

**Computer and Network Security**  
**Fall Semester 2002**

**Solution to Quiz No. 1**  
July 30, 2002  
Time Allowed: 20 Minutes

Name: **SOLUTION**

**Total: 20 Points**

Multiple choice questions carry one point each and short questions carry two points each

1. The requirement that only authorized parties can modify the computer system assets is called:

- a. *Integrity*      b. *Availability*      c. *Secrecy*      d. *Authenticity*

2. Interruption is an attack on the:

- a. *Integrity*      b. *Availability*      c. *Secrecy*      d. *Authenticity*

3. Attacks which are difficult to detect because there is no modification of data are called:

- a. *Replay Attacks*      b. *Dictionary Attacks*      c. *Active Attacks*      d. *Passive Attacks*

4. Which of the following is a passive attack:

- a. *Interruption*      b. *Traffic Analysis*      c. *Modification*      d. *Fabrication*

5. Encryption can protect from Traffic Analysis.

- a. *True*      b. *False*

6. Data padding and filler sequences can protect from Traffic Analysis.

- a. *True*      b. *False*

7. DES is a security mechanism.

- a. *True*      b. *False*

8. SSL is a security protocol.

- a. *True*      b. *False*

9. Computer security is constrained by societal factors.

- a. *True*      b. *False*

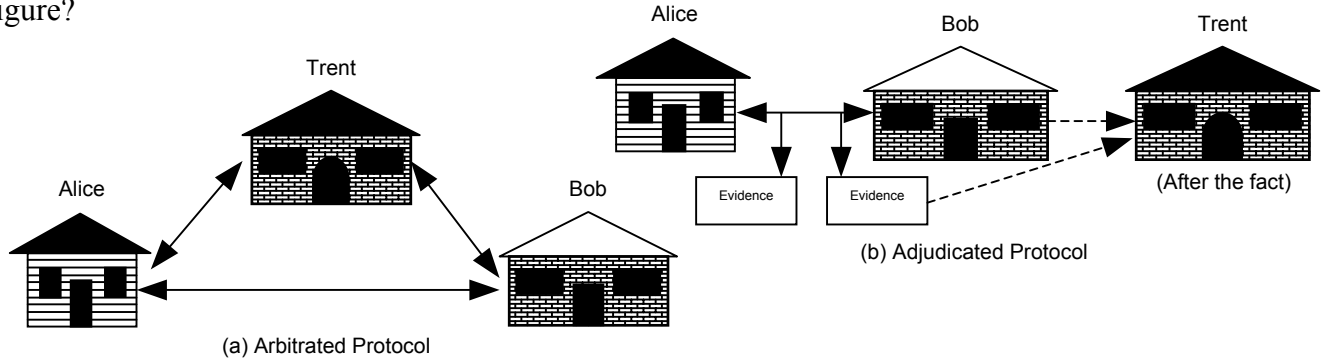
10. The type of attack in which an entity pretends to be another entity is called:

- a. *Masquerade*      b. *Replay*      c. *Modification of Messages*      d. *Denial of service*

11. Differentiate between two types of authentication.

There are two types of authentication (1) Principal Authentication and (2) Message Authentication. Principal Authentication is used to verify the identities of entities involved in an information exchange to each other whereas message authentication serves the purpose of verifying that each individual message/packet has actually come from the entity it is alleged to have come from.

12. Differentiate between an adjudicated protocol and an arbitrated protocol with the help of a figure?



13. Differentiate between encryption and steganography in one sentence.

Encryption scrambles a piece of information to make it unintelligible by using an encryption algorithm and a key whereas steganography hides a piece of information in a bigger piece of information to keep it from being detected.

14. What is the job of each of the following characters in a security protocol?

- (1) Alice: First participant in all the protocols
- (2) Mallory: Malicious active intruder
- (3) Trent: Trusted arbitrator
- (4) Eve: Eavesdropper
- (5) Dave: Participant in four-party protocols

15. Label the parts of the figure given below:

