Capítulo 7

Criptografia por Chave Pública

Prof. Ricardo Felipe Custódio, D.Sc.
INE-CTC-UFSC

Plano de Curso

- Princípios
- RSA
- Gerenciamento de Chaves
- Troca de Chaves por Diffie-Hellman
- Curva Elíptica - IEEE P1363

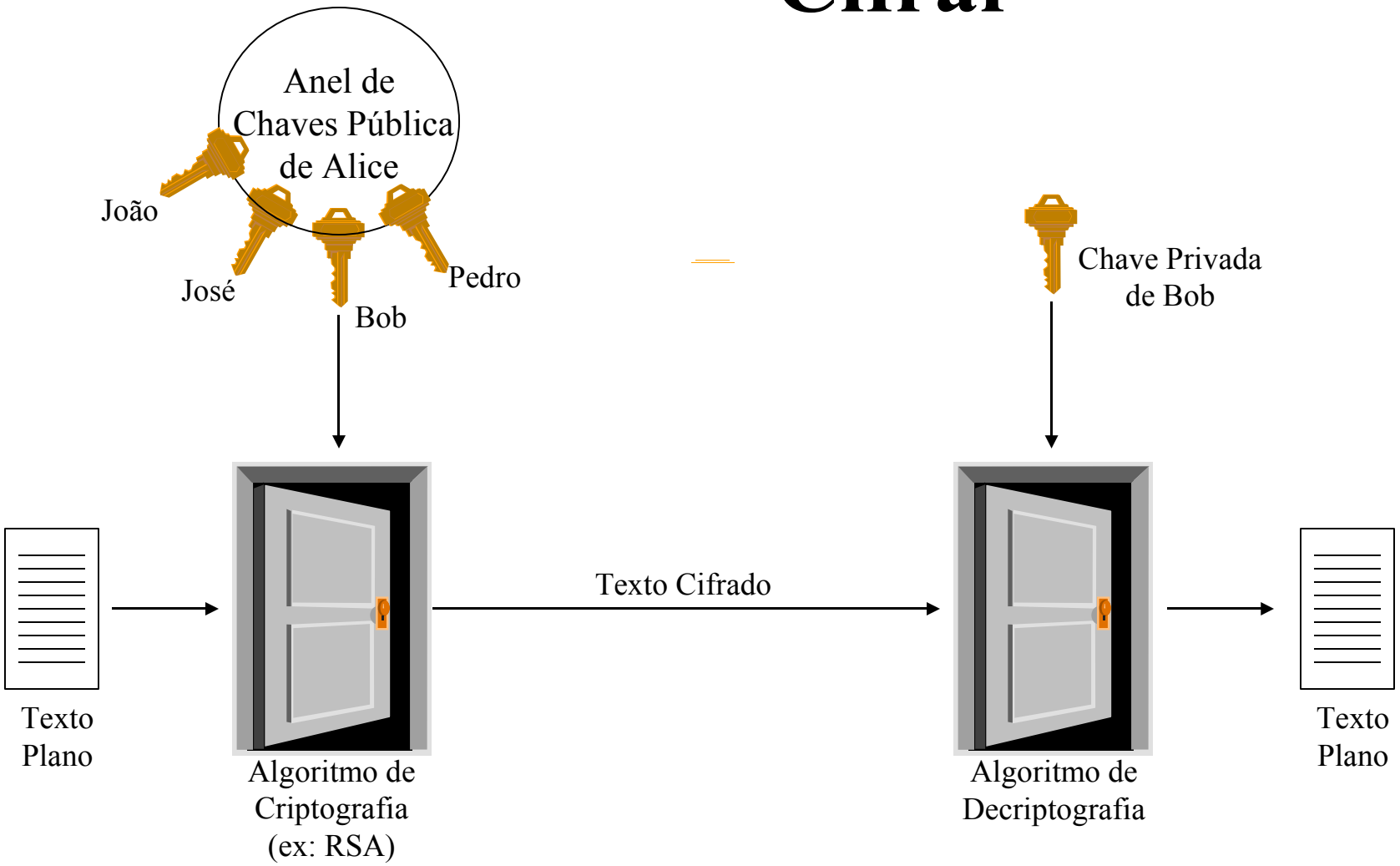
Chave Pública X Chave Secreta

- **Segurança -** Depende do tamanho da **Chave**
- **Não** é de propósito geral
  - Chave Pública - Aplicações de gerenciamento de chaves e a assinatura
- Gerenciamento das Chaves **Não** é Simples

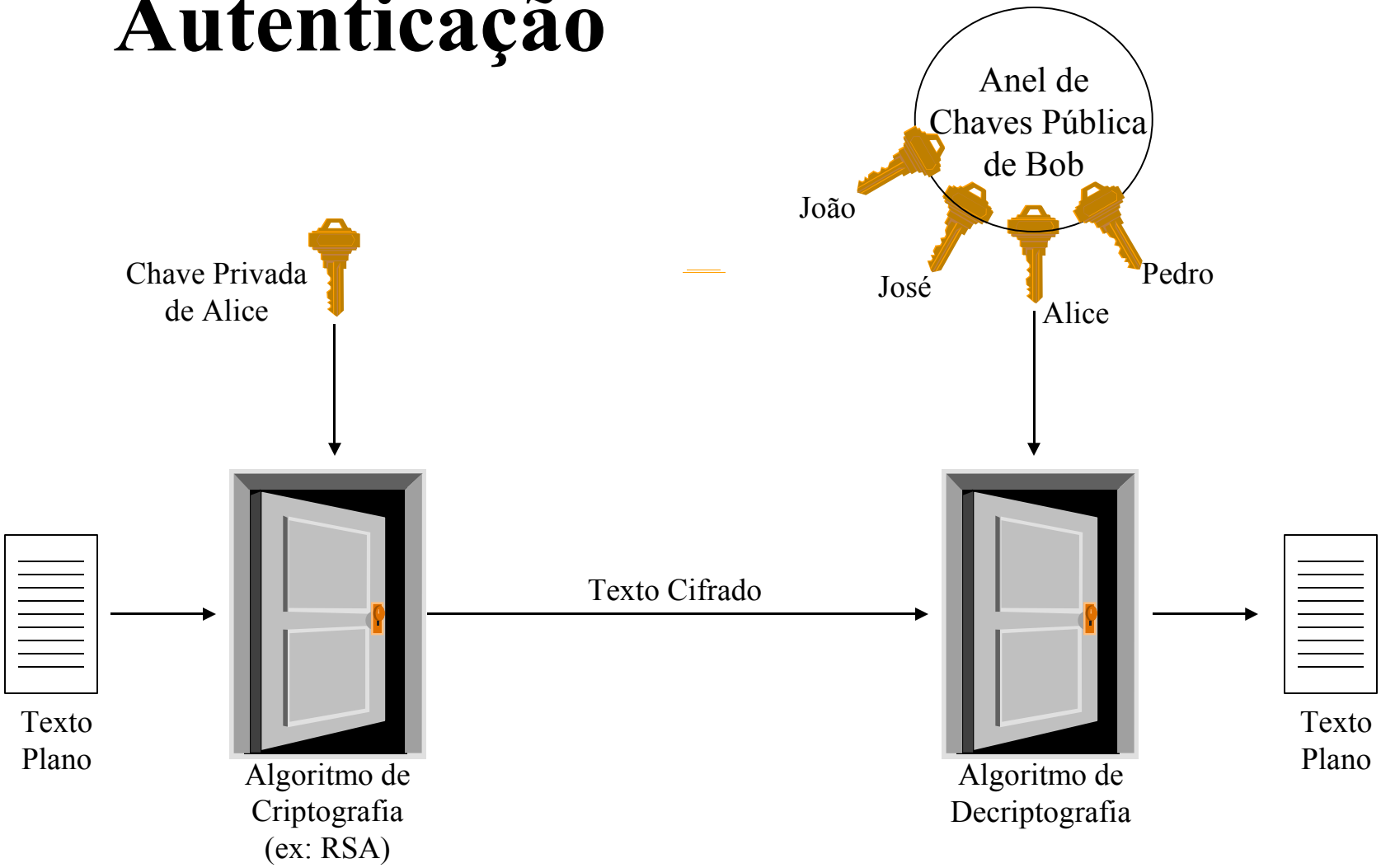
Características Importantes

- Impossibilidade de se obter a chave privada, dados a chave pública e o algoritmo
- Alguns Algoritmos
  - Permitem que as duas chaves possam ser usadas para encriptar ou decriptar

