A-2 Why is it important to have a large volume of traffic in anonymous communication?
If you want to identify who is sending data and you know that only a few people are using that connection you have a large probability of a guess being correct, while if the connection is more populated the probability will drop.

Grade: 1.0
Motivation:
Good answer. The slides about anonymity provides the same information.

A-10 When using 2 mixes and an untraceable return address, show how the addressee prepares the return message to the original sender.

K1(R1, K2(R2, Ax))),Kx(R0, M)

The first part is the address for the original sender that gets decrypted by the mixes along the way to find Ax. The second part is the message that will be encrypted along the way.

Grade: 0.7
Motivation:
The answer could have been elaborated a bit more. What is R1 and R2 for example? Otherwise good and correct.

A-13 It is straightforward to generalize the N − 1 attack to an N − k attack, 0 < k < N. Describe the N −k attack.

N-K is the number of senders the attacker controls, As this number increases the list of possible senders for a message will decrease and the attack has a higher chance of finding a link between unknown sender and receiver.

Grade: 1.0
Motivation:
I had the same question and your answer was much better. It was difficult to find information about the n-k attack except for the slides and lecture notes (which did not mention n-k but only n-1), so it is difficult to truly know if the answer is correct. However, the answer provided here sounds very reasonable.

A-14 Consider the long term intersection attack. Explain how the number of users and the sizes of each batch will affect the efficiency of the attack.

Assuming you can link different messages to one anonymous sender. Check what users could have sent a message at a time t and do this for multiple times until the sender is uniquely identifiable. E.g if at one anonymous sender sends a message at time T1 when only N={A,B,C,D} are sending and again at T2 for M= {D,E,F,G} you can link two messages to

sender D. As the set of users increases the number of checks the attacker has to do to find a unique link will increase rapidly, especially if the users are all active at similar times.

Grade: 1.0
Motivation:
Once again a very good and clear answer. Nice with an example as well. Goes well with the information provided on the lecture slides and notes about anonymity.

A-16 When negotiating a symmetric key with an onion router, what is the purpose of the H(K1) message sent from the router to Alice?

Alice can verify that the key exchange protocol was successful and that the message came from the router she sent the original message to as it is the only thing that can compute the hash.

Grade: 1.0
Motivation:
Correct answer that says the same as the lecture notes about anonymity (p. 11).

A-17 When Alice creates a Tor circuit, who selects the relays that are used?

The previous router in the path. Any one router (or user) is only aware of router that are one step away. So Alice creates a circuit, each node in the circuit is the mapped to a router by the router preceding it in the ciruit. The router then keeps track of that all traffic from Alice meant for a specific node is meant for a certain router in the next step.

Grade: 1.0
Motivation:
Very well-put answer. Pretty much the same answer can be found in this document: https://www.onion-router.net/Publications/locating-hidden-servers.pdf

A-20 Which different types of cells are available in Tor? Describe them briefly.

Control cells and Relay cells. Control cells are intended for and read by the router that receives it and is used mostly for the key exchange protocol. Relay cells are what is used to send the data and is only read by the last node in the circuit.

Grade: 1.0
Motivation:
Good answer that agrees with the information on page 27 from the slides about anonymity.

A-27 In a Tor node, give the algorithm for checking whether a cell should be sent to the next node in the chain or interpreted. Describe under what circumstances this will cause a premature interpretation

Two fields are relevant: recognized and the digest. Recognized is set to 0x0000 and digest is calculated by the sender. The fields are then encrypted using the keys of the routers along the path. Then for every router:
check recognized, if this is 0x0000 then we also have to check hash.If this is also correct the router assumes it is time for interpretation. As it is a 6byte hash value the probability for premature interpretation will be the same as for a 6 byte collision of hash values so 1 in 2^48.

If the fields do not match the expected value the router sends it along as it will be meant for another node.

Grade: 0.9
Motivation:
Overall a good answer that is correct according the the lecture notes about anonymity. The answer is however a bit rushed and sloppy.

Total score: 7.6