Elgamal digital signature: Trusted publishes p and α

- **Alice**
  - Key Creation
    - Picks exponent d, publishes $\beta = \alpha^d \mod p$
  - Sign message x
    - Choose ephemeral k_E
    - Compute

$$r \equiv \alpha^{k_E} \mod p$$
$$s \equiv (x - d \cdot r) k_E^{-1} \mod p - 1$$

    - Send $(x, (r, s))$
- **Bob**
  - Compute $t \equiv \beta^r r^s \mod p$
  - If $t \equiv \alpha^x \mod p$ then valid signature
    If $t \not\equiv \alpha^x \mod p$ then invalid signature

Alice is using $p = 509$, $\alpha = 16$ and $\beta = 179$ for Elgamal signatures

Suppose Oscar sees that Alice has sent the messages

$$(240, (441, 207))$$
$$(390, (441, 289))$$

Help Oscar find Alice's private d.

What mischief can Oscar now cause?