Cifrar


Anel de
Chaves Pública
de Alice
João
José
Bob
Pedro
Chave Privada
de Bob
Texto
Plano
Algoritmo de
Criptografia
(ex: RSA)
Texto Cifrado
Algoritmo de
Decriptografia
Texto
Plano

Autenticação



Chave Secreta X Chave Pública

Para Usar

- Um algoritmo e uma chave
- Alice e Bob compartilham o algoritmo e a chave

Para a Segurança

- Chave secreta
- Impossibilidade de decifrar a msg
- Algoritmo + amostras do texto cifrado não devem ser suficientes para determinar a chave

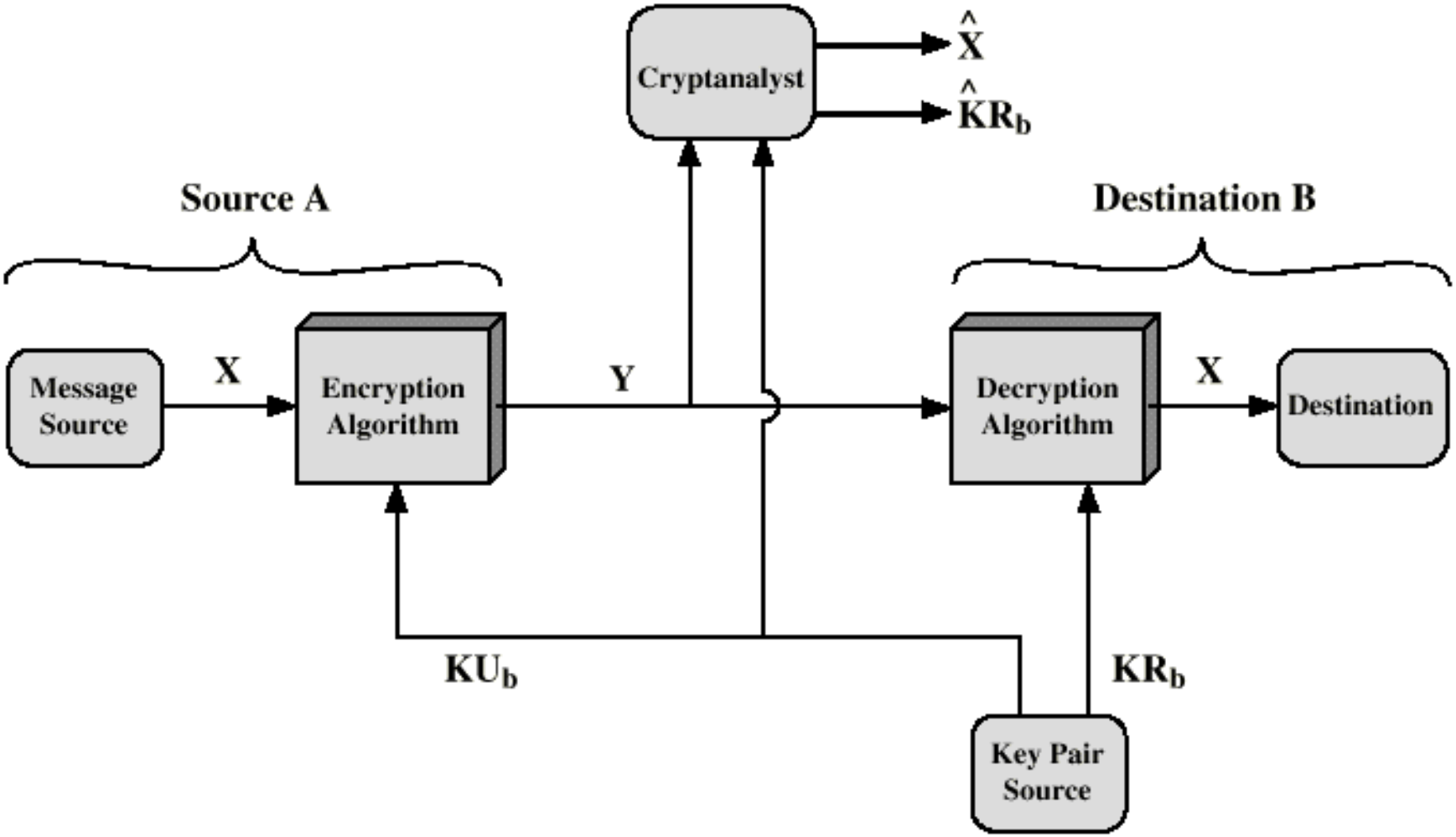
Para Usar

- Um algoritmo e duas chaves
- Alice e Bob compartilham um par de chaves

Para a Segurança

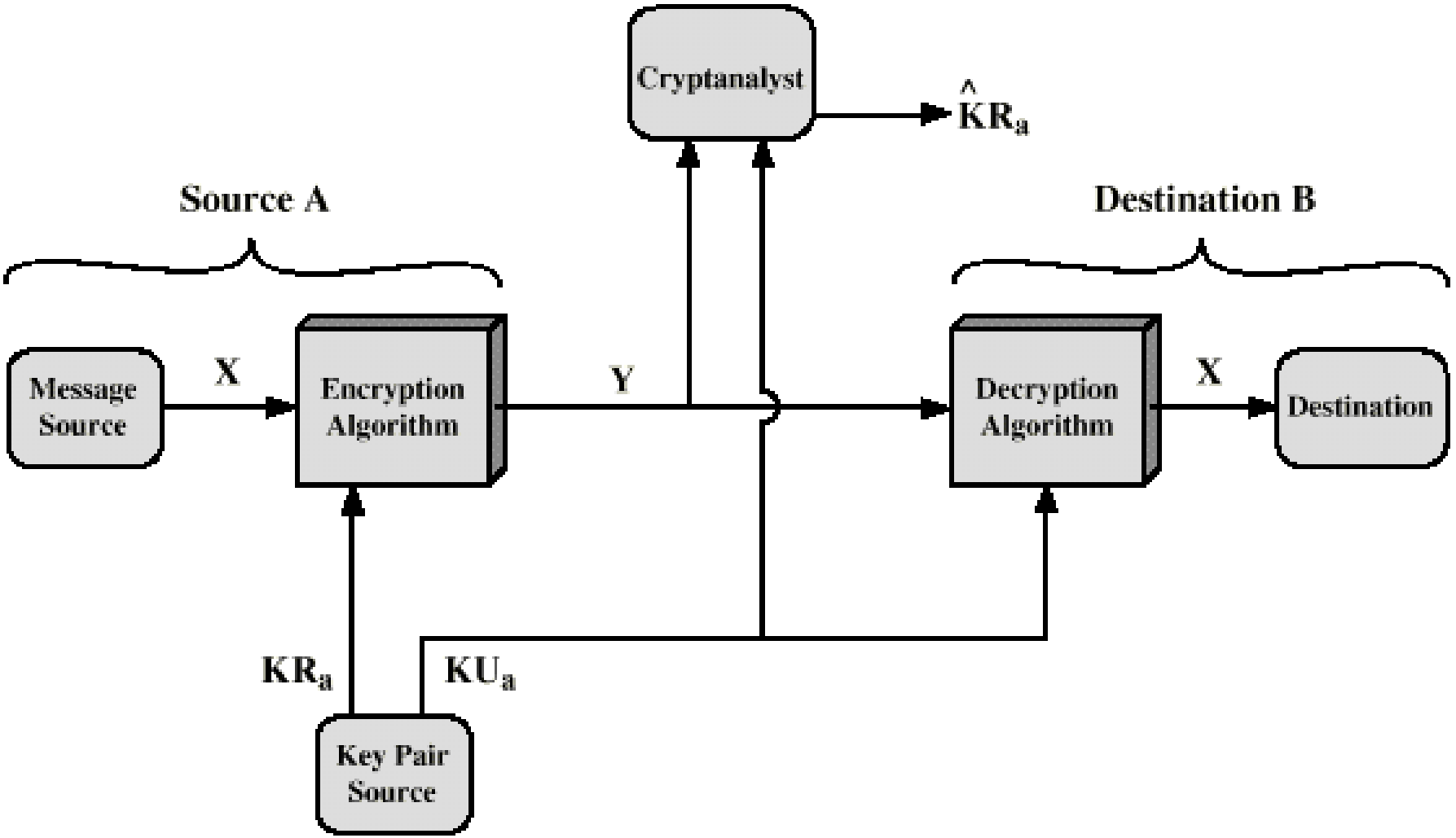
- Uma das duas chaves é secreta
- Impossibilidade de decifrar a msg
- Algoritmo + amostras do texto cifrado + uma das chaves não devem ser suficientes para determinar a outra chave

Segredo por Chave Pública

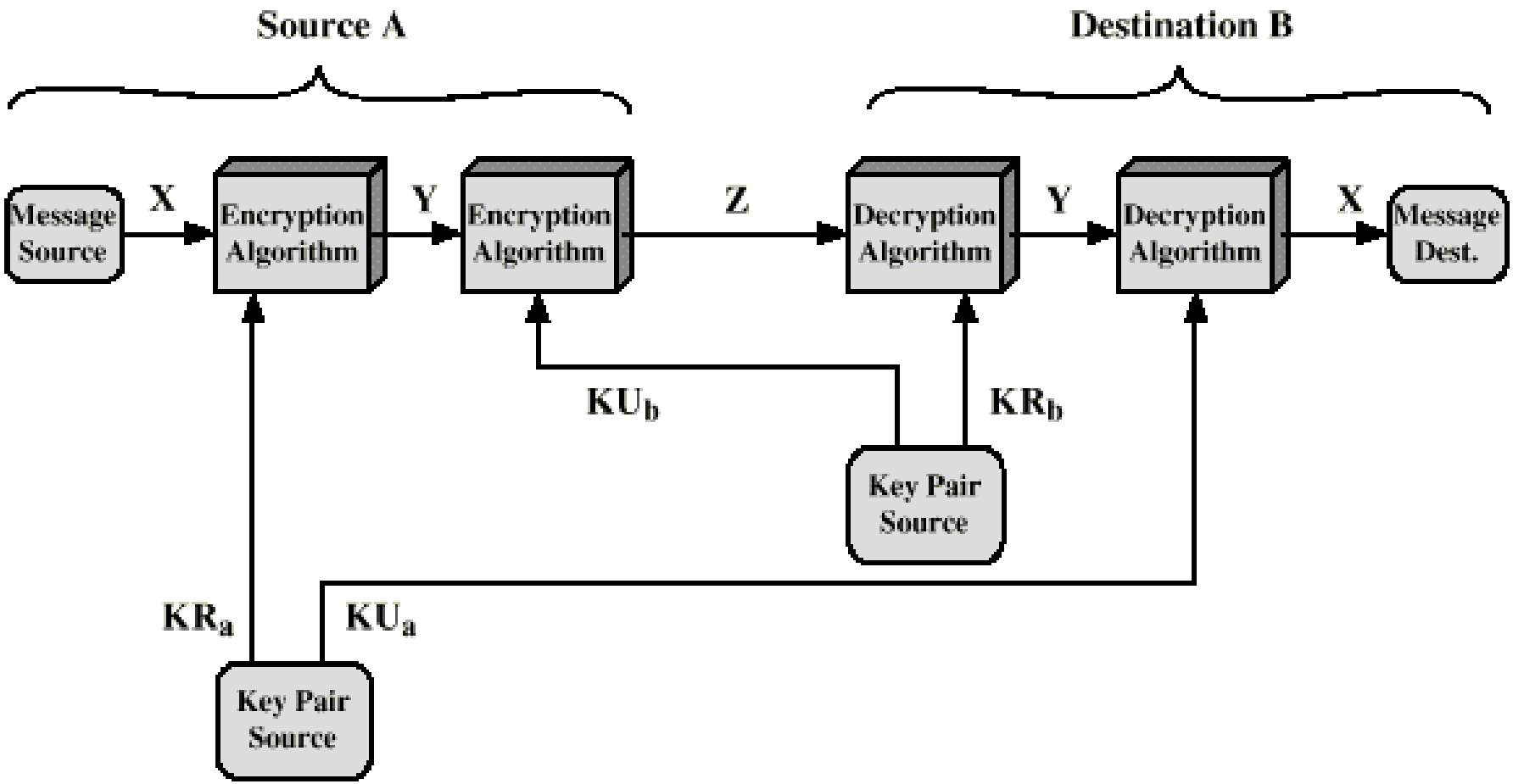


Prof. Ricardo Felipe Custódio, D.Sc.
INE-CTC-UFSC

Autenticação



Autenticação e Segredo



Requisitos

- Fácil **B** de gerar KU_b e KR_b
- Fácil **A** fazer $C = E_{KUb}(M)$
- Fácil **B** determinar $M = D_{KRb}(C) = D_{KRb}[E_{KUb}(M)]$
- Difícil determinar KR_b de KU_b
- Difícil determinar M a partir de KU_b e C
- $M = E_{KUb}[D_{KRb}(M)]$

Função de Caminho Único

$Y = f(X)$	fácil
$X = f^{-1}(Y)$	difícil

Função de Caminho Único c/ **trapdoor**

$Y = f_k(X)$	fácil
$X = f_k^{-1}(Y)$	fácil se k conhecidol
$X = f_k^{-1}(Y)$	difícil se k desconhecido

Aplicações

Algoritmo	E/D	Assinatura Digital	Troca de Chaves
RSA	Sim	Sim	Sim
Diffie-Hellman	Não	Não	Sim
DSS	Não	Sim	Não

Criptoanálise

- Complexidade não é linear com o número de bits da chave
- Compromisso (Força Bruta e Viabilidade)
- Calcular KR a partir de KU
- Ataque da Mensagem Provável (56 bits DES)

1978

Ron Rivest, Adi Shamir e Len Adleman

Blocos com valores binários menores que **n**
Tamanho do Bloco é k bits, onde $2^k < \mathbf{n} \leq 2^{k+1}$

Texto Cifrado

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Texto Plano

KU = {e,n}
KR = {d,n}

Requisitos do Algoritmo

- É possível encontrar **e**, **d**, **n** tal que $\mathbf{M^{ed} = M \bmod n}$ para todo $\mathbf{M < n}$
- É relativamente fácil calcular $\mathbf{M^e}$ e $\mathbf{C^d}$ para todos os valores de $\mathbf{M < n}$
- É improvável determinar **d** dado **e**, **n**

Detalhes Matemáticos

Dados **p** e **q** primos,
n e **m** inteiros tal que **n = pq**, **0 < m < n**
e um **k** arbitrário

