CPTR 5760 **Test #2** **SUMMER 2016**

Instruction:

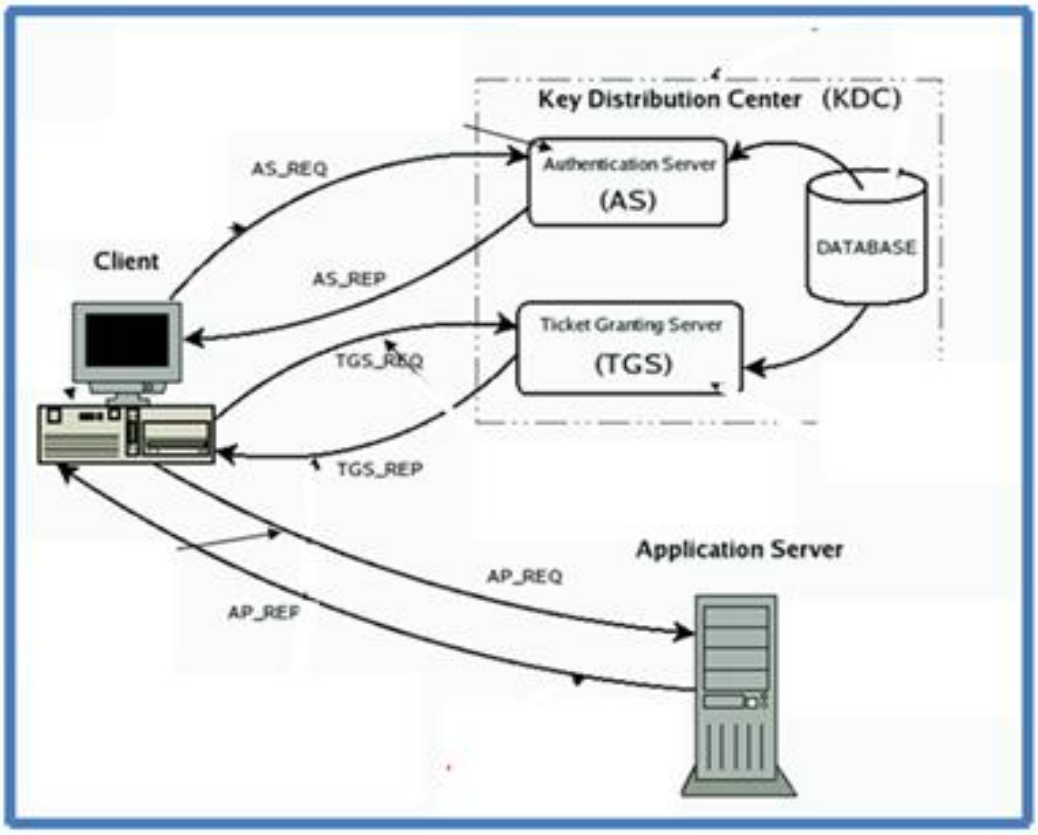
To receive a grade for this test, you must:

1. Start each problem on a new page (*if not you will loose 2 points*)
2. Work on the problems in the order they are presented in the test (*if not you will loose 2 Points*)
3. Show, for all problems, all the necessary works

