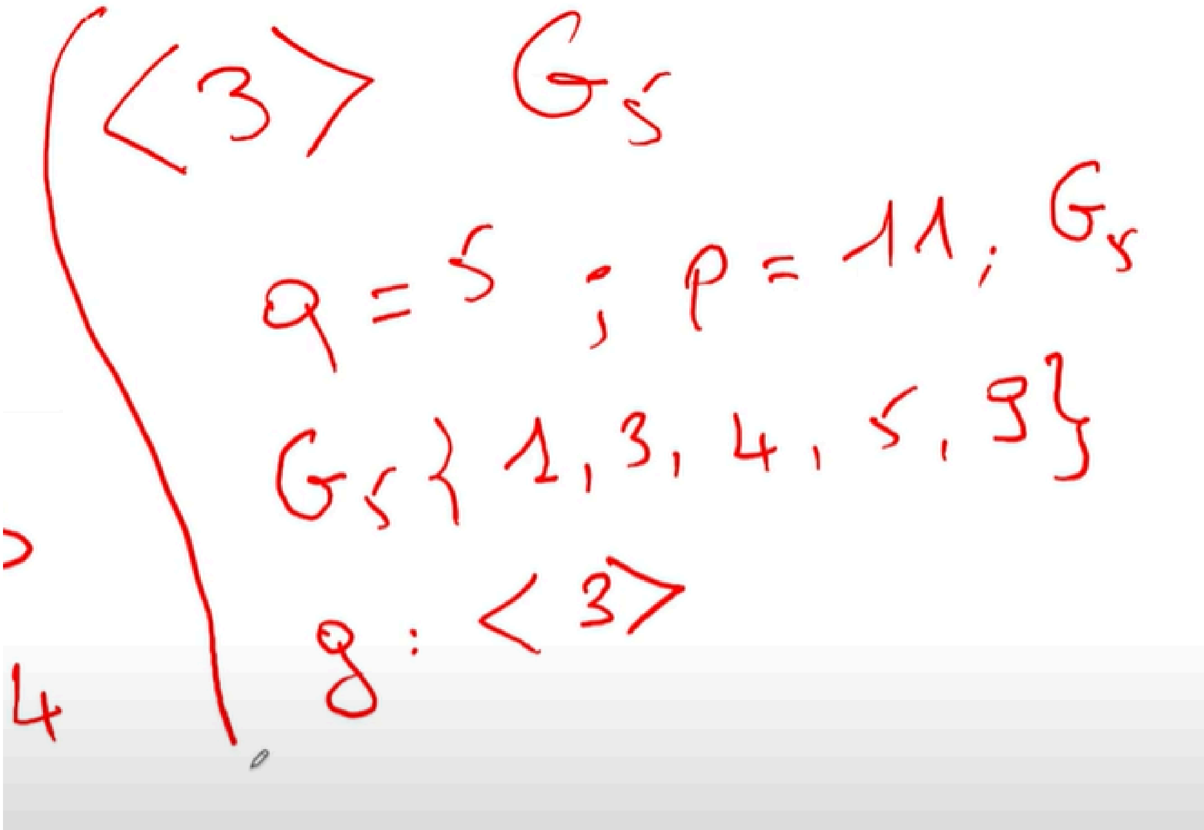
<u>ElGamal</u>

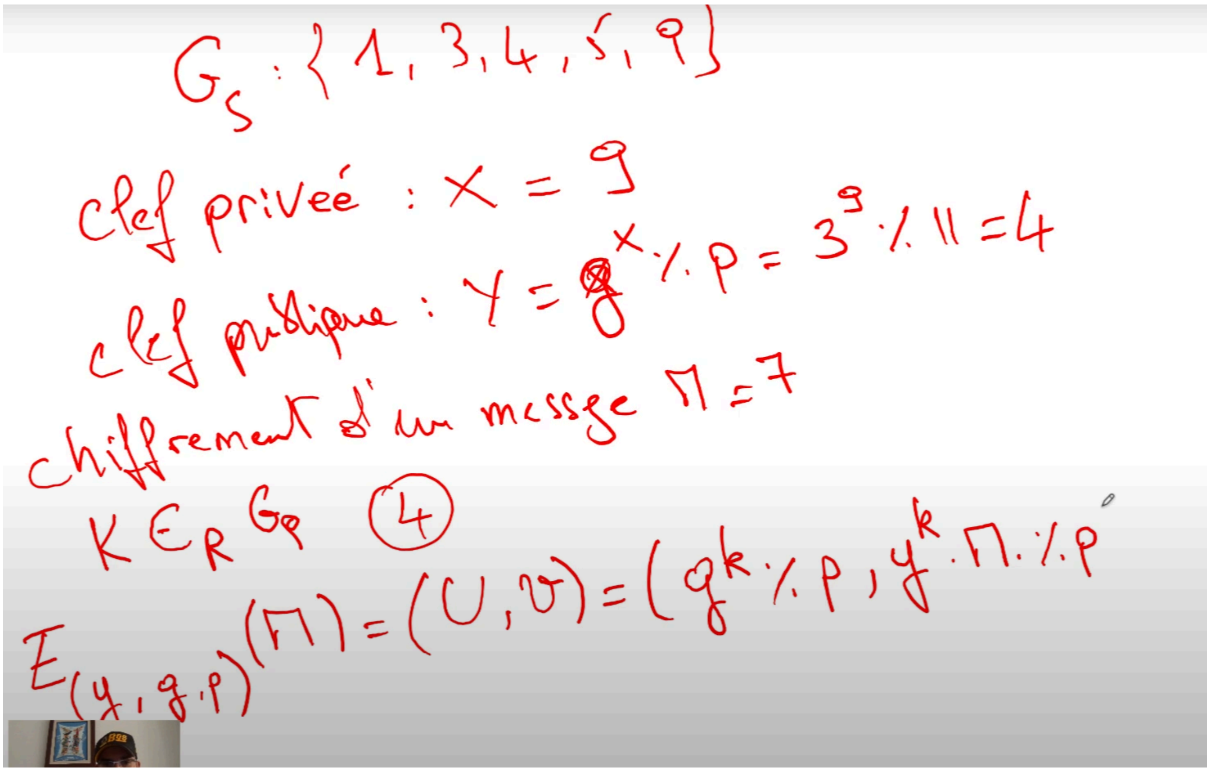
p et q 2 nombres premiers

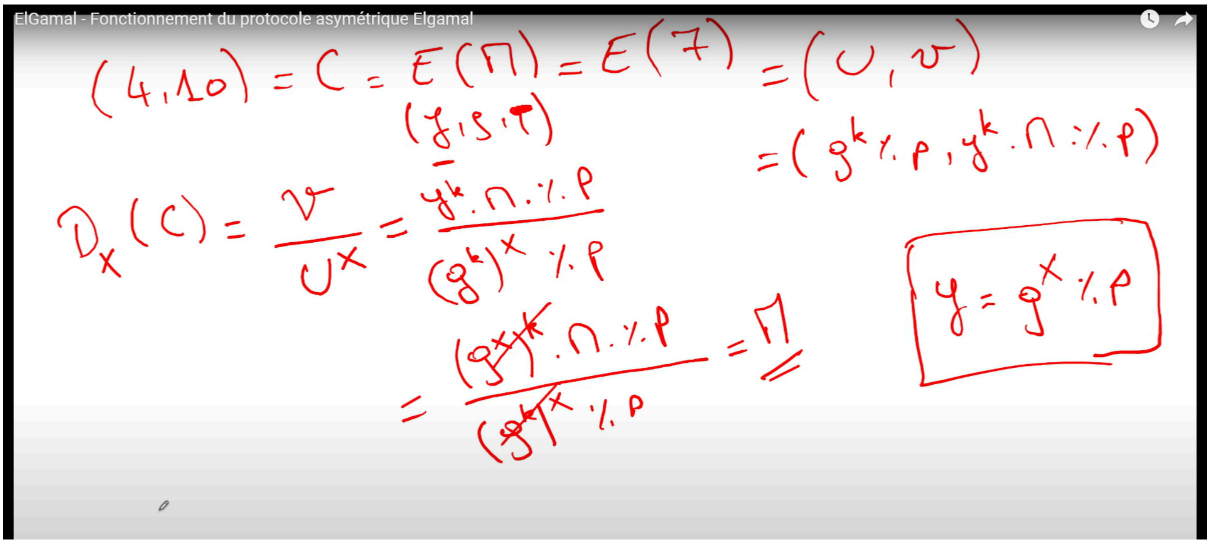
Groupe cyclide de q éléments
Loi du groupe : g^k % p avec g un nombre dis le “générateur” du groupe et k appartenant à [0 ; q-1]. Il est cyclide, la puissance q doit être égale à la 0 !



On prend comme clé privée un membre de notre groupe cyclique noté x
Clé publique : y = g^x % p

On chiffre un message sous la forme d’un entier
On choisit aléatoirement un nombre de notre groupe k
On chiffre avec la clé publique





(4,10) est le chiffrement de M = 7

A noter que l'élément k n'est jamais connu de l'entité qui reçoit le message, elle n'en a pas besoin