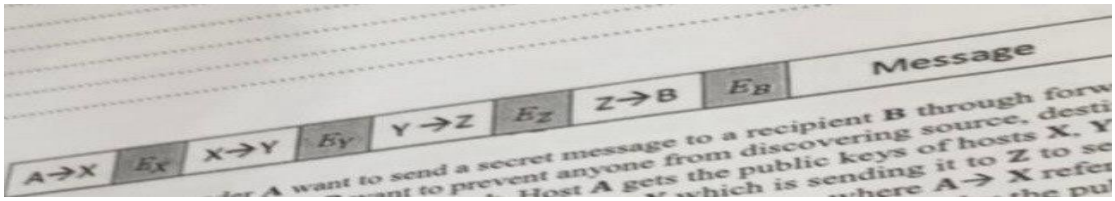
1. Write a simple code (using any programing language) that shows how off-by-one error could exploit the buffer overflow vulnerability.

2. Suppose a sender **A** want to send a secret message to a recipient **B** through forwarding hosts **X, Y**, and **Z**. Hosts **A** and **B** want to prevent anyone from discovering source, destination, or content of message in transit in the network. Host **A** gets the public keys of hosts **X, Y, Z** and **B**. Host **A** sends the message to **X** which is sending it to **Y** which is sending it to **Z** to send it to **B**. The secret message from **A** to **B** is shown in the following figure, where **A -> X** refers to the header where the message is sent from **A to X**, and Ex refers to the encryption by the public key of host **X -** the same for the other hosts.



a) Which cryptographic mechanism Host A is trying to implement?

b) How many keys in total are used in this scheme that includes 5 hosts?

c) Which key Host B needs to decrypt the message?

3. Suppose a team m of 6 students want to establish pair-wise secure communication them?

a) How many keys are needed if they decide to use asymmetric cryptography?

b) How many keys are needed if they decide to use symmetric cryptography?

4. Ahmed and Belal want to establish a secure communication between them using REA They selected the prime factors p=13 and q= 23. Ahmed selected e=7 to generate its
   public key =(e,n), and he sent it to Belal. Belal wants to send the message M=17 to Ahmed as an encrypted message. Show how Belal achieves that, and compute the encrypted message.

5. Suppose two branch offices need to communicate through a secure channel over the public network, what is the appropriate security mechanism for this scenario?

6. The following Table shows a sample of packet filtering rules for an institutional network 192.168/16:

a) Which ich rules would be matched and the action taken for the following cases?

i. Outgoing SMTP traffic to the external mail server www.gmail.com.

ii. Incoming http traffic to the internal webserver.

Rule	Source Address	Destination Address	Protocol	Destination Port	Action
1	192.168/16	Outside of 192.168/16	TCP	80	Allow
2	Outside of 192.168/16	192.168/16	TCP	25	Allow
3	Outside of 192.168/16	192.168/16	TCP	80	Allow
4	192.168/16	Outside of 192.168/16	TCP	25	Allow
5	Any	Any	Any	Any	Deny

b) What are the expected changes in the above cases of a) if the first and fifth rules are exchanged?

7. ///
8. What is the security tool which the operating system presents each the appearance of a system with only the resources the user entitled to use?

9. Do you agree with this phrase "Demilitarized zone (DMZ) is NOT a safe subnet for installing the institutional database server"? Why or why not?

10. Ali works at the traffic administration as a computer records clerk, where he has access to files of traffic violation records for a scientific study, a researcher, Belal, has granted access to just the numerical portion of some records, but for more information, Belal asked Ali to retrieve the names and telephone numbers, corresponding with certain properties to do further study.

    a) Regarding the rule-deontology theory, should Ali release the names and telephone numbers? Why or why not?

b) Regarding teleological theory, if Ali decided to help Belal by giving him the required names and telephone numbers, what is the expected action from Ali's supervisor when he discovers that?