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 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 answers:

E_K (M): Message M is encrypted using key K

D_K (M): Message M is decrypted using key K

Question 1:

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?

Answer 1:

Alice is A, Bob is B.

To create ciphertext (C)Alice encrypts M_1 using Bob's public key Pu(B)

Alice sends (C)

Bob receives (C)

To decrypt C using (Pr(B)), his private key to get original M_1. D_Pr(B)(C) = M_1

Question 2:

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

Answer 2:

Same as in the last question Alice encrypts the message (M_3) using Bob's public key (Pu(B)) to create the ciphertext (C). Which is E_Pu(B)(M_3) = C

Alice sends the (C) to Bob over the Internet.

Bob receives the (C) from Alice.

Bob decrypts the ciphertext (C) using his private key (Pr(B))

This obtains the original message (M_3). Notated as D_Pr(B)(C) = M_3

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.

Question 3:

How would Alice send the message?

To do this Alice would use the digital signature scheme in order for no one in the middle to be able to change the message in an undetectable manner. To do this these are the steps she takes.

1. Alice computes (H) a hash value of M_2. H = Hash(M_2)
2. Alice to encrypt M_2 with H creates a digital signature (S) using her private key (Pr(A)). S = E_Pr(A)(H)
3. Alice needs to then send M_2 and S to Bob.

Question 4:

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

To verify that the message is from Alice and not tampered with Bob can do these steps.

1. First he needs here public key (Pu(A))
2. Then he decrypts using Alice's public key to acquire the (H). D_Pu(A)(S) = H
3. Bob must then compute H' of M_2
4. Bob compares H' with H. if they are the same the message is from Alice, and it has not been tampered with.