**Q1. (RSA protocol)**

**Both public keys are known = Pu(A) Pu(B)**

//Alice Private Key

**Pr(A)**

//Cypher Text i.e the number sent to Bob

**K1 = Pu(B) ^ Pr(A)(mod Pu(A))**

//Bob Private Key

**Pr(B)**

//The Value sent back to Alice

**K2 = Pu(B) ^ Pr(B) (Mod Pu(A))**

//To Decipher Alice

**K2 ^ Pr(A)(Mod Pu(A)) = TEXT**

//To Decipher Bob

**K1 ^ Pr(B)(Mod Pu(A)) = TEXT  
  
NOTE: K1 ^ Pr(B)(Mod Pu(A)) == K2 ^ Pr(A)(Mod Pu(A))**

**Q2. Using digital signature**

**Alice Turns the message into a hash function and padding, and then encrypts it using her private key**