1. **Review 22.4** What is DKIM?

   DKIM means DomainKeys Identified Mail. Is a method for cryptographical signing e-mail messages, permitting a signing domain to claim responsibility for a message in the mail stream. Is basically a method that makes sure the email that is being received, was actually sent and authorized by the owner of that domain. (Page 664)

2. **Review 22.5** What protocols comprise SSL

   -The Record Protocol. Provides two services for SSL connections which are: Confidentiality and Message integrity.
   -Change Cipher Spec Protocol. Is one of the four TLS-specific protocols that use the TLS Record Protocol, and it is the simplest. Consists of a single message with the purpose of causing the pending state to be copied into the current state, which updates the cipher suite to be used on this connection. The message consists of a single byte with the value 1.
   -Alert Protocol. Is used to convert alerts to the peer entity. Alert messages are compressed and encrypted, as specified by the current state.
   -Handshake Protocol. This protocol allows the server and client to authenticate each other and to negotiate an encryption and MAC algorithm and cryptographic keys to be used to protect data sent in an TLS record. (Page 669-670)

3. **Problem 22.2** Consider the following threats to Web security and describe how each is countered by a particular feature of SSL:

   (a) *Man-in-the-middle attack: An attacker interposes during key exchange, acting as the client to the server and as the server to the client.*

   For this case the SSL can use a certificate validation method by using the public key certificates, to authenticate the correspondence between the server and the client, this will keep secured the keys and won't allow the middle man to attack.

   (b) *Password sniffing: Passwords in HTTP or other application traffic are eavesdropped.*

   For this SSL can encrypt the user's data to protect the passwords in HTTP or other application traffic.

   (c) *IP spoofing: Uses forged IP addresses to fool a host into accepting bogus data.*

   This one is encounter by the SSL public-key or certificate by checking it against the IP spoofing and since the IP spoofing has no public-key or certificate the the communication with the server cannot be established.

(d) *IP hijacking: An active, authenticated connection between two hosts is disrupted and the attacker takes the place of one of the hosts.*

Here again the SSL can encrypt the user's data to prevent the attack by using the **secret key** between the sender and receiver to verify that it is really them.

(e) *SYN flooding: An attacker sends TCP SYN messages to request a connection but does not respond to the final message to establish the connection fully. The attacked TCP module typically leaves the "half-open connection" around for a few minutes. Repeated SYN messages can clog the TCP module.*

SSL cannot provide any service to protect in this case.

4. **Review 23.9** What is a public key infrastructure?

The RFC defines the public-key infrastructure as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates cased in asymmetric cryptography. The principal objective for developing a PKI is to enable secure, convenient, and efficient acquisition of public keys.
(Page 694)

5. **Problem 23.4** Using your Web browser, visit any secure Web site (i.e. one whose URL starts with https). Examine the details of the X.509 certificate used by that site. This is usually accessible by selecting the padlock symbol. Answer the same questions as for problem 23.3.

(a) Identify the key element in this certificate, including the owner's name and public key, its validity dates, the name of the CA that signed it, and the type and value of signature.

The page I am checking is : *https://www.yahoo.com/*

-Owner's name : This website does not supply ownership information.
-But it was issued by (CN) : DigiCert SHA2 High Assurance Server CA
-Public Key:

```
Modulus (2048 bits):
ee 5a ff a6 87 d9 fd e7 f3 7f 48 b2 59 e0 da 98
20 71 31 02 c2 b5 de 1f 0f 4a 87 a7 da 90 df b4
30 e9 78 71 40 1b eb e2 6a d4 4a f6 db 85 fc 8f
81 1c 65 9f 6e 6a 4f 47 c7 da 6c 85 4f ef 33 c9
```

```
85 b2 62 65 1b 25 cc 23 f8 34 51 1e 64 a0 01 d8
e3 93 0d a4 94 e8 57 be 53 31 d9 b4 e8 b8 82 07
31 92 29 57 dc 57 7b 2a 8c ba af 0c 3b 03 5e 13
ce 5d c9 84 c6 d9 3f 56 72 a6 28 40 b1 f1 d1 c6
5f ff 7f e7 ea 29 d5 88 fd f3 fe 30 5f ae 91 ab
c1 65 f9 d1 0f 30 63 45 e6 a2 0b e4 20 1b 08 aa
ef 9f 83 8d f1 56 4b a4 9b 08 18 5c 0c 7e 26 23
bf b7 36 1a c1 79 b5 d6 39 1c 62 12 a7 d3 c2 15
04 ac fa 5d a5 be de a3 20 ce ab 67 d6 97 d1 4f
da 71 18 8c 0b 98 ac 49 a5 79 b6 4c 1c 09 2e 83
03 e8 06 34 eb 7b 1e 68 f9 8d 8c 96 23 1c 5e c7
fb 81 61 3d 28 19 31 fe d3 7b 79 a4 71 5d 94 a9
Exponent (24 bits):
65537
```

-Validity dates:

```
NOT BEFORE
August 12, 2018, 6:00:00 PM GMT-6
(August 13, 2018, 12:00:00 AM GMT)
NOT AFTER
February 14, 2019, 5:00:00 AM GMT-7
(February 14, 2019, 12:00:00 PM GMT)
```