$m^{k\phi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n$ (Eq. 7.8 - Corolário do Teor. Euler)

- $\phi(n)$ é a função totiente de Euler
  Número de Inteiros Positivos menor do que **n** e relativamente primos a **n**
- $\phi(pq) = (p-1)(q-1)$

$M^{ed} = M \bmod n$
$ed = k\,\phi(n) + 1$
$ed \equiv 1 \bmod \phi(n)$
$d \equiv e^{-1} \bmod \phi(n)$

Relativamente primos a $\phi(n)$

Algoritmo RSA

Geração da Chave

Selecione **p**,**q**	**p** e **q** primos
Calcular **n** = **p** x **q**	
Calcular $\phi(n) = (p-1)(q-1)$	
Selecionar **e** inteiro	$\gcd(\phi(n),e) = 1;\ 1 < e < \phi(n)$
Calcular **d**	$d = e^{-1} \bmod \phi(n)$
Chave Pública	**KU={e,n}**
Chave Privada	**KR={d,n}**

Cifrar

Texto Plano:	$M < n$
Texto Cifrado:	$C = M^e \pmod n$

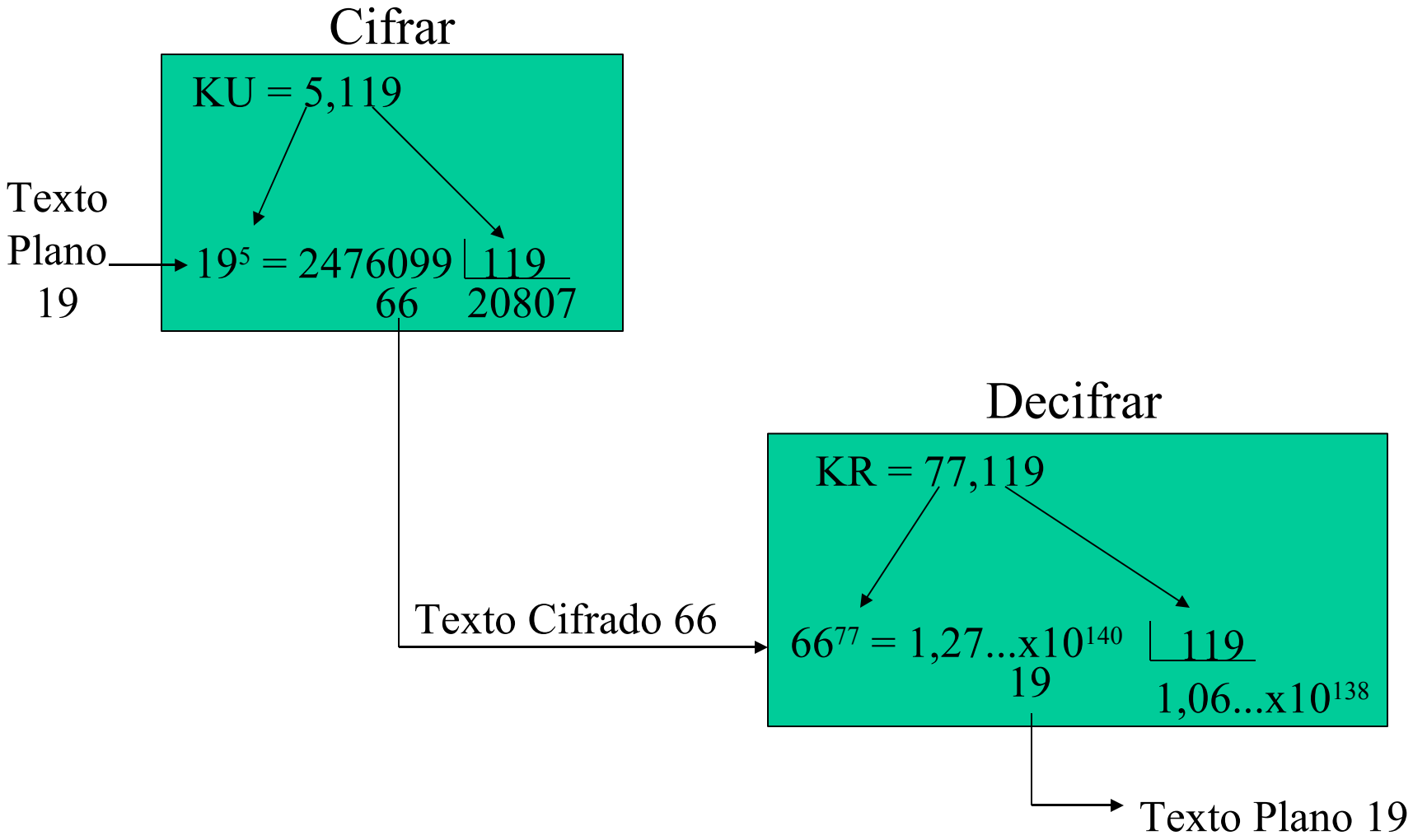
Decifrar

Texto Plano:	C
Texto Cifrado:	$M = C^d \pmod n$

Exemplo

- Selecionar dois números primos: $p = 7$ e $q = 17$
- Calcular $n = pq = 7 \times 17 = 119$
- Calcular $\phi(n) = (p-1)(q-1) = 96$
- Selecionar **e** tal que **e** é relativamente primo a $\phi(n)$ e menor que $\phi(n)$; $e = 5$
- Determinar d tal que $de = 1 \bmod 96$ e $d < 96$; $d = 77$, pois $77 \times 5 = 385 = 4 \times 96 + 1$
- $KU = \{5,119\}$ e $KR = \{77,119\}$

Continuação do Exemplo



Aspectos Computacionais E/D

$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Seja $m = b_k b_{k-1} \ldots b_0$

$$m = \sum_{b_i \neq 0} 2^i$$

$$a^m = a^{\sum_{b_i \neq 0} 2^i} = \prod_{b_i \neq 0} a^{2^i}$$

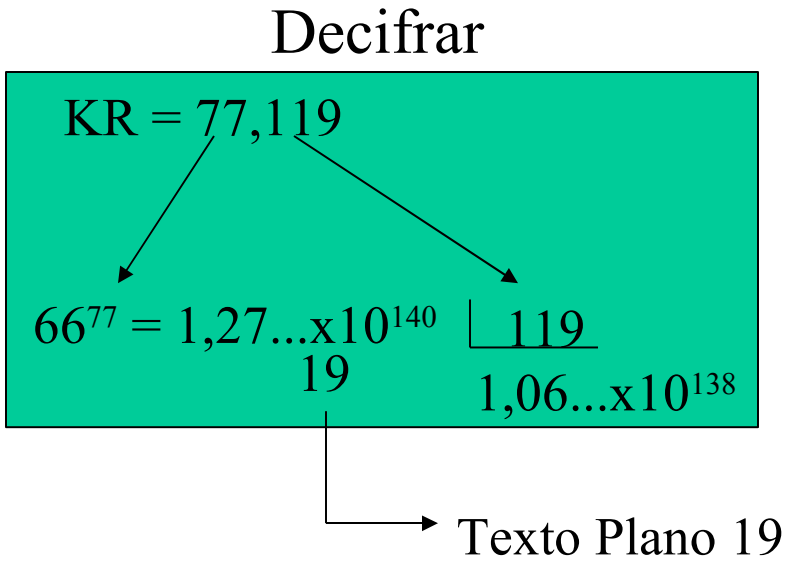
$$a^m \bmod n = \left[\prod_{b_i \neq 0} a^{2^i} \right] \bmod n = \prod_{b_i \neq 0} a^{2^i} \bmod n$$

$d = a^b \bmod n$

```
d = 1
para i = k passo -1 até 0 faça
      d = (d x d) mod n
      se b_i = 1 então
            d = (d x a) mod n
      fim se
fim para
retorna d
```

[CORM 90]

Exercício



Usar o algoritmo para calcular

$d = a^b \bmod n$

$d = 66^{77} \bmod 119 = ?$

Aspectos Computacionais Chaves

- Determinar dois primos **p** e **q**
  - n = pq é conhecido
    - **r** randômico ($\approx 2^{200} \rightarrow$ tentativas = $\ln(2^{200})/2 = 70$
    - **a < r** randômico
    - Testa r para primalidade
    - Se r passa em vários testes, aceita-se r
- Selecionar **e** ou **d** e calcular o outro
  - Algoritmo Estendido de Euclides

Segurança do RSA

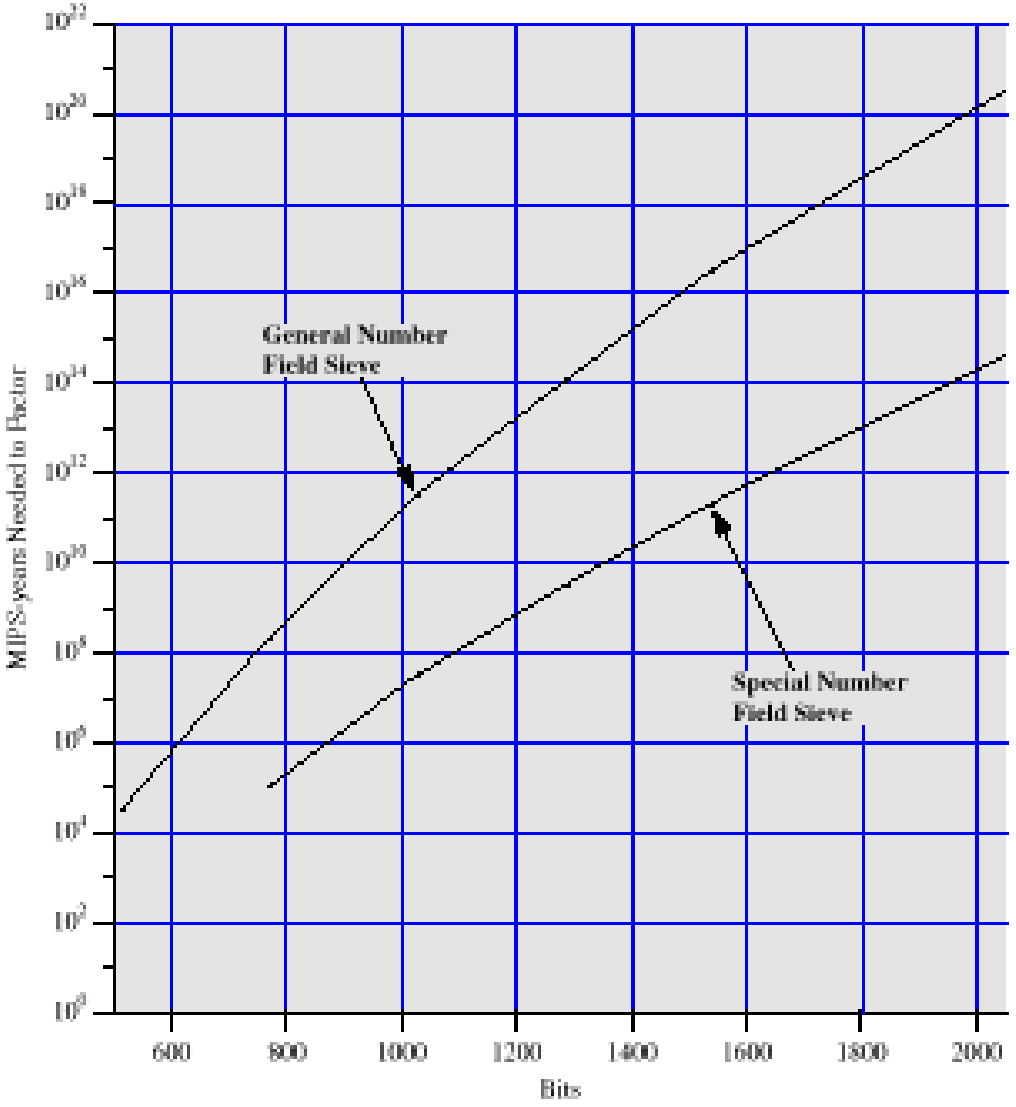
- Força Bruta
- Ataques Matemáticos
  - Fatorar Números Primos
  - Determinar $\phi(n)$ diretamente
  - Determinar d diretamente
- Ataques temporais

Fatoração

Número de dígitos Dec.	Aproximado de bits	Data	MIPS - Ano	Algoritmo
100	332	04/1991	7	sieve quadrático
110	365	04/1992	75	sieve quadrático
120	398	06/1993	830	sieve quadrático
129	428	04/1994	5000	sieve quadrático
130	431	04/1996	500	No. de campo sieve generalizado

Pentium 200 MHz = 50 MIPS

MIPS ano para fatorar

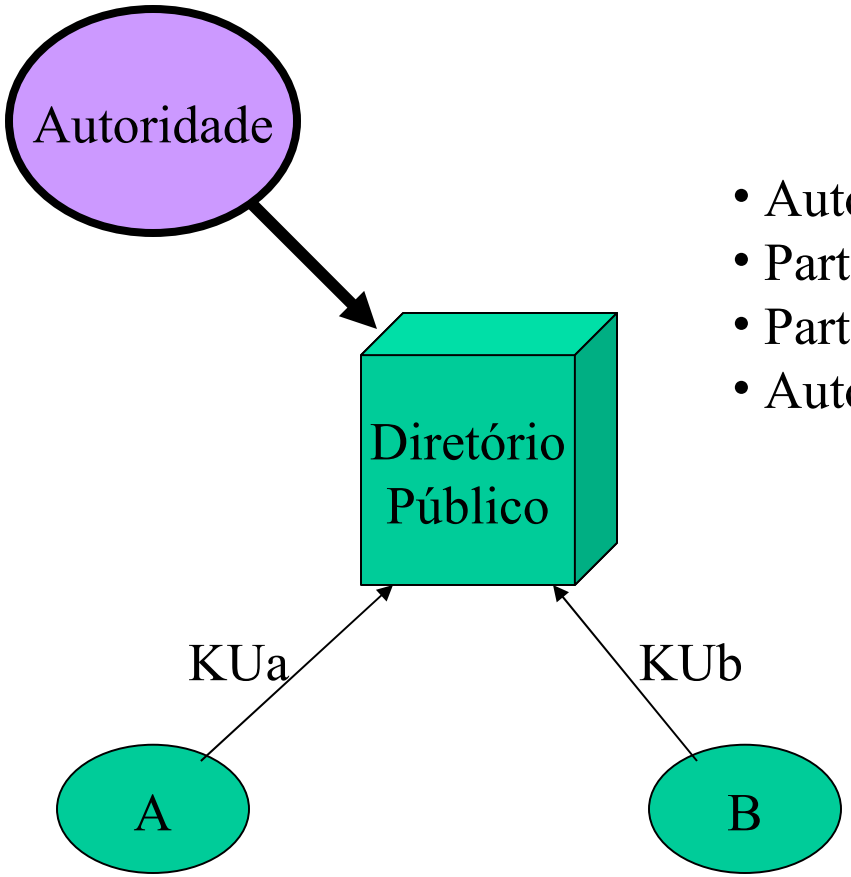


Prof. Ricardo Felipe Custódio, D.Sc.
INE-CTC-UFSC

Gerenciamento de Chaves

- Distribuição de Chaves Públicas
  - Anúncio Público (Ex: PGP)
  - Diretório Público
  - Autoridade de Chave Pública
  - Certificados de Chave Pública
- Chave Pública para Distribuir Chave Secreta
  - Distribuição Simples de Chaves Secretas
  - Distribuição com Confidencialidade e Autenticação
  - Esquema Híbrido

