Capítulo 10

Figura 10.1 Distribuição não controlada de chaves públicas.

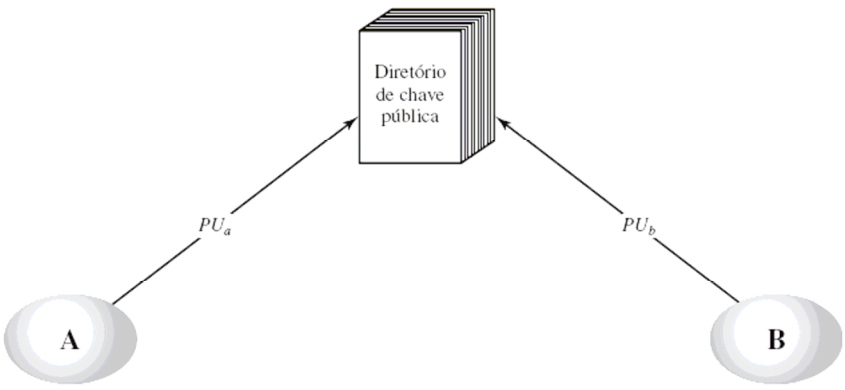

Figura 10.2 Publicação de chave pública.

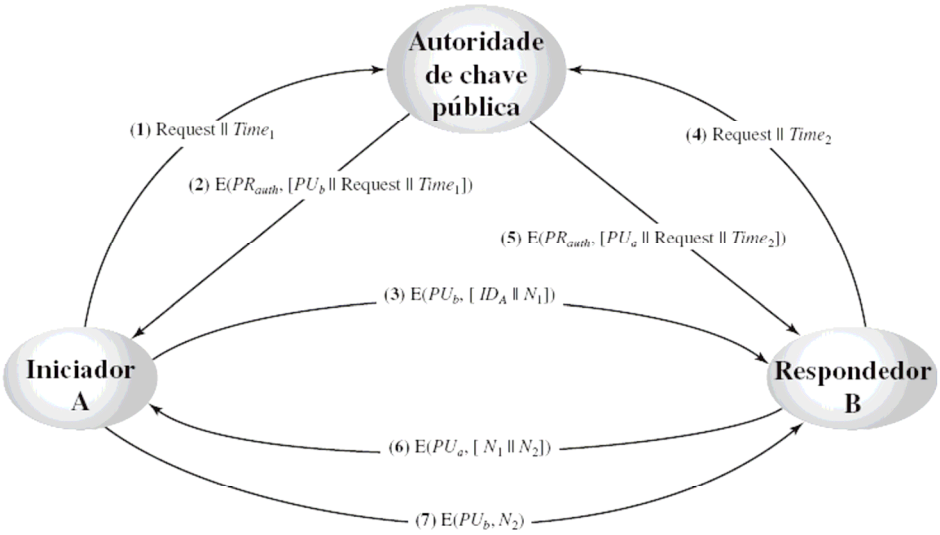

Figura 10.3 Cenário de distribuição de chave pública.

