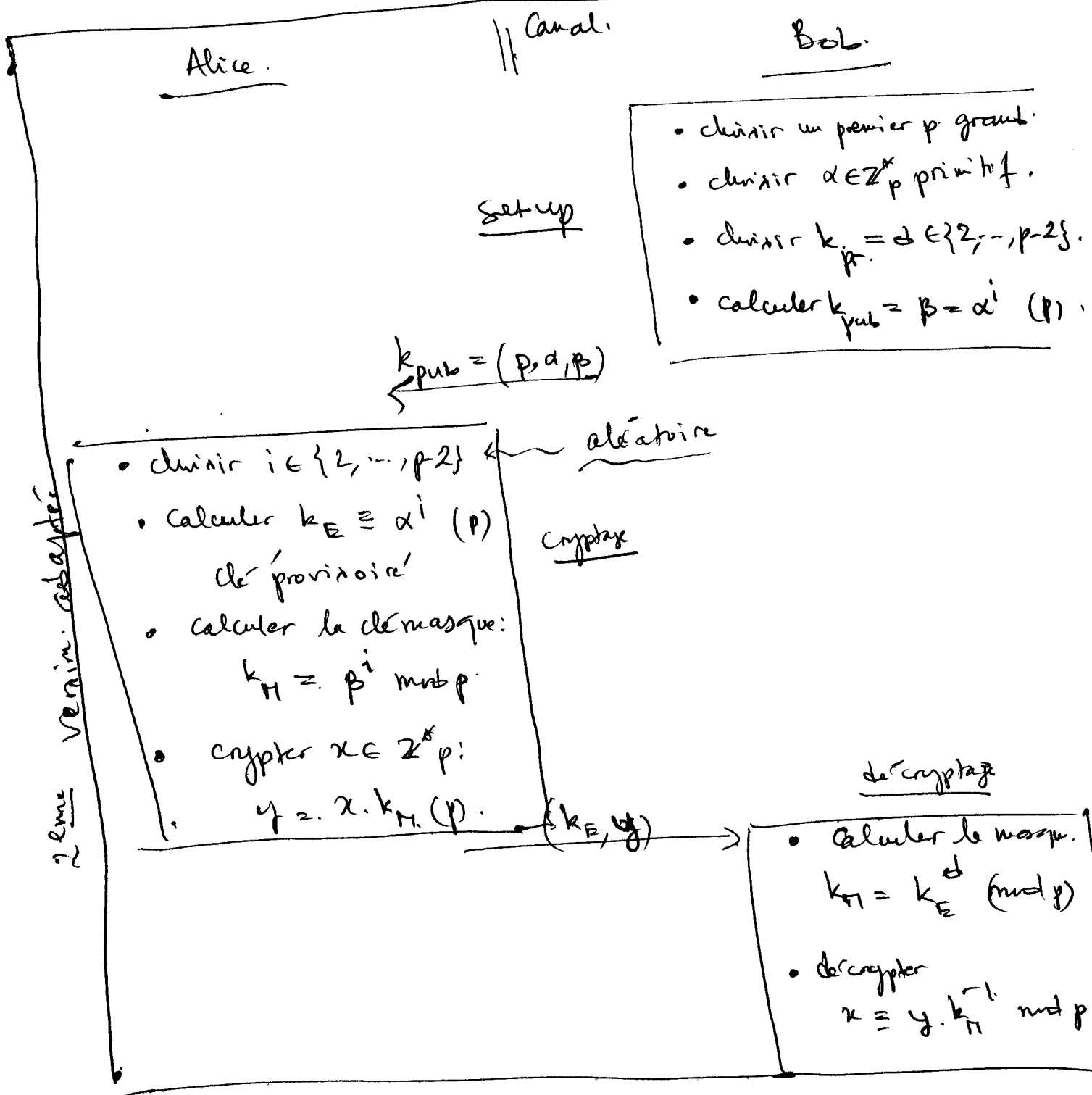


Protocole EL. GAMAL. (modifié)



ona: $d_{k_{pr}}(k_E, y) = y \cdot k_H^{-1} \pmod{p}$.

$$= (x \cdot k_H) \cdot (k_E^{\beta})^{-1} \pmod{p}$$

$$= (x \cdot \alpha^{\beta i}) \cdot ((\alpha^i)^{\beta})^{-1} \pmod{p}$$

$$= x \cdot \alpha^{di} \cdot \alpha^{-\beta i} \pmod{p} \equiv x \pmod{p}$$