Diffie-Hellman Key Exchange
Trusted publishes p and $g \in \mathbb{F}_p^*$ of large prime order

- **Alice** picks secret $a \in \mathbb{Z}$, sends $A \equiv g^a \mod p$ to Bob
  Bob picks secret $b \in \mathbb{Z}$, sends $B \equiv g^b \mod p$ to Alice
- **Alice** computes $A' \equiv B^a \mod p$
  Bob computes $B' \equiv A^b \mod p$
- Shared key is $A' = B'$

Elgamal encryption
Trusted publishes p and $g \in \mathbb{F}_p^*$ of large prime order

- **Alice** picks private key $a \in \mathbb{F}_p$ and publishes $A \equiv g^a \mod p$
- **Bob** has plaintext message $m \in \mathbb{F}_p^*$
  - Picks random $k \in \mathbb{F}_p$ for ephemeral key
  - Computes $c_1 \equiv g^k \mod p$ and $c_2 \equiv mA^k \mod p$
  - Sends ciphertext (c_1, c_2) to Alice
    Note A^k acts as masking key k_M from last semester
- **Alice** decrypts by $(c_1^a)^{-1} \cdot c_2 \equiv m \mod p$

1. Build an addition table for $\mathbb{Z}/4\mathbb{Z}$

   Relabel $\{0, 1, 2, 3\} \to \{e, a, b, c\}$ and rebuild your table

2. Build a multiplication table for $\mathbb{F}_5^*$

   Relabel $\{1, 2, 3, 4\} \to \{e, a, c, b\}$ and rebuild your table

3. Compare your relabeled tables