Exercise 1

1. We covered (cryptographic) hash functions in the lecture. What are two general properties of hash functions? What properties constitute cryptographic hash functions? Explain them in simple words.

2. Alice wants to play "Rock, Paper, Scissors" with Bob via an internet connection. Both want to win and are afraid their opponent will just wait for the message and respond accordingly, as no one knows when the other sent the message. Create a scheme in which it is not possible to cheat.

3. It is best practice to store only hashed user login information. Often, the hash not only contains the password itself, but also some additional user-specific information. Explain why this is a better approach than just storing user-passwords.

4. We want to create a search puzzle. Use the puzzleID "BBSE_E01" and the SHA_256 hash function. Assume d to be "0000f00...".

   (a) What is the value x that solves the puzzle? How long does your computer execute until it finds a result? Select your favorite programming language and develop this search puzzle.

   (b) Three computers (hashing power $A = 50\%, B = 30\%, C = 20\%$, overall 100 000 hashes per second) participate in this search puzzle. All computers iterate through all x with $x + 1$. Which one wins the search puzzle?

   (c) Is there a way for the losing computers to increase their chances of winning?

(d) Can we design the puzzle in such way that the users win in accordance to their hashing power?

5. Take a look at the Merkle tree in Figure 1. It contains four data elements. How would you create a Merkle tree with five elements building upon the given structure?

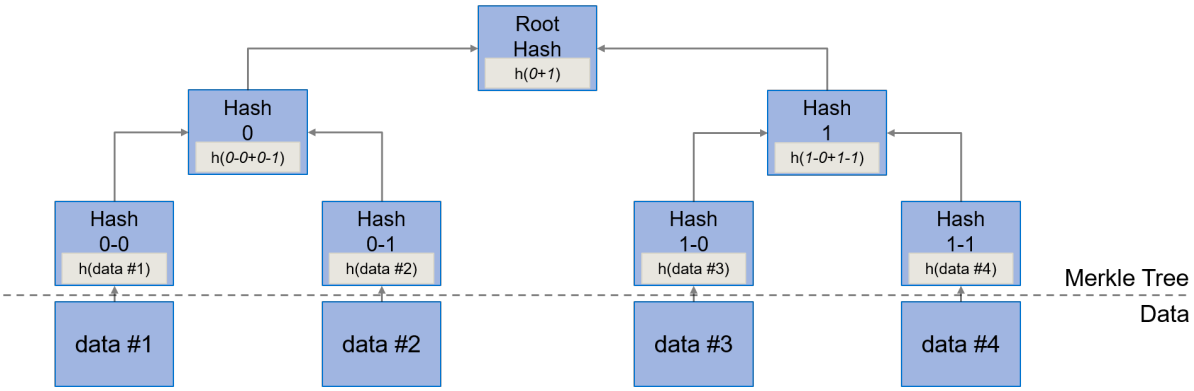

Figure 1: Merkle Tree

6. The Technical University of Munich (TUM) offers a service for companies and other interested parties to validate certificates it has issued. Therefore, the administration decided to:

   1. Hand out a PDF-document to each student with his diploma and
   2. Publish all hashes of these diplomas on www.certificates.tum.de. This website provides an easy way for anyone to validate the document.

   If a student wants to prove she got a certificate of TUM, she gives the PDF-document to the company. The company hashes the file and verifies that this hash is indeed published at www.certifcates.tum.de.

   (a) The administration decided that it might not be the best idea to just publish all hashes, as it reveals the number of diