**Chapter 2: Crypto-inclass exercises**

1. With a public-key encryption, suppose John wants to send an encrypted and signed message to Paul. What are the keys for Paul and John. Show what steps and the keys used by John to create a message so that only Paul can decrypt the message but a third party can verify that the message came from John. Let M be the plain text message, show what is the signed message; what is the encrypted and signed message. Show what steps Paul needs to perform to decrypt the message?
2. Consider the following protocol. Ann wants to send a message M securely to Bob but there is no shared secret key between Ann and Bob, Ann does not even know Bob’s public key. However, using the properties of RSA (in particular the commutative property), Ann proposes the following protocol, where E(M, K) indicates encryption/decryption of message M with key K, “||” means concatenation of messages, KpubA means the public key of A, KprivA means private key of A.

Message1: Ann ->Bob: IDA || E(M, KpubA)

Message 2: Bob -> Ann: IDB || E[(E(M, KpubA)), KpubB)