claro: $M < n$

Texto cifrado: $C = M^e \bmod n$

Decriptografia

Texto cifrado: C

Texto claro: $M = C^d \bmod n$

Exemplo do RSA

1. Selecione 2 primos: $p=17$ & $q=11$
2. Calcule $n = pq = 17 \times 11 = 187$
3. Calcule $\phi(n)=(p-1)(q-1)=16 \times 10=160$
4. Selecione e: mdc(e,160)=1; escolhi $e=7$
5. Determine d: $de \equiv 1 \pmod{160}$ e $d < 160$
   Valor é d=23, pois $23 \times 7=161$, e $(1 \bmod 160) = (161 \bmod 160)$
6. Divulgue a *public key* PU={7,187}
7. Mantenha secreta a *private key* PR={23,187}

Obs.: mdc → decomposição em fatores primos !

$a \equiv b \pmod{n}$ se $(a \bmod n) = (b \bmod n)$ → congruência

Usando o RSA

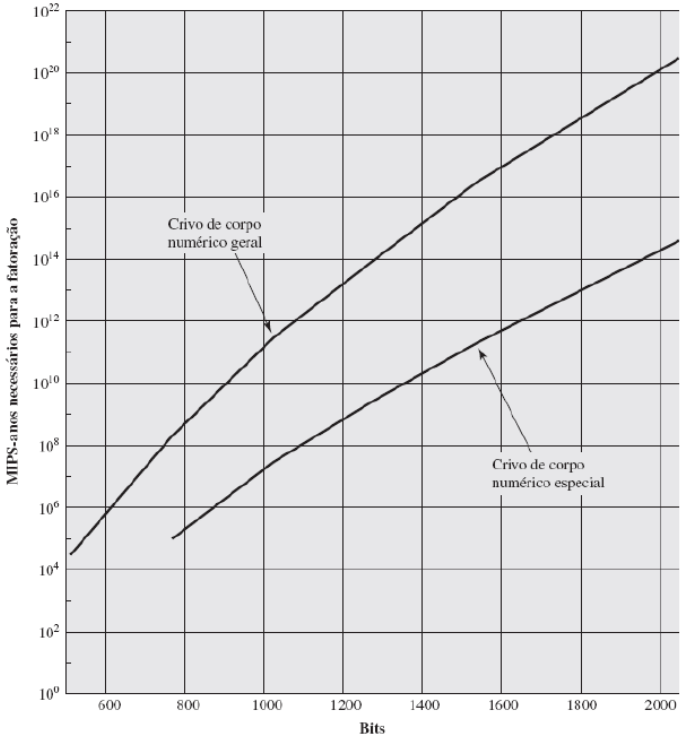
- Mensagem $M = 88$
  - Observe-se que $88<187$
- Encriptação:

  $C = 88^{7} \bmod 187 = 11$
- Decriptação:

