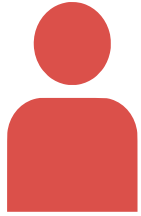


Alice

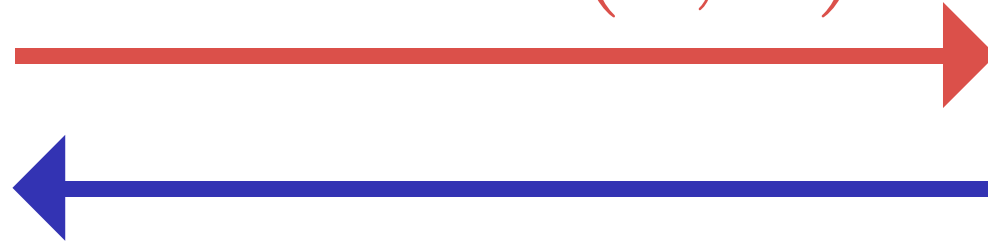


Possède :
sa clé publique :
 d, n

sa clé privée:
 e, n

Oublie :
 p, q et $\varphi(n)$

Envoie (d, n)



Envoie $m_{chiffre}$

Bob



Garde :
une clé publique :
 d, n

Chiffre M :

Condition : $M < n$

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