1. Suppose UTK implements a “Top-Down with Name Constraints” PKI model with two-level hierarchy. The root CA is pki.utk.edu, which has two delegated CA servers, pki.eecs.utk.edu and pki.math.utk.edu, at the second layer for the EECS department and the MATH department, respectively. Suppose alice@eecs.utk.edu wants to learn the public key of bob@math.utk.edu. The following statements explain how this PKI model works. Is each of the following statements TRUE or FALSE? Explain your answer briefly.

a. Every machine in UTK is configured with the public key of the root CA.

TRUE. In a “Top-Down with Name Constraints” PKI model, everyone must be configured with the root CA’s public key.

b. The domain of eecs.utk.edu has a CA server (pki.eecs.utk.edu) that is delegated from the root CA (pki.utk.edu). The domain of math.utk.edu also has a CA server (pki.math.utk.edu) that is delegated from the root CA.

TRUE. In a “Top-Down with Name Constraints” PKI model, the root CA delegates other CAs.

c. The root CA generates certificates for pki.eecs.utk.edu responsible for the sub-domain eecs.utk.edu and for pki.math.utk.edu responsible of the sub-domain math.utk.edu.

TRUE. The root CA generates certificates for the delegated CAs.
d. Alice@eecs.utk.edu is pre-configured with the public key of pki.eecs.utk.edu and bob@math.utk.edu is pre-configured with the public key of pki.math.utk.edu.

FALSE. Alice@eecs.utk.edu and bob@math.utk.edu are pre-configured with the public key of the root CA.

e. alice@eecs.utk.edu and bob@math.utk.edu obtain certificates from their own CAs, which are pki.eecs.utk.edu and pki.math.utk.edu, respectively.

TRUE. The delegated CA issues certificates for their portions of the namespace.

f. In order for alice@eecs.utk.edu to authenticate the public key of bob@math.utk.edu, bob@math.utk.edu must send its certificate and its CA’s certificate to alice@eecs.utk.edu.

TRUE. The only trust path in a top-down model is from the root to the target. Alice use root CA’s public key to verify the certificate of pki.math.utk.edu. Then she uses that public key to verify the public key of Bob@math.utk.edu.
2. Explain how PCBC is used to provide both privacy and integrity protection. Identify one vulnerability of PCBC.

Refer to Figure 13-5 for PCBC.

PCBC relies on a variant of CBC for privacy protection. Before encryption, a message block is XORed not only with the previous ciphertext block but also with the previous message block. For integrity protection, it appends recognizable data at the end of a message and then encrypts the appended message. If the receiver can recover the recognizable appendix, it will accept the message as a genuine one. Due to XORing with the previous message block, PCBC achieves integrity protection with one pass of encryption, which cannot be done by CBC. When one-pass CBC encryption is done with a recognizable appendix, if a ciphertext block is modified in transit, only this and the next message blocks are garbled at the receiving side. The recognizable appendix will stay the same, which defeats integrity protection. On the contrary, when PCBC is used, modifying a ciphertext block will garble the rest of the message, including the recognizable appendix.

PCBC also has vulnerability. When two adjacent ciphertext blocks are swapped, only the corresponding message blocks are garbled, while the recognizable appendix will stay correct.

3. Specify the Kerberos messages involved from the time a user first walks up to a workstation to the time the user is successfully talking to something in another realm. [Kaufman 13.4]

![Kerberos Message Flow Diagram]

After Bob receives AP_REQ, he decrypts the ticket to get the temporary shared key between Alice and Bob $K_{AB}$, and verifies the timestamp in the authenticator.
4. In what circumstances should the tunnel mode or the transport mode of IPSec be used? In those cases, can one mode be replaced with the other? Why?

Transport mode is the default mode of IPSec. It is used for end-to-end communications (e.g. client-server communication). Because tunnel mode has the cost of an additional IP header, transport mode is most logical when IPsec is applied on end-to-end communications between two hosts.

The common use of tunnel mode is firewall-to-firewall or host-to-firewall. Tunnel mode protects traffic between different networks, when traffic must pass through an intermediate, untrusted network.