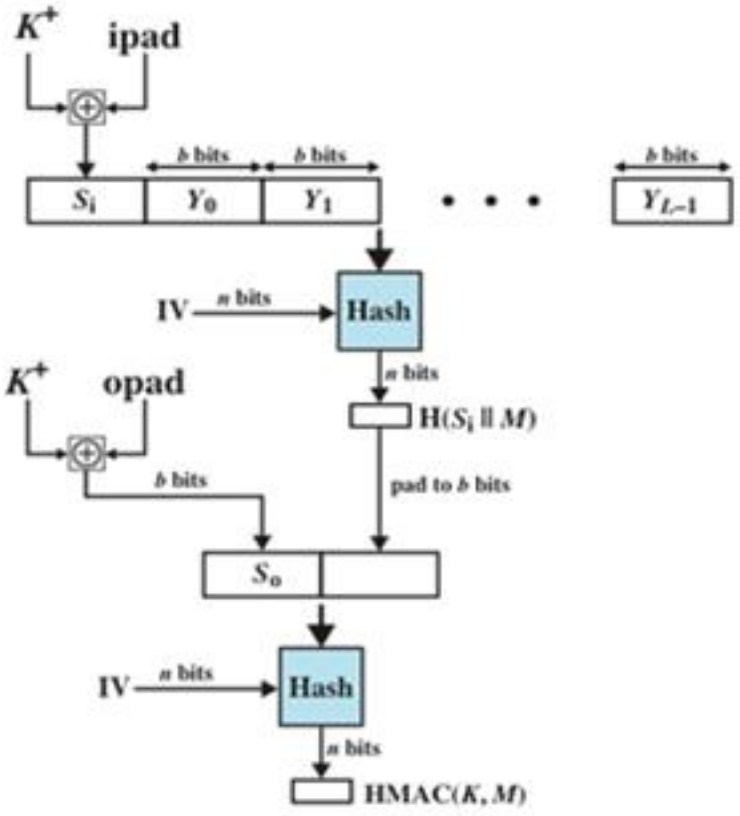
Good luck!!!

Problems

1. Specify the Kerberos messages involved from the time a user first walks up to a client workstation to the time the user is successfully talking to the application server

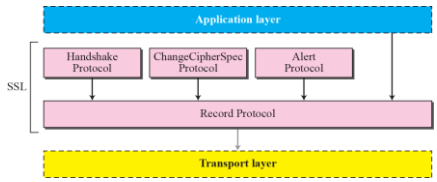


2. The HMAC Algorithm is outlined in the following block diagram. Write the five steps of the process, in the correct sequence, for generating the Message authentication code



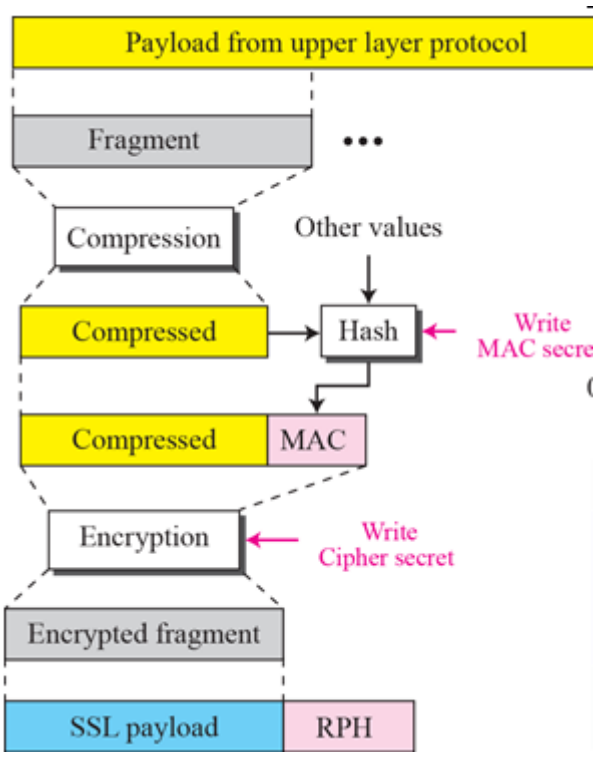
3. Consider a protocol in which messages are not encrypted. However, a message authentication code (*MAC) is* included for each message and the *MAC* is sent with each message *x* over an open channel. If an attacker (*Oscar)* alters the contents of the message *x*, describe how *Alice* will detect the alteration of the message sent by *Bob*.

4. As we discussed in class, SSL consists of two layers of protocols as shown below



Briefly describe the service provided by:
(a) The Handshake Protocol
(b) The ChangeCipherSpec protocol
(c) The Alert Protocol
(c) The Record Protocol

5. The operation of SSL Record protocol is presented in the following Figure



Write how this process is performed at sending and the receiving end

.

