Wireshark. ... cop 1. Select the first Client Hello packet in the trace file. a) How many cipher suites are supported by this email client? Cipher Suites (23 Suites) 2. Select the first Server Hello packet in the trace file. a) Which cipher suite did the remote email server choose for the exchange? 3. Select the first Certificate packet. Expand the Secure Sockets Layer section in the center of the Wireshark screen. Expand the Diffie-Hellman Server Params section within the Secure Sockets Layer section. a) What is the length of the Public Key? b) What Signature Hash Algorithm is used? c) What Signature Hash Algorithm Signature is used? d) What is the length of the signature? 4. Select the first Application Data packet. Find the Transmission Control Protocol section. a) What is the SRC (source) port for this packet? b) Which protocol is used by this port? 5. Decrypting encrypted email with Wireshark is possible if a number of requirements are met. Wireshark can only decrypt SSL/TLS packet data if RSA keys are used to encrypt the data. If a Diffie-Hellman Ephemeral (DHE) or RSA ephemeral cipher suite is used, the RSA keys are only used to secure the DH or RSA exchange, not to encrypt the data. a) If DHE or RSA ephemeral cipher suite is used, even if you've got the correct RSA private key, you won't be able to decrypt the data with Wireshark. b) When checking the Server Hello packet, if the cipher suite specified begins TLS\_DHE or SSL\_DHE, you will not be able to decrypt the data. c) If the server sends a ServerKeyExchange message, you won't be able to decrypt the data. Given these parameters, would you be able to decipher the e-mail message captured in the IT Encrypted Email.pcapng trace file? Why or why not?