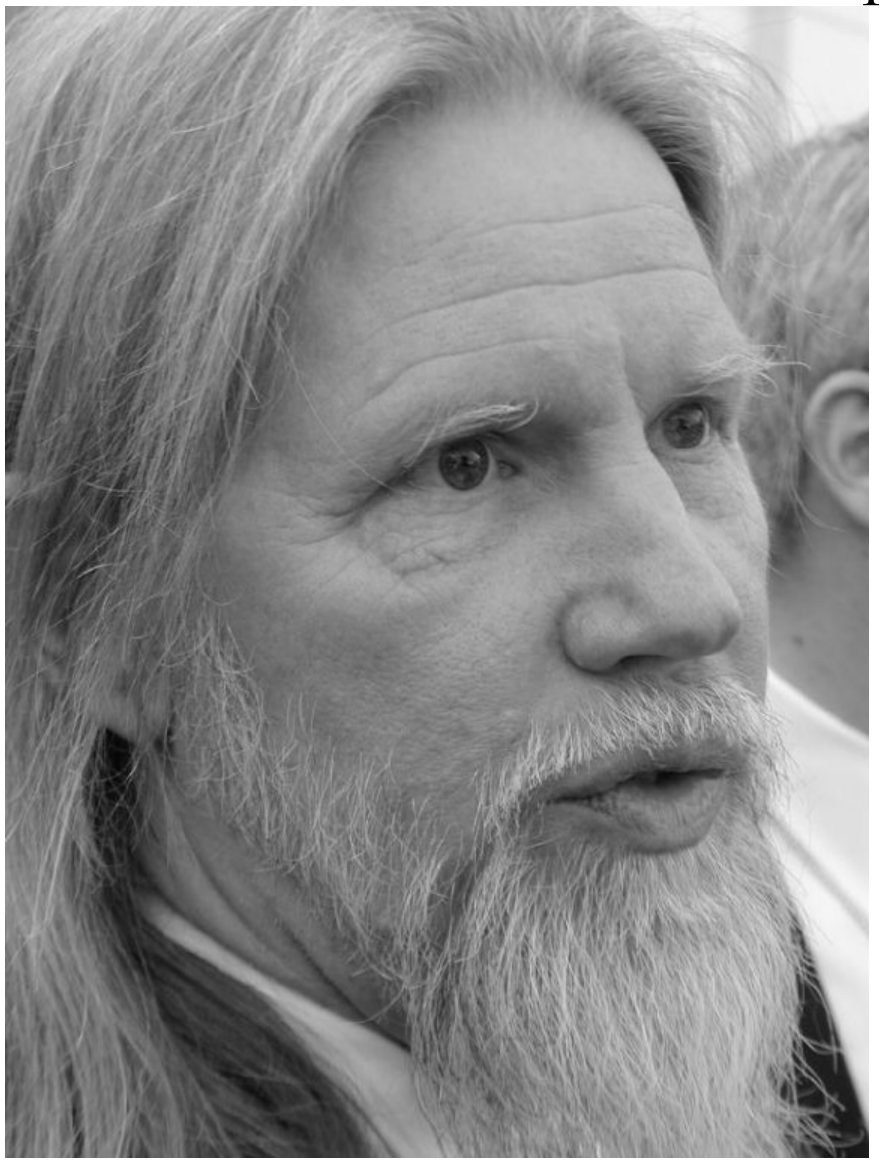
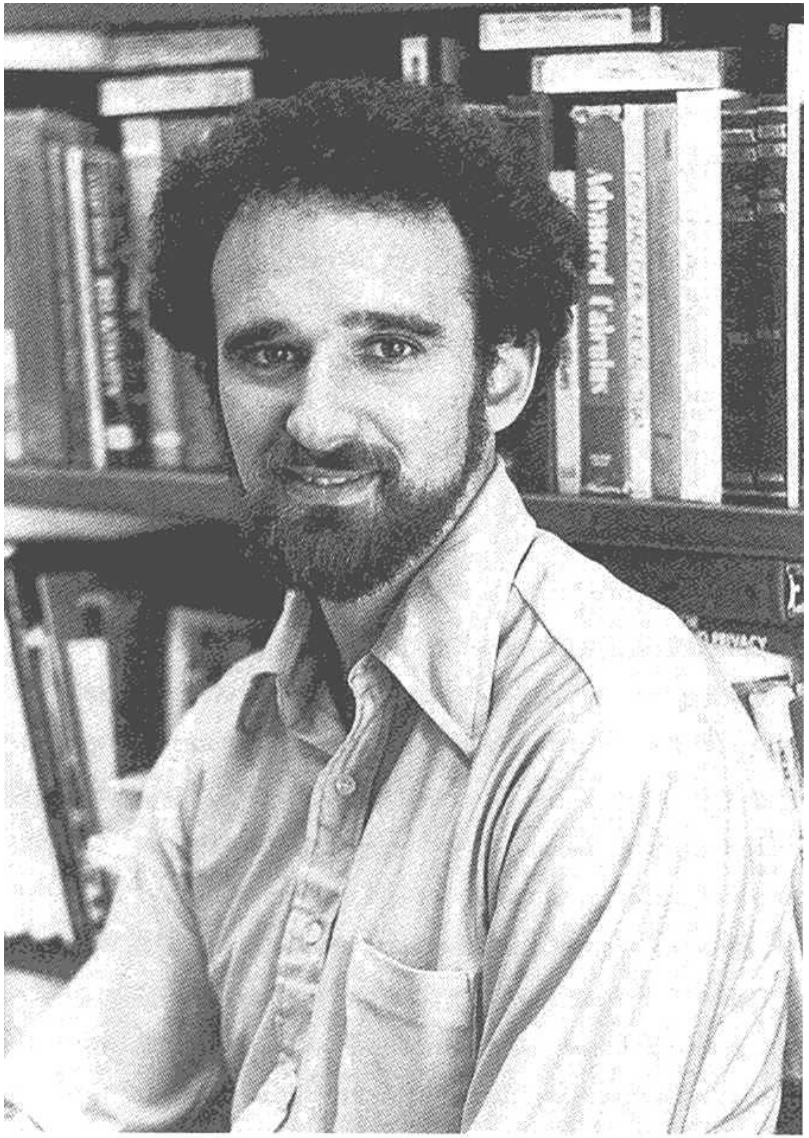
Criptografia por Chave Pública Diffie e Helmann

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

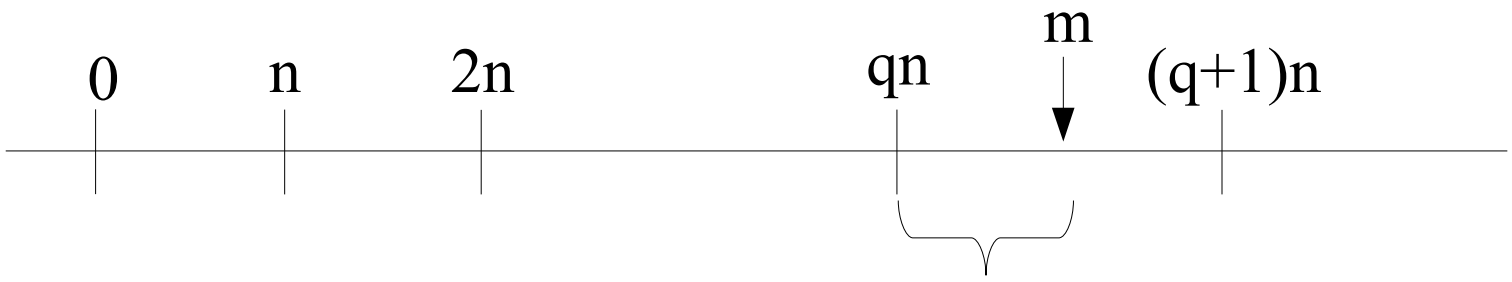
Diffie 1976 **Hellman**





Divisão de Inteiros

$$\begin{array}{r|l} m & n \\ \hline r & q \end{array}$$



Aritmética Modular

Dois inteiros **a** e **b** são congruentes módulo **n** se

(a mod n) = (b mod n)

ou

a ≡ b mod n

Exemplo:

