Ground Rules. You may choose to work with one other student if you wish. Only one submission is required per group, please ensure that both group members names are on the submitted copy. Work must be submitted in hard copy by the start of class.

1) I can prove that is the root!
   In all of the following systems assume a secure node ID assignment scheme is used that prevents an adversary from controlling where in the ID topology their nodes are.

   • A (2 pts) - One possible solution to the problem of capturing lookups on a DHT is to require nodes to present their full finger table along with the response. This allows the node doing the query to ensure that the response matches the state of the queried node’s finger table. Does this solution provide integrity for lookups? Why or why not?

   • B (4 pts) - An alternative approach is to require the neighbors of a node to conduct lookups for each other’s fingers, essentially building their own copy of each other’s finger table, which they then sign. These are then supplied by a lookup responding node, along with the response. The theory being that if there was at least one honest node it would return a finger table that had the correct response in it. Queries are rejected if they do not have the correct number of signed copies of the responder’s finger table, which match the responder’s table. Ignoring key management issues, does this system work as described? Can the adversary use this method to increase the fraction of queries that fail?

   • C (4 pts) - Assume a trusted central authority with global knowledge signs a list of which nodes are the root for what range of IDs. Nodes present these signatures when they respond that they are the root, the central authority gives nodes updated signatures as nodes churn in and out. Does this prevent an adversary from falsely claiming that they are the root of an ID? Why or why not?

2) Shuffle Issues.
   Pretend I have an email anonymizer based around a Chaum mix. In order to do timely delivery, the Chaum mix receives messages, waiting until the anonymity set size reaches a certain fixed value, and then flushes, sending the emails.

   • A (3 pts) - Pretend you are an adversary watching the network traffic of the mix. How can that adversary launch an attack which de-anonymizes a single user?

   • B (5 pts) - Build a solution which protects a user sending a single email.

   • C (2 pts) - Does this solution hold up if the user talks to the same recipient multiple times spread out over multiple rounds.
Paper Review If you are a graduate student, you are expected to also include with this exercise set a paper review of one of the papers posted as graduate reading over these two weeks. Your paper review is not supposed to be a full paper in and of itself, but rather a summary in your own words and some evidence that you’ve thought about what the paper is trying to do, if they achieve their goals, how useful their goals are, and how it could be improved. Your paper review should have the following components.

- A brief summary in your own words about what the paper was about. You should cover what problem the paper was trying to solve or highlight, how the authors proposed achieving their goals, and how the authors evaluated their success. This should NOT simply be a re-statement of the abstract hit with a thesaurus until un-recognizable, I do not mind if you did not fully understand the paper, if something was confusing, or you did not understand a concept, feel free to state that. (1-2 paragraphs)

- State one problem with the paper. Every paper has a problem, be it an evaluation that does not actually measure what it should, a poor assumption, an incorrect threat model, an obvious attack/defense, etc. Find one thing that you think is a flaw in the paper, and briefly explain why you think it is a flaw. (2-3 sentences)

- State two possible things that could be done for future work. This could be expanding the attack/defense to work under different assumptions or in different deployments. It could be a different set of evaluations. It could be an improvement to how the system is constructed. Try to be specific. (1-2 sentences each)

Choose a paper from the weeks listed as “Peer to Peer Systems” or “Censorship and Anonymity”.