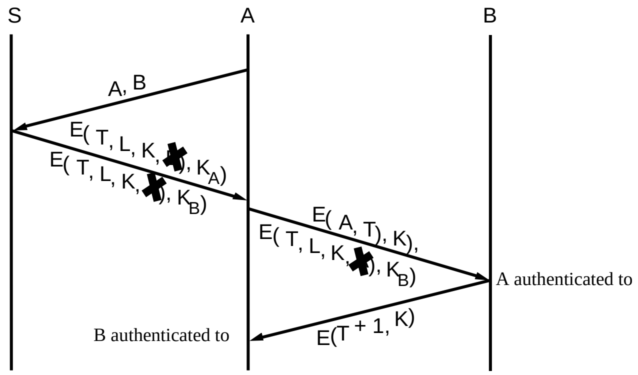
CS 640 Introduction to Computer Networks

Quiz 7

Write your name on the exam. Write something for every question. Students who do not write something for everything lose out over students who write down wild guesses. You will get some points if you attempt a solution but nothing for a blank sheet of paper. Write something down, even wild guesses. Problems take long to read but can be answered concisely.

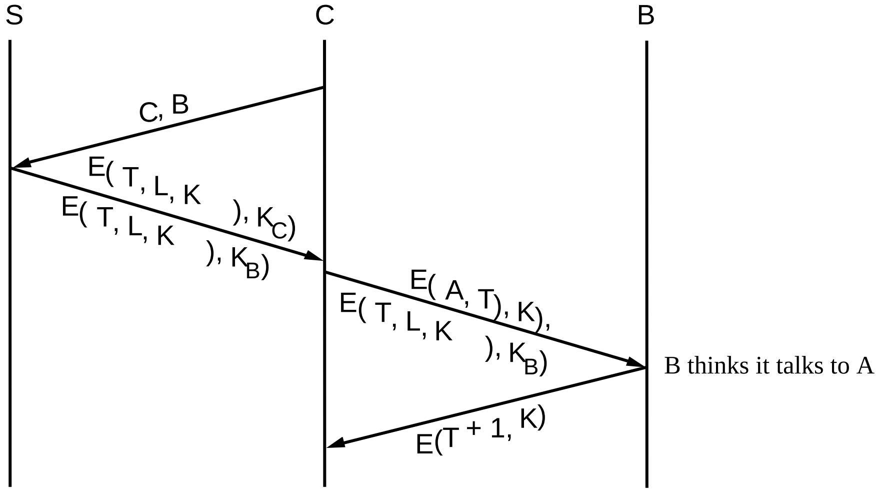
Question	Maximum	Score
1	10	
2	10	
Total	20	

Question 1 – Kerberos



Hugh Hopeful is a junior software engineer at Megasoft Corporation that implements a popular implementation of the Kerberos. He came up with an idea to make the protocol more efficient that reduces message sizes, and the CPU load on the authentication server and the clients by removing some fields from the messages exchanged as shown in the figure. Explain what type of attack is made possible by the modification proposed by Hugh.

Imagine a malicious user C that has the power to intercept all IP packets sent to A and fake IP packets that seem to come from A using IP spoofing. C can fool B thinking it is talking to A as shown by the example below.



Question 2 – miscellanea

a) RSA needs to raise numbers to large powers (modulo some large number). Assuming that you are given a primitive, ‘*’, that performs the multiplication of numbers in the required base, write a procedure that raises x to the power 100 using the smallest possible number of invocations of ‘*’. (Note: your procedure need not work for a general exponent.)

It is possible to compute x100 using 8 invocations of the (expensive) multiplication operation.

```
x2=x*x
x4=x2*x2
x8=x4*x4
x16=x8*x8
x32=x16*x16
x64=x32*x32
x96=x64*x32
result=x96*x4
```

b) Gnutella-like (unstructured) peer to peer protocols perform “overlay maintenance”: each node removes from its neighbor list nodes that are no longer responsive and adds new ones. Hugh Hopeful proposes a performance improvement through aggressive overlay maintenance: nodes should discard every 5 seconds their neighbor with the longest roundtrip time and they should pick one of the neighbors of their existing neighbors as a new neighbor instead. This is meant to facilitate the creation of “short links” in the overlay and thus improve query response times. What problem can this modification lead to?

The problem with this approach is that it can lead to partitioning the overlay into many “islands” that are not connected. Say there are 100 nodes on our campus and each has two local neighbors and eight neighbors that are off campus. At each round of the overlay maintenance a node will drop an off-campus peer and with certain probability acquire a new on-campus peer that has better roundtrip time. With high probability, after a few dozens of rounds all nodes on campus will have only peers on campus and thus none of them will be connected (even indirectly) to the rest of the overlay network.