⟹ retrouver x en trouvant $d_A = k_{prB}$:

$$d_A = \log_\alpha \beta \pmod p$$

ensuite,

$$x \equiv y_2 \cdot \left(k_E^{d_A}\right)^{-1} \bmod p.$$

⟹ Retrouver la clé aléatoire i d'Alice :

$$i = \log_\alpha k_E \pmod p$$

et $$x \equiv y_1 \cdot (\beta^i)^{-1} \bmod p$$

→ Attaques actives :

- L'authenticité de la clé de Bob doit être vérifiée ;

Sinon Oscar peut convaincre Alice que la nouvelle clé forgée par lui même est celle d'Alice : les certificats sont utilisés dans ce cas.

- La clé secrète (éphémère) d'Alice doit être renouvelée de préférence. En effet, supposons qu'Alice utilise i pour crypter x_1 et x_2. Alors $k_1 = \beta^i$ et le même et aussi k_E.

Alice $\xrightarrow[(y_1, k_E)]{\text{II}^\text{e}}$ Bob

Alice $\xrightarrow[(y_1, k_E)]{}$ Bob

Supp O connaît m_1, il peut crypter le 2ème message :

$$x_2 = y_2 \cdot k_1^{-1} \pmod p \text{ où } k_1 = y_1 \cdot x_1^{-1} \pmod p$$

Rq. On peut utiliser PRNG mais en changeant la base.