Computer Networking Protocols
CSI4118

University of Ottawa
Fall 2017

Assignment #3
Matthew Langlois - 7731813
Dec. 4

Question 1

a) Yes Bob will get more bandwidth than the other users. This is because he as more connections at one given time.

b) Even if the other users switch to parallel connections Bob must continue using parallel connections otherwise he will get less bandwidth.

Question 2

Base64 Encode the data:
$\lceil 4560/3 \rceil \cdot 4 = 6080$

After the Base64 encoding the CR+LFs need to be inserted every 110 bytes:
$\lceil 6080/110 \rceil = 56$

Insert the CR and LF bytes into:
$56 \cdot 2 + 6080 = 6192$

$\therefore$ the total size of the encoded binary file with the CR+LF bytes is 6192 bytes.

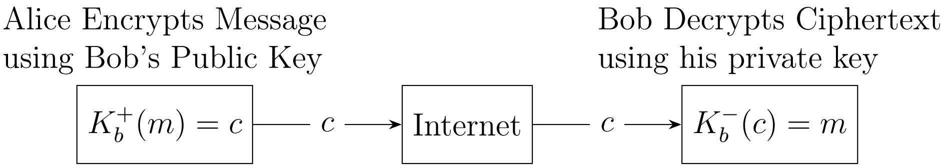
Question 3

Since Alice and Bob both know each other's keys Trudy needs to intercept the communication from Bob during the initialization. To do this Trudy waits for Bob to start the communication and send her the noonce value R. Trudy then replies to bob using the same noonce value R, which Bob encrypts using $K_{AB}(R)$ and sends to Trudy. Trudy now has the encrypted value of R so she can simply reply to Bob using $K_{AB}(R)$ since she knows what the encrypted value is. Bob accepts this, believing Trudy is Alice.

Question 4

1. No it is not possible for bob to verify that Alice has generated the message. To do so Alice would require a unique private/public key pair for which she could use to sign a message.

2. Yes it is possible to create a scheme in which there is confidentiality when Alice sends a message to Bob. She would need to use the certificate which Bob has provided her to encrypt the data with his public key K_B^+.


Alice Encrypts Message using Bob's Public Key
Bob Decrypts Ciphertext using his private key
$K_b^+(m) = c$
c
Internet
c
$K_b^-(c) = m$

Question 5

1. RTP streams in different session are identified by the multicast address to which the stream is directed.

2. RTP streams in the same session are identified by the SSRC, which is a unique number set when the stream is initialized. The SSRC number is essentially the port which the stream knows to use.

Question 6

1. A SIP registrar is a SIP endpoint which accepts REGISTER requests for clients. Once a client is registered it provides a way to lookup the client within the network returning the IP and SIP URI for the client.

2. The SIP registrar is similar to that of a DNS server since they both offer mechanisms to resolve information. For example the DNS server resolves the IP of the website while the SIP registrar resolves the IP of the client.

Question 7

In Mobile IP (MIP) when an agent connects to a foreign network it must first communicate with the home network. Thus when an agent connects the data must travel from the foreign network back to the home network before being redirected out. This end-to-end communication will certainly introduce some delay.

Question 8

Yes it is possible for two foreign devices to have the same care of address of the same foreign agent connecting to the same network to have the same care of addresses. This happens because they need to identify what their home agent is to create the tunnel. Their proper individual addresses will be resolved when the tunnel is created to the home network.

Question 9

1. Request-Response Mode:

   Request response mode will generally have more overhead since each piece of information received by the manager requires two messages: the poll and the response. If the manager really only wants to be notified when a condition occurs, polling has more overhead, since many of the polling messages may indicate that the waited-for condition has not yet occurred. If a message is lost in request-response it would be obvious since the response is never received thus requiring another poll to be conducted.

2. Trapping Mode:

   Trapping only required the single message to the sender thus having less overhead. Furthermore Trapping will immediately notify the manager when an event occurs thus having much less overhead. The only downside is that if a trap message is lost, the managed device will not send another copy.

Question 10

Pre-Computation required for encryption and decryption:

$$n = p \cdot q$$
$$n = 3 \cdot 11$$
$$n = 33$$

$$\phi = (p - 1) \cdot (q - 1)$$
$$\phi = (3 - 1) \cdot (11 - 1)$$
$$\phi = 20$$

Public key exponent:
$e = 17$ since the $gcd(17, \phi) = 1$.

Private key exponent:
$d = 13$ since the modular inverse of $13 = e^{-1} \mod \phi$

a) Encryption of the word "soup"

Text (val)	Cipher Text ($m^e \mod n = c$)
S (19)	$19^17 \mod 33 = 13$
O (15)	$15^17 \mod 33 = 27$
U (21)	$21^17 \mod 33 = 21$
P (16)	$16^17 \mod 33 = 25$

b) Decryption of the word "soup"

Cipher Text	Plain Text ($c^d \mod n = m$)
13	$13^13 \mod 33 = 19$
27	$27^13 \mod 33 = 15$
21	$21^13 \mod 33 = 21$
25	$25^13 \mod 33 = 16$

$\therefore$ The encryption and decryption of the word SOUP works correctly using RSA.