73 ≡ 4 mod 23; 21 ≡ -9 mod 10

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

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

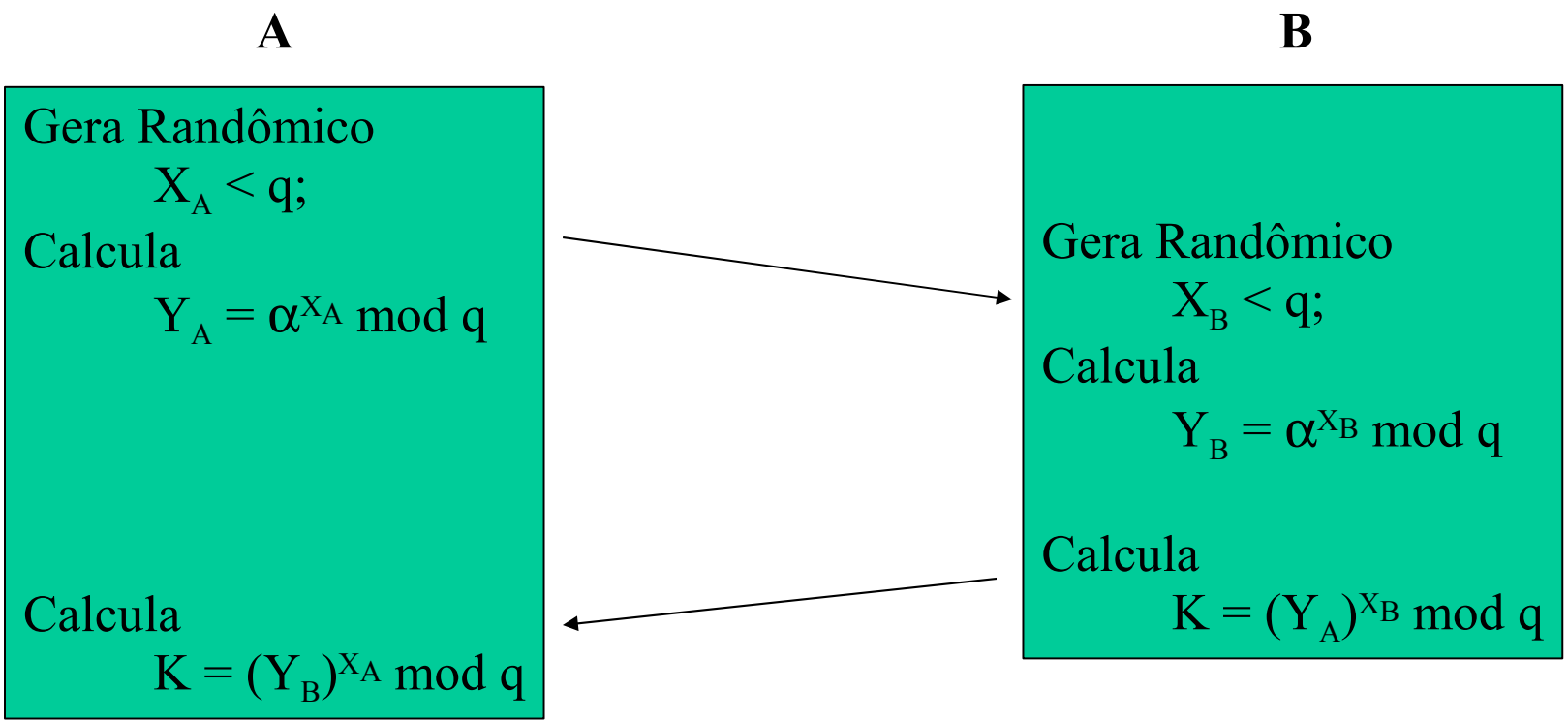
a	a^2	a^3	a^4	a^5	a^6
1					
2					
3					
4					
5					
6					

