Home Assignment 2

Rasmus Olofzon, 9104192472

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

A-6 What is the purpose of the random values R_1 in a Mix?

A-7 When sending a mail through several Mixes, there are several public keys involved: $K_1, K_2, \ldots, K_n$ and K_a. What happens if one does not use K_a? Does this risk the anonymity of the sender?

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-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-15 In the disclosure attack on mixes, explain m, N, n and why a Mix is insecure if $m \leq \lfloor N/n \rfloor$.

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.