Como gerar as chaves

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 busca 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 abaixo:

A geração dessas chaves se dá a partir de números aleatórios, normalmente números primos. Podemos resumir esse processo como segue, simulando o algoritmo RSA, um dos mais aplicados:

- 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 (e :$número\ primo\ qualquer$, então, escolha um número)
- Calcule $e\cdot d(mod\ z)=1$
- O par (e,n) é a chave pública, e o par (d,n) é a chave privada.

Acompanhe um exemplo prático:

Suponha dois números primos: p = 29 e q = 37
Resolvendo:
Adotando: $e=71$

Então, agora podemos montar o par de chaves:
Chave pública = (e,n) = (71,1073)
Chave privada = (d,n) = (1079,1073)

undefined