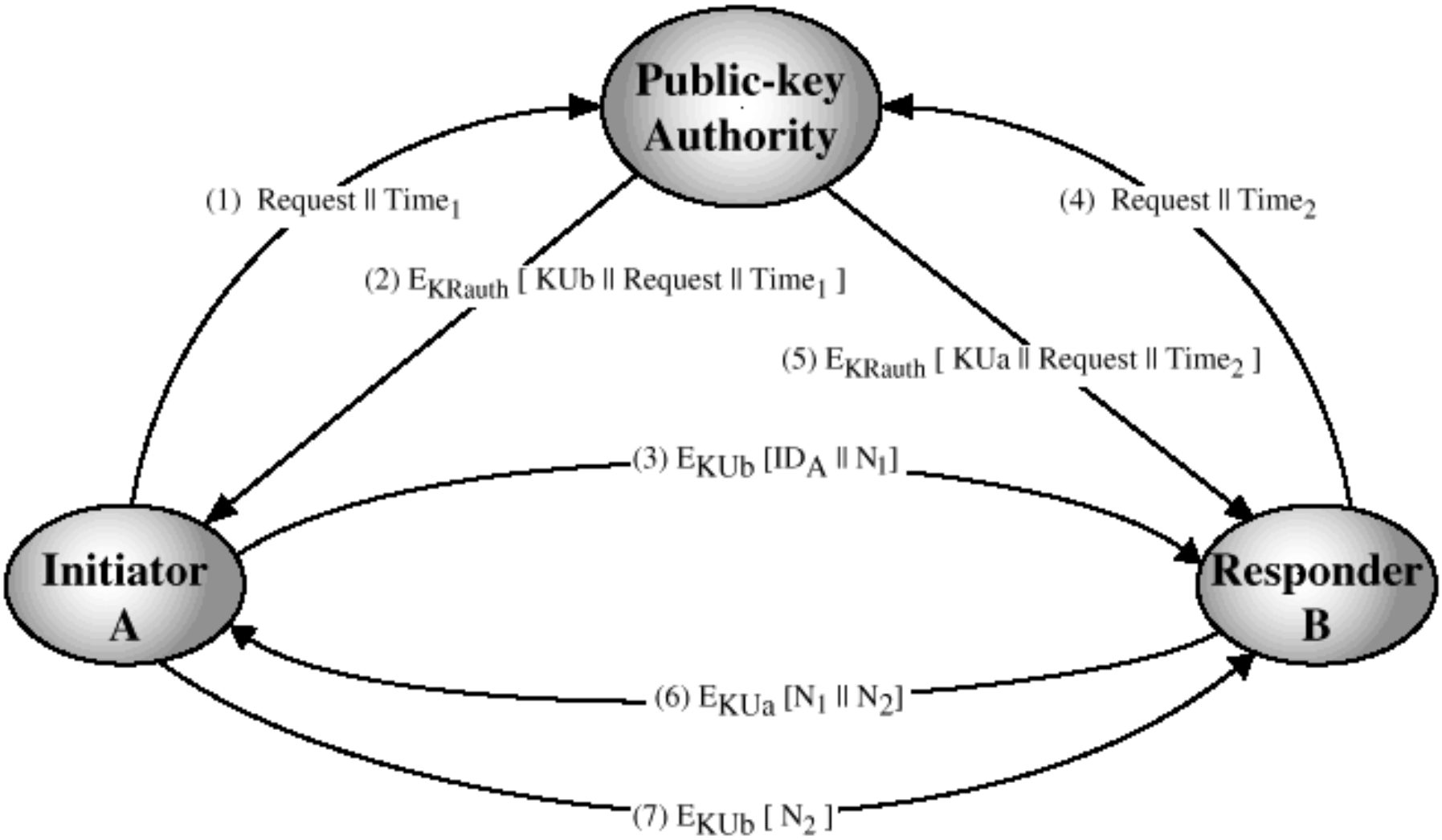
Diretório Público



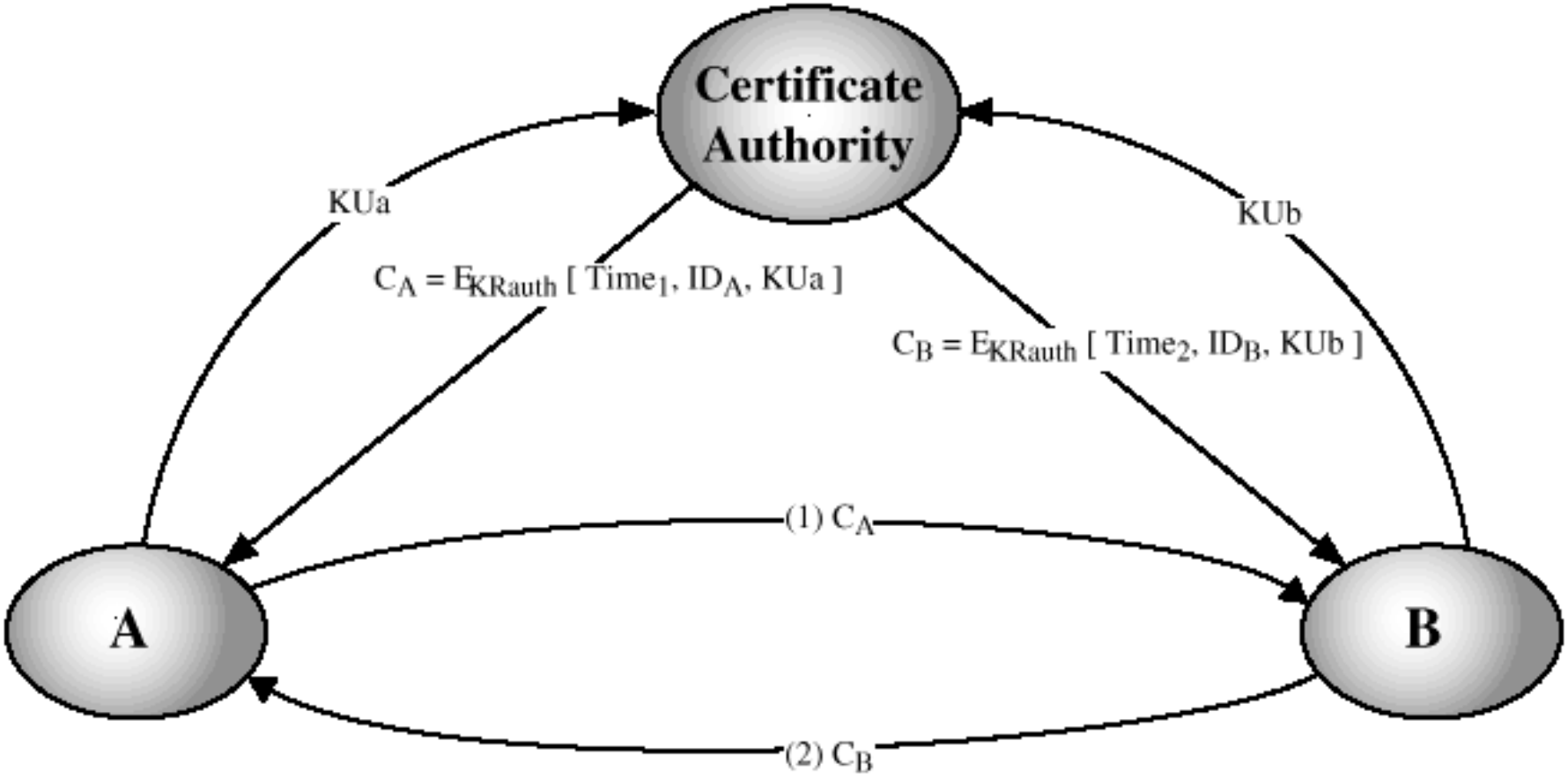
Elementos

- Autoridade Mantém {**Nome**; **Chave Pública**}
- Participante Registra sua Chave Pública
- Participante pode trocas sua Chave Pública
- Autoridade publica Diretório Periodicamente

