Home Assignment 2

Niklas Jnsson, 9208273772

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

A-4 What is an anonymity set and why is it important that it is large? Given two anonymity sets AS_i and AS_j $(i \neq j)$, how would you interpret $AS_i \cap AS_j$?

A-11 When returning a message using an untraceable return address, why does each Mix encrypt the return message with the randomness R_i?

A-12 Regarding replay attacks on Mixes, two protections are suggested in the lecture notes. Which? Would you say that any of them is the better choice? Show how the two strategies can be combined and how this can make the protection more efficient.

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

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-26 A TCP handshake consists of the client and the server exchanging three messages: SYN, SYN-ACK and ACK. Explain why, in Tor, Alice can connect to a webserver and expect the TCP handshake with the server to be performed with low latency.

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