**LAB 13**

1. **How would Alice send the message**

Firstly alice would need to encrypt the message M1 using bobs public key PU(b) E = {Pu(B)} M1

Bob then needs to decrypt the message using his private key which is:  
D {PR(B)} (E = {PU(B)} M1

He can now read the message

1. **Let us denote the message Alice sent as M3. How would bob decipher the message**

Bob would use his private key to decrypt the encrypted message e = {PR(B)} M3

After decrypting the message Bob will be able to read the original message that alice encrypted.

1. **In this situation, Alice does not Care if anyone can read her message. But she does care no one in the middle can change the message. Let us denote the message as M2**

Alice creates a digest of the message using a hash function H(M2)

Alice will need to encrypt using her private key E= {PR(A)} H(M2)

Alice attaches the digest to the encrypter message M2 || E = {PR(A)} H(M2)

Finally Alice can now send that message to Bob over the internet

1. **What would bob do to verify that the message indeed came from Alice?**

Bob would receive the message, Bob would then need to separate the digest from the original message. Bob would then decrypt the encrypted message D = {Pu(A} E = {PR(A)} H(M2). Bob creates a digest of the received message using the same hash function as Alice H(M2) As a result bob can compare the decrypted digest with the digest of the received message. If they are the same Bob knows the message had not been tampered with.