Home Assignment 2

Filip hfelt, 9405313173

Complete the eight A-assignments below and solve them individually.

A-3 Give some examples of data which can be used in traffic analysis.

A-8 Briefly explain how using several Mixes versus an onion routing circuit differ both in terms of latency and in cryptographic primitives used for encrypting the traffic.

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

A-22 If you are using the Tor network for you own communication, would you be more or less safe if you would participate as a relay for others in the network as well?

A-23 Several users can use the same exit node in Tor, but different intermediate nodes. How can the exit node know where to send the response from the target?

A-24 Alice is negotiating keys during a chain construction in Tor. It is reasonable to assume that sending material to and back again from OR_1 takes some time. Can she use this time to prepare for negotiating with OR_2, OR_3, ...? How/why not?

A-25 Explain what the point of the recognized field in a Tor cell is and how it makes communication more efficient.

A-28 Show that the SSL/TLS handshake, when RSA is used, does not provide perfect forward secrecy.