

Angelo R.

Algoritmo RSA

Devo lembrar que este é meu primeiro projeto público, disfrute de todo conteúdo, pois é permitido o uso para fins de aprendizagem e comercialização.

Rivest-Shamir-Adleman, ou RSA, é um antigo sistema de criptografia de chave pública. Este sistema usa uma chave pública, que serve para encriptar, e uma privada para a deciptação. A assimetria é devido à dificuldade prática da fatoração do produto de dois números primos grandes.

No meu código, eu tentei seguir o esquema de lógica do algoritmo, sem copiar de outros códigos, somente com estudos do processo de cálculo necessário para obter a encriptação e deciptação. Apliquei esse processo em uma mensagem, basicamente então o meu código pega uma mensagem, encriptografa e descriptografa ela.



Origem do RSA

A sigla RSA é simplesmente as iniciais dos sobrenomes dos fundadores da empresa **“RSA Data Security, inc.”**, Ron **R**ivest, Adi **S**hamir e Leonard **A**dleman, três professores do Instituto MIT (Instituto de Tecnologia de Massachusetts). Fundada em 1982 e sediada em Bedford, Massachusetts, porém, a fundação sucede os acontecimentos que deram origem ao algoritmo...

Em 1977, um ano depois da ideia do sistema de criptografia de chave pública assimétrica atribuída a **Whitfield Diffie** e **Martin Hellman** serem publicadas, **Ron Rivest**, **Adi Shamir** e **Leonard Adleman** em abril, tiveram a descoberta do algoritmo RSA, que seria a solução do problema de realizar uma função unilateral, problema que Whitfield Diffie e Martin Hellman não tinham resolvido. Após curtirem uma noite de festa de Páscoa, todos foram para suas casas dormir, porém **Ron Rivest** teve uma longa noite de estudo, até que às 1 ou 2 horas da manhã, Leonard Adleman (responsável por quebrar os algoritmos criados pelos dois criptógrafos) recebe a ligação de Ron Rivest falando sobre o algoritmo que ele passou a noite planejando, deixando Leonard Adleman impressionado.

Sendo esta história o início de tudo, pois em 1978 foi publicado o artigo original ***“A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”***, que explica todo o Algoritmo RSA.