Lab 6

Author: Lukas Kmitas

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*

1. 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?

How would Bob decipher the message?

1. 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

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

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