  $M = 11^{23} \bmod 187 = 88$

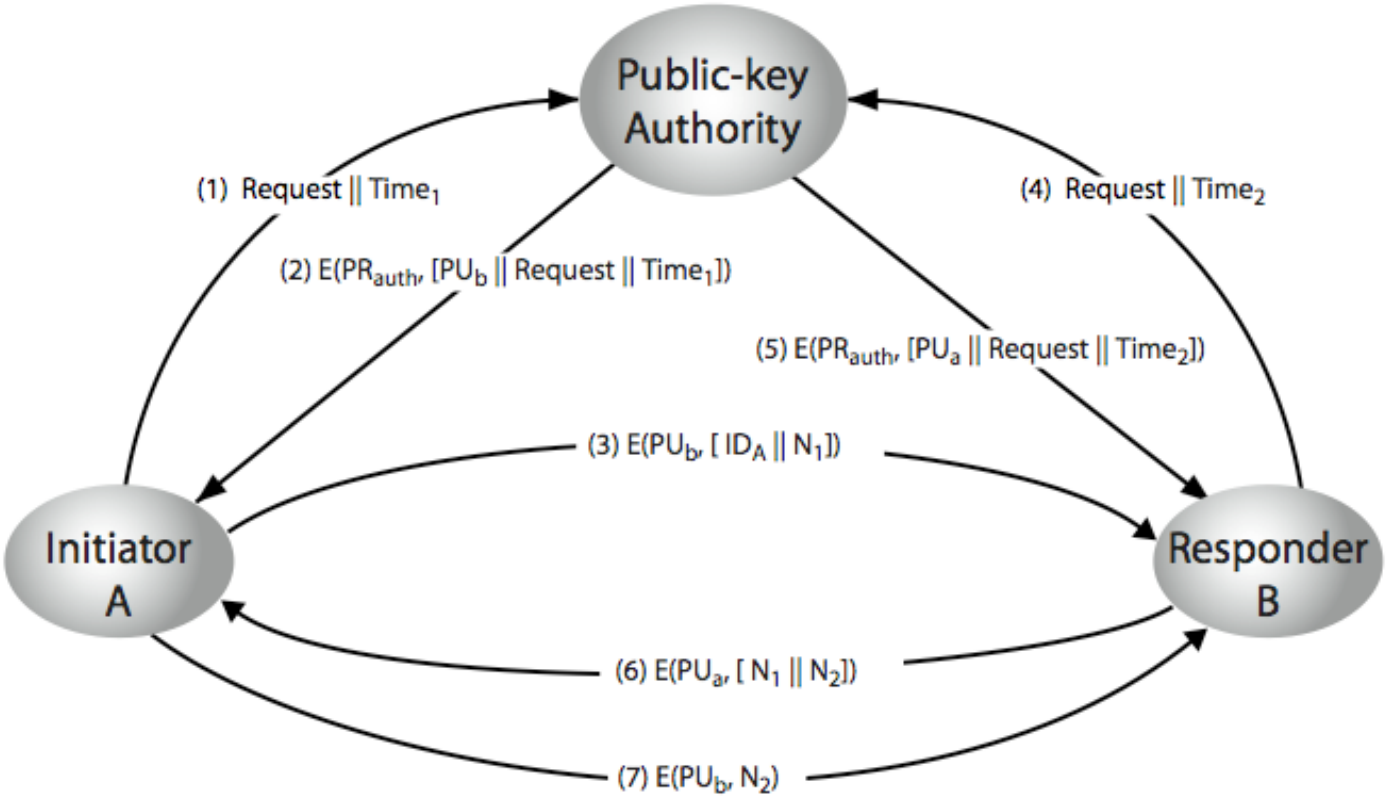
Ataques ao RSA

- Força Bruta
- Temporização
  - Chave obtida pelo tempo levado para cifrar → já conhecido e “driblado” pela RSA
- Texto Cifrado escolhido
  - Ataque simples e real contornado através de *padding* na mensagem original
- Matemáticos
  - Fatorar n em seus primos p e q



