

1. (a) Explain the terms "Confusion" and "Diffusion" with respect to a cryptographic system. Explain their importance.
(b) Suppose Bob has an RSA cryptosystem with a very large modulus N for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25 ($A \rightarrow 0, \dots, Z \rightarrow 25$), and then encrypting each number separately using RSA with large e and large N . Is this method secure? Explain your answer.
2. (a) We know that doing a signature with RSA alone on a long message would be too slow. Suppose we could do division quickly. Would it be reasonable to compute an RSA signature on a long message by first computing what the message equals mod n , for some fixed n and then signing this computed value only. Why or why not?
(b) Consider a network of client workstations and a server with the following password based authentication protocol. In order to log in, a user *Alice*, types in a password, say *nachos*, at the client workstation. The workstation then computes the hash value of the password, $Y = H('nachos')$, and sends the user id *Alice* to the server. The server then picks a random number R which it sends to the client workstation. The client workstation computes $Hash(Y, R)$ which it sends to the server. The server has in its database, a password file, containing the hashed values of all user passwords. It reads the hash value of Alice's password, say Z and it computes $Hash(Z, R)$. The server will then permit the log in only if this is the same as the $Hash(Y, R)$ it received from the client workstation. Is this protocol secure against eavesdropping? Is it secure if the servers password file gets disclosed? Explain why or why not?
3. (a) With reference to IPSEC answer the following:
 - i. How does ISAKMP/Oakley provide defense against denial of service attacks? Explain.
 - ii. In which mode does IPSEC does provide a limited amount of traffic confidentiality? Explain how in detail with the aid of a figure.
 - iii. Explain the difference between transport and tunneling modes.(b) Briefly describe the architecture of SSL and each of it's sub-protocols. Can SSL be used to provide the following services. Explain why or why not?
 - i. Secure web transactions.
 - ii. Securing DNS traffic sent over UDP.
 - iii. Secure Email.
 - iv. A secure version of FTP that includes authentication and encryption.
 - v. Authentication of IP packets.
 - vi. Defense against Denial of Service attacks.
4. Compare and contrast the following:
 - (a) Knowledge-based and Behaviour-based Intrusion Detection Systems.
 - (b) Host-based and Network-based Intrusion Detection Systems.

5. Consider the following ipchains rules script:

```
#!/bin/sh
EXTERNAL_INTERFACE="eth0" LOOPBACK_INTERFACE="lo"
LOCAL_INTERFACE_1="eth1" IPADDR="10.10.1.2"      # external
interface LOCALNET_1="10.20.2.0/24" INTERNAL_IP="10.20.2.1"
ANYWHERE="any/0" LOOPBACK="127.0.0.0/8" PRIVPORTS="0:1023"
UNPRIVPORTS="1024:65535"

ipchains -P input DENY
ipchains -P output REJECT
ipchains -P forward DENY

ipchains -A input -i $LOOPBACK_INTERFACE -j ACCEPT
ipchains -A output -i $LOOPBACK_INTERFACE -j ACCEPT

ipchains -A input -i $LOCAL_INTERFACE_1 -s $LOCALNET_1 -j ACCEPT
ipchains -A output -i $LOCAL_INTERFACE_1 -d $LOCALNET_1 -j ACCEPT

ipchains -A forward -i $EXTERNAL_INTERFACE -s $LOCALNET_1 -j ACCEPT
ipchains -A forward -i $LOCAL_INTERFACE_1 -d $LOCALNET_1 -j ACCEPT

ipchains -A input -i $LOCAL_INTERFACE_1 -p tcp \
-s $LOCALNET --source-port $UNPRIVPORTS \
-d $ANYWHERE 23 -j ACCEPT

ipchains -A output -i $LOCAL_INTERFACE_1 -p tcp \
-s $ANYWHERE 23 \
-d $LOCALNET --destination-port $UNPRIVPORTS -j ACCEPT

ipchains -A output -i $EXTERNAL_INTERFACE -p tcp \
-s $LOCALNET --source-port $UNPRIVPORTS \
-d $ANYWHERE 23 -j ACCEPT

ipchains -A input -i $EXTERNAL_INTERFACE -p tcp \
-s $ANYWHERE 23 \
-d $LOCALNET --destination-port $UNPRIVPORTS -j ACCEPT

exit 0
```

- (a) From the rules script what can tell about the machine it's running?
- (b) From the rule script describe what incoming traffic and outgoing traffic is allowed?
- (c) Modify the above rule set such that all incoming telnet traffic to the local network is accepted and all outgoing traffic is denied.
- (d) How would you modify the rule script if the subnet mask of the internal network were changed to 255.255.0.0?