Transport mode is not strictly necessary for host-to-host IPSEC. Tunnel mode can replace transport mode with additional overhead (i.e., an extra IP header with the identical source/destination addresses). However, transport mode cannot replace tunnel mode for firewall-to-firwall IPSEC because of a few reasons. First, the original source/destination addresses can be private addresses and the packets rely on firewalls’ public addresses to be routable across the Internet. Second, the packets that are IPSECed at one firewall must be routed to the peer firewall in order to be unIPSECed before reaching the receiving host. The only way that guarantees the packets to pass the peer firewall is for their destination addresses to be the firewall’s address.

5. AH integrity-protects some fields in the IP header, but not TTL. Why?

TTL will change at every hop so it is a mutable field. AH does not integrity protect mutable fields.
6. Explain what ESP, AH, and IKE achieve, respectively. Suppose host1 and host2 are communicating with end-to-end AH, transport mode, while firewall1 and firewall2 enforce ESP, tunnel mode on all traffic between them.

```
host1 --- firewall1 --- Internet --- firewall2 --- host2
```

Consider a packet from host1 to host2. Describe the packet structure at the time when the packet is in the Internet. (Write down the headers in the correct order and describe what portion of the packet the AH/ESP headers protect, respectively.)

ESP provides encryption and/or integrity protection.
AH provides integrity protection only.
IKE establishes IPSec SA for ESP or AH. It does mutual authentication and shared key establishment, cipher negotiation, and parameter negotiation.

```
Outer IP Header       // src = firewall 1, dst = firewall 2
ESP Header            // protecting Inner IP Header, AH Header, Data
Inner IP Header       // src = host 1, dst = host 2
AH Header             // protecting Inner IP Header, and Data
Data
```
7. The following figure illustrates the SSL handshaking protocol. Explain how the following is achieved.
   a) server authentication.
   b) session key negotiation.
   c) message integrity protection.

![Diagram of SSL handshaking protocol]

---

a) server authentication
   SSL/TLS uses public key cryptography. A client requests a connection with a server (message 1). Server should reply a certificate issued by a recognized CA (message 2). The client verifies the certificate and extracts the server’s public key. It then picks a random number S from which the session keys will be computed, and sends S to server, encrypted with server’s public key (message 3). The server proves he knows the session keys by sending a keyed hash of all the handshake messages (message 4). Since the session keys are derived from S, this proves he knows server’s private key. In this way, server is authenticated to the client.

b) session key negotiation
   A pre-master secret encrypted with the server’s public key is sent in message 3. The secret is randomly generated for each SSL session and used for symmetric encryption of data. The server decrypts the secret with its private key. At this point both client and server have the same pre-master secret, based on which they both calculate the same master secret, from which the session keys are generated. The keys are encryption, integrity, and IV in each direction, so there are six session keys derived. (In SSLv2, only two session keys)
c) message integrity protection
The server is securely identified by a validated server certificate. The client can make sure that tampering of the handshake messages would be detected by sending a hash of the master secret $K$ and the handshake messages (message 3), encrypted and integrity-protected with the client’s write keys. The server also sends the keyed hash of all the handshake messages, encrypted with the server’s write-encrypted key, and integrity-protected with the server’s write-integrity keys.

8. The following figure shows the aggressive mode of IKE phase one with public signatures as the means of authentication.

![Protocol 18-5. Public signature keys, aggressive mode](image)

An eavesdropper will learn the identities of the two parties, “Alice” and “Bob”. How to improve the protocol to hide the identity information from the eavesdropper?

In the second message, “Bob” can be encrypted by a secret key derived from the Diffie-Hellman exchange. “Alice” is moved from the first message to the third message and should also be encrypted by the secret key.
9. Consider the following bottom-up PKI system with name constraint. An arrow $x \rightarrow y$ means a certificate is issued by $x$ for $y$’s public key. A double arrow $x \leftrightarrow y$ means $x$ and $y$ issue certificates for each other. For A.B.D to learn A.C.F’s public key, what is the chain of certificates that A.B.D must acquire? Assume anyone knows only its own public/private keys.

For bottom-up, A.B.D $\rightarrow$ A.B, A.B $\rightarrow$ A, A $\rightarrow$ A.C, and A.C $\rightarrow$ A.C.F