**Final Exam (DE) 2016**

**Question 1 (Malicious logic)**

1- Write any 5 types of the viruses.

2- What is Hoax? How is it like Worm (In which way)?

3- The textbook gave the following example of a rabbit:

while true

mkdir x (create a directory named x)

chdir x (make the newly created directory the current directory)

done

Would this still be a rabbit if you removed the chdir x?

**Question 2**

What is the difference between authentication and authorization?

**Question 3:**

There is a conflict between Economy of mechanism and Psychological Acceptability, describe why?

**Question 3: (Questions about DMZ)**

1- What is DMZ?

2- Briefly describe what are the components of DMZ? (Means the DMZ Servers).

3- Describe how DMZ components apply the principle of least privilege.

**Question 4**

This question was about Asymmetric Encryption/Digital Signature and checksum: be accurate so don’t write just public key or private key but write: Alice’s public key or Bob’s public key. If Alice wants send a message to Bob:

1- If Alice wants to encrypt the hash of the message, which key she’s going to use?

2- If Alice wants to digitally sign the message, which key she’s going to use?

**Question 5**

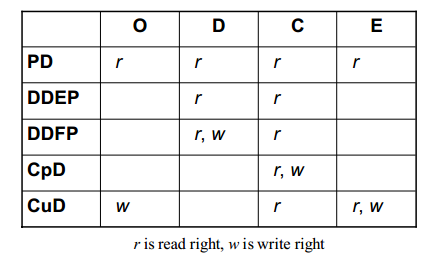
What are the goals of Intrusion Detection System?

**Question 6**

What are the three models of the Intrusion detection?

**Question 7**

Complete the following table by writing w for write right and r for read right.



**Question 8**

1- What is the Buffer overflow?

2- How the Java language prevent the Buffer overflow?

3- Is any program runs under JVM is going to be Immune?

**Question 9**

Write two of your favorite SCI principles.