Home Assignment 2

Fredrik Magnusson, 9502163596

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

A-2 Why is it important to have a large volume of traffic in anonymous communication?

A-5 What is the purpose of the random value R_0 in a Mix?

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

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.

A-18 Why is onion routing called onion routing?

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