(3.1) Échange 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 :

A.	(canal non sécurisé)	B.
✓ Choisir $a \in \{2, \dots, p-2\}$, $a = k_{prA}$ (clé privée de A)		✓ Choisir $b = k_{prB} \in \{2, \dots, p-2\}$.
✓ Calculer $A = k_{pubA} \equiv \alpha^a \bmod p$.		✓ Calculer $B = k_{pubB} \equiv \alpha^b \bmod p$
	$A \longrightarrow$	
	$\longleftarrow B$	
✓ $k = k_{AB} = k_{pubB}^{k_{prA}} = B^a \bmod p$.		$k = A^b \bmod p$.

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

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

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