L'attaque précédente est parée par le padding. (voir par. page 268). 14.5

§.4.2. Signature ElGAMAL :

Différent de RSA, ici, le cryptage et la signature sont assez distincts.

SETUP : génération de clés

1. Choisir un premier p assez grand
2. Choisir un élément primitif $\alpha \in \mathbb{Z}^*_p$ un sous-groupe de $\mathbb{Z}^*_p$.
3. Choisir aléatoirement $d \in \{2, 3, \dots, p-2\}$
4. Calculer $\beta = \alpha^d \pmod p$

La clé publique $k_{pub} = (p, \alpha, \beta)$, clé privée $k_{pr} = d$.

Génération de la signature.

1. Choisir aléatoi une clé éphémère $k_E \in \{0, \dots, p-2\}$ tq $pgcd(k_E, p-1) = 1$ (i.e. k_E est inversible mod $p-1$).
2. Calculer la signature :

$$(r, \Delta) = \left(\alpha^{k_E} \bmod p,\ (x - d \cdot r) k_E^{-1} \bmod p-1\right).$$

$Sig_{k_{pr}}(x, k_E) = (r, \Delta)$

Vérification : 1. Calculer $t = \beta^r \cdot r^\Delta \bmod p$.

2. Vérifier :

$$t \begin{cases} \equiv \alpha^x \bmod p \Rightarrow \text{signature valide} \\ \not\equiv \alpha^x \bmod p \Rightarrow \text{“ invalide} \end{cases}$$

$ver_{k_{pub}}(x, (r, \Delta))$