Alice wishes to electronically transmit an important message *M* to Bob using public key cryptography. Let us denote private key of Alice as *Pr(A)*, private key of Bob as *Pr(B)*, public key of Alice as *Pu(A)*, and public key of Bob as *Pu(B)*.

Please use the following notation in presenting your answer:

: Message *M* is encrypted using key *K*

: Message *M* is decrypted using key *K*

: One way hash or secure digest of message *M*

1. **Alice wants to transmit *M* to Bob in a manner that no one other than Bob can access the data. Let us denote the message as .**

**What should Alice transmit to Bob assuming we are restricted to public key cryptosystems? Use the notation above.**

**When large messages must be encrypted, symmetric key cryptography is usually preferred to public key cryptography. Explain why.**

(i a) Alice will encrypt her key using Bob’s public key because you need to use Bob’s private key to decrypt it, and its safer. Alice will send E\_Pu(B) (M\_1) then Bob will receive this and decrypt it with his key Pr(B) which goes into -> D\_Pr(B) (E\_Pu(B) (M\_1)) = M\_1

Symmetric Key Cryptography is preferred for longer messages because its faster than other encrypting/decrypting ways. The other reason is theres much less computational overhead

1. **In this situation, Alice does not mind other people viewing the data she sends Bob. However, she is concerned that Dr. Evil might intercept her message, and send fake data to Bob pretending that he is Alice.**

**What should Alice transmit to Bob, to enable Bob to verify that it was indeed Alice who sent the message. *Use the notation above. Do not worry about computational efficiency concerns.***

**If computational efficiency is a concern, what should Alice transmit to Bob to enable him to verify it was Alice who sent the message? Use public key cryptography along with other mechanisms as appropriate.**

(ii a)

For Bob to ensure the message came from Alice, Alice will decrypt her message using her own private key as she is the only one with access to it. Then Bob will use Alice’s public key to decrypt the message sent

Alice will send E\_Pr(A) (M) then Bob will decrypt with D\_Pu(A) (E\_Pr(A) (M)) = M

If computational efficiency is a concern Alice can send a hashed version of her message. Getting the has is requires way less processing power -> H(M)

Alice then sends M and E\_Pr(A) (H(M)) as well

Bob will then decrypt -> D\_Pu(A) (E\_Pr(A) (H(M)))

This is faster because Hashing is a very fast operaertion and only a small hash gets encrypted, not the whole long message