Lab 11

# i)

## Encryption)

In order for Alice to encrypt the message and send the cyphertext to Bob so he can decrypt it Alice needs to complete the following steps.

* She needs to encrypt the message M using Bob’s public key Pu(B).
* She optionally needs to use her own private key Pr(A) to sign the message so bob can use her public key to verify that the message is from Alice.

Once she has the two steps above done, she then has Ek(m), the encrypted cypher text that she can now send to Bob.

## Decryption)

After Bob receives the encrypted cyphertext Dk(m) he can apply his own private key Pr(B) to decrypt the message and receive the message M. He can also check the signature that is on the cypher text and verify that it was Alice that sent him the message by using Alice’s public key Pu(A).

## Symmetric Key cryptography)

Symmetric key uses a different style of encryption, so when encrypting large messages since using symmetric key cryptography the cipher text is at worse the same size as the original, but it can become many times smaller, in contrast while asymmetric encryption is a safer method at best the cipher text will be the same size, but it can be many times larger.

# ii)

As mentioned above, when Alice sends Bob the encrypted Cipher text, she can optionally encrypt a digital signature using her own private key Pr(A), so Bob can use her public key to validate the authenticity of the message. This will allow Bob to make sure Dr.Evil did not alter the message while it was in transit.

If computational efficiency is a concern Alice and Bob could simply send Bob the authentication code for the message by running the message through a one way hash function H(m). This would allow Bob to also run the message through the same function and make sure that the code’s match. This will allow Alice and Bob to confirm that the message has not been tampered with in transit.

They could also add key to the hashing function, that would be something they would have to decide for themselves, the function would work with the message alone.