§§1.2. Signature par RSA.

Bob veut signer un message x par RSA :

SET UP

- $k_{pr} = k_{pr_B} = (d)$.
- $k_{pub} = k_{pub_B} = (n, e)$.

$x \in \{0, \dots, n-1\}$.

Protocole de Base signature RSA.

Alice		Bob
		• $k_{pr} = d$, $k_{pub} = (n,e)$.
	$\xleftarrow{(n,e)}$	
		• $s = sig_{k_{pr}}(x) \equiv x^d \pmod n$.
	$\xleftarrow{(x,s)}$	
• $x' = s^e \pmod n$		
$x' \equiv x \pmod n \Rightarrow$ signature valide		
$x' \not\equiv x \pmod n \Rightarrow$ signature invalide		

ona : $s^e \equiv (x^d)^e = x^{de} \equiv x \pmod n$.

Car $de \equiv 1 \pmod{\phi(n)}$

Rq. Noter que les rôles de k_{pr} et k_{pub} sont échangés :

on signe avec la clé privée et on vérifie par k_{pub}.