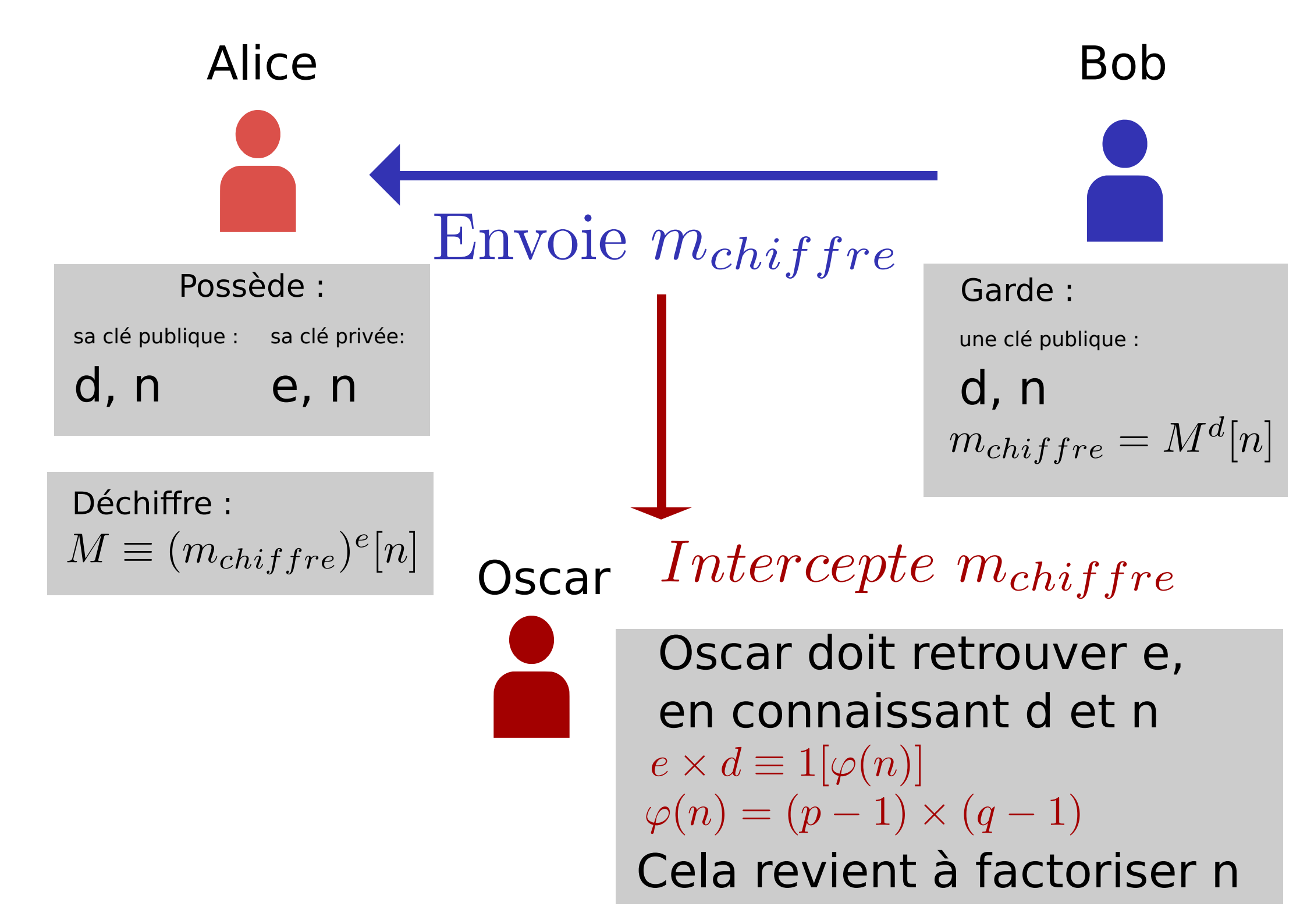
Alice
Bob
Envoie $m_{chiffre}$
Possède :
sa clé publique :
sa clé privée:
d, n
e, n
Garde :
une clé publique :
d, n
$m_{chiffre} = M^d[n]$
Déchiffre :
$M \equiv (m_{chiffre})^e[n]$
Oscar
$Intercepte\ m_{chiffre}$
Oscar doit retrouver e,
en connaissant d et n
$e \times d \equiv 1[\varphi(n)]$
$\varphi(n) = (p-1) \times (q-1)$
Cela revient à factoriser n