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

   DomainKeys Identified Mail (DKIM) is a specification for cryptographically signing e-mail messages, permitting a signing domain to claim responsibility for a message in the mail stream. Message recipients (and agents acting on their behalf) can verify the signature by querying the signer's domain direclty to retrieve the appropriate public key and thereby can confirm that the message was attested to by a party in possession of the private key for the signing domain.

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

   Record Protocol
   Change Cipher Spec Protocol
   Alert Protocol
   Handshake Protocol

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 the server to the client.

   Mutual authentication with certificates.

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

   Encrypted Passwords.

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

   SLL doesnt use IP addresses to authenticate server client.

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

The attacker does not konw the encryption key so when they send a message, the Alert protocol of the other party should detect this.

(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.

SLL is vulernable to this and does not directly detect / have a solution on its own to this security threat.

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

Public Key infrastructure is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates ased on asymmetric cryptography. The principle of its developement is to enable sercure, convenient, and efficient acquisition of public keys.

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 elements in the 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 owner's Common Name is: *.reddit.com

The public key is: CF E9 9A 54 A3 A4 1A E2 29 2D 45 81 72 B3

A8 8B 4C CE 2B BB A2 D7 3D 9E 69 6C F3 32 D1 68 AC 03 1D 1A 70 55 F8 86 5A 42 DC 90 E7 EF 86 7E FD 53 6C EA C0 38 A5 27 B4 CA 7A 96 E3 5E 0A 5A EE 65 20 B3 96 D7 E4 3A 99 3D 78 72 7D 5D 61 14 3E BA 45 14 22 DB 05 5B BD D6 C9 74 11 8B DD 5A CA 65 52 51 20 8A 53 B5 CD D0 D7 AF 45 22 C9 4D 29 B7 3D 78 6A B5 9F 03 BF 44 48 48 E5 DC 43 08 70 28 1F 02 E9 A7 E5 DF 6E 39 01 24 6C E5 80 A2 01 74 11 DE 77 AE CA 15 55 0A 16 F8 75 45 56 A7 54 95 0D 1B A2 24 01 75 E7 3D 94 A2 83 07 C0 DB 00 47 DD 08 2E 39 CD 58 C6 CC 0F 07 87 0E 1F 9B 1D 65 E0 09 43 A8 FD AD 2C 4D AA 36 6D 86 85 78 DC B6 B9 9E C5 58 C5 1B 6B 78 9F 28 A1 5E 59 5F F7 6C 2F B0 41 06 45 9F 17 F6 9C 55 25 37 7F B5 FB 5E 21 73 DB 7B EB B9 0C 81 35 02 93 D8 72 97 C2 07

The certificate expires Wednesday, September 2, 2020 at 6:00:00 AM Mountain Daylight Time and was issued Thursday, August 16, 2018 at 6:00:00 PM Mountain Daylight Time.

The CA that signed was DigiCert SHA2 Secure Server CA

The the type of signature was RSA Encryption with a value of BD 3A C1 39 6E 33 8E BF 1D 15 A3 07 C5 69 CB A3 17 15 35 91 80 E2 91 7F 74 04 7D 74 E9 73 FB 61 02 04 C4 69 A3 67 D9 A8 E4 08 BA 52 03 07 51 22 18 3B 8B 0D 15 C6 58 62 4E 8D ED B7 7B E4 AD 22 F1 4F 17 D8 07 28 21 F8 82 E9 56 1D AF 0E 1E DA B3 4C 5D 6D 74 0B 32 21 D4 2A 3F B7 AE 50 67 D2 AD B9 65 D6 C3 14 09 60 9B 88 70 BB 10 4F B3 06 EF E2 B8 F1 92 4D 4A C0 7D 56 EB B3 A8 D7 9B C5 26 53 CA 11 01 32 C3 74 DF 4F CE CB 50 A2 52 CA BE 9D E9 19 7E 26 DC 00 7C 5C E4 BE 89 1B CB 05 9D 6E 91 E2 E4 EE 1A 0D 6A 66 CB EB F7 92 99 8B 99 69 A1 43 84 D9 49 1D 38 AD 93 1B B9 ED 9F B2 4B 63 80 B8 62 FD 95 18 AA E7 C4 68 AA 6A 37 0A C2 47 61 D1 AE B1 0B 51 17 63 D2 4E 6C D7 33 81 AB 82 3B 9E BE 7F CF B1 71 1A 19 A5 30 04 FC 9B 72 C3 05 65 FB E6 EB 51 EA 0B 2D 47 42 56 D8 71.

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

This is a end-user certificate since this verifies that www.reddit.com is a legit site and is what it says it is. Otherwise the certificate would

also say its usage would be a CA with the ability to sign for other certificates in the chain.

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

It is valid since the decrypted signature matches what was signed with the private key (for the CA). And the validity dates are still met.

(d) State whether there are any other obvious problems with the algorithms used in this certificate.

None

6. **Problem 23.5** Now access the "Trust Store" (list of certificates) used by your Web browser. This is usually accessed 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 elements in the 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 owner's Common Name is: Apple Root Certificate Authority

The public key is: E4 91 A9 09 1F 91 DB 1E 47 50 EB 05 ED 5E 79 84 2D EB 36 A2 57 4C 55 EC 8B 19 89 DE F9 4B 6C F5 07 AB 22 30 02 E8 18 3E F8 50 09 D3 7F 41 A8 98 F9 D1 CA 66 9C 24 6B 11 D0 A3 BB E4 1B 2A C3 1F 95 9E 7A 0C A4 47 8B 5B D4 16 37 33 CB C4 0F 4D CE 14 69 D1 C9 19 72 F5 5D 0E D5 7F 5F 9B F2 25 03 BA 55 8F 4D 5D 0D F1 64 35 23 15 4B 15 59 1D B3 94 F7 F6 9C 9E CF 50 BA C1 58 50 67 8F 08 B4 20 F7 CB AC 2C 20 6F 70 B6 3F 01 30 8C B7 43 CF 0F 9D 3D F3 2B 49 28 1A C8 FE CE B5 B9 0E D9 5E 1C D6 CB 3D B5 3A AD F4 0F 0E 00 92 0B B1 21 16 2E 74 D5 3C 0D DB 62 16 AB A3 71 92 47 53 55 C1 AF 2F 41 B3 F8 FB E3 70 CD E6 A3 4C 45 7E 1F 4C 6B 50 96 41 89 C4 74 62 0B 10 83 41 87 33

8A 81 B1 30 58 EC 5A 04 32 8C 68 B3 8F 1D DE 65 73 FF 67 5E 65 BC 49 D8 76 9F 33 14 65 A1 77 94 C9 2D

The certificate was issued Wednesday, February 9, 2005 at 5:18:14 PM Mountain Standard Time and expires Sunday, February 9, 2025 at 5:18:14 PM Mountain Standard Time.

The CA that signed was Apple Root Certificate Authority

The the type of signature was RSA Encryption with a value of 9D DA 2D 28 58 2F 7D 76 04 B9 04 D3 3E CE B7 66 63 4E 8F 2F D4 FE 4B AD 72 BD A3 39 C6 52 4D 05 98 52 F5 89 51 01 24 79 BE 1A 32 F7 E5 44 8B 4B 44 07 39 82 D6 5A CA B4 20 5E D9 AE 15 5D 1D 8C 1D 32 BF 38 31 62 48 5D C7 E1 90 B1 F8 24 40 F8 5F 58 9B 51 5D 57 9D C1 E5 FF 3C CC 72 21 6E C4 E9 E9 A1 77 D7 2C 17 26 C3 3F EB 9A E8 0B 03 BA E9 B3 4A 72 EB 33 09 5B AD E6 62 31 6A E8 AF 2F D5 AF 1E 57 76 8F 7F 37 2D 2E 02 5C DD 63 C9 F2 71 B8 26 40 DF 15 8D 75 44 3F 79 BD E6 1D 99 E1 43 2C 3E AD 6F BE B9 A4 FE 0E 35 19 51 63 B1 C3 DE B5 92 3E 51 78 01 73 8A A4 23 CA A4 88 F1 1E 5C 1F 41 16 2D 7E 95 0A AA E9 89 41 98 1B 1A DD CB 20 BF 47 5E 0C 26 C5 55 35 4D C6 30 8B 99 67 14 C7 09 1F BA 47 C7 DA 01 09 87 24 42 95 BD 13 60 19 0A EF EA 7F 0E 6E CD C1 44 43 3A 4A D5 E3

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

This is a CA since its usage can be to sign other certificates.

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

It is valid since the dates are valid and the decrypted signature matched what was signed with the private key.

(d) State whether there are any other obvious problems with the algorithms used in this certificate.

None.