Mid Term Old Questions Answers:

1) What is digital signature?(5)
2) Let m be a message. Suppose Alice and Bob share a secret key k. Alice sends bob m | | {m}k (i.e. the message and it's encipherment under k). Is this a digital signature? Why or why not? Explain your answer.(7)
3) Describe briefly the roles of the 3 different servers used in Kereberos.(6)
4) What is a potential problem of the Kereberos protocol?(5)
5) Policy restricts the use of e-mail on a particular system to faculty and staff. Students cannot send or receive e-mail on that host. Classify the following mechanisms as secure, precise, or broad and briefly justify your answer. (9)
    a) The e-mail sending and receiving programs are disabled.(3)
    b) As each letter is sent or received, the system looks up the sender (or recipient) in a database. If that party is listed as faculty or staff, the mail is processed. Otherwise, it is rejected. (Assume that the database entries are correct.) (3)
    c) The e-mail sending programs ask the user if he or she is a student. If so, the mail is refused. The e-mail receiving programs are disabled.(3)
6) In Bell-LaPadula model, the security levels are TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories are A, B, and C. Specify what type of"access (read, write, both, or neither) is allowed in each of the following situations.Also briefly explain your answer. Assume that discretionary access controls allow anyone access unless otherwise specified. (9)
    a) [3] Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, {B}).
    b) [3] Paul, cleared for (TOP SECRET, {A, C}), wants to access a document classified (SECRET, {B, C}).
    c) [3] Sammi, cleared for (TOP SECRET, {A, C}), wants to access a document classified (CONFIDENTIAL, {A}).
7) Briefly explain how Clark-Wilson integrity model supports the principle of separation of duty. (6)
8) Difference between a known plaintext attack and a chosen plaintext attack. (6)
9) We've learnt 12 design principles in this course till now. Please relate 2 of them to the SCI principles that we've studied. [Hint: Principle of complete meditation - infinity at a point] (6)
10) What is the cipher text for word "SECURITY" using rail-fence cipher with a key of 3? (4)
11) Briefly explain any 3 advantages of CAs (Certificate Authorities) over KDCs (Key Distribution Center) (9)
12) Please give an example of a trade-off between the principle of psychological acceptability and the principle of least privilege (6)
13) Consider a computer system with the three users: Alice, Bob and Cyndy. Alice owns the file Alicerc, and Bob and Cyndy can read it. Cyndy can read and write the file Bobrc, which Bob owns, but Alice can only read it. Only Cyndy can read and write the file Cyndyrc, which she owns. Assume the owner of each of these file can execute it. Create the corresponding access control matrix. (6)

14) Considering role of trust, sometimes a “back-door” is purposefully used through which the security mechanism can be bypassed. The trust resides in the belief that this back door will not be used except as specified by the policy.Based on your experience as an IT professional, briefly describe a situation in which planting a back door would be needed and explain how it could be used and misused. (8)
15) Let’s say that I can control some process by sending a “stop” and “start” message to a server. The fact that I am starting and stopping the process is not a secret, so I don’t have to encrypt the start and stop message. But it is important that I am the only person who can stop and start the process. Therefore. I digitally sign the “stop” or “start” message with my private key. The server then decrypts the hash with my public key to make sure that I was the one who sent the message. Briefly describe what is wrong with this protocol. (8)
16) Bob’s password is “flower”, but one day by accident he discovers that the password “blowfish” also works. This is a complete mystery to him because he has never used “blowfish” as a password. Please give an explanation for this behavior. The following answers are not acceptable.
    a) “There is a bug in the program”
    b) “Blowfish” was a back door planted by the vendor
    c) Bob added “blowfish” and forget about it.