Man-in-the Middle Attack formulation

1. Darth generating two random private keys X_{D1} and X_{D2} and then compute the public Keys Y_{D1} and $Y_{D2.}$
2. Alice transmits her private Key X_A Public key $Y_A = \alpha^{XA} \bmod q$, Alice transmits public Key Y_A to Bob; Bob transmit his private Key X_B Public key $Y_B = \alpha^{XB} \bmod q$,
3. Darth intercepts Alice's Public Key Y_A and transmits his public Key Y_{D1} to Bob. Darth Calculates $k_2 = (Y_A)^{XD2} \bmod q$
4. Bob receives public Key Y_{D1} now he calculates key $K_1 = (Y_{D1})^{XB} \bmod q$
5. Bob transmits his public key Y_B to alice

6. Darth intercepts and transmits his second public key Y_{D2} to alice. Darth calculates $K_1 = (Y_B)^{XD1} \bmod q$
7. Alice receives the key Y_{D2} and calculates the shared key $k_2 = (Y_{D2})^{XA} \bmod q$

Darth private key X_{D1} and X_{D2}
Public Keys $Y_{D1} = \alpha^{Xd1} \bmod q$; and $Y_{D2} = \alpha^{Xd2} \bmod q$
Session Keys $K_1 = (Y_B)^{XD1} \bmod q$; $k_2 = (Y_A)^{XD2} \bmod q$

Alic's Private key X_A
Alice's Public key $Y_A = \alpha^{XA} \bmod q$
Alic's Shared Key $K_2 = (Y_{D2})^{XA} \bmod q$

Bob's Private key Y_B

Bob's public Key $Y_B = \alpha^{XB} \bmod q$

Bob's Shared Key $K_1 = (Y_{D1})^{XB} \bmod q$