Lab 13:

Alice wants to send a message to Bob so that no one else can read it. Let us denote the message as M\_1.

How would Alice send the message?

To send a message M\_1 to Bob, Alice would use Bob’s public key (Pu(B)) to encrypt the message. The encryption would be performed as follows:

E\_Pu(B) (M1)

Let us denote the message Alice sent as M\_3. How would Bob decipher the message?

Once Bob receives the encrypted message M\_3, he would use his own private key (Pr(B)) to decrypt it as follows:

D\_Pr(B) (M3) = D\_Pr(B) [E\_Pu(B) (M1)]

In this situation, Alice does not care if anyone can read her message. But she does care that no one in the middle can change the message (in an undetectable manner). Let us denote the message as M\_2.

How would Alice send the message?

To send a message M2 to Bob, Alice would use her own private key (Pr(A)) to digitally sign the message. The signing would be performed as follows:

S\_Pr(A) (M2)

What would Bob do to verify that the message indeed came from Alice?

Once Bob receives the signed message M2, he would use Alice's public key (Pu(A)) to verify the signature as follows:

V\_Pu(A) [S\_Pr(A) (M2)] = V\_Pu(A) [S\_Pr(A) (M2), Pu(A)]