**Lab 6**

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:

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

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

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

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

**How would Alice send the message?**

Alice encrypts the message M with Bob's public key (Pu(B)):

*EPu*(*B*)​(*M*)=*M*1​

Alice sends M1 to Bob

**How would Bob decipher the message?**

*Bob decrypts the received message using his private key (Pr(B)):*

*DPr(B)​(M1​)=M*

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 Alice sent as

Alice generates a secure digest (hash) of the message M:

*H*(*M*)=*Mhash*​  
Alice encrypts the message hash using her private key (Pr(A)):

*EPr*(*A*)​(*H*(*M*))=*Msig*​  
Alice appends the signature *Msig*​ to the message M.

Alice sends the signed message *M*∣∣*Msig*​ to Bob.

**If computational efficiency is a concern, how would Alice send the message?**

If computational efficiency is a concern and confidentiality is not, Alice can simply send the message in plaintext without encryption

Alice sends the plaintext message M to Bob

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

Bob separates the received message into the actual message (M) and the signature (M\_sig)

Bob decrypts the signature using Alice's public key (Pu(A)):

*DPu*(*A*)​(*Msig*​)=*H*(*M*)

Bob generates the hash of the received message (M) and compares it with the decrypted signature hash (H(M))

If the hashes match, Bob can be confident that the message indeed came from Alice and hasn't been altered in transit.