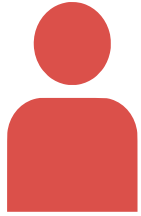


Alice



Possède :

sa clé publique :

d, n

sa clé privée:

e, n

Déchiffre :

$$M \equiv M^{d \times e}[n]$$

$$M \equiv (m_{chiffre})^e[n]$$

Bob



Garde :

une clé publique :

d, n

$$m_{chiffre} = M^d[n]$$



Envoie $m_{chiffre}$