Problem 1: Certificate Authorities.

How can web browsers protect users from each of the following:

(a) forged certificates where the forger signs with a key not certified by a CA?
(b) a compromised certificate authority?
(c) “re-signing” certificates installed by “privacy tools” like PrivDog or Komodia?

Problem 2: Tor Anonymity System.

Install and play around with the Tor browser:

https://www.torproject.org/projects/torbrowser.html.en

Read the self-written overview of Tor and the privacy properties it provides here:

https://www.torproject.org/about/overview.html.en

What privacy properties do the Tor browser provide? Against what type of adversaries? Specify any important caveats in Tor’s privacy guarantees.

Problem 3: Location Privacy.

Say NYC is able to collect data on the commute trajectories of NYC residents (i.e., paths followed by people from home to work and back). Consider the following technique for the anonymized publication of this dataset: filter the dataset to include only trajectories that occur at least 1,000 times.

Is this a good technique for publishing anonymized trajectories? Explain why or why not.
Problem 4: Privacy Policies.

The following question is from the in-class exercise on privacy policies. Part (a) can be submitted once per group. Part (b) should be completed and submitted individually.

(a) According the privacy policy reviewed answer the following questions based on your in-class pair number.

Pairs 1-7
- What information is collected through the website?
- How is the information collected?
- What information is collected about site visitors from third parties?
- Are these third parties specified? (e.g. data brokers)
- Does the site mention conditions under which information is collected from users? Collected from third parties? (i.e. transmission principles)
- How long is the information held? Is it ever deleted/destroyed?

Pairs 8-15
- Does the site disclose information to third parties?
- Does the site specify who the third parties are? (e.g., data brokers, government agencies, ad companies)
- What information is disclosed? Is this information specified?
- Does the site mention conditions under which information is disclosed?
- Can the privacy policy change? How are visitors notified of changes?
- What happens to personal data if the ownership of the site changes?

ALL Pairs (Optional)
- Can you identify any collection or disclosure actions taken by the site not clearly indicated in the privacy policy?

(b) What does your research suggest about the adequacy of the privacy policy approach to privacy protection online?