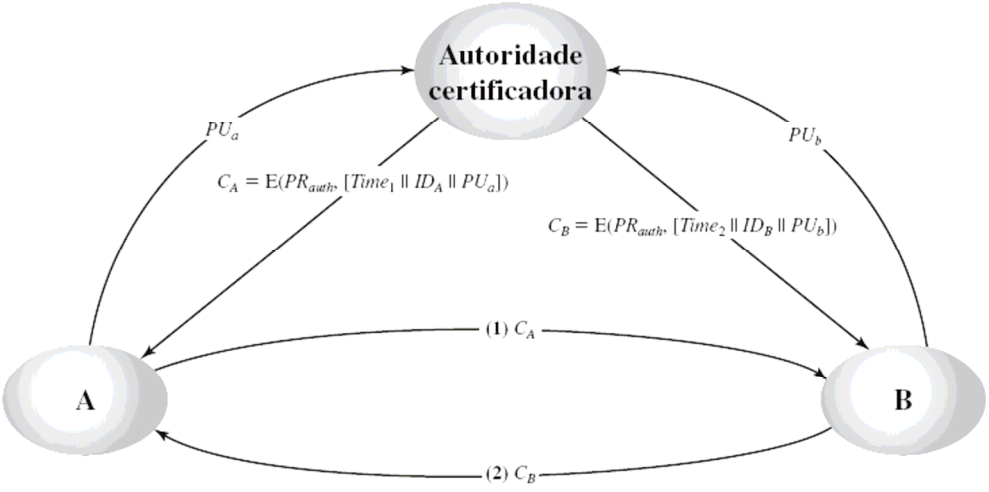

Figura 10.4 Troca de certificados de chave pública.

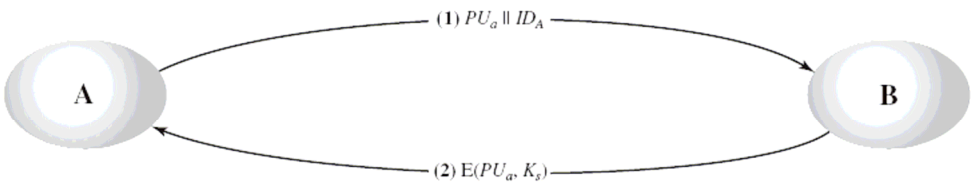

Figura 10.5 Uso simples da criptografia de chave pública para estabelecer uma chave de sessão.

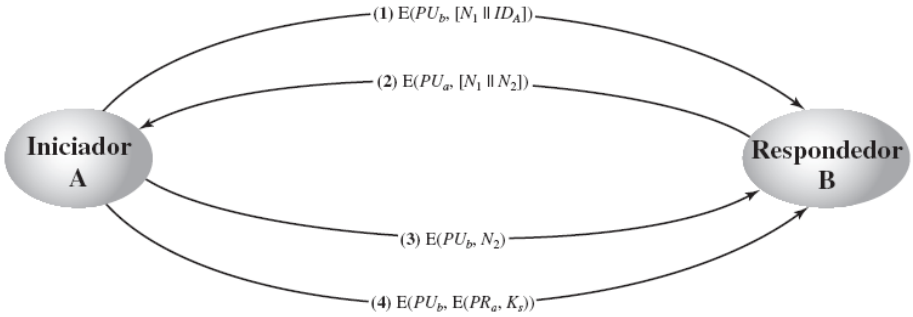

Figura 10.6 Distribuição de chaves secretas por chave pública.

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

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

Figura 10.7 O algoritmo de acordo de chaves Diffie-Hellman.

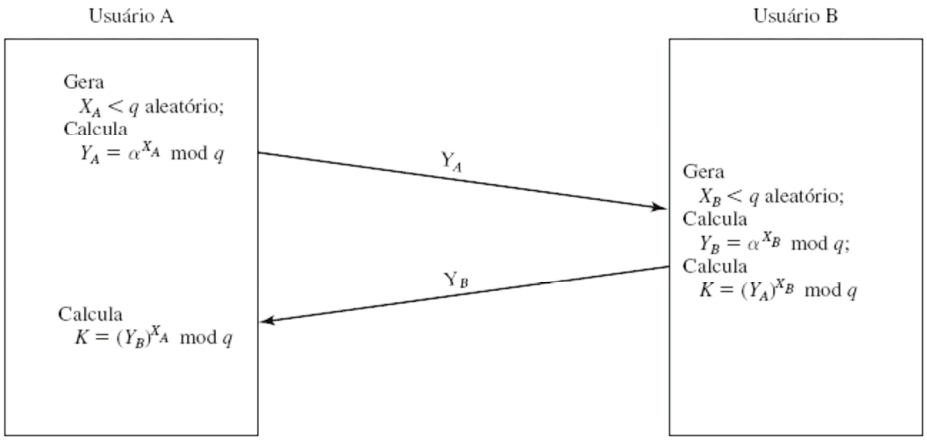

Figura 10.8 Acordo de chaves Diffie-Hellman.

