UAB COLLEGE OF ARTS AND SCIENCES
The University of Alabama at Birmingham

Department of Computer Science

CS 445/645/745: Modern Cryptography
Instructor: Dr. Yuliang Zheng (yzheng@uab.edu)

Immutable Records using One-Way Hash

This assignment implements a strategy that makes it impossible for someone to alter the contents of a public platform at a later time. The public platform can be a discussion forum, a bulletin board or a social network such as FaceBook and Twitter. The strategy uses a one-way hash such as SHA256 in Python's "hashlib" and works like this:

1. At the end of Day 1, a snapshot of all contents on the platform is taken. Data in the snapshot is then hashed using SHA256. The outcome of the hash computation, H_1, is published to the entire world, such as by printing it on the next day's New York Times.
2. At the end of Day 2, a snapshot of all contents on the platform is taken. Data in the snapshot, together with the hash of the previous day H_1, is then hashed using SHA256. The outcome of the hash computation, H_2, is published to the entire world, such as by printing it on the next day's New York Times.
3. At the end of Day 3, a snapshot of all contents on the platform is taken. Data in the snapshot, together with the hash of the previous day H_2, is then hashed using SHA256. The outcome of the hash computation, H_3, is published to the entire world, such as by printing it on the next day's New York Times.
4. Likewise, the same operation is applied at the end of Day 4, 5, ……. The chain of hash values H_1, H_2, H_3, ……, together with the chain of snapshots, forms an immutable record for the public platform.

Your task is to implement the strategy using Python, especially SHA-256 in "hashlib". To simplify your implementation, you may make the following shortcuts:

1. You may use a flat directory of files to simulate a snapshot of contents in a public platform. Use Merkle hash tree to build a hash of the snapshot. Note that the number of files and their contents may vary from snapshot to snapshot, and the order in which files are hashed is important.
2. You may use a web site or a simple public file to simulate New York Times.
3. You may use an all-0 H_0 as the hash value of the snapshot of a non-existent Day 0.

Submit

1. Your code
2. A report
    a. detailing your design and implementation of the code
    b. screenshots of test runs
    c. discussions on
        i. why the system you build is immutable
        ii. vulnerability of your system
        iii. pros and cons of shortened time intervals between snapshots

    d. your implementation may be further improved by taking into consideration the following aspects. Discuss how you might implement these and other improvements you can think of, if you have time later.
        i. using digital signature,
        ii. allowing a snapshot to be composed of a hierarchy of nested directories each of which may contain both files and sub-directories.

3. Slides for presentation

Presentation

Students will have an opportunity to present their work to the entire class.