Criptografia assimétrica

ou Criptografia de Chave Pública

- Chaves diferentes são usadas na cifragem e na decifragem.
- Uma dessas chaves é tornada pública e a outra é mantida secreta (privada).

$C = E(K_{pub}, M)$ $\qquad\qquad$ $M = D(K_{priv}, C)$

- Em alguns algoritmos, as chaves são intercambiáveis.

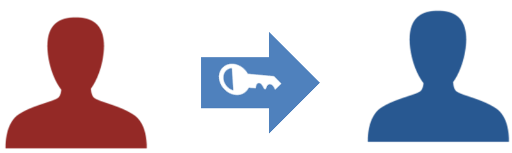
$C = E(K_{priv}, M)$ $\qquad\qquad$ $M = D(K_{pub}, C)$

Criptografia assimétrica

ou Criptografia de Chave Pública

$C = E(K_{pub}, M)$ $\qquad$ $M = D(K_{priv}, C)$

Cada um tem
o seu par
de chaves



$C = E(K_{pub}, M)$ $\qquad$ $M = D(K_{priv}, C)$

Princípio matemático

- Criação de um função unidirecional, facilmente computada, mas difícil de ser invertida.
- Exemplo:
  - é fácil multiplicar dois números primos grandes, mas é difícil fatorar o resultado para descobrir os números originais (sem se ter pelo menos um deles).
- Um algoritmo assimétrico pode ser até 10.000 vezes mais lento do que um algoritmo simétrico.

Algoritmo RSA

Rivest – Shamir – Adelman

- Escolha dois números primos extensos, p e q (maiores de 10100)
- Calcule $n = p * q$ e $z = (p - 1) * (q - 1)$
- Escolha um número relativamente primo a z e chame-o de d
- Escolha e de forma que $(e * d)\ mod\ z = 1$
- Para cifrar, calcule $C = P^e\ mod\ n$
- Para decifrar, calcule $P = C^d\ mod\ n$
- A chave pública será composta por e e n
- A chave privada será composta por d e n`

Algoritmo RSA

Rivest – Shamir – Adelman

$p = 3$
$q = 11$
$n = p \cdot q = 33$
$z = (p-1)(q-1) = 20$
$d = 7$, primo em relação a z
$e = 3$, pois $(e \cdot d) mod\ z = 1$

Cifragem

Texto	P	P^3	$C = P^3 mod(33)$
A	1	1	1
T	20	8.000	14
A	1	1	1
Q	17	4.913	29
U	21	9.261	21
E	5	125	26

Decifragem

C	C^7	$P = C^7 mod(33)$	Texto
1	1	1	A
14	105.413.504	20	T
1	1	1	A
29	17.249.876.309	17	Q
21	1.801.088.541	21	U
26	8.031.810.176	5	E