1. **TCP/IP Security** Consider the following modifications to ARP and TCP:

- ARP is replaced with SARP (Secured ARP) to avoid ARP cache poisoning and ARP spoofing. SARP works as follows: In SARP all request and replies are encrypted. Each node has a set of 100 predefined DES keys $K_i$ which are common to all nodes. When node A tries to resolve the IP address of node B it broadcasts following:

$$E_{K_i}( <\text{A's MAC}> | \text{ff:ff:ff:ff:ff} | <\text{A’s IP}> | <\text{B’s IP}> | <\text{Request ID}> | <\text{A’s PUBLIC KEY}> )$$

where $K_i$ is a key randomly chosen from the 100 predefined DES keys, and request ID is a random number.

Now, node B first stores A’s public key and IP in a table and replies for the request by sending

$$E_{A’sPubkey}( <\text{B’s MAC}> | <\text{A’s MAC}> | <\text{B’s IP}> | <\text{A’s IP}> | E_{K_{i+2}\text{mod100} }(<\text{A’s Request ID}> ) | <\text{B’s PUBLIC KEY}> )$$

Node A stores B’s public key along with node B’s IP address in a table and all subsequent ARP transactions between A and B are encrypted using their public key.

- Does the above modification solve the ARP spoofing and ARP cache poisoning attacks. Explain clearly why or why not.

- TCP is replaced with STCP (Secured TCP) to avoid session hijacking. STCP works as follows: STCP avoids session hijacking by encrypting the TCP sequence number using private key cryptography. A pr key is derived using Diffie-Hellman key exchange protocol during the three way hand shake process of TCP. This session key is used to encrypt the sequence number. The session key and the IP address is stored in a table and reused in future sessions.

- State three problems with the solution listed above. Problems in the sense of security and cost.

2. **Firewalls** Consider the following firewall rules

```bash
#!/bin/sh
ipchains -P input ACCEPT
ipchains -P forward ACCEPT
ipchains -P output ACCEPT
ipchains -A input -s 0/0 -d 0/0 22 -p tcp -y -j ACCEPT
ipchains -A input -s 0/0 -d 0/0 -i lo -j ACCEPT
ipchains -A input -s 128.238.2.38 53 -d 0/0 -p udp -j ACCEPT
ipchains -A input -s 0/0 -d 0/0 -p tcp -y -j REJECT
ipchains -A input -s 0/0 -d 0/0 -p udp -j REJECT
```
(a) From the rule script describe what incoming traffic and outgoing traffic is allowed?
(b) Modify the above rule set such that all incoming telnet traffic accepted and all other outgoing traffic is denied.
(c) How would you modify the rule script to accept all traffic from 10.1.2.0/24 subnet, but deny telnet connection from 10.1.2.33 and http connection from 10.1.2.67?

3. **Intrusion Detection**
   
   Give two advantages and disadvantages each of *Knowledge-based* and *Behavior-based Intrusion Detection* Intrusion Detection Systems. Which one would be more suitable as a Network IDS and which one for a Host IDS. Why?
   
   (a) Explain what is *Base Rate Fallacy* with the aid of a numerical example.

4. **Cryptography** Please mark the following statements as true or false.
   
   (a) Private key cryptography is susceptible to a man-in-the-middle attack.
   (b) In RSA the encryption key and the decryption keys are inverses of each other modulo N, where N is a product of two primes P and Q.
   (c) A Cryptographic Hash Function is a hash function that uses a secret key to compute a hash value.
   (d) The usual way to sign a message using RSA is to encrypt the entire message using the RSA private key.
   (e) Digital Signatures provide authentication as well as non-repudiation.
   (f) Double DES (2-DES) is essentially no more secure than single DES.
   (g) A crypto system with a large key space is necessarily secure.
   (h) A crypto system with a small key space can be secure.
   (i) In a public key crypto system encryption and decryption are done with different keys.
   (j) The great advances civilization has made in science and technology have been matched by equal if not greater social advances. We have less hatred in the world today than ever before.

5. **Secure Email/SSL**
   
   (a) Can SSL be used to provide the following services. Very briefly explain why or why not? Answers without explanations will not be given any credit.
      i. Securing ARP broadcasts.
      ii. Securing DNS traffic sent over UDP.
      iii. Secure Email.
      iv. A secure version of FTP that includes authentication and encryption.
      v. A secure information collection system using which your company plans to conduct surveys about their products.
      vi. Defense against Denial of Service attacks.
   (b) What is Cipher Spec rollback attack? Why would this attack work on SSL 2? How does SSL 3 protect itself against this attack?