

QUIZ 5

Let $p = 11$ and $g = 2$. Alice has supplied her public key as $A = 10$ and Bob wants to use the Elgamal PKC to send the message $m = 8$ to Alice. He chooses $k = 3$ at random. What does he send to Alice?

Suppose a hacker came and told you they stole Alice's private key from her machine. They claim $a = 4$ is Alice's secret key. Do you believe them?

Can you recover a (by hand) in the allotted time?