Protocole EL GAMAL (modifié)

Alice || Canal || **Bob**

Setup

Bob :
- choisir un premier p grand
- choisir $\alpha \in \mathbb{Z}_p^*$ primitif
- choisir $k_{pr} = d \in \{2, \dots, p-2\}$
- calculer $k_{pub} = \beta = \alpha^d \ (p)$

$k_{pub} = (p, \alpha, \beta)$

Cryptage

Alice :
- choisir $i \in \{2, \dots, p-2\}$ ← aléatoire
- calculer $k_E \equiv \alpha^i \ (p)$ clé provisoire
- calculer la clé masque : $k_M \equiv \beta^i \ \text{mod } p$
- crypter $x \in \mathbb{Z}_p^*$: $y \equiv x \cdot k_M \ (p)$

(k_E, y)

Décryptage

Bob :
- calculer le masque : $k_M = k_E^d \ (\text{mod } p)$
- décrypter : $x \equiv y \cdot k_M^{-1} \ \text{mod } p$

2ème version adaptée

On a : $d_{k_{pr}}(k_E, y) \equiv y \cdot k_M^{-1} \ (\text{mod } p)$.

$\equiv (x \cdot k_M) \cdot (k_E^d)^{-1} \ (p)$

$= (x \cdot \alpha^{di}) \cdot ((\alpha^i)^d)^{-1} \ (p)$

$= x \cdot \alpha^{di} \cdot \alpha^{-di} \ (p) \equiv x \ (\text{mod } p)$.

☒