Introduction to Modern Cryptography, Fall 2021
Homework 3 - due November 23

November 10, 2021

The goal of this exercise is to authenticate against the course roster using hash trees. We used the hash function SHA-256 to compute a hash tree over the names in the file "students.txt" containing 64 names. The tree's root encoded in hex is:

40c239bf3880461563d09da5078cc28cbef4917c51afb2e21ca1e42dc89c3fa2

In more detail, the root is computed as follows:

1. For each line in the file, read the name, transform it into a sequence of bytes using ASCII encoding, hash the bytes and write back the hash.
2. For each pair of lines in the file, read the two hash values and concatenate them. Hash the resulting 512 bits and write back the hash.
3. Repeat step (2) until there is only one line left in the file, containing the root.

Find your name in the file and compute its authentication path in the following format:

1. Each line in the path should include two hash values (512 bits) encoded in hex.
2. Either the first or second half of the first line should be a hash of your name.
3. Either the first or second half of each line (except the first) should be the hash of the previous line.
4. The hash of the last line should be the root given above.

For example, the authentication path for the name Omer Paneth is given in the file "Omer Paneth.txt".

What to submit. Submit a single zip file named "solution.zip" that contains:

- A text file named "#NAME.txt" (replace #NAME with your full name as it appears in the file "students.txt") that includes your authentication path in format describe above.
- A folder named "code" containing all the source code you used to get to your solution.