1. Alice and Bob generate a session key using the Diffie-Hellman key establishment protocol. They agree on a finite cyclic group $(\mathbb{Z}/23\mathbb{Z})^\times$ generated by 5. What is the order of $(\mathbb{Z}/23\mathbb{Z})^\times$? Suppose that Alice's private exponent is 2, and Bob's private exponent is 3, what is the session key generated by Alice and Bob?

2. Consider the following key agreement protocol between Alice (A) and Bob (B). Prior to starting any communication, Alice and Bob generate their secret keys ω_A and ω_B. Alice generates the session key K. To share K with Bob, the following sequence of messages is executed.

   (1) Alice $\rightarrow$ Bob: $\omega_A \oplus K$.

   (2) Bob $\rightarrow$ Alice: $\omega_B \oplus \omega_A \oplus K$

   (3) Alice $\rightarrow$ Bob: $\omega_A \oplus \omega_B \oplus \omega_A \oplus K = \omega_B \oplus K$

   After receiving the last message, Bob computes $\omega_B \oplus \omega_B \oplus K = K$. At this point Alice and Bob have the shared key K which they use to encrypt the communication. Can adversary Carol obtain the key K by eavesdropping on the communication channel?