RSA

Origem: Wikipédia, a enciclopédia livre.
(Redirecionado de **Rsa**)

Se procura a empresa, veja RSA Data Security, Inc.

RSA é um algoritmo de criptografia de dados, que deve o seu nome a três professores do Instituto MIT (fundadores da actual empresa RSA Data Security, Inc.), Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman, que inventaram este algoritmo — até a data (2008), a mais bem sucedida implementação de sistemas de chaves assimétricas, e fundamenta-se em teorias clássicas dos números. É considerado dos mais seguros, já que mandou por terra todas as tentativas de quebrá-lo. Foi também o primeiro algoritmo a possibilitar criptografia e assinatura digital, e uma das grandes inovações em criptografia de chave pública.

Índice

Funcionamento

O RSA envolve um par de chaves, uma chave pública que pode ser conhecida por todos e uma chave privada que deve ser mantida em sigilo. Toda mensagem cifrada usando uma chave pública só pode ser decifrada usando a respectiva chave privada. A criptografia RSA atua diretamente na internet, por exemplo, em mensagens de emails, em compras on-line e o que você imaginar; tudo isso é codificado e recodificado pela criptografia RSA.

Geração das chaves

No RSA as chaves são geradas desta maneira:

1. Escolha de forma aleatória dois números primos grandes p e q, da ordem de 10^{100} no mínimo.
2. Compute $n = pq$