6. What parameters identify an SA? and what parameters characterize the nature of a particular SA?

7. Consider the following protocol:

$A \rightarrow KDC$: $ID_A || ID_B || N_1$

$KDC \rightarrow A$: $E(K_a, [K_s || ID_B || N_1 || E(K_b, [K_s || ID_a])])$

$A \rightarrow B$: $E(K_b, [K_s || ID_A])$

$B \rightarrow A$: $E(K_s, N_2)$

$A \rightarrow B$: $E(K_s, f(N_2))$

(a) Explain the protocol
(b) Can you think of a possible attack on this protocol? Explain how it can be done
(c) Mention a possible technique to get around the attack--not a detailed mechanism, just the basics of the idea.

8. (a) Compare and contrast the advantages and disadvantages of PKIs and key Kerberos servers.
(b) Describe one example application for which you would use a PKI. Justify your decisions.
(c) Describe one example application for which you would use a key Kerberos server. Justify your decisions.

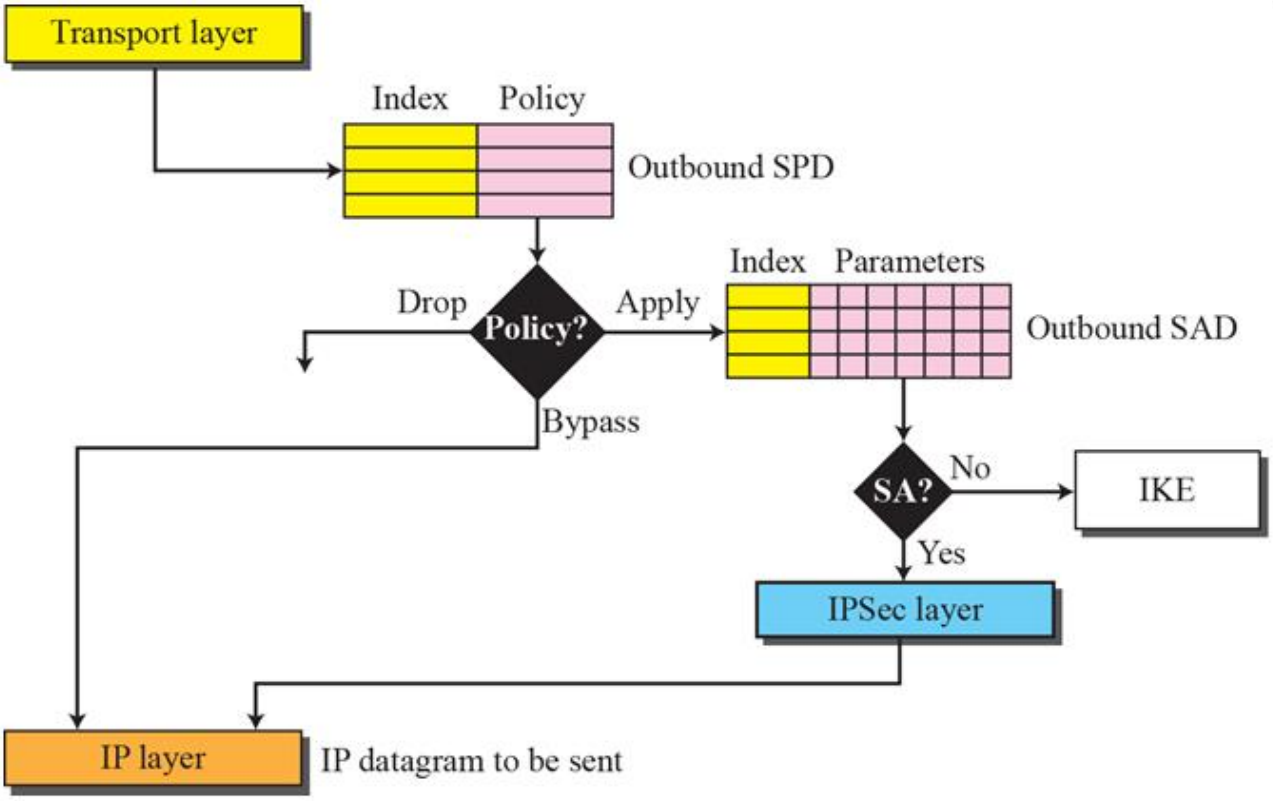
9. The SSL Handshake Protocol must be executed to establish a Connection before data transmission may take place. The Protocol proceeds according to the following process.
Phase 1: Establishing Client/Server Capabilities
Phase 2: Server Authentication and Key Exchange
Phase 3: Client Authentication and Key Exchange
Phase 4: Protocol Completion

