Universidade de Brasília
Departamento de Ciência da Computação

Disciplina: Segurança computacional 2020/1
Prof. João José costa Gondim
Aluno: Diego Antônio Barbosa Cardoso 16/0005116

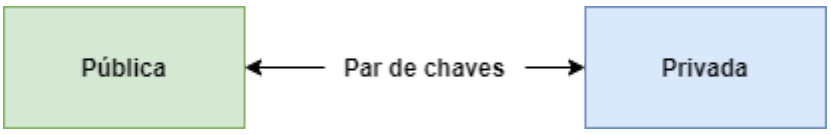
- Gerador/verificador de assinaturas RSA-

Geração de chaves:

Para o funcionamento do **RSA**, são gerados um par de chaves contendo uma chave pública e uma chave privada. A chave pública pode ser usada para cifrar qualquer dado arbitrário, mas não pode decifrá-lo. Já a chave privada pode ser usada para decifrar qualquer dado cifrado por sua chave pública correspondente, isso significa que podemos dar nossa chave pública para quem quisermos e eles podem cifrar todas as informações que desejam nos enviar, e a única maneira de acessar essas informações é usando nossa chave privada para decifrá-la. A Geração de chaves é feita da seguinte maneira:

1. São escolhidos de forma aleatória dois números primos grandes **P** e **Q** que tem um tamanho mínimo de 1024 bits.
2. É calculado um valor **N** que é igual a: **P * Q.**
3. depois é calculado a função **totient phi(N)** que é igual a: **(P - 1) * (Q - 1).**
4. Depois devemos escolher um número inteiro **E** que siga a seguinte regra: **1 < E < phi(N)** e além disso eles devem ser coprimos.
5. Depois devemos calcular o **D** que é o módulo inverso de **E** e **phi(N).**

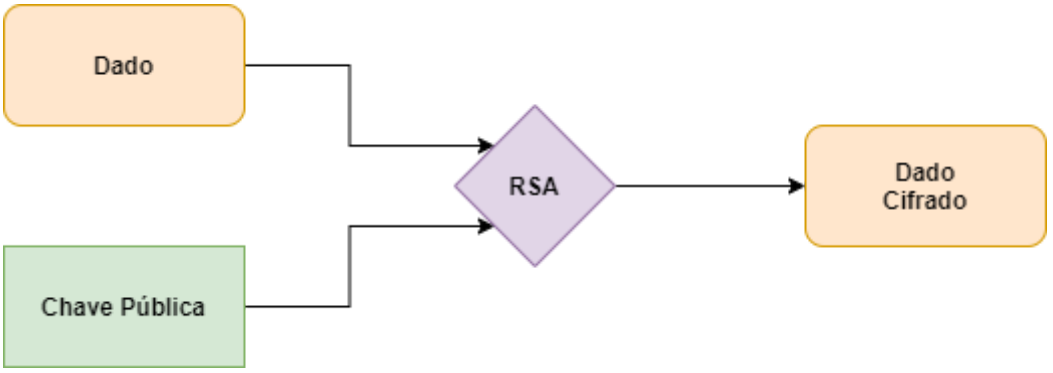
Após seguir essa sequência de passos temos as duas chaves sendo,
[N, E] a chave pública e **[N, D]** a chave privada.



Cifração:

Para cifrar uma mensagem precisamos dos números **N** e **E** que foram descritos anteriormente, pois eles são nossa chave pública, então utilizando uma potenciação modular entre **N, E** e a **mensagem** para conseguir gerar uma cifra. O processo de cifração ocorre da seguinte maneira:

1. Devemos pegar a mensagem recebida e convertê la para um número
2. Aplicação do **OAEP** para adicionarmos um padding para aumentar a segurança do **RSA** o transformando em um esquema probabilístico.
3. Realizar o seguinte cálculo $m^e \equiv c \mod n$ onde **m** é a mensagem e tanto **n** e **e** são os números gerados anteriormente.
4. O número **C** é a mensagem cifrada.

