FIRMA DIGITAL.

El proceso de **firma digital** es una de las aplicaciones más importante del algoritmo R.S.A.

Para este proceso tenemos dos interlocutores A y B que disponen ambos de claves públicas:

- Para el interlocutor A tenemos n_A, d_A y e_A que dan lugar a un cifrado C_A y un descifrado D_A.
- Para el interlocutor B tenemos n_B, d_B y e_B que dan lugar a un cifrado C_B y un descifrado D_B.

Pretendemos enviar de A a B un mensaje firmado: **m**. Procedemos del siguiente modo.

1. A cifra el mensaje **m** usando su clave secreta (lo firma):
$$\mathbf{S} = D_A(m) = m^{d_A} \text{ mód } n_A.$$
2. Ahora usando la clave pública de B encripta su mensaje firmado **S** y lo envía
$$C_B(S) = S^{e_B} \text{ mód } n_B.$$
3. B recibe $C_B(S) = S^{e_B} \text{ mód } n_B$ y lo descifra usando su clave
$$D_B(S^{e_B}) = S \text{ mód } n_B.$$
4. Por último, B descifra **S** usando la clave pública de A

$$C_A(S) = C_A(D_A(m)) = (m^{d_A})^{e_A} = m^{d_A e_B} = m^{1+k\phi(n_A)} \equiv \mathbf{m} \text{ mód } n_A.$$

De este modo, B está convencido que **m** procede de A, ya que lo ha descifrado usando la clave de A. Por otro lado, solo B puede descifrar el mensaje enviado por A ya que estaba cifrado con la clave pública de B.

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

E-mail address: Cesar_Ruiz@mat.ucm.es