Our trusted party publishes $p = 132\,347$ and $\alpha = 36$ to use with DHKE and Elgamal digital signatures.

1. Verify that p and α are reasonable choices.

2. If Alice's public value is $\beta = 18\,305$, which of the following are valid Elgamal signatures?

   (a) $(78\,931, (18\,105, 77\,414))$

   (b) $(14\,931, (39\,013, 44\,059))$

3. You want to sign the message $x = 73\,172$ using an Elgamal signature.

   (a) Use $d = 4023$ to compute your public β.

   (b) Is $k_E = 66\,173$ a valid choice for the ephemeral key? How about $k_e = 901$?

   (c) Use the key k_E from (b) that is valid to sign your message.

4. You notice that Alice from #2 has sent the following two messages signed with Elgamal:

   $$(7381, (82\,553, 116\,148))$$
   $$(1430, (82\,553, 14\,981))$$

   (a) How can you tell that Alice has used the same ephemeral key in both signatures?

   (b) Use this fact to find Alice's private key d.

   (c) What mischief does this allow you to manage?