Lab 13

Alice and Bob wish to communicate with each other over the Internet. Each uses RSA, the common asymmetric cryptography protocol. Thus, each has his/her own private key and knows the public key of the other. Let us denote the private key of Alice as Pr(A), private key of Bob as Pr(B), the public key of Alice as Pu(A), and the public key of Bob as Pu(B).

Please use the following notation in presenting your answers:
E_K (M): Message M is encrypted using key K
D_K (M): Message M is decrypted using key K

Alice wants to send a message to Bob so that no one else can read it. Let us denote the message as M_1.

How would Alice send the message?

Let us denote the message Alice sent as M_3. How would Bob decipher the message?

In this situation, Alice does not care if anyone can read her message. But she does care that no one in the middle can change the message (in an undetectable manner). Let us denote the message as M_2.

How would Alice send the message?
What would Bob do to verify that the message indeed came from Alice?

1) Alice would encrypt M_1 with E_K and then send it to Bob
2) Bob would decypher M_3 with D_K
3) To do this Alice will have to use her own public key Pu(A) to encrypt the message.
4) He would have to have Pr(A) to decrypt the message and see if Alice sent the message and encrypted it.