No RSA as chaves são geradas desta maneira:

* Primeiramente é necessário escolher 2 números primos de forma aleatória, vou chamar esses números primos de “p” e “q”, para fins didáticos;
* Calcule N, ele é o resultado do produto dos dois números primos anteriormente escolhidos;
* Calcule a função de Carmichael: Θ(N)=(p-1) \*(q-1)
* Só é necessário mais um passo para criptografar sua mensagem, é necessário escolher um número “E”. Esse número “E” tem que ser maior que 1 e menor que Θ(N), de forma que “E” e Θ(N) sejam primos entre si;

Vamos supor que queira criptografar a letra b para isso vou atribuir um valor numérico para b, b agora vale 2(escolhi esse número, pois b é a segunda letra do alfabeto), agora vamos aplicar o que vimos anterior mente:

* Aplique a função: b^E(mod N)

2^5(mod 14)

32(mod 14) = 4

* Temos o numero 4 e usando a mesma lógica com que atribuímos o valor a b vamos fazer com o numero 4, qual é a quarta letra do alfabeto? D e essa é sua letra criptografada

Depois de criptografar sua mensagem vamos precisar de uma maneira para decriptografar:

* Para decriptografar sua letra vamos ter que encontrar um número “D” e para isso vamos usar a seguinte formula: D\*E\*(mod Θ(N)) =1

5\*D\*(mod 6) =1

5\*11\*(mod 6) =1

* Temos nosso número “D”, mas você deve estar se perguntado o porque eu não user o D = 5, fiz isso porque “D” não pode ser igual a “E” então peguei o próximo numero que satisfazia a formula.
* Aplique a função: d^D(mod N)

4^11(mod 14)

4194304(mod 14) = 2

* Temos o numero 2 agora é só pegar a segunda letra do alfabeto que é a letra b, sua mensagem está decriptografada .

Links:

<https://www.youtube.com/watch?v=4zahvcJ9glg>

<https://www.youtube.com/watch?v=oOcTVTpUsPQ&t=1s>

<https://pt.wikipedia.org/wiki/RSA_(sistema_criptogr%C3%A1fico)>

<https://medium.com/@tarcisioma/algoritmo-de-criptografia-assim%C3%A9trica-rsa-c6254a3c7042>