Remarque. ELGAMAL est probabiliste par le cryptage. par le choix de $i \in \{2, \dots, p-2\}$. Ainsi même si

$$x_1 = x_2 \not\Rightarrow Cry(x_1) = Cry(x_2). \quad \square$$

§§4.2. Infrastructure et sécurité.

(A)

- **Génération de clés** : (voir page 3.17 §§.4.1). Un entier p doit être généré utilisant un vrai RNG. par ex. nombres (dans le § RSA) et qui doit être de taille au moins 1024 bits. En plus on a utilisé une exponentiation modulaire à calculer rapidement par square-and-multiply. (S and M). on a utilisé aussi un RNG.
- **Cryptage** : les opérandes ont une longueur $\lceil \log_2 p \rceil$: utiliser aussi S and M. algorithme.
- **Décryptage** ; exponentiation $k_M = k^d$ (S and M) et une inversion utilisant l'algo d'Euclide Etendu.

(B) Sécurité :

→ Attaques passives : retrouver x à partir de $(p, \alpha, \beta = \alpha^b, k_E = \alpha^i, y = x \cdot \beta^i)$ est protégée par le fait que le PDL est difficile.

Supposons que O. possède un moyen 'rapide' de calcul du LD :