Assignment #3

1) Suppose a link is shared by Bob with four other users. Bob uses parallel instances of non-persistent HTTP, and the other four users use non-persistent HTTP without parallel downloads.
   a) Do Bob's parallel connections help him get Web pages more quickly? Why or why not?
   b) If all five users open five parallel instances of non-persistent HTTP, then would Bob's parallel connections still be beneficial? Why or why not?

2) A binary file is 4560 bytes long. How long will it be if encoded using base64 encoding, with a CR+LF pair inserted after every 110 bytes sent and at the end?

3) In the authentication protocol (ap4.0), we saw the use of once-in-a-lifetime value (R) and then checking the returned value K_{A-B} (R), in which Bob can make sure that Alice is both who she says she is (since she knows the secret key needed to encrypt R) and live (since she has encrypted the nonce, R, that Bob just created). Now suppose that while Alice is authenticating herself to Bob, Bob must authenticate himself to Alice. Give a scenario by which Trudy, pretending to be Alice, can now authenticate herself to Bob as Alice.

4) Suppose Alice wants to send an email to Bob. Bob has 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 share the same has function H(.).
   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.

5) How are different RTP streams in different sessions identified by a receiver? How are different streams from within the same session identified?

6) What is the role of a SIP registrar? How is the role of an SIP registrar same as that of an authoritative name server in DNS?

7) In mobile IP, what effect will mobility have on end-to-end delays of datagrams between the source and destination?

8) Consider two mobile nodes in a foreign network having a foreign agent. Is it possible for the two mobile nodes to use the same care-of-address in mobile IP?

9) Consider the two ways in which communication occurs between a managing entity and a managed device: request-response mode and trapping. What are the pros and cons of these approaches, in terms of (1) overhead, (2) notification time

when exceptional events occur, and (3) robustness with respect to lost messages between the managing entity and the device?

10) Using RSA, choose p = 3 and q = 11, and encode the word “soup”. Apply the decryption algorithm to the encrypted version to recover the original plaintext.