Chave assimétrica

A criptografia assimétrica é baseada em duas chaves: a chave privada e a chave pública. Imagine que você deseja transmitir um arquivo em uma rede e quer garantir que apenas o destinatário possa ler seu conteúdo. Para isso, você pode fazer uso da chave pública desse destinatário para cifrar o documento, criptografando-o. Somente com a chave privada (que fica em posse do destinatário) será possível decifrar o texto. Observe a imagem a seguir que ilustra essa situação:

Fonte: SENAI-SP

A geração dessas chaves se dá a partir de números aleatórios, normalmente, números primos. Podemos resumir esse processo conforme o exemplo a seguir, simulando o algoritmo RSA, um dos mais utilizados:

Escolha dois números primos distintos, *p* e *q*;

Calcule *n*: $n = p \cdot q$.

Calcule *z*: $z = (p - 1) \cdot (q - 1)$.

Obtenha um número *e* (sendo *e* um número primo qualquer, logo, escolha um número).

Calcule $e \cdot d(mod\ z) = 1$.

O par (*e*, *n*) é a chave pública, ao passo que o par (*d*, *n*) é a chave privada.

Acompanhe um exemplo prático:

Suponha dois números primos: p = 29 e q = 37.

$$n = p \cdot q$$
$$\text{para } p = 29 \text{ e } q = 37$$
$$n = 29 \cdot 37 = 1073$$

$$z = (p - 1) \cdot (q - 1)$$
$$z = (29 - 1) \cdot (37 - 1) = 28 \cdot 36 = 1008$$

Adotando *e* = 71, temos:

$$e \cdot d\ (mod\ z) = 1$$
$$71 \cdot d\ (mod\ 1008) = 1$$
$$d = 1079$$

Então, agora podemos montar o par de chaves:

Chave pública = (*e*, *n*) = (71, 1073)

Chave privada = (*d*, *n*) = (1079, 1073)