True/False:
1. Public key cryptography requires participants to distribute a secret keys
False. With public key cryptography a participant does not need to distribute her private key; it needs to distribute only the public key (which is not a secret).

Short Answer:
1. What are three common ways of compromising passwords?
Answer:
a). Password guessing.
b). Dictionary Attack
c). Dumpster Diving

2. What are four security requirements, explain them:
Answer:
Authentication: Ensures that a user is who is claiming to be.
Data integrity: Ensure that data is not changed from source to destination or after being written on a storage device.
Confidentiality: Ensures that data is read only by authorized users.
Non-repudiation: a). Sender/client cannot later claim didn't send/write data; b). Receiver/server can't claim didn't receive/write data.

3. What do DES, and AES stand for? Are they symmetric key encryption?
Answer:
DES: Data Encryption Standard
AES: Advanced Encryption Standard
Yes.

4. Does the following mutual authentication work? Why? If not, please provide a working version.
Alice's public key Pub_A, private key Pri_A.
Bob's public key Pub_B, private key Pri_B.
Alice and Bob know all each other public keys.
Alice: Send E(E(N_x, Pri_A), Pub_B)
Bob: Receive msg from Alice. Send back E(E(N_x, Pri_B), Pub_A)
Alice: Receive msg from Bob. Start to send real message E(E(N_x, Pri_A) + msg, Pub_B)
N_x is a random message generated by Alice.

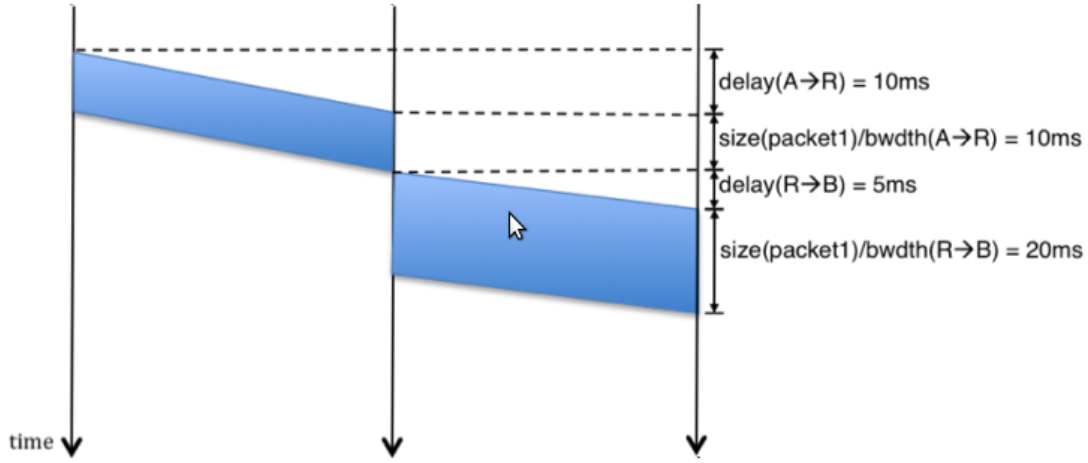
Answer:
No. Bob can not be sure that he is talking with Alice.
Alice: Send E(E(N_x, Pri_A), Pub_B)
Bob: Receive msg from Alice. Send back E(E(N_x + N_y, Pri_B), Pub_A)
Alice: Receive msg from Bob. Start to send real message E(E(N_x+N_y, Pri_A) + msg, Pub_B)
N_x is a random message generated by Alice.
N_y is a random message generated by Bob.

Long Answer:

1. Hosts A and B are connected to each other via router R. R is a store-and-forward router. The bandwidth from A to R is 2 Mbps, and the bandwidth from R to B is 1 Mbps. The latency of link A-R is 10ms and the latency if link R-B is 5ms. Assume A sends a packet of 2500 bytes to R. Unless otherwise specified, there are no other packets in the network, and the arrival time of the packet is the time the receiver gets the last bit of the packet.

