INE 5429
Acordo de Chaves de Hellman

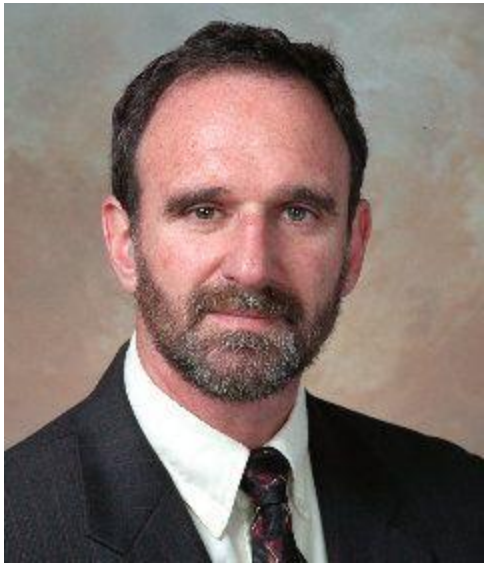
Prof. Ricardo Felipe Custódio
custodio@inf.ufsc.br

Nascimento: 5 de Junho de 1944

Graduado em Matemática: 1964 pelo MIT

Doutorado: Stanford University.

Vice-presidente da ICANN.



Nascimento: 2 de Outubro de 1945

Graduado: 1966

Mestrado e Doutorado: Stanford University em 1967 e 1969.

Professor Emetirus da Stanford University.

Raiz Primitiva

Operador Multiplicação sobre Z_p^*

p - Número Primo
a < q - Raiz Primitiva de p

Raiz Primitiva a de p é um número x tal que

$$\{x \bmod p, x^2 \bmod p, \ldots x^{p-1} \bmod p\}$$

são todos disjuntos e consistem dos números inteiros de 1 a p-1

Exemplo

Verifique se a = 3 é uma raiz primitiva de p = 7

$\{3 \bmod 7, 3^2 \bmod 7, 3^3 \bmod 7, 3^4 \bmod 7, 3^5 \bmod 7, 3^6 \bmod 7\} =$

{3, 2, 6, 4, 5, 1}

Portanto, 3 é uma raiz primitiva de 7.

Raízes Primitivas de 7

Operador Multiplicação

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

Pode-se observar que 7 tem duas raízes primitivas: 3 e 5.

Exemplos de Raízes Primitivas de a

a	Raízes Primitivas											
2												
3	2											
5	2	3										
7	3	5										
11	2	6	7	8								
13	2	6	7	11								
17	3	5	6	7	10	11	12	14				
19	2	3	10	14	15							
23	5	7	10	11	14	15	17	19	20	21		
29	2	3	8	10	11	14	15	18	19	21	26	27
31	3	11	12	13	17	21	22	24				

Encontrando Raízes Primitivas

Não existe uma fórmula geral simples para se determinar raízes primitivas

Existem métodos mais rápidos que simplesmente tentar todos os candidatos

Algorítmo para Determinar uma Raiz Primitiva

1. Determine Ø(n)
2. Determine os diferentes fatores primos (p_1, p_2, ..., p_k) de Ø(n)
3. Para todo m de Z_{n^*}, compute $m^{Ø(n)/pi}$ mod n, para i = 1,...,k
4. Um número m para o qual todos esses k valores sejam diferentes de 1 é uma raiz primitiva

Exemplo: n = 13, Ø(13) = 12 = 3 x 2^2

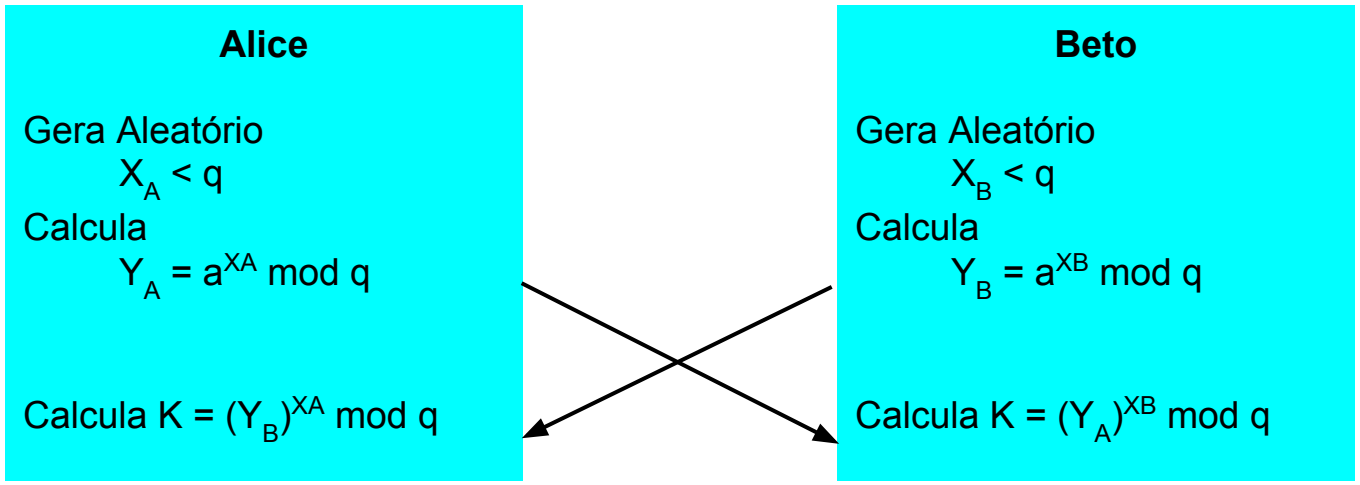
m	$m^{Ø(13)/3}$ mod 13	$m^{Ø(13)/2}$ mod 13
2	$2^4 = 3$	$2^6 = 12$
3	$3^4 = 3$	$3^6 = 1$
4	$4^4 = 9$	$4^6 = 1$
5	$5^4 = 1$	$5^6 = 12$
6	$6^4 = 9$	$6^6 = 12$
7	$7^4 = 9$	$7^6 = 12$
8	$8^4 = 1$	$8^6 = 12$
9	$9^4 = 9$	$9^6 = 1$
10	$10^4 = 3$	$10^6 = 1$
11	$11^4 = 3$	$11^6 = 12$
12	$12^4 = 1$	$12^6 = 1$

Acordo de Chave de Diffie-Hellman

1976

Parâmetros Públicos

q = Número Primo
a = Raiz Primitiva



Exemplo

Parâmetros Públicos

q = 97
a = 5

Alice

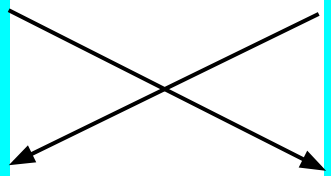
Gera Aleatório
$X_A = 36$
Calcula
$Y_A = 5^{36} \bmod 97 = 50$

Calcula $K = 44^{36} \bmod 97 = 75$

Beto

Gera Aleatório
$X_B = 58$
Calcula
$Y_B = 5^{58} \bmod 97 = 44$

Calcula $K = 50^{58} \bmod 97 = 75$



K = 75