1 O algoritmo

1.1 Gerar chaves

- Escolhe-se de forma aleatória 2 numeros primos, definimos variáveis p e q para eles.
- Em seguida, calcula-se: $n = p * q$
- Calcula-se então: $\Phi(n) = (p-1) * (q-1)$
- Escolhe-se então um inteiro e, tal que $1 < e < \Phi(n)$ de forma que e e $\Phi(n)$ sejam primos entre si
- Então se calcula d de forma que $d * e \equiv 1$

Na saída dos processos acima, temos o par (n, e) que é a chave pública e a tripla (p, q, d) como chaves privadas.

1.2 Encriptação

Para transformar a mensagem m, em que $1 < m < n-1$, em uma mensagem cifrada c, utiliza-se a chave pública para calcular $m^e \equiv c \text{ mod}(n)$.

1.3 Decriptação

Para recuperar a mensagem m a partir de c, utiliza-se a chave privada do receptor n e d. Calcula-se então: $c^d \equiv m \text{ mod}(n)$.

1.4 Assinatura digital

Para implementar um sistema de assinaturas digitais com RSA, o utilizador que possua uma chave privada d poderá assinar uma dada mensagem (em blocos) m com a seguinte expressão: $s = m^d \text{ mod}(n)$.

O receptor recupera a mensagem utilizando a chave pública e do emissor: $s^e = (m^d)^e \text{ mod}(n = m) \text{ mod}(n)$.