Given the following numbers:

- Prime number $q = 13$
- Generator $\alpha = 2$
- Alice's private key $X_a = 5$
- Bob's private key $X_b = 4$
- Eve's private key $X_e = 7$

The following steps illustrate how Alice and Bob can establish a shared secret key K using the Diffie-Hellman key exchange protocol:

1. Alice computes $Y_a = \alpha^{X_a} \mod q = 2^5 \mod 13 = 6$ and sends Y_a to Bob, But Eve intercepts the message.
2. Eve computes $Y_e = \alpha^{X_e} \mod q = 2^7 \mod 13 = 11$ and sends Y_e to Alice
3. Alice computes $K_a = Y_e^{X_a} \mod q = 11^5 \mod 13 = 7$.
4. Eve computes $K_a = Y_a^{X_e} \mod q = 6^7 \mod 13 = 7$.
5. Now Eve and Alice share a secret key $K_a = 7$, however, Alice still thinks she is sharing the secret key with Bob.
6. Bob computes $Y_b = \alpha^{X_b} \mod q = 2^4 \mod 13 = 3$ and sends Y_b to Alice, But Eve intercepts the message.
7. Eve use the same Y_e to send to Bob
8. Bob computes $K_b = Y_e^{X_b} \mod q = 11^4 \mod 13 = 3$.
9. Eve computes $K_b = Y_b^{X_e} \mod q = 3^7 \mod 13 = 3$.
10. Now Eve and Bob share a secret key $K_b = 3$, however, Bob still thinks he is sharing the secret key with Alice.
11. when Alice and Bob try to communicate, Eve can intercept the message and decrypt it using the secret key $K_a = 7$ and $K_b = 3$. So she can read the message and even modify it before sending it to the other party with ease.