Report No. 2

Information Security — October 9, 2020 — Group: 23

Antonin Thioux (s3791378) & Xiaoyu Guan (s3542807)

1. See code on Themis.
2. See code on Themis.
3.

Solution:
The birthday attack method produces a collision every $2^{L/2}$ hashing done where L is the length of the hashing output. Since we are using SHA256, $L = 256$. Which means we need to hash 2^{128} times before we get a collision.

Per year we have $7,800,000,000 \times 365$ attacks or about $8 \times 10^9 \times 512 \approx 2^3 \times 2^{30} \times 2^9$ being slightly generous. We find that it will take $2^{128-42} = 2^{86}$ or 10^{29} years to get a single collision.

4.

Solution:

- It is ok to use keep the URI available, since check sum is an algorithm that can detect the error during the transmission by computing the current data and then compare with the one that was stored if they are same then people can know the data is transmitting in a right way. And when download from this website three checksums are provided to check the if the file is changed or not.
- Can increase the quality of downloading and reduce the possibility that people download the broken file

  It is safer than old one since the check sum can detect the correction of file, and by doing that it can help people avoid the unnecessary virus that may caused by downloading the file online.
- If a user is using a link that they expect redirects to a different website a hacker could give them a link that redirects them to a different nefarious website. In this case the checksum does nothing to protect the user from downloading viruses because the hacker could provide it's own different check sums and the victim would be none the wiser.

5.

Solution: