Home Assignment 2

Marcus Rodan, 9407087932

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

A-21 In August 2013, a large botnet used Tor Hidden Services to communicate with the Command and Control server. This resulted in an increase from 1 million to 6 million daily clients using Tor in just three weeks. As a result, the time required for downloading a 50 KiB file doubled from 1.5 seconds to 3.0 seconds. However, the amount of traffic on the network did not change very much? Why is that?

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.

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.