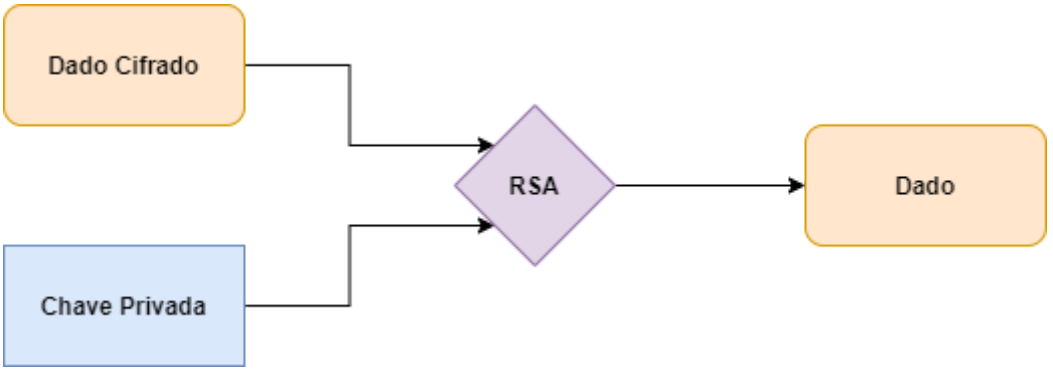


Decifração:

Para decifrar uma mensagem precisamos dos números **N** e **D** , pois eles são nossa chave privada, de maneira similar a **cifração** devemos realizar uma potenciação modular entre **N, D** e a **mensagem cifrada** para conseguirmos decifrar a mensagem. O processo de decifração ocorre da seguinte maneira:

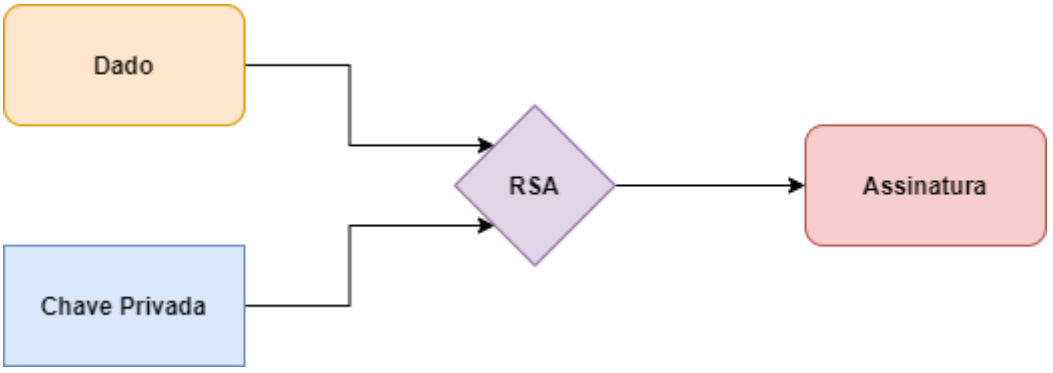
1. Realizar o seguinte cálculo $c^d \equiv m \mod n$ dessa forma obtendo a mensagem sem a cifra.

2. Realizar a remoção do **OAEP padding** para voltar a mensagem para o seu formato numérico.
3. Converter o número de volta para string.



Assinatura:

O processo de assinatura é bastante parecido com o descrito anteriormente na parte de cifração, as únicas duas diferenças são que ao invés de utilizarmos a chave pública, utilizamos a chave privada no processo de criação da cifra e além disso utilizamos uma função de hash para para criar uma assinatura pois quando formos verificar se essa assinatura bate podemos verificar se o hash é o mesmo da mensagem e se a própria mensagem é a mesma recebida.



Verificação:

Para realizarmos a verificação de uma assinatura devemos primeiro utilizar a mesma função de hash no dado bruto e checar se o hash enviado e o gerado são os mesmos caso isso ocorra, devemos agora utilizar a mesma técnica de decifração citada anteriormente na mensagem que foi assinada utilizando a chave pública, caso ambos os dados batam também então significa que a assinatura é válida caso em alguns destes dois testes mencionados ocorra um erro significa que a assinatura não é válida.