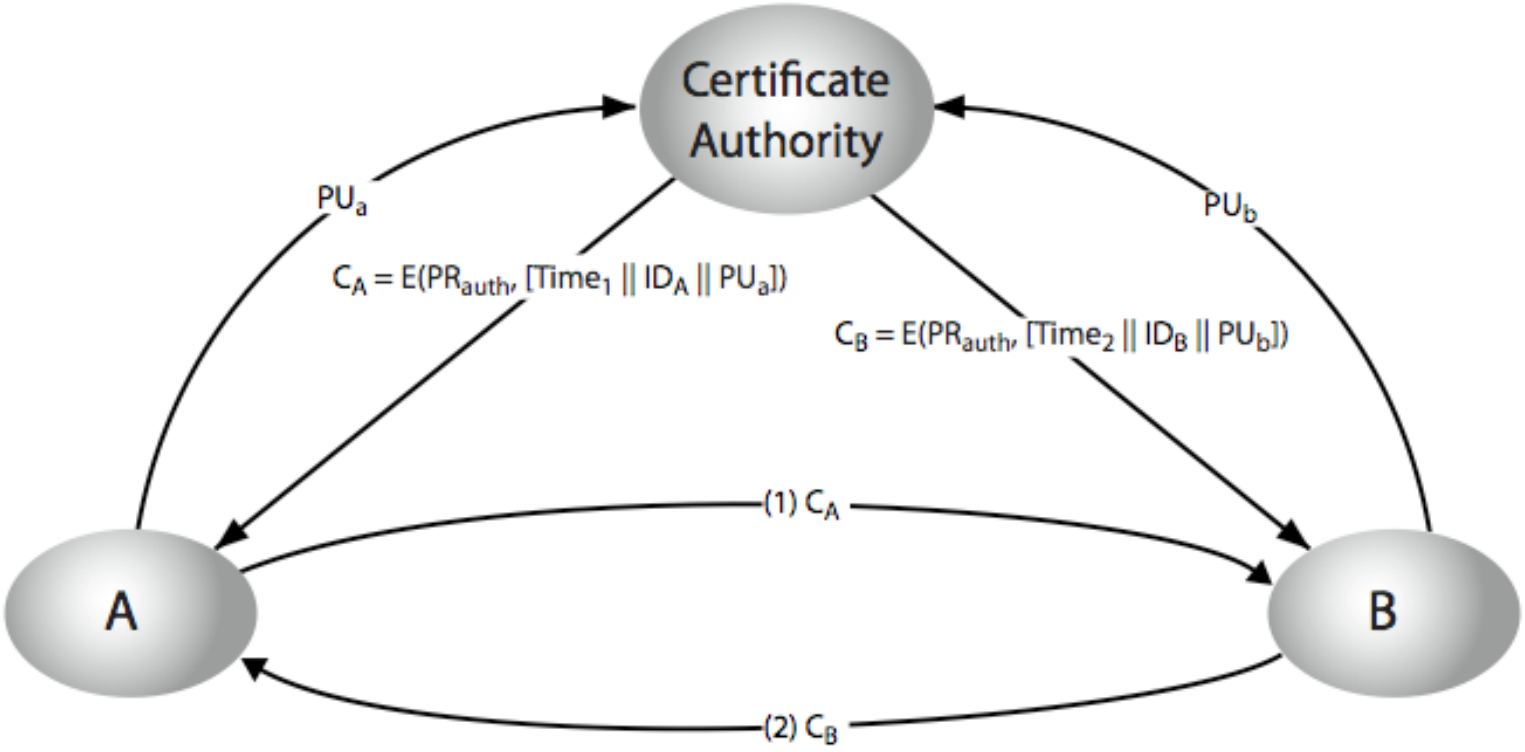
Distribuição de Chaves Públicas

- Para Confidencialidade e Autenticidade global, o uso de repositórios públicos parece ser a solução
- A adoção de autoridades possibilita maior controle



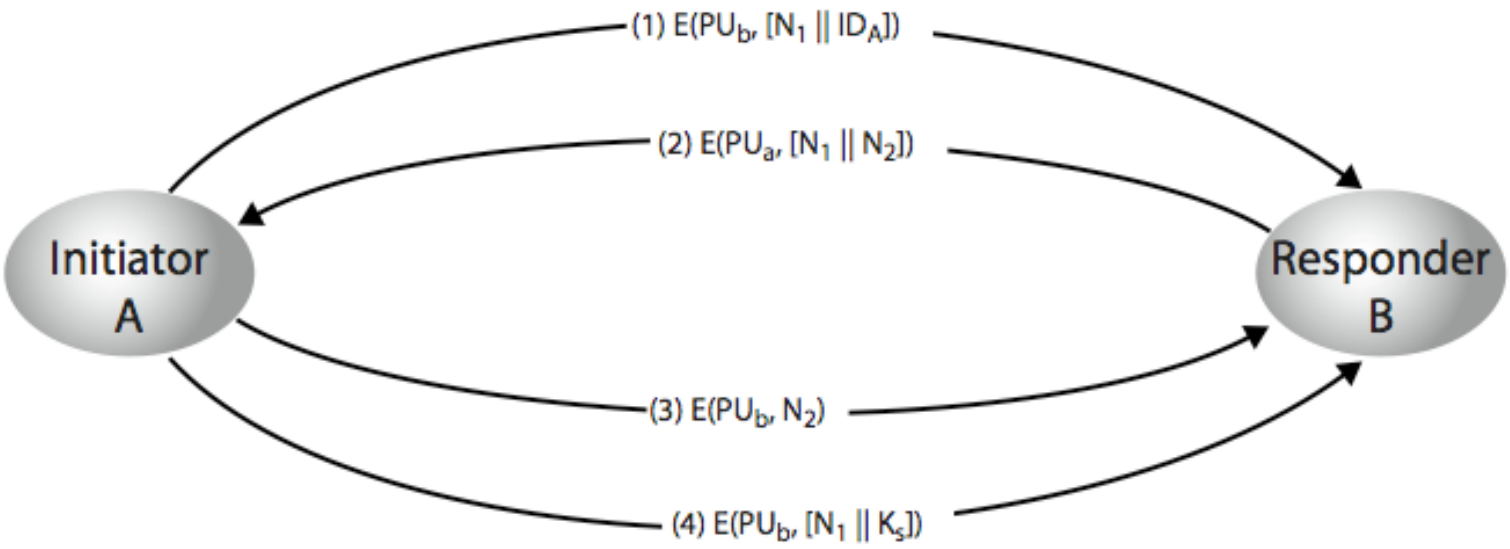
Uso de Certificados

- Dispensam o acesso em tempo real às AC
- Dependem da posse da *public-key* da AC