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

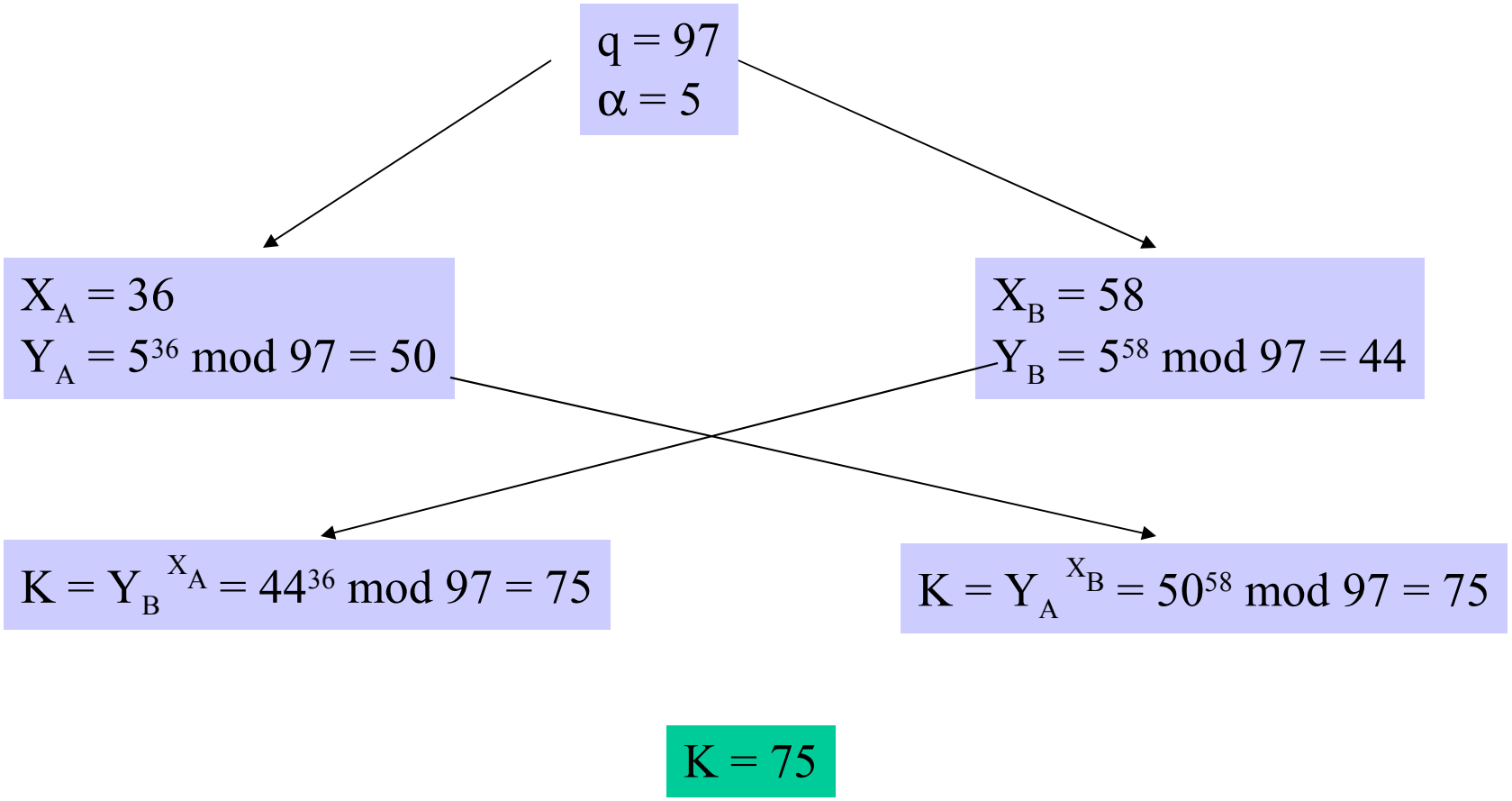
1976

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