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.

EPu(B)(M)

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

Symmetric key cryptography uses only one key rather than a public , private key pair. Also the resources and length of the keys are less.

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.*

EPr(A)(M)

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.

Alice should send a hash encrypted by her private and send it to bob that way bob can tell it was alice.