



# Crypto101 Express

## Key Exchange

DaVinciCode

25/06/20



- chiffrer un message de taille aléatoire efficacement 
- problème de transmission des clés 

# Ce que l'on cherche à faire

- Alice et Bob
  - veulent se mettre d'accord et trouver un secret commun (une clef par exemple)
  - ils communiquent via un canal qui n'est pas sécurisé (n'importe qui peut voir les messages qu'ils s'échangent)

# Protocole Diffie-Hellman

- Whitfield Diffie et Martin Hellman
- se base sur le fait que certains problèmes mathématiques sont faciles à résoudre dans un sens, mais pas dans l'autre

# Protocole Diffie-Hellman

- analogie avec des pots de couleurs
- mélanger deux couleurs est facile, mais l'opération inverse est très compliquée
- nous allons suivre la suite de messages échangés par Alice et Bob
  - Eve a accès à tout ces messages

# Protocole Diffie-Hellman

- Alice et Bob se mettent d'accord sur une couleur de base



# Protocole Diffie-Hellman

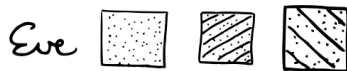
- Alice et Bob choisissent tous les deux une couleur aléatoirement, et la mélangent avec la couleur de base

$$\text{Alice} \quad \boxed{\text{dots}} + \boxed{\text{diagonal}} = \boxed{\text{diagonal dots}}$$

$$\text{Bob} \quad \boxed{\text{dots}} + \boxed{\text{diagonal}} = \boxed{\text{diagonal dots}}$$

# Protocole Diffie-Hellman

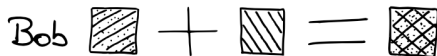
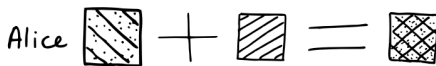
- Alice et Bob s'échangent les mélanges qu'ils ont fait





# Protocole Diffie-Hellman

- Alice mélange la couleur que Bob lui a envoyé avec sa couleur secrete
- Bob mélange la couleur qu'Alice lui a envoyé avec sa couleur secrete



# Protocole Diffie-Hellman

- Problème du logarithme discret:  $y \equiv g^x \pmod{p}$