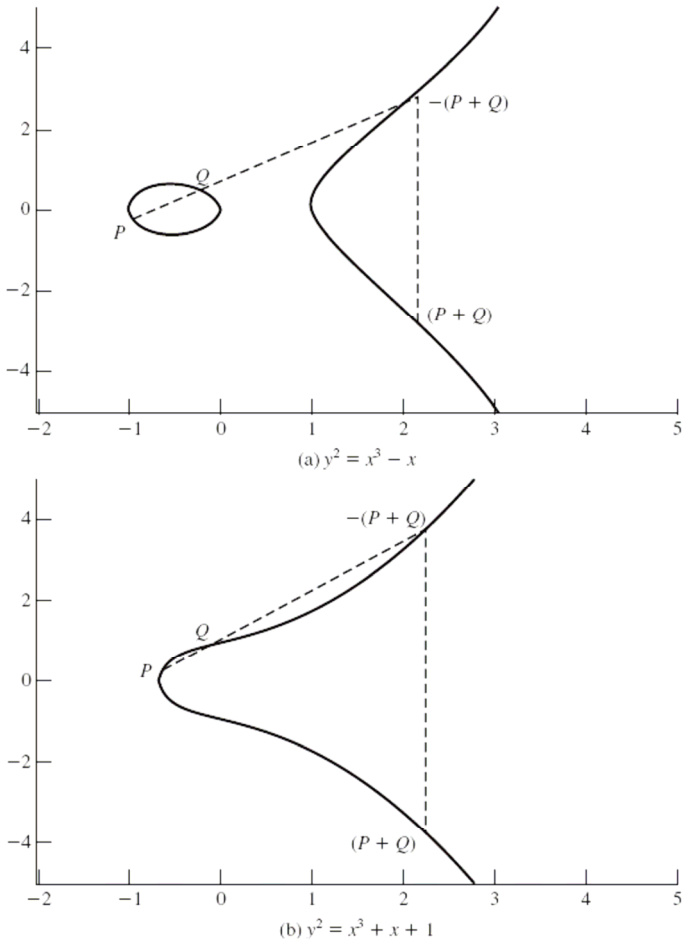

Figura 10.9 Exemplo de curvas elípticas.

Tabela 10.1 Pontos na curva elíptica $E_{23}(1, 1)$

(0, 1)	(6, 4)	(12, 19)
(0, 22)	(6, 19)	(13, 7)
(1, 7)	(7, 11)	(13, 16)
(1, 16)	(7, 12)	(17, 3)
(3, 10)	(9, 7)	(17, 20)
(3, 13)	(9, 16)	(18, 3)
(4, 0)	(11, 3)	(18, 20)
(5, 4)	(11, 20)	(19, 5)
(5, 19)	(12, 4)	(19, 18)

