Alice

Bob

Envoie (d, n)

Envoie $m_{chiffre}$

Possède :

sa clé publique :

d, n

sa clé privée:

e, n

Garde :

une clé publique :

d, n

Oublie :

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

Chiffre M :

Condition : M < n

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