Paul Diaz
HW9

1.The last message. RA and RB prevents the attack
2.In K = g^(ab) mod p, finding a and b requires a difficult Mathematical operations. It is nearly impossible to solve discrete log.
3.Alice will see that it’s doesn’t match Bob’s certificate with the one she computed.so she’ll turn down the communication. Trudy can’t forge Bob’s signature.
d.There’s no point in the encrypting the final message.