Supposons $G = \mathbb{Z}_p^*$, alors si $\mathcal{O}$ peut résoudre PLD alors il peut résoudre PDH :

car $\mathcal{O}$ calcule $a = \log_\alpha A = k_{pr.A} \pmod p$

et calcule $k_{AB} = B^a \bmod p$. ☒

D'où pour assurer la sécurité de PDH, on doit choisir p assez grand.

§4. EL GAMAL.

§§4.1. Cryptage et Décryptage

basé sur le PLD et le PDH. On verra ici la méthode sur $\mathbb{Z}_p^*$. Il provient du protocole DH d'Echange de clé. Alice chiffre un message x en le multipliant par k_{AB}.

Cryptosystème de cryptage.

Alice.	Canal.	Bob.
		(a). choisir $d = k_{priv\,B} \in \{2, \dots, p$
	$\leftarrow B$	(b) calculer $\beta = k_{pub\,B} = \alpha^d$ m
(c). choisir $i \in \{0, \dots, p-2\}$.		
(d) Calculer $k_E = k_{pub\,A} = \alpha^i \bmod p$.		
	$\xrightarrow{k_E}$	(f) Calculer $k_M = k_{Fz}^d$.
(e) Calculer $k_M = \beta^i \bmod p$.		
(g) crypter $x \in \mathbb{Z}_p^*$: $y \equiv x \cdot k_M \bmod p$.	$\xrightarrow{y}$	
		(h) décrypter : $x = y \cdot k_M^{-1} \pmod p$