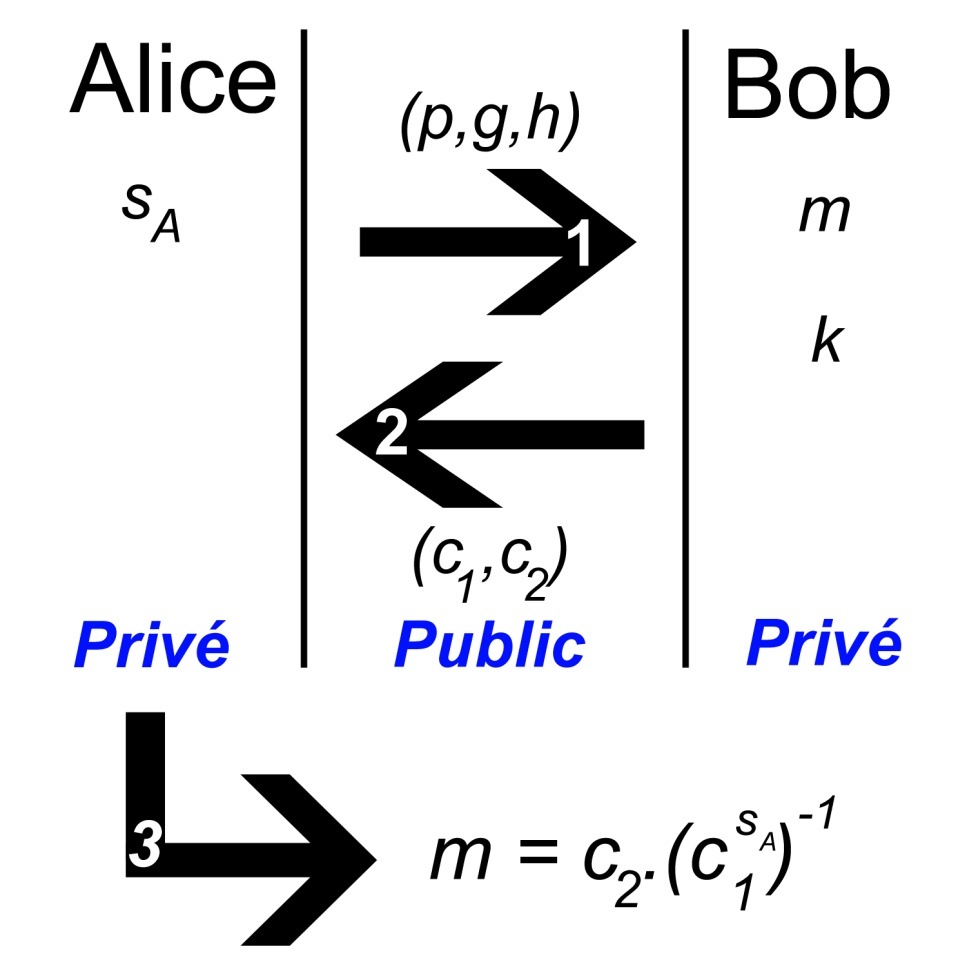
I/ a) Crypto-système d’El Gamal et problème du logarithme discret.

*Propriété 1 :* Pour p un nombre premier, (, .) est un groupe.

De plus, ce groupe est cyclique, c'est-à-dire qu’il existe tel que :



*p* nombre premier.

*g* générateur de G =

et

*Définition 1 :* Soit G un groupe cyclique d’ordre *p* dont la loi est notée multiplicativement, soit *g* un élément générateur de G et *y* un élément de G. On appelle logarithme discret le plus petit entier *k* tel que : .