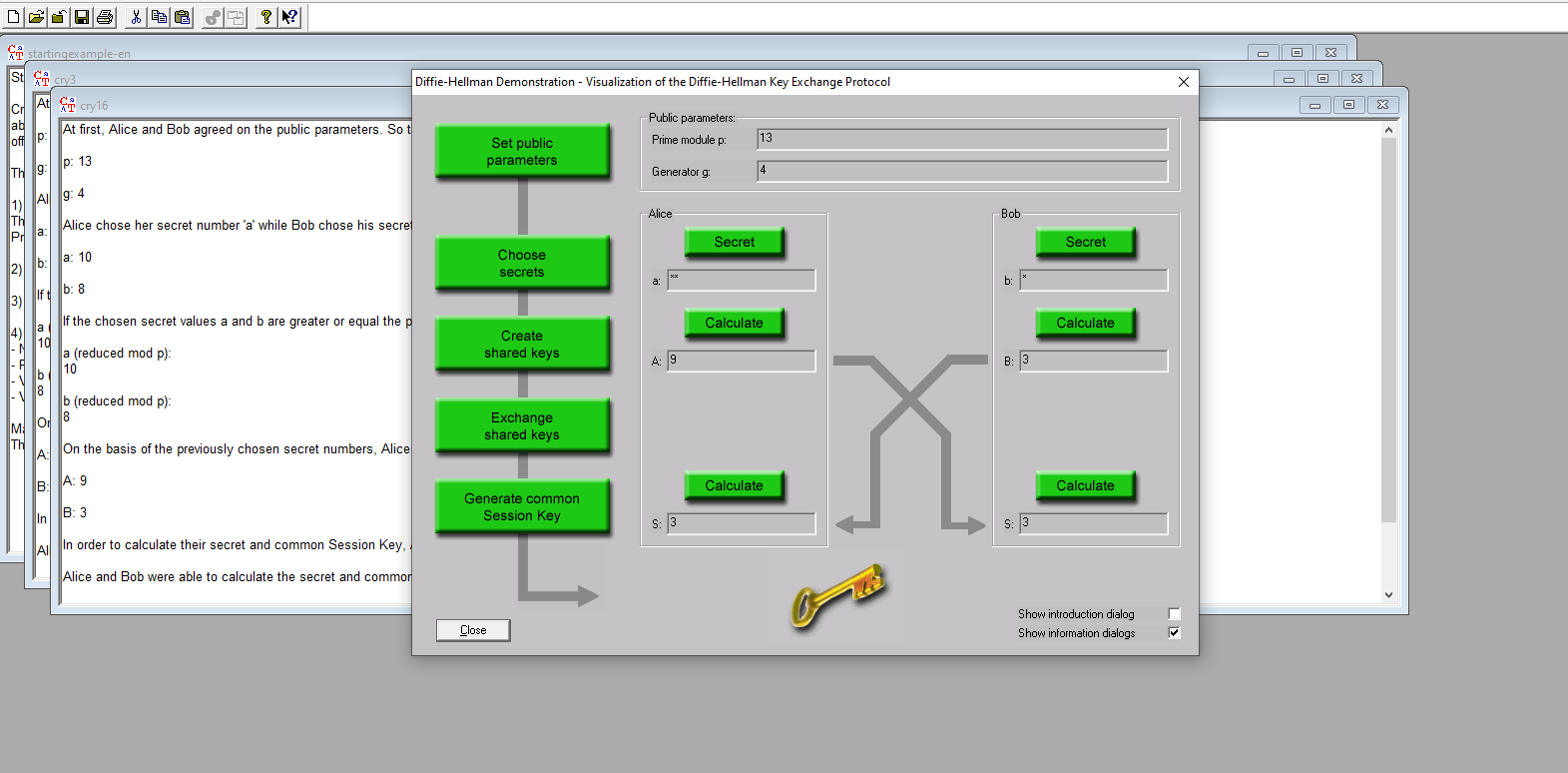
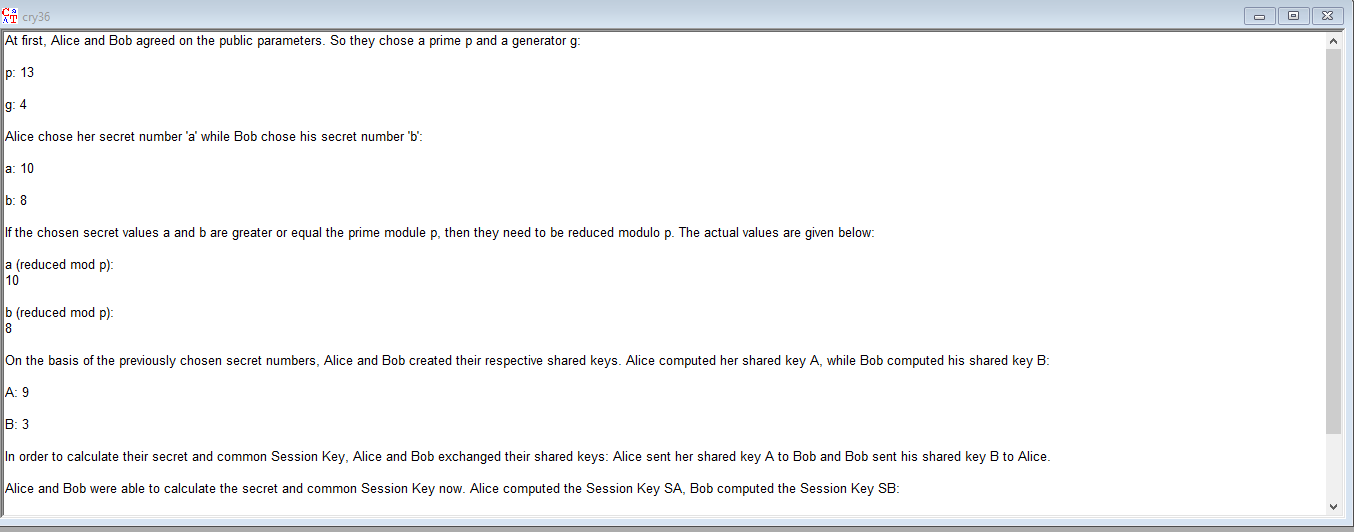
**Lab 08**

**Object: Diffie Helman Key Exchange Method**

**Exercise**

1. **Calculate the Symmetric Key using Diffie-Hellman Key Exchange method while considering the  following values g=4, p=13 and a=10, b=8. Verify the Cryptool generated key with the manual  calculations.**





1. **How Man in the Middle Attach is possible in Diffie-Hellman Key Exchange method.**

A Man-in-the-Middle (MitM) attack in Diffie-Hellman occurs when an attacker intercepts and alters the public keys exchanged between Alice and Bob. The attacker, Eve, substitutes her own public keys for Alice's and Bob's, creating two separate shared keys with each participant. This allows Eve to intercept, decrypt, modify, and re-encrypt messages without either Alice or Bob knowing, as they each believe they are securely communicating directly with each other. To prevent this, digital signatures or certificates are needed to authenticate the public keys.