Lab 11

i a)

Alice Encrypts her message using bob's public key. Ek(PU(B)).

Bob then decrypts the message using his own private key DK(PR(B)).

i b)

Symmetric key cryptography is used more commonly than public key cryptography because there is a lot less overhead which makes it a lot faster to use. This is due to low use of resources and because the keys are a lot shorter.

ii a)

Alice would need to send a hash encrypted using her private key.

H(PR(A)). Using this hash with Alices private key will let Bob know that the message truly is from Alice.

ii a)

For Computer efficacy I would recommend using the algorithm called

SHA-256