O Melhor dos Mundos

- Visando agregar a rapidez da criptografia simétrica com a independência do canal seguro da Assimétrica...



Diffie-Hellmann

- Algoritmo de chave pública para distribuição de chaves secretas

Elementos públicos globais

q	número primo
α	$\alpha < q$ e α uma raiz primitiva de q

Geração de chave do usuário A

Selecionar X_A privada	$X_A < q$
Calcular Y_A pública	$Y_A = \alpha^{X_A} \bmod q$

Geração de chave do usuário B

Selecionar X_B privada	$X_B < q$
Calcular Y_B pública	$Y_B = \alpha^{X_B} \bmod q$

Cálculo da chave secreta pelo usuário A

$$K = (Y_B)^{X_A} \bmod q$$

Cálculo da chave secreta pelo usuário B

$$K = (Y_A)^{X_B} \bmod q$$

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Raiz Primitiva

Raiz Primitiva

Por exemplo, fui dar uma olhada no que é a *raiz primitiva* de um módulo. Descobri que um número *g* é a raiz primitiva de um módulo *n* quando este número elevado às potências de 1 até n-1 (mod n) fornecer todos os resíduos possíveis deste módulo. Por exemplo, 3 é uma raiz primitiva do (mod 5) porque:

$3^1 \pmod 5 = 3 \pmod 5 = 3$
$3^2 \pmod 5 = 9 \pmod 5 = 4$
$3^3 \pmod 5 = 27 \pmod 5 = 2$
$3^4 \pmod 5 = 81 \pmod 5 = 1$

Estas operações resultaram em todos os resíduos que o módulo 5 pode oferecer. O fato de não estarem em ordem não tem importância, pois a premissa é que todos apareçam uma vez. Apenas para fixar esta noção, observe o comportamento de 4 no módulo 5:

$4^1 \pmod 5 = 4 \pmod 5 = 4$
$4^2 \pmod 5 = 16 \pmod 5 = 1$
$4^3 \pmod 5 = 64 \pmod 5 = 4$
$4^4 \pmod 5 = 256 \pmod 5 = 1$

Estes cálculos nos mostram que 4 não é uma raiz primitiva do módulo 5. Quando o valor dos módulos é pequeno, pode-se fazer o cálculo com lápis e papel, mas, se o valor do módulo for muito grande, a calculadora não vai ter espaço para os dígitos e os cálculos vão levar um tempo enorme. Ainda bem que os matemáticos acham atalhos que facilitam a nossa vida. Conforme Burton publicou em 1986, um dos atalhos que podemos pegar é

Se o MDC(g,n)=1 (ou seja, g e n são primos entre si)
e a ordem multiplicativa de g (mod n) for igual a $\varphi(n)$, onde $\varphi(n)$ é a função totiente,
então g é uma raiz primitiva do módulo n.

Fonte: http://www.numaboa.com/criptografia/chaves/353-Diffie-Hellman?start=2

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

GnuPG

- Livre e gratuito, baseado no openpgp (rfc 2440)
- Focado no sigilo e autenticação de email
- Componentes:
  - GnuPG: implementação do openpgp
  - WinPT: Gerenciador de chaves
  - GPA: Gerenciador de chaves
  - GPGol: plugin para o Microsoft Outlook 2003
  - GPGee: plugin para o Explorer (*file encryption*)
  - Claws Mail: programa de email com plugin para o gnupg

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Gnupg

- Usar o manual “for novices”
- Após a instalação, deve ser criado um par de chaves com o GPA
- Por questão de cultura, faça o *backup* em *pendrive* e a apague da máquina
- Para treinar, pode-se usar o robô “Adele” (adele@gnupp.de)
- Use o WinPT para decifrar a msg
- Importe chaves dos seus colegas para seu keyring através do GPA
- Criptografe o texto de um email para um de seus colegas com o WinPT