

Alice and Bob agree to use $p = 13523$ and $\alpha = 63$ for Elgamal encryption

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