-Type signature : PKCS #1 SHA-256 With RSA Encryption
-Value of the signature:

```
Size: 256 Bytes / 2048 Bits
08 4a a3 b8 87 dc 6e f0 81 61 05 f0 3e bc 75 05
14 7a c9 af b3 92 c9 bb 46 fc e8 11 0d d5 93 2a
3e 6e e5 f2 b8 23 62 60 2b 27 f7 31 fb 92 b2 cc
8a bf 80 99 3c 4d 40 14 79 cb 6a d0 99 37 a3 a9
bf 27 86 c4 26 1e 74 f5 11 91 a8 6d 37 44 47 80
de 35 1b 13 1b af 7a da ed 57 53 e4 6a e5 06 e2
18 fc 38 63 ca 0d 90 51 0a e4 9e f3 6f de ec d2
aa 48 68 93 bc 36 50 9b 1a 71 37 c9 07 22 10 19
11 30 ec ed ff 5b a7 18 65 d3 86 9e db de bd c6
64 f7 88 32 bb 79 c9 fa 21 72 75 fe 61 ad 6b e0
44 50 b3 5f 2d 44 d7 5d ac 09 92 d7 3a c9 68 f3
ea 15 d8 9e 3b d7 58 f9 8d 0f 8d d6 17 91 99 7d
```

```
37 60 af 82 a2 af 02 87 d5 64 1c 1d 3f 6a 4a 57
e4 8a 40 4d 72 f4 11 df 74 a8 40 09 b8 1a 65 6e
ad 66 ef 42 30 5f 9d 4d 6f 2c b8 c4 31 6a 64 e8
a3 72 dc 64 f1 66 b4 2b 57 31 a3 24 6b 0f 22 84
```

(b) State weather this is a CA or end-user certificate, and why.
It's a CA because can use extensions to issue a certificate

(c) Indicate whether the certificate is valid or not, and why.

6. **Problem 23.5** Now access the "Trust Store" (list of certificates) used by your Web browser, This is usually access via its Preference settings. Access the list of Certificate Authority certificates used by the browser. Pick one, examine the details of its X.509 certificate, and answer the same questions as for Problem 23.3.

(a) Identify the key element in this certificate, including the owner's name and public key, its validity dates, the name of the CA that signed it, and the type and value of signature.

The page I am checking is : *https://www.yahoo.com/* and the CA selected is Baltimore CyberTrust Root

-Owner's name : issued by (CN) : Baltimore CyberTrust Root
-Public Key:

```
Modulus (2048 bits):
a3 04 bb 22 ab 98 3d 57 e8 26 72 9a b5 79 d4 29
e2 e1 e8 95 80 b1 b0 e3 5b 8e 2b 29 9a 64 df a1
5d ed b0 09 05 6d db 28 2e ce 62 a2 62 fe b4 88
da 12 eb 38 eb 21 9d c0 41 2b 01 52 7b 88 77 d3
1c 8f c7 ba b9 88 b5 6a 09 e7 73 e8 11 40 a7 d1
cc ca 62 8d 2d e5 8f 0b a6 50 d2 a8 50 c3 28 ea
f5 ab 25 87 8a 9a 96 1c a9 67 b8 3f 0c d5 f7 f9
52 13 2f c2 1b d5 70 70 f0 8f c0 12 ca 06 cb 9a
e1 d9 ca 33 7a 77 d6 f8 ec b9 f1 68 44 42 48 13
d2 c0 c2 a4 ae 5e 60 fe b6 a6 05 fc b4 dd 07 59
02 d4 59 18 98 63 f5 a5 63 e0 90 0c 7d 5d b2 06
7a f3 85 ea eb d4 03 ae 5e 84 3e 5f ff 15 ed 69
bc f9 39 36 72 75 cf 77 52 4d f3 c9 90 2c b9 3d
```

```
e5 c9 23 53 3f 1f 24 98 21 5c 07 99 29 bd c6 3a
ec e7 6e 86 3a 6b 97 74 63 33 bd 68 18 31 f0 78
8d 76 bf fc 9e 8e 5d 2a 86 a7 4d 90 dc 27 1a 39

Exponent (24 bits):
65537
```

-Validity dates:

```
NOT BEFORE
May 12, 2000, 12:46:00 PM GMT-6
(May 12, 2000, 6:46:00 PM GMT)
NOT AFTER
May 12, 2025, 5:59:00 PM GMT-6
(May 12, 2025, 11:59:00 PM GMT)
```

-Type signature : PKCS #1 SHA-1 With RSA Encryption -Value of the signature:

```
Size: 256 Bytes / 2048 Bits
85 0c 5d 8e e4 6f 51 68 42 05 a0 dd bb 4f 27 25
84 03 bd f7 64 fd 2d d7 30 e3 a4 10 17 eb da 29
29 b6 79 3f 76 f6 19 13 23 b8 10 0a f9 58 a4 d4
61 70 bd 04 61 6a 12 8a 17 d5 0a bd c5 bc 30 7c
d6 e9 0c 25 8d 86 40 4f ec cc a3 7e 38 c6 37 11
4f ed dd 68 31 8e 4c d2 b3 01 74 ee be 75 5e 07
48 1a 7f 70 ff 16 5c 84 c0 79 85 b8 05 fd 7f be
65 11 a3 0f c0 02 b4 f8 52 37 39 04 d5 a9 31 7a
18 bf a0 2a f4 12 99 f7 a3 45 82 e3 3c 5e f5 9d
9e b5 c8 9e 7c 2e c8 a4 9e 4e 08 14 4b 6d fd 70
6d 6b 1a 63 bd 64 e6 1f b7 ce f0 f2 9f 2e bb 1b
b7 f2 50 88 73 92 c2 e2 e3 16 8d 9a 32 02 ab 8e
18 dd e9 10 11 ee 7e 35 ab 90 af 3e 30 94 7a d0
33 3d a7 65 0f f5 fc 8e 9e 62 cf 47 44 2c 01 5d
bb 1d b5 32 d2 47 d2 38 2e d0 fe 81 dc 32 6a 1e
b5 ee 3c d5 fc e7 81 1d 19 c3 24 42 ea 63 39 a9
```

(b) State weather this is a CA or end-user certificate, and why.
It is an end-user certificate

(c) Indicate whether the certificate is valid or not, and why.