CS 5433 SP23: Homework 1

Instructor: Ari Juels
TAs: Andres Fabrega, Zhi Liu, Sishan Long
Due: 22 February 2023

Policies and Submission

Submit your written solutions and code to CMSX.

Integrity. For all assignments, you may make use of published materials, but you must acknowledge all sources, in accordance with the Cornell Code of Academic Integrity. Additionally, you must ensure that you understand the material you are submitting; you must be able to explain your solutions to the course instructor or TA if requested. You must complete this homework assignment *on your own.*

Compatibility. Your submitted code must be compatible with `python3.9`. The directory structure of your submission must be as specified at the end of this document.

Problem 1: The Original Proof-of-Work Digital Currency

In this problem, we'll explore the first proof-of-work-based digital currency we're aware of, called *Micromint*. It was devised by Ron Rivest and Adi Shamir and first published in 1996.

In this scheme, a coin is represented by a k-way *hash collision.* Finding such collisions is expensive. Creating coins therefore requires a substantial initial investment, but after a time, collisions quickly cascade. In other words, during the minting process, which involves hashing randomly generated preimages, it is the case that after the first collision is found, others accumulate soon afterward. This situation replicates the economics of a real-world mint: The up-front manufacturing costs for currencies is high, but the incremental cost for producing units of currency is low.

In this problem, we use the notation $[x]_i$ to denote the first i bits of a bitstring x (we mean the most significant bits).

Each coin you produce will include a "watermark." Specifically, each preimage includes a sixteen-bit value $w = [H(\mathsf{nid})]_{16}$, where nid is the ASCII encoding of your NetID. The purpose of the watermark is to ensure that coins are tied to the mint that produced them.

Coin format: A coin $C = (c_1, c_2, \ldots, c_k)$ such that $[H(c_i)]_n = y$ for all $i \in [1, \ldots, k]$ and for some value y. Each preimage c_i must be 8 bytes (64-bits) long and have w as its first 16 bits. Note that computing $H(c_i)$ using the Python's hash library requires representing c_i in bytes (make sure you input **8 bytes** to your hash function). Remaining parameters are set as follows: $k = 4, n = 28$ and the hash function H is `SHA-256`. We do not expect generating collisions to take more than a few minutes if implemented correctly.

Problem parts:

A) *Coins:* In a file `coin.txt`, provide one valid coin C for your mint. The file must have exactly k lines with the ith line storing c_i in hexadecimal form (without the leading "0x").

B) *Forging watermarks:* For your coin C, forge an alternative netid nid^*. That is, present a netid $\mathsf{nid}^* \neq \mathsf{nid}$ that is valid a valid watermark for your coin C. Your watermark must take the form $\ell^i d^j$, where ℓ is a letter, d is a digit, $i \in \{2, 3\}$, and $j \in \{1, \ldots, 10\}$. An example is provided below. Please specify the forged netid nid^* in a file `forged-watermark.txt`.

Example: To help with testing and also explain the format, we provide a valid coin. Assuming nid = af535, the watermark is $w =$ 1000011001111010 and the coin is $C =$(867a95c2a8781d95, 867a79c683c4b9de, 867a18839dcbd23f, 867aee195b47b3d2). A forged watermark is nid* = qn00061. In addition, to help you debug and test your answers, in `verify_coin.py` we have provided you with a function to test if your coin is valid. You will **not** get full credit in this problem if your coin does not pass this test!

Note: Micromint is a centralized scheme—a requirement to prevent double-spending. It is not a full-blown cryptocurrency.

Problem 2: Merkle Trees

As discussed in class, a Merkle tree is a way to authenticate a large number of digital objects (leaves of the tree) using just a small digest (sometimes called a "commitment") that consists of the root of the tree.

