Missing Solutions and Corrections:

Problem 7

7a)

Can be both stolen and replaced with with another exam

7b)

Cannot be replaced, but can be stolen. Private key only authenticates, it does not encrypt the exam and so does not provide confidentiality.

7c)

Cannot be stolen, but can be replaced. Only Dave can decrypt the exam, but anyone could pretend to be Srini and send a different exam.

7d)

This works

7e)

This works

7f)

Diffie-Hellman was not covered. But in case you were curious,
http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

Part D

Question 9 is deadly tedious. Don't worry if you fall asleep halfway through.

9A)
(Dst,Final Label) = (B, 1)

9B)
Switch Tuples:
(S1, 4, 2), (S3, 4, 1), (S2, 3, 1)
(Dst,Final Label):
(B, 19)

9C)

Switch Tuples:
(S3, 2 , 1), (S3, 3, 2),
(Dst, Final Label):
(B, 15)

11)
There is a loop in the switch network, so that packet traverses it forever. This impedes valid traffic

Part H

15b) Correction: If B is sending data to C, C is not going to send an RTS, it will send a CTS. So the answer is D heard the CTS from C

Part J

18a) Just 10.0.0.32
18b) Answer is E. Note that A and D would work, but would also block hosts in Sparky's Network

19)

INTERNAL – Sparky's Addresses
EXTENAL – Addresses in the firewalled range.

SRC IP/MASK	Src Port	Dst IP/Mask	Dst Port	ACK set	Action
INTERNAL	ANY	EXTERNAL	80	EITHER	ALLOW
EXTERNAL	80	INTERNAL	ANY	YES	ALLOW

ACK set means that the ACK bit in the packet is set.
Note that in real TCP, the ACK bit is set on all packets except the initial SYN.

20)
Just spoof the source IP address on the packet. Using port 80 as your destination port may achieve some effect, but this won't help as much as you still won't be able to exploit the machines by connecting to them, as a packet with a SYN|ACK set will likely be dropped if its not the response to another SYN.