PROBLEMS 765

- P18. Suppose Alice wants to send an e-mail to Bob. Bob has a public-private key pair (K_B^+, K_B^-) , and Alice has Bob's certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function $H(\cdot)$.
 - a. In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message? If so, show how with a block diagram for Alice and Bob.
 - b. Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? If so, show how with a block diagram for Alice and Bob.
- P19. Consider the Wireshark output below for a portion of an SSL session.
 - a. Is Wireshark packet 112 sent by the client or server?
 - b. What is the server's IP address and port number?
 - c. Assuming no loss and no retransmissions, what will be the sequence number of the next TCP segment sent by the client?
 - d. How many SSL records does Wireshark packet 112 contain?

ම ssl_trace - Ethereal	X
Elle Edit View Go Capture Analyze Statistics Help	
Efter: ssl 💌 Expression Qear Apply	
No Time Source Destination Yotocol Info 106 21.805705 128.238.38.162 216.75.194.220 SSLV2 Client Hello, 108 21.830201 216.75.194.220 SSLV3 Server Hello, 1112 21.835202 216.75.194.220 SSLV3 Server Hello, 1112 21.876168 128.238.38.162 SSLV3 Certificate, server Hello Done 112 21.876168 128.238.38.162 SSLV3 Certificate, server Hello, Done 113 21.945667 216.75.194.220 SSLV3 Change Cipher Spec, Encrypted Handshake M 113 21.945667 216.75.194.220 SSLV3 Change Cipher Spec, Encrypted Handshake M 114 21.944189 128.238.38.162 S1LV3 Application Data 120 216.75.194.220 216.75.194.220 SSLV3 Change Cipher Spec, Encrypted Handshake Message 114 21.944189 128.238.38.162 216.75.194.220 SSLV3 Application Data 120 210.272 210.272 210.272 210.272 210.272	
 B Frame 112 (258 bytes on wire, 258 bytes captured) B Ethernet II, Src: Ibm_10:60:99 (00:09:6b:10:60:99), DST: All-HSRP-routers_00 (00:00:0c:07:ac:00) B Internet Protocol, Src: 128.238.38.162 (128.238.38.162), DST: 216.75.194.220 (216.75.194.220) B Transmission Control Protocol, Src Port: 2271 (2271), DST Port: https (443), Seq: 79, Ack: 2785, Len: 204 B Escure Socket Layer B SSLV3 Record Layer: Handshake Protocol: Client Key Exchange Content Type: Handshake (22) Version: SSL 3.0 (0x0300) Length: 132 	
 ■ Handshake Protocol: client Key Exchange Handshake Type: Client Key Exchange (16) Length: 128 ■ SSLV3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec Content Type: Change Cipher Spec (20) Version: SSL 3.0 (0x0300) Length: 1 Change Cipher Spec Message ■ SSLV3 Record Layer: Handshake Protocol: Encrypted Handshake Message Content Type: Handshake (22) Version: SSL 3.0 (0x0300) Length: 56 Handshake Protocol: Encrypted Handshake Message 	
0030 fd if c2 d9 00 00 16 03 00 00 84 10 00 00 80 bc IIGx.G 0040 49 49 47 29 aa 25 90 47 7F d0 39 05 6a c7 89 56 IIGx.G 0050 c7 NF 12 af 08 b4 7c 60 9e 61 10 4b 0f P6 83 ec IIGx.G 0050 c7 NF 12 af 08 b4 7c 60 9e 61 10 4b 0f P6 83 ec IIGx.G 0050 c7 NF 12 af 08 b4 7c 60 9e 61 10 4b 0f P6 83 ec IIGx.G 0070 9b 45 11 c7 3f bd ee c0 92 c4 27 50 ff fd d1 fb 95 A 0080 42 3d 34 b7 71 ee c0 ff c3 ce b2 ed 60 90 6c d7 B=q 0080 44 29 f1 c6 ba 64 58 79 46 9e 3e c4 fd d7 9b 7a D)dxy F.>2 0040 04 29 12 c6 ba 64 58 79 46 9e 3e c4 fd d7 9b 7a D)dxy F.>2 0040 04 14 81 54 f5 04 be c2 df 0c d0 5b c4 44 88 e8 c4H.OPK	<