In this exercise, you'll build a Merkle tree and create an interface that allows users to query a leaf and receive a proof of inclusion of the leaf in the tree. Note that the proof size and time to generate the proof must be $\mathcal{O}(\log n)$ where n is the number of objects. You will also implement the verification algorithm to authenticate the objects, which again must run in $\mathcal{O}(\log n)$ time.

For the purposes of this question, the Merkle tree you will build must be a complete binary tree, and you will use SHA-256 as the hash function. Complete and submit the `merkle.py` file, please stick to the given functions and do not modify them.[Ari: Complete doesn't necessarily mean all leaves are present. Up to you what to do in this case.]

Problem parts:

1. Implement the `Prover.build_merkle_tree` method that takes in a list of objects represented as strings, builds a Merkle tree and returns a corresponding commitment. The commitment must be a string of hexadecimal digits (as in hexdigest) of length 64. Complete the `Prover.get_leaf` method that returns the object at the particular leaf index. Note that index starts from 0, left to right. Return `None` if there is no object at the given index.

   Hint: Complete binary trees can be implemented as arrays (multi-dimensional arrays also an option).

2. Complete the `Prover.generate_proof` method that takes as input a leaf index and returns the proof string. Return `None` if there is no object at the given index.

3. Complete the `verify` function that takes as input an object string, a proof string, and a commitment string, and returns True if the proof is valid for the given object with respect to the commitment, else returns False.

   Note: Your `verify` function must be compatible with the methods implemented in the previous parts, but should not share any state with the `Prover` class. Except for any import statements, write all your code in the `Prover` class and the `verify` function.

You can use the provided `test.py` to test your code, although it will not cover all the test cases, you can get a sense of how we use the `Prover` class and `verify` function in the final test.

This exercise will serve as a stepping stone for Problem 3.

Problem 3: Signing via Hashing

Hash functions are useful for many things, among them building digital signature schemes. (The Merkle signature scheme is the best known such construction.)

In this exercise, you'll explore a hash-based signature scheme that is a variant on the Merkle scheme. Our scheme makes use of a Merkle tree. The basic idea is that a message is mapped to a collection of leaves of the tree. A signature consists of preimages of those leaves, along with corresponding paths from the leaves to the root such that a verifier (by means of the algorithm Verify) can check that these preimages are indeed correct.

The Merkle tree in this exercise is of depth $d + 1$. The root of the tree is the public key pk. Every leaf value $s_i \in \{0,1\}^\ell$ is the image of a secret preimage $s_i^{-1} \in \{0,1\}^\ell$ generated uniformly at random. The private key sk is the set of preimages $\{s_i^{-1}\}$ of all leaves.

To sign a message m, the signer performs the following procedure for $j \in \{1, 2, \ldots, k\}$ and $d \leq \ell$: The signer computes $z_j = H(j \parallel m) \bmod 2^d$, where $H : \{0,1\}^* \to \{0,1\}^\ell$ is a hash function (SHA-256 for this exercise), j is a big-endian binary representation of j of length 256 and $\parallel$ denotes concatenation. Each z_j value lies in $\{0, \ldots, 2^d - 1\}$ and points to a leaf of the Merkle tree. The signer computes $\sigma_j = s_{z_j}^{-1}$ and the resulting signature sig on m is $\sigma = \sigma_1 \parallel \ldots \parallel \sigma_k$, along with "**S**ibling **P**aths" from each corresponding leaf to the root of the tree. (See below for more details.)

The parameters (d, k), as we shall see, determine how secure the signature scheme is. (We'll use a fixed value $\ell = 256$ for this exercise.)

