# Criptografia RSA

A criptografia RSA é um dos algoritmos de encriptação mais seguros e populares existentes atualmente. Seu funcionamento baseia-se em princípios matemáticos, e se trabalhado com chaves grandes o suficiente, é sem duvidas um excelente algoritmo para se implementar. O nome RSA, vem das letras iniciais dos nomes de seus desenvolvedores: Ronal Rivest, Adi Shamir e Leonard Adleman. O método utilizado pela criptografia RSA é revelar publicamente uma chave, chamada de chave pública, e esconder a chave de decodificação correspondente, chamada de chave privada.

Antes de falarmos sobre como funciona a criptografia RSA, devemos lembrar alguns conceitos importantes da matemática, o qual a criptografia RSA se baseia bastante.

**Números primos**: são os números naturais que têm apenas dois divisores diferentes: o 1 e ele mesmo. Exemplos: 2, 3, 5, 7, 11, 13, ...

**Números coprimos**: são chamados de coprimos, ou primos entre si, os números onde o único divisor comum entre eles é apenas o número 1. Exemplo: (2 e 3), (8 e 9), (27 e 29).

**Função Phi (Função Totiente)**: Para um número natural n, a função Phi (φ) é definida como sendo igual à quantidade de números menores que n, coprimos com respeito a ele. Exemplo: φ(8) = 4, pois 1, 3, 5 e 7 são coprimos de 8.

Função de Phi de um número primo é sempre o este número menos 1. Portanto, se x é primo, φ(x) = x - 1. Exemplos: φ(5) = 4 (1, 2, 3, 4). Se p e q são primos, φ(pq) = (p - 1)(q - 1).

Após relembrados alguns conceitos matemáticos importantes, vamos ver como funciona a lógica por trás da criptografia RSA.

Para iniciarmos, definiremos duas variáveis (**p**, **q**) com um número primo em cada. Em nosso código, definimos ***p*** *= 17* e ***q*** *= 23*.

Logo após, definiremos o produto desses dois números de **n** = **pq**. Fazendo a soma segundo os valores inseridos inicialmente, ***n*** *= 17 X 23 =>* ***n*** *= 391.* n será nossa primeira chave publica do código. Essa chave pode ser divulgada para a pessoa que queria montar uma mensagem criptografada e esta mensagem só poderá ser decodificada com as chaves que iremos montar a seguir.

Próximo passo, iremos montar a função Phi de **n**, representada por **φ(n)**. Como mostramos anteriormente, a função Phi de n será o resultado de ***φ(n)*** *= (****p*** *- 1)(****q*** *- 1)*. Seguindo nosso código, ***φ(n)*** *= (16)(22)* => ***φ(n)*** *= 352*.

Para definirmos o valor de *e*, precisamos escolher um número que satisfaça a condição de *1 >* ***e*** *>* ***φ(n)***, ou seja, ***e*** precisa ser um coprimo de ***φ(n)***. Neste caso, o primeiro coprimo de 352, é 3, portanto ***e*** *= 3*. Desta forma, temos nossa segunda chave pública, totalizando como chaves públicas “***n****”* e “***e****”*.

Para gerar a nossa chave privada, devemos resolver o valor de ***b*** *= (2* ***φ(n)*** *+ 1)/****e.*** Seguindo nosso código, ***b*** *= (2 X 352 + 1) / 3* => ***b*** *= 235*.

Sendo assim, temos como chaves publicas, (***n*** *= 391* e ***e*** *= 3*), e chaves privadas (***b*** *= 235*).

No próximo passo, escolheremos ‘ola’ como nossa palavra que será codificada usando RSA. Criamos um padrão de números equivalentes para cada letra do alfabeto. Esse padrão será uma sequencia, inciado por “a” valendo 10 e finalizado por “z” valendo 35. Portanto, podemos definir que a nossa palavra ‘ola’, no fim, se torne as sequencias de números “24 - 21 - 10”.

Para codificar esta frase, utilizaremos a função de codigficação:

C = M^e mod (n)

Onde “M” é a nossa mensagem para ser codificada e C, o resultado gerado pela codificação. Seguindo nosso exemplo, temos:

C = 24^3 mod (391)

O resultado de C será então, 139. Este é o valor codificado através da criptografia RSA. Ao fazermos o mesmo com os outros valores da nossa frase, teremos um retorno parecido com “139 268 218”.

Para decodificarmos esses valores agora, iremos fazer o uso da nossa chave privada. Por isso é importante que esta chave não esteja sobre controle de ninguém que não deva decodificar nossa frase. Para realizar essa operação, utilizaremos a fórmula:

M = C^d mod (n)

Onde “C” será o nosso código que queremos passar para o valor em equivalência à nossa frase, e “M” o resultado desse valor. Seguindo nosso exemplo, teremos:

M = 139^235 mod (391)

O resultado de M, será novamente, 24, o valor equivalente a letra “o”. Após passar todos os valores por essa fórmula, obteremos os valores “24 - 21 - 10”, que, ao transformarmos para as suas respectivas letras, voltam a ser a palavra “ola”.