Homework Assignment 7 Solutions
ECE 151 / CMPSC 171 - Spring 2013

MARKING SCHEME:
Problem 2 - 20 points
Problems 3,5 - 15 points

1. (a) Explain the difference between confidentiality and integrity. Can we have one without the other?

Confidentiality is a property by which there is no unauthorized disclosure of secure information. Integrity is a property by which there is no malicious alterations of information even by unauthorized identities. Confidentiality and integrity have to go together to constitute a secure system and having one without the other is meaningless. Consider the case where Trudy intercepts the encrypted message sent by Alice to Bob and obtains the secure information by decoding the encrypted message by secretly knowing the private key of Bob. Trudy then sends the message intact to Bob. In this case even though the integrity of message is preserved the information has been leaked to an intruder to which it is not supposed to be.

(b) Explain the difference between integrity and authentication. Can we have one without the other?

Integrity is a property by which there is no malicious alterations of information even by unauthorized identities. Authentication is a property in a secure system by which a piece of information is delivered only to those recipients who are intended to receive it. It is meaningless to have one without the other. Consider the case where Alice' message is authenticated but it is intercepted by Trudy, who tampers with its contents, but leaves the authentication part intact. Here authentication has become meaningless.

2. Consider the RSA algorithm, described in Lecture 12, Slides 18 and 19, which is used for public key cryptography.
(a) Given the values *p = 7* and *q = 13*, find the smallest legitimate value of *d* and the corresponding value of *e*.
(b) Using the RSA algorithm and the value of *e* that you found, encrypt "ACE" where A is represented by 1, C is represented by 3, and E is represented by 5.

p=7 q=13 d=5 e=29
A--- 1
C--- 61

3. (a) Explain the "key" difference between symmetric cryptography and asymmetric cryptography.
(b) Discuss the advantages and disadvantages of symmetric cryptography and asymmetric cryptography.

Symmetric cryptography uses single key for encryption and decryption. This single key is secret and shared between sender and receiver. In asymmetric cryptography, different keys are used for encryption and decryption. One of them is a public key while the other is a private key. These two keys form a unique pair.

Advantages of symmetric cryptography: Fast, simple, if key is stolen only communication between two nodes is compromised
Disadvantages of symmetric cryptography: More number of keys in system, difficult to authenticate, requirement for secure key exchange

Advantages of asymmetric cryptography: No need for secure key exchange, easy to authenticate users.
Disadvantages of asymmetric cryptography: Slow, if (private) key is stolen communication of that node with all other nodes is compromised.

4. Consider the Needham-Schroeder protocol for authentication, as corrected with the additional nonce RB1, given in Lecture 12, Slide 30.
(a) Why is the additional nonce RB1 necessary?

The additional nonce RB1 is necessary because an intruder can discover Alice's private key KA,KDC and he can use it to decrypt a possibly old ticket for a session with Bob, and convince Bob to talk to him using the old session key.

(b) The KDC puts B (Bob) into its reply message and A (Alice) into the ticket. Why does the KDC do so?

The KDC puts Bob into the reply message to inform Alice that the shared key session K(A,B) which it is delivering is for Alice to communicate with Bob. Alice could have sent many requests to KDC asking for shared session keys to initiate sessions with different people and Alice could be waiting for the responses for those requests. Hence putting Bob in the reply message is imminent to inform Alice for which session it can use the shared key for.

The KDC puts Alice into the ticket sent to Bob to indicate to Bob that Alice has obtained a legitimate permission from KDC to communicate with Bob and shared key K(A,B) can be used to start a secure session with Alice.

(c) In the KDC's message to Alice, the ticket is encrypted with the shared secret key KA,KDC. Why is it necessary to encrypt the ticket?

The reply sent by KDC to Alice is encrypted with Alice's secret key because if this message is not secured, then an intruder can access the shared session key K(A,B) and can start a session with Bob.

5. In public-key cryptography, explain the difference in the use of the public key and the private key for (a) secrecy and (b) authentication.

Suppose A sends message to B by encrypting with B's public key. B decrypts the message using its private key (which is secret). Hence secrecy is maintained.

Suppose A signs the message to B with its private key. B can decrypt this message using A's public key. Hence B can authenticate A as the user who sent the message.

6. Consider the Diffie Hellman Key Exchange as given in Lecture 13, Slide 22.
(a) Construct an example consisting of specific numbers n, g, x and y.
(b) Show the specific numbers that Alice and Bob send to each other in Steps (1) and (2) of the algorithm.
(c) Show that Alice and Bob constract the same shared secret key in Steps (3) and (4) of the algorithm.

Alice and Bob agree on the numbers n=4 and g=5.
Alice chooses x=2 which she keeps private and Bob chooses y=3 which he keeps private.

(1) Alice send (4,5,1) to Bob [$g^x \bmod n = 5^2 \bmod 4 = 1$].
(2) Bob sends (1) to Alice [$g^y \bmod n = 5^3 \bmod 4 = 1$].
(3) Alice computes K(A,B) = $(g^y \bmod n)^x = (1 \bmod 4) = 1$
(4) Bob computes K(A,B) = $(g^x \bmod n)^y = (1 \bmod 4) = 1$