

A trusted party publishes $p = 132\,347$ and $\alpha = 36$ to use with DHKE

You are playing the dastardly role of Oscar in this problem and are implementing a MITM attack where you can intercept and alter any messages that Alice and Bob send to each other.

You choose to use a private key of $c = 1341$.

Alice's value for DHKE is $A = 91\,371$ and Bob's value is $B = 126\,585$.

You intercept these and apply a MITM attack.

1. What is the symmetric key that Alice will use for encrypting/decrypting messages to Bob?
2. What is the symmetric key that Bob will use for encrypting/decrypting messages to Alice?
3. If you had not implemented the MITM attack, what is the symmetric key that Alice and Bob would use?