Assignment 1: Mixnets

Santiago Aragón

s.e.aragonramirez@student.utwente.nl

Owais Ahmed

o.ahmed@student.utwente.nl

University of Twente

Assignment 1

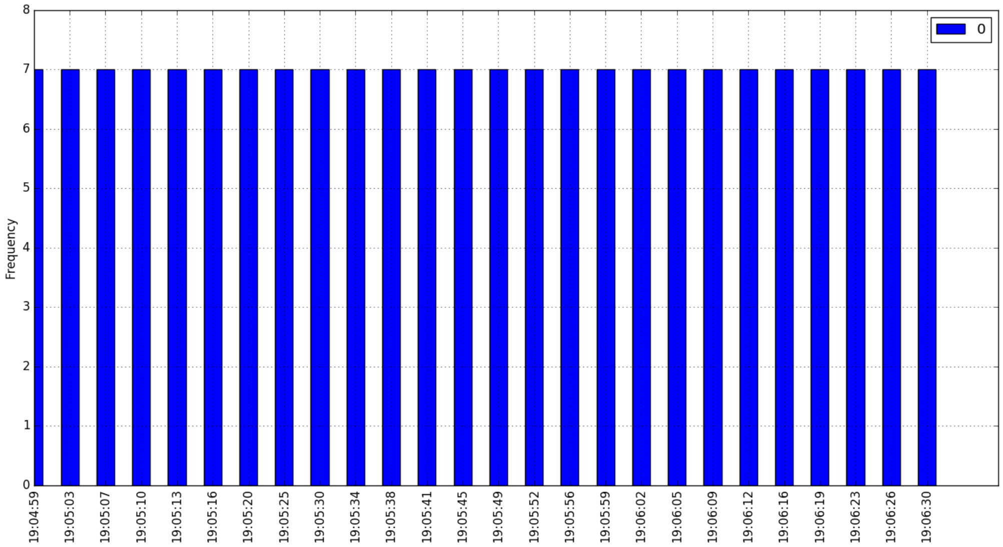
Part A: We developed an application mixnets.py [Appendix A] to send messages via the three mixs and the cache node that forwards the individual messages to the recipient.

Part B: We sent a message to TIM from the send message method as shown below in mixnets.py application [Appendix A].

```
send_message('TIM     ','s1750542  and  s1736574')
```

Part C:

Figure 1: Frequency of messages received against time in the same second.



We parsed the cache log to analyse the data fields of individual messages separately and performed frequency analysis as shown in Figure: 1 by counting the number of messages received in a particular second and plotted the results in a bar chart graph. We observed that mostly seven messages were received in the cache log in a particular second, however in certain instances, the average of messages received in two seconds was seven. We therefore concluded that :

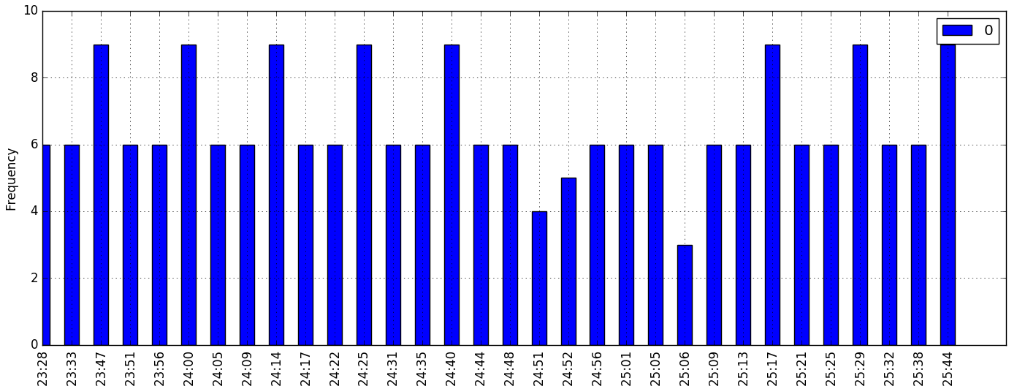
$$\text{Threshold of } n_A = n_B = n_C = 7$$

Assignment 2

Part A:

We sent individual messages one by one with a short time delay and observed the output via the cache log by parsing the message fields. We observed that the messages forwarded by MIX C to the CACHE NODE had a frequency of mostly 6 or 9. We learned that the sum of messages received in one or two seconds was always a factor of 3, as shown in Figure: 2. Therefore, we came to the conclusion that threshold of n_C is 3.

Figure 2: Frequency of messages received against time in the same second.



We kept a count of the messages entering the second mixnet via MIX A and the messages received in the cache log after reaching the threshold n_C. After the initial 8 messages passed through MIX A, only 6 messages were displayed in the cache log, that denotes that the threshold of MIX B and MIX A is ≤ 8. We sent more messages one by one until a second batch of 6 messages were received in the cache log. We noted that after sending 7 more messages, another batch of 6 messages was received in the cache log, this further helped us to analyse and conclude that the threshold of MIX B and MIX A is ≤ 7, because the minimum threshold of MIX A can be 1 and since there were 2 unreceived messages, therefore MIX B required 6 more messages to reach its threshold of 7 messages. We also kept a count of the messages sent into the mixnet that were not received by the cache log.

Keeping in mind the maximum threshold possible for MIX B to receive the next batch of 6 message in the cache log.
We observed that after ..
We learned...

Threshold of n_A is 2
Threshold of n_B is 7
Threshold of n_C is 3

Part B:

Assignment 3

Part A: ....

Part B: ....

Appendix A. Mixnet 1

Appendix B. Mixnet 2

Appendix C. Mixnet 3

References