   (a) Describe in detail how Phase 1 is completed (*you must outline the messages exchanged between the client server including what the messages contain*)

   (b) Briefly describe how the other three phases of the protocol are completed

10. In class we discussed the working and implementation of the IPsec protocol; in light of the explanations given for the functioning of the various protocols in IPsec answer the following questions
(a) What are the three main protocols for IPsec? (list and describe the protocols)
(b) What services are provided by IPsec?
(c) Compare and contrast the advantages and disadvantages of Transport mode and Tunnel mode of operations

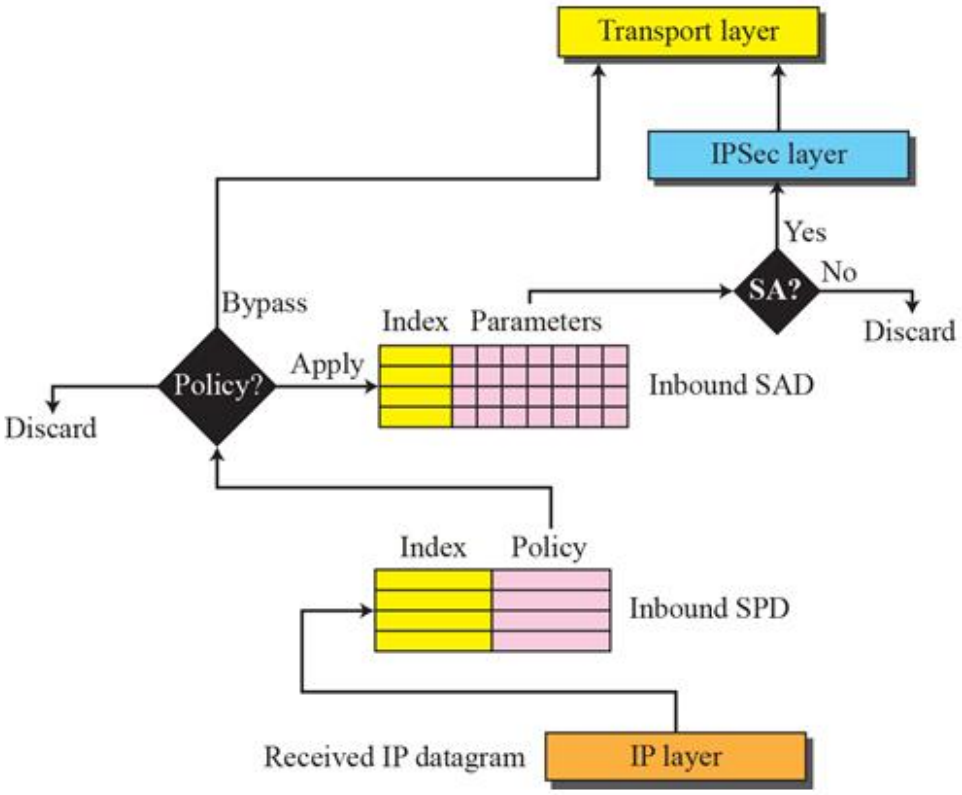
11. (a) When IPsec is implemented, as shown in the following Figure, each ***outbound IP packet*** is processed by the IPsec logic before transmission; describe and explain the processes shown in the figure.



   (b) Describe the role of the outbound SAD

   (c) Describe the role of the outbound SPD

12. (a) When IPsec is implemented, as shown in the following Figure, each ***incoming IP packet*** is processed by the IPsec logic before transmission; describe and explain the processes shown in the figure.



(b) Describe the role of the inbound SAD

(c) Describe the role of the inbound SPD