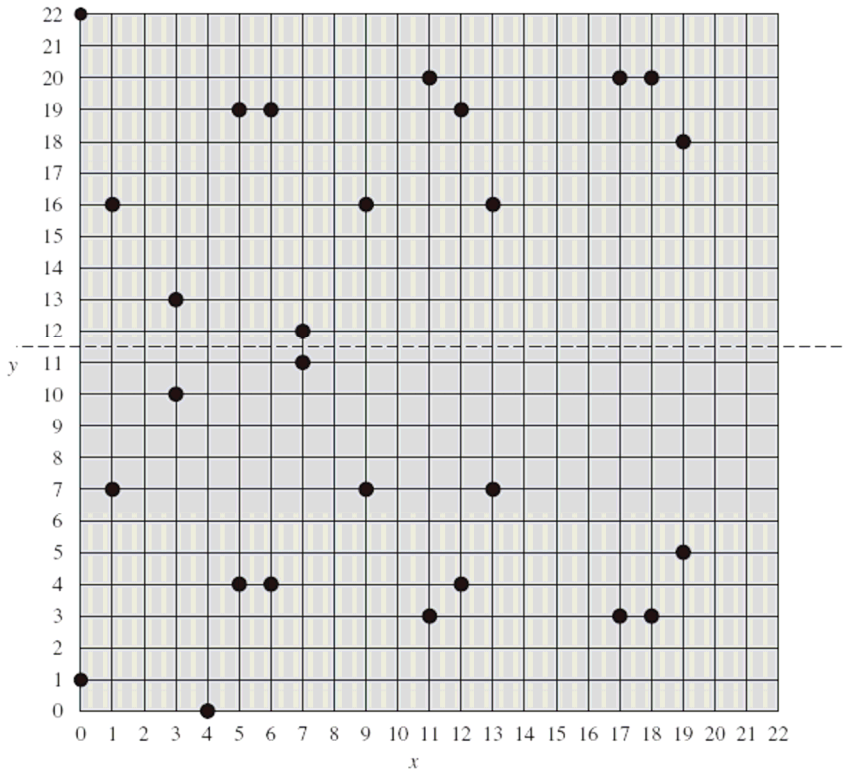

Figura 10.10 A curva elíptica $E_{23}(1, 1)$.

Tabela 10.2 Pontos na curva elíptica $E_{2^4}(g^4, 1)$

$(0, 1)$	(g^5, g^3)	(g^9, g^{13})
$(1, g^6)$	(g^5, g^{11})	(g^{10}, g)
$(1, g^{13})$	(g^6, g^8)	(g^{10}, g^8)
(g^3, g^8)	(g^6, g^{14})	$(g^{12}, 0)$
(g^3, g^{13})	(g^9, g^{10})	(g^{12}, g^{12})

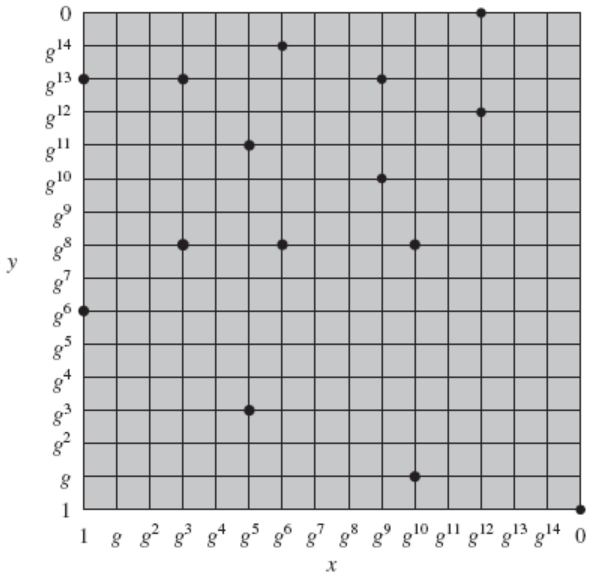

Figura 10.11 A curva elíptica $E_{2^4}(g^4, 1)$

Elementos públicos globais

$E_q(a, b)$	curva elíptica com parâmetros a, b e q, onde q é um primo ou um inteiro na forma 2^m
G	ponto na curva elíptica cuja ordem é o valor grande n

Geração de chave do usuário A

Selecione privada n_A	$n_A < n$
Calcule pública P_A	$P_A = n_A \times G$

Geração de chave do usuário B

Selecione privada n_B	$n_B < n$
Calcule pública P_B	$P_B = n_B \times G$

Cálculo da chave secreta pelo usuário A

$K = n_A \times P_B$

Cálculo da chave secreta pelo usuário B

$K = n_B \times P_A$

Figura 10.12 Acordo de chaves Diffie-Hellman elíptico.

Tabela 10.3 Tamanhos de chave comparáveis em termos de esforço computacional de criptoanálise

Esquema simétrico (tamanho da chave em bits)	Esquema baseado em ECC (tamanho de n em bits)	RSA/DSA (módulo tamanho em bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Fonte: Certicom