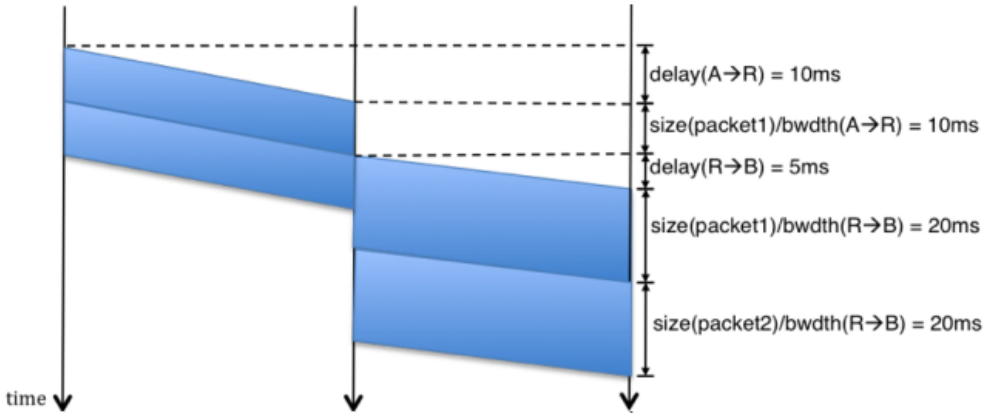
a). Assuming A starts sending the packet at time t=0 (i.e., the first bit is sent at time t=0), what is the arrival time of the packet at B?

45 ms.



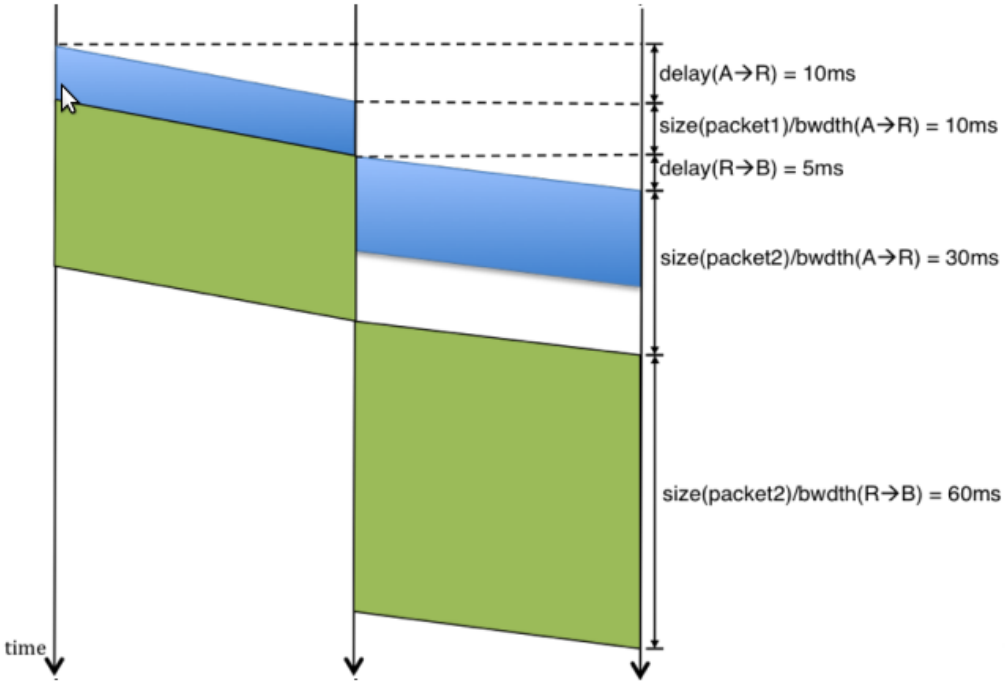
b). Assume A sends a second packet of same size right after the first one. What is the arrival time of the 2nd packet at B?

65 ms.



c). Repeat (b) if the size of the 2nd packet is 7500 bytes (i.e., 60 Kbits).

115 ms.



d). Repeat (b) if the size of the 2nd packet is x bytes, i.e., give a formula for the arrival time of 2nd packet as a function of 2nd packet size x. (This is a generalization of (b).)

Let x = size(packet2). Then, by comparing figures at points (b) and (c) you can generalize to
arrival_time(packet2) = delay(A,R) + size(packet1)/bwdth(A,R) + delay(R,B) + x/bwdth(R,B) + max(x/bwdth(A, R), size(packet1)/bwdth(R,B))
or numerically
arrival_time(packet2) = 25ms + x/1Mbps + max(x/2Mbps, 20ms)