# Lab 2

i) Alice should encrypt the message using Bob’s public key since only Bob’s private key can decrypt it.

EPu(B)(M1)

Alice transmits EPu(B)(M1)E_{Pu(B)}(M1)EPu(B)(M1) to Bob. Only Bob, who possesses Pr(B)Pr(B)Pr(B), can decrypt it:

DPr(B)(EPu(B)(M1))=M1D_{Pr(B)}(E_{Pu(B)}(M1)) = M1DPr(B)(EPu(B)(M1))=M1

Symmetric key cryptography is preferred because it’s much faster and efficient, requires fewer computational resources and provides the same level of security but with smaller key sizes.

ii)Alice should sign the message using her private key so that Bob can verify her identity using her public key.

EPr(A)(M1)

Bob verifies the authenticity of the message by decrypting it with Alice’s public key:

DPu(A)(EPr(A)(M1))=M1D_{Pu(A)}(E_{Pr(A)}(M1)) = M1DPu(A)(EPr(A)(M1))=M1

Since only Alice's private key could have produced EPr(A)(M1)E_{Pr(A)}(M1)EPr(A)(M1), Bob knows that Alice sent the message.

Instead of encrypting the entire message with her private key, Alice can send a digital signature.

**Steps**:

-Compute a hash of the message:
H(M1)H(M1)H(M1)

-Sign the hash with Alice’s private key:
EPr(A)(H(M1))E_{Pr(A)}(H(M1))EPr(A)(H(M1))

-Send both the message and the signed hash:
M1,EPr(A)(H(M1))M1, E_{Pr(A)}(H(M1))M1,EPr(A)(H(M1))

Bob verifies the signature as follows:

-Compute the hash of the received message:
H(M1)H(M1)H(M1)

-Decrypt the signed hash using Alice’s public key:
DPu(A)(EPr(A)(H(M1)))=H(M1)D_{Pu(A)}(E_{Pr(A)}(H(M1))) =
H(M1)DPu(A)(EPr(A)(H(M1)))=H(M1)

-If the computed hash matches the decrypted hash, Bob is sure that Alice sent the message and that it was not altered.