Alice

Bob

Génère :

2 nombres premiers :

p, q

Calcule :

$$n = p \times q$$

$$w = \varphi(n) = (p-1)(q-1)$$

Trouve :

$$e \ tel \ que \ e \wedge \varphi(n) = 1$$

$$d \ tel \ que \ e \times \ d \equiv 1[\varphi(n)]$$

Clé publique :

d, n

Clé privée :

e, n