Alice, con claves pública (n_a, e_a) y privada d_a, quiere enviar, un mensaje m cifrado y firmado a Bob, cuya clave publica es (n_b, e_b) y la clave privada d_b, el protocolo usando el RSA es el siguiente:

Firma digital RSA

Algoritmo 7 Firma RSA

Entrada: Las claves pública (n_a, e_a) y privada d_a, de Alice y la clave pública de Bob (n_b, e_b).

Salida: Mensaje cifrado y firmado (r, f).

1: Alice calcula el resumen (hash) del mensaje a firmar: $h(M) = m$.

2: Alice cifra el resumen del mensaje usando su clave privada y obtiene r :

$$r = m^{d_a} \bmod n_a.$$

3: Alice calcula su firma f para ello cifra r, con la clave pública de Bob,

$$f = r^{e_b} \bmod n_b.$$

4: **return** (r, f)