1 (a)

The 5 different type of network attacks are:

- Denial of Service is where the source is prevented from being able to communicate with the destination. This affects availability as potentially legitimate users are unable to access the services due to the attack. This does not affect integrity and confidentiality.
- Sniffing is where traffic is also copied and sent to another destination (the attacker). This affects confidentiality as an unauthorized party receives the information. This does not affect integrity or availability.
- Passive wiretapping is where traffic is diverted to the attacker and then the attacker sends it to the intended destination. Note that information is not modified here, hence integrity is maintained. This affects confidentiality as an unauthorized party receives the information. This does not affect availability.
- Tampering is where data is changed by the intermediate node, so data is different when it arrived to the destination than what is sent by the source. This affects integrity as data is modified in transit and it affects confidentiality as the unauthorized intermediary can see the data. This does not affect availability.
- Creation is when the source never sends any data to the destination, but some other adversarial source creates information and send it to the destination and puts the header information that looks like it came from the source. This affects integrity as data is added by a party that is not who the recipient thinks he is. This does not affect confidentiality and availability.

1 (b)

Tor provides anonymity to both users and websites.

For users, Tor anonymizes the origin of the traffic, hence providing privacy. This means that an attacker could not figure out who the sender of the packets is, assuming a single honest router in the circuit and that the exit and entry nodes are not colluding. This is because all onion routers on the path will not know who the sender and the recipient at the same time.

For websites, Tor provides anonymity through onion services. The server has a special onion URL obtained by running a TOR software on top of the web server where the IP address is not public. With this, the client does not know the IP address of the site and the site does not know who the client is, creating anonymity in both ways.

1 (c)

Tor cannot protect against a global adversary; hence the government can do the following to confirm that the onion service is inside the country:

- The government can try to communicate with the onion service, setting up a Tor circuit with them.
- The government can then observe the entry relay and the exit relay, where he can do end-to-end timing attacks by inducing timing signatures on the traffic. From observing both ends of the communication channel, he can confirm suspicion that the onion service is in the country if the volume and timing patterns of the traffic on the connection are distinct enough and with the ability that he can observe all network traffic in the country. In other words, he can correlate the volume and timing information on the two sides.

1 (d)

C paid for the meal. C saw 1, 1 and 1 and the result of 1 XOR 1 XOR 1 is 1. However, he announces 0, which is the negation of the result. This is only done if C has paid for the meal. The others report the XOR of their observed coin flips.

1 (e)

(i) The sender is anonymous to the recipient.

(ii) The most vulnerable part is the email server records which store the original email address mapped to the random email address. If this is removed, then anonymity of sender is lost.

(iii) The adversary can still mount an attack if he knows the buffer size.
Firstly, he will have to figure out the buffer size which can be done by trial and error through adding messages to the server and checking if he receives them immediately by setting the recipient to him. If he does, then he can slowly reduce the number of messages he sent that will allow him to immediately receive the messages to find out the buffer size.
Next, after knowing that the buffer size is 100, he can send 99 messages to the server, allowing him to then link the sender of the 100th message with its recipient. He can be sure that this is true by checking if he receives all 99 messages during that time period. This attack can be prevented by generating dummy messages.