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 decriptação. 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 decriptação. 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 Diffe** 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 Diffe 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.

Operação

Como já foi mencionado algumas vezes, o Algoritmo RSA é um sistema de criptografia assimétrica, ou seja, que utiliza duas chaves (pública e privada).

As chaves são feitas com base na escolha de **dois números primos**, exemplo:

P = 3

Q = 11

Claro que estes números pequenos são apenas para o exemplo, num algoritmo real são utilizados números primos enormes, para dificultar a quebra do algoritmo.

Após escolher os números primos, é calculado o produto destes números:

N = P * Q

N = 3 * 11 = 33

Agora surge uma parte mais complexa... Calcular a ***função totiente de Euler - φ (x).***

A função totiente de Euler, ou função phi, é uma fórmula descoberta pelo matemático suíço **Leonhard Euler (1707 – 1783)**, resumidamente ela conta a quantidade de inteiros positivos que são **coprimos e menores** que x.

E para quem não sabe o que são **coprimos**, simples, **são números que o único divisor comum deles é 1**. Por exemplo:

$\phi(8) = 4$

Pois os **coprimos** de **8** são: **1**, **3**, **5** e **7**.

Então, se você entendeu o que é a função totiente de Euler, prosseguiremos com o uso dela no algoritmo. Agora terá que calcular o $\phi(N)$, porém existe um truque, pois como os valores de N são P e Q, dois números primos, existe um jeito simples:

$\phi(N) = (P - 1) * (Q - 1)$

$\phi(N) = (3 - 1) * (11 - 1) = 20$

$L = \phi(N) = 20$

Essa facilidade ocorre, pois, os coprimos de um número primo, são todos os divisores com exceção do 1.

Agora precisamos escolher um valor para a chave pública "e", assumindo que $1 < e < N$.