Lab 13

Robin Meyler

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?
E_Pu(B)(M_1)
Alice Encrypts the message with Bobs Public key because it can only be decrypted by Bob's private key which only he has. Thus, only Bob can see it.

Let us denote the message Alice sent as M_3. How would Bob decipher the message?
D_Pr(B)(M_3)
Bob decrypts the message using Bob's Private Key since it was encrypted with his public key.

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?
E_Pr(A)(M_2)
Alice doesn't care if others can see the message so she uses her own private key to encrypt the message, this way others can authenticate that it is, in fact, her that has sent it and not some middle man.

What would Bob do to verify that the message indeed came from Alice?
D_Pu(A)(M_2)
Since the message was encrypted with Alice's private key, Bob (along with anyone) must use Alice's public key to decrypt the message, this way the message is not hidden but Bob can be sure that no one has intercepted the message and altered it in any malicious way.

If computational efficiency is important, you may hash the message with SHA-3 or other with the likes of:
M_2 || E_Pr(A)(H(M_2))
Message appended with a hashed message of 128/256 bits to make it faster and still secure as the receiver can use the same algorithms to decrypt the hash