

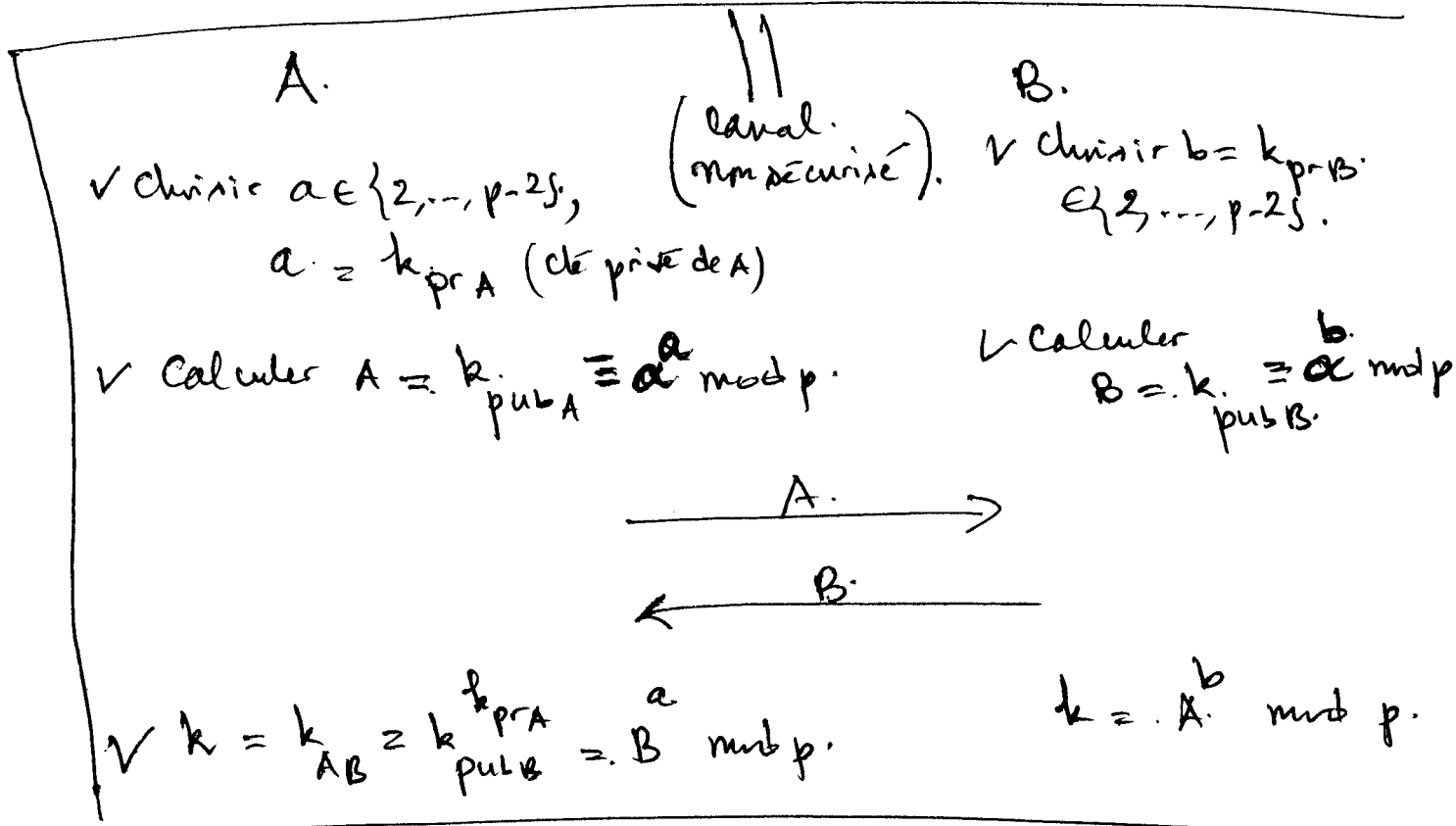
(3.1) Echange de clés DH (Construction de clés DH)

•

SET UP

1. Soit p un entier premier assez grand
2. Choisir $\alpha \in \{2, 3, \dots, p-2\}$.
3. Publier p et α .

- Alice (A) et Bob (B) peuvent construire une clé commune :



Noter que les calculs se font dans \mathbb{Z}_p^* et que

$$B^a \equiv (\alpha^b)^a = \alpha^{ab} \pmod{p}, \quad A^b \equiv \alpha^a \pmod{p}.$$

Ainsi $k_{AB} = \alpha^{ab}$ est la clé commune.