

# Alice and Bob agree to use $p = 227$ and $\alpha = 190$ for Elgamal encryption

1. Verify that  $p$  and  $\alpha$  are reasonable choices
2. Pick a private  $d$ , compute  $\beta$ , and write on the board
3. Pick a plain text  $x \in \mathbb{Z}_{227}^*$ , encrypt using Elgamal and write on board
4. Decrypt message sent to you, and write decrypted message on board