Problem parts:

1. *Signature scheme construction:* Implement the algorithms (KeyGen, Path, Sign) for this signature scheme so that it runs for any $d, k \in [1, 20]$. Specifically, you should complete the following three functions in `signature.py` in the order that follows. Here are necessary details:

   - KeyGen: This function should as a first step generate 2^d preimage / image pairs (s_i^{-1}, s_i). It generates them from a secret (pseudorandom) seed r (to make it easier for us to verify your results). We are providing a function to generate the full set of such pairs: KeyPairGen in `signature.py`. It takes as input a parameter d and the seed r, which takes the form of an integer, and returns 2^d preimage / image pairs.[1]

     Given leaf values, KeyGen should build a Merkle tree over the set of values $\{s_i\}$, i.e., these values constitute the leaves of the tree. As in Problem 2, you will use `SHA-256` as the hash function. For a non-leaf node A in the Merkle tree at depth $d' \in [0, 1, \ldots, d]$, its value will be calculated as `SHA-256`$(i \parallel l \parallel r)$, where $i \in [0, 1, \ldots, 2^{d'})$ is the 256-bit binary representation of the index of A among the nodes at depth d', l, r are 64-byte hexadecimal strings representing value of node A's left child and right child respectively.

     Your code for KeyGen should take as input the parameter d and a random seed r. It will output the hexadecimal string pk.

   - Path: This function returns the path SP_j of a given leaf index z_j. We now precisely define SP_j. The path in the Merkle tree from s_{z_j} to the root has $d + 1$ nodes, call them $A_{j0}, \ldots, A_{jd}$, with $A_{j0} = s_{z_j}$ being the leaf and $A_{jd} = pk$ being the root. We know that A_{ji} is a child of $A_{j(i+1)}$. For Verify to calculate the next node $A_{j(i+1)}$ recursively, it must know the other child of $A_{j(i+1)}$, which is the sibling node of A_{ji}. We denote this node by sib_{ji}, so that value of $A_{j(i+1)} = H(b \parallel A_{ji} \parallel sib_{ji})$ where b is the index of $A_{j(i+1)}$. SP_j is now defined as $SP_j = sib_{j0} \parallel \ldots \parallel sib_{j(d-1)}$. Your code should take the input $cur = z_j$, and output SP_j.

   - Sign: Continue to use `SHA-256` as the hash function here. The function Sign should take as input an arbitrary string m, the depth parameter d, a signature security parameter k, and a random seed r as secret key. It will generate and output a signature $sig = \sigma \parallel paths$. Here σ is as described above (with each σ_j in hexadecimal notation), while $paths = SP_1 \parallel \ldots \parallel SP_k$ denotes the sequence of nodes that are needed to verify (using the public key) that each s_{z_j} is a leaf of the tree.

[1] Note that KeyPairGen is *not cryptographically secure* and neither it nor its components should be used to build secure applications. We've designed it for this exercise just to keep things simple.

You can use the provided `test.py` to test your code.

Tips: You can use `format(j, "b").zfill(256)` in `python` to transfer an integer `j` to a 256-bit binary string.

2. *Signature forgery:* For poor choices of (d, k), an adversary that is given just one signature can forge a second one. Run your scheme with $d = 10$, $k = 2$ and $r = 2023$. Sign a message m of your choice, yielding signature σ. Find a message $m' \neq m$ such that σ is a valid message for m'. (*Extra credit*: Provide m, m' that are grammatically correct English sentences. Mention in `double.pdf` whether you have found one.) Output your m and m' in `forgery.txt`, each in one line.

3. *Double signatures:* Suppose $k = 1$, and a signer has signed 200 messages $m_1, \ldots, m_{200}$. There is some probability that there exists among these messages a pair m_i, m_j, with $m_i \neq m_j$, such that both messages have identical signatures. How large does d have to be to ensure that this probability is less than 50%? (You may assume a predetermined set of messages. The probability here is then over invocations of KeyGen.) Explain your reasoning in `double.pdf` (can also be .txt, .doc or an image).

Submission Instructions

Directory Structure:

```
hw1-<NetID>
├── p1
│   ├── coin.txt
│   ├── forged-watermark.txt
│   └── generate.py
├── p2
│   └── merkle.py
└── p3
    ├── signature.py
    ├── forgery.txt
    └── double.pdf
```