Public/Private Key Cryptography

3. (a) Fill in the blanks in the following text describing Alice and Bob correctly communicating securely. Each blank needs to be filled in using one of the following words: (6)

   - Encrypt, encrypted, encrypts
   - Decrypt, decrypted, decrypts
   - Sign, signed, signs, signature
   - Public
   - Private

   Alice wants to send an encrypted and signed message to Bob who she has met in the past. When they last met in person they verified and then ***signed*** each other's _____ keys using their respective _____ keys.

   To send an email to Bob, Alice first ***signed*** the message using her _____ key and then _____ the resulting message using Bob's _____ key. Alice then sends the message over an untrusted connection.

   Bob receives the message and first _____ it using his _____ key. He then verifies that the message really was from Alice by verifying the ***signed*** using Alice's _____ key.

   (b) Research, such as the *Why Johnny Can't Encrypt* paper, often mentions "confusing metaphores" in regards to encryption interfaces. Give a specific example of a metaphor related to encryption that is likely confusing for people. (4)

(c) Would Alice and Bob's security in the interaction above be improved by using a Certificate Authority (CA)? State 'Yes' or 'No' and then briefly explain what a CA would do to help Alice and Bob OR explain why their current security practices are equal to or better than what a CA would provide. (6)