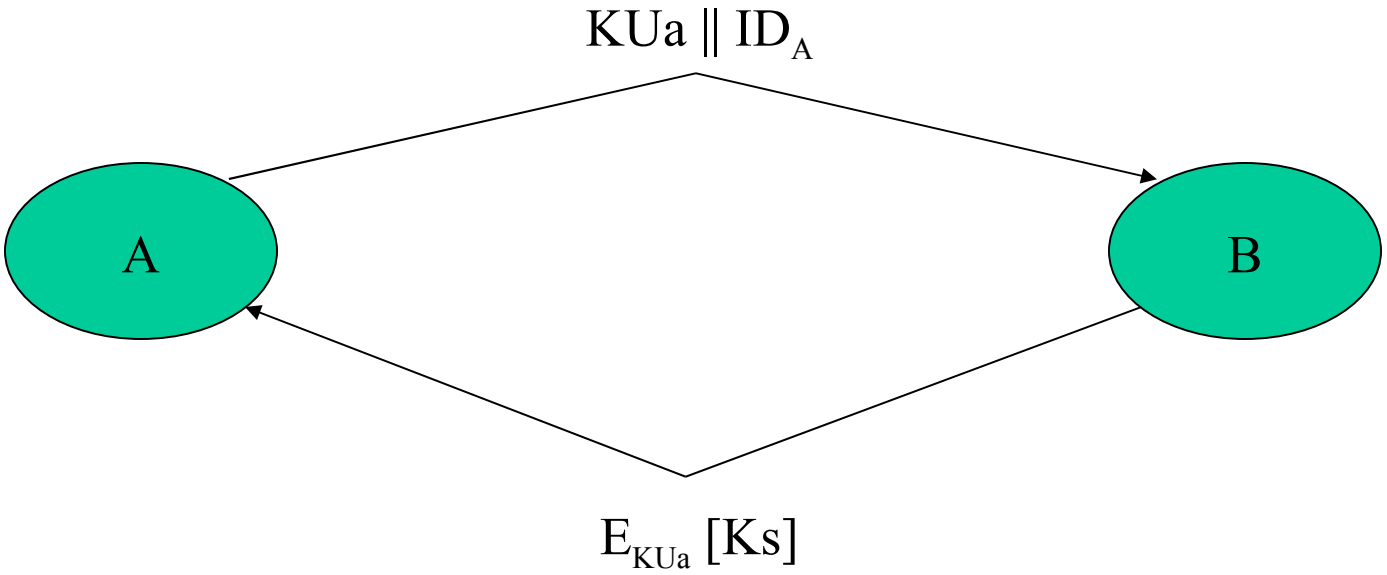
Autoridade de Chave Pública



Certificados de Chave Pública

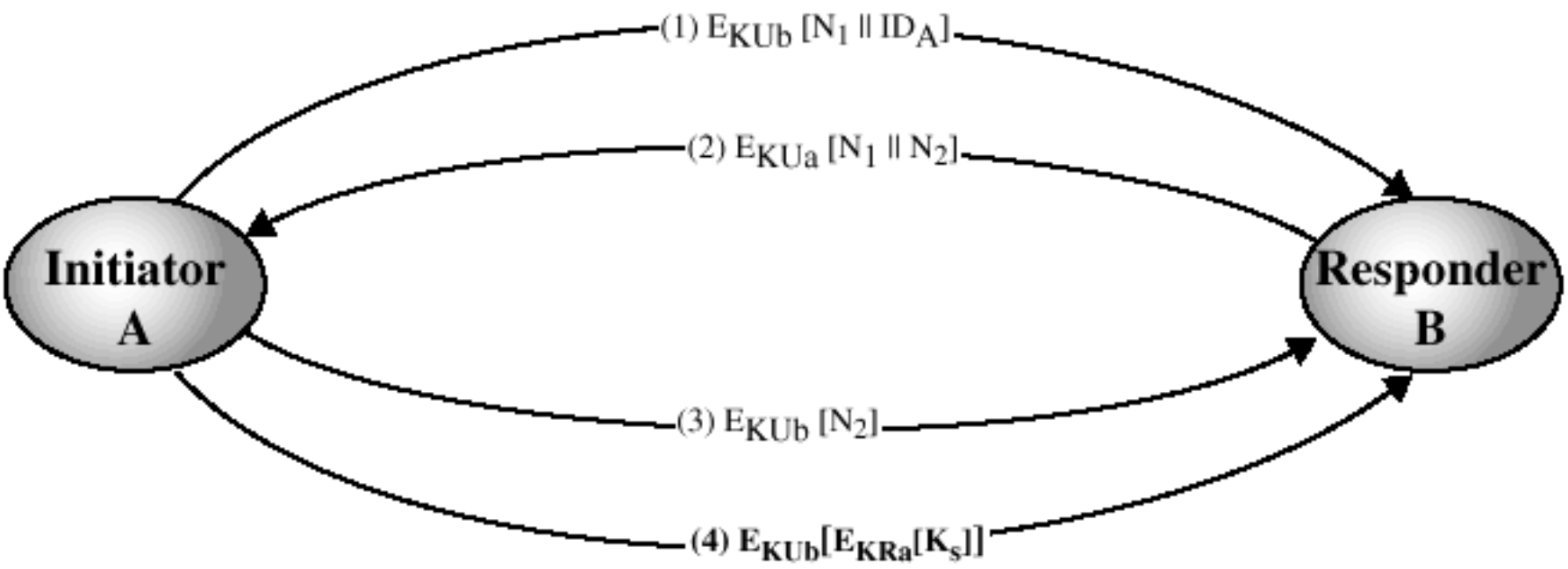


Distribuição Simples de Chaves Secretas



- Protocolo Simples
- As chaves só existem durante a comunicação
- Problema com a Interceptação

Distribuição de Chaves Secretas com Confidencialidade e Autenticação



Esquema Híbrido

- KDC - Key Distribution Center
- Usa chave pública para troca de chave mestre
- Usa chave mestre para troca de chave de sessão

Usado pela IBM nos mainframes
Motivo: Desempenho

Raiz Primitiva e Logaritmo Discreto

q - Número Primo
α < q - raiz primitiva de **q**

Raiz Primitiva **a**:
{**a mod p, a^2 mod p, ..., a^{p-1} mod p**} são distintos e consistem dos inteiros de 1 a p-1

Logaritmo Discreto **i**:
$b = a^i \bmod p$, onde $0 \leq i \leq (p-1)$
$ind_{a,p}(b)$

Exercício

Calcular as raízes primitivas de 7

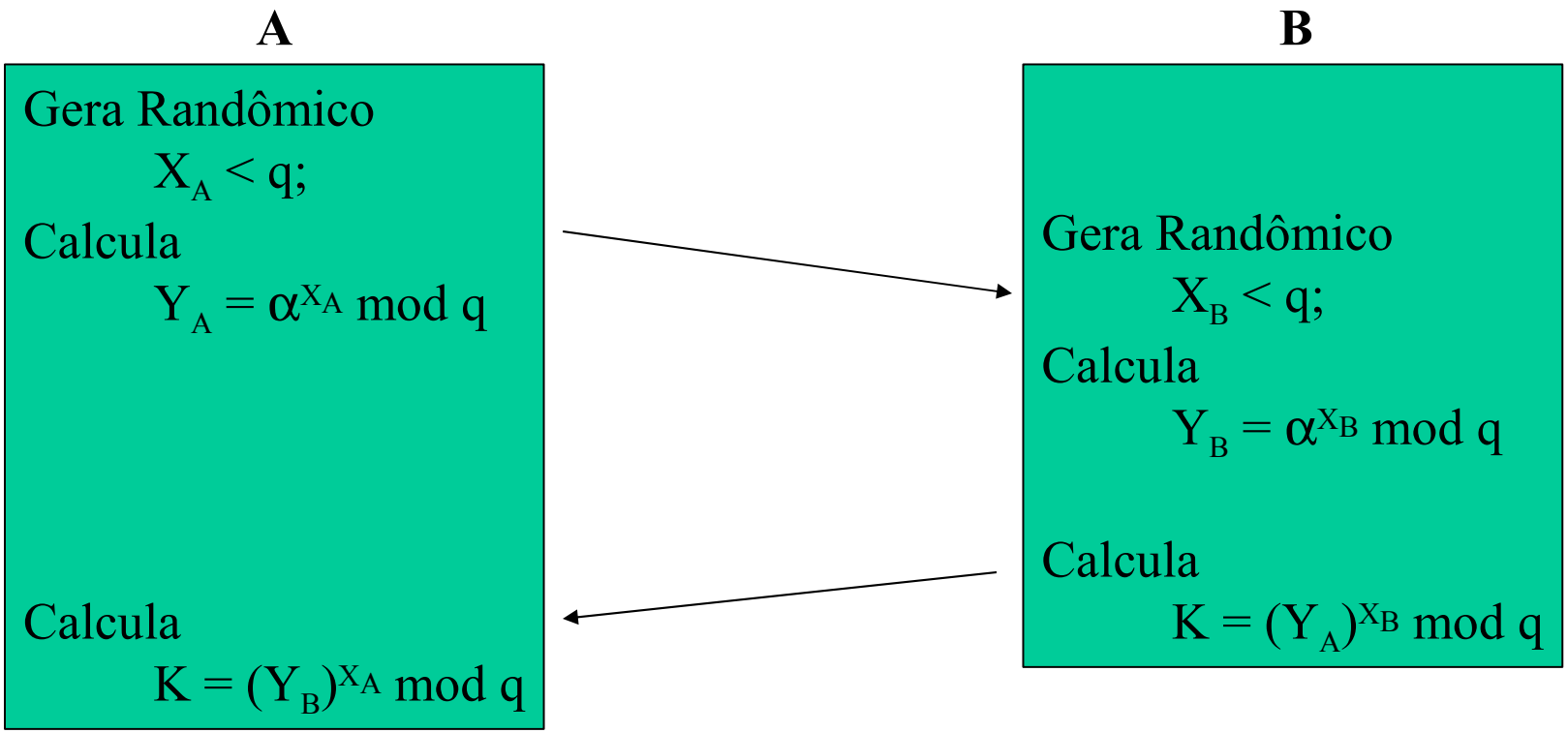
a	a^2	a^3	a^4	a^5	a^6
1					
2					
3					
4					
5					
6					

Prof. Ricardo Felipe Custódio, D.Sc.
INE-CTC-UFSC

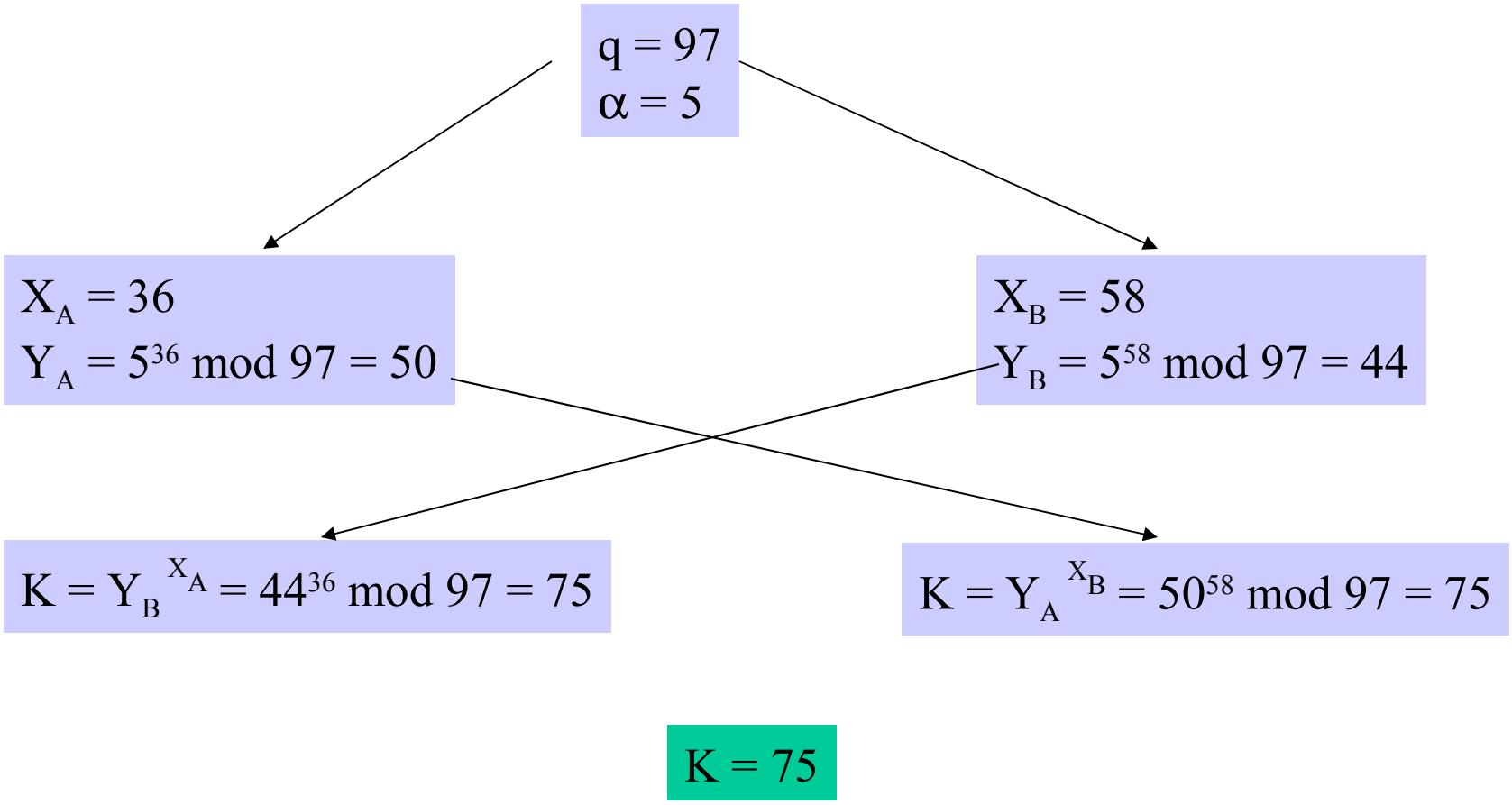
1976

Troca de Chaves por Diffie-Hellman

q - Número Primo, $\alpha < q$ - raiz primitiva de q



Exemplo


q = 97
α = 5
$X_A = 36$
$Y_A = 5^{36} \bmod 97 = 50$
$X_B = 58$
$Y_B = 5^{58} \bmod 97 = 44$
$K = Y_B^{X_A} = 44^{36} \bmod 97 = 75$
$K = Y_A^{X_B} = 50^{58} \bmod 97 = 75$
K = 75