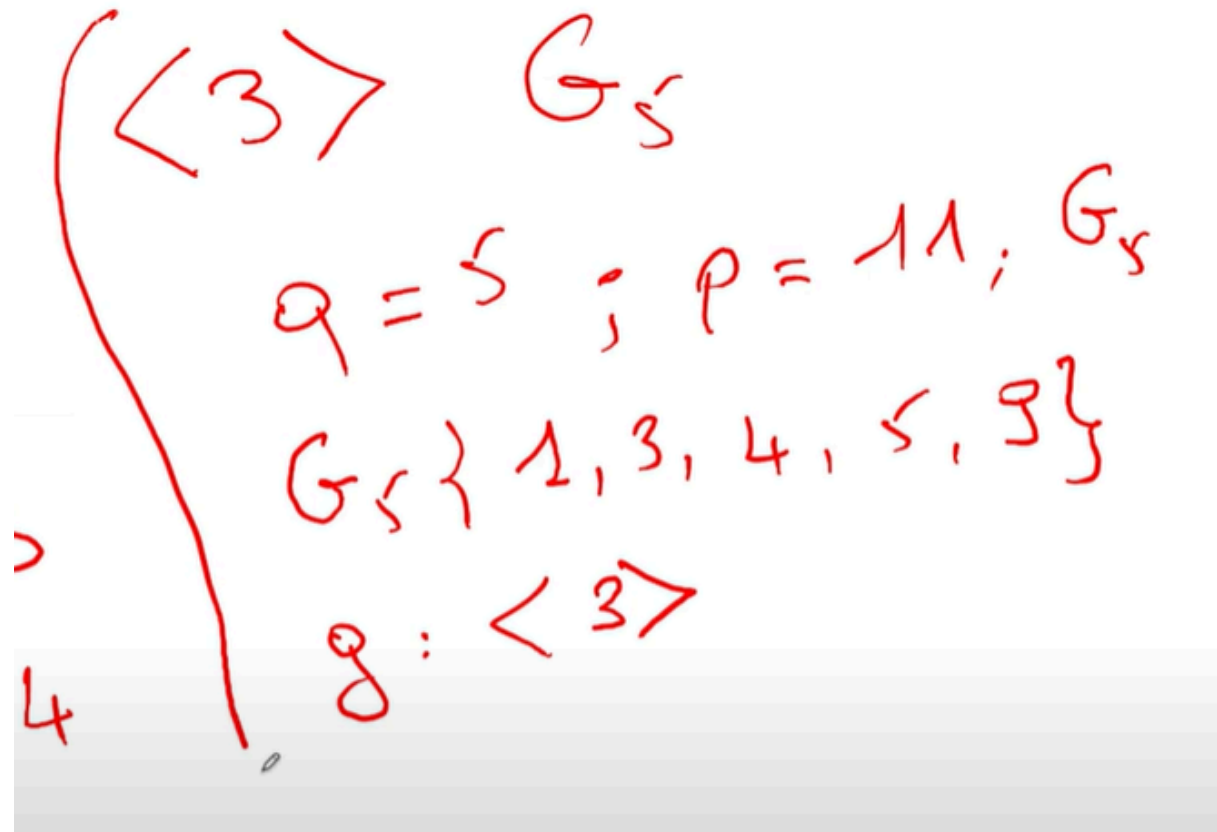


ElGamal

p et q 2 nombres premiers

Groupe cyclique de q éléments

Loi du groupe : $g^k \% p$ avec g un nombre dit le "générateur" du groupe et k appartenant à $[0 ; q-1]$. Il est cyclique, 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

$$G_S : \{1, 3, 4, 5, 9\}$$

clé privée : $x = 9$

clé publique : $y = g^x \cdot p = 3^9 \cdot 11 = 4$

chiffrement d'un message $m = 7$

$k \in_R G_p$ (4)

$$E_{(y, g, p)}(m) = (u, v) = (g^k \cdot p, y^k \cdot m \cdot p)$$

ElGamal - Fonctionnement du protocole asymétrique ElGamal

$$\begin{aligned} (4, 10) &= C = E(m) = E(7) = (u, v) \\ &= (g^k \cdot p, y^k \cdot m \cdot p) \\ D_x(C) &= \frac{v}{u^x} = \frac{y^k \cdot m \cdot p}{(g^k)^x \cdot p} \\ &= \frac{(g^x)^k \cdot m \cdot p}{(g^x)^k \cdot p} = m \end{aligned}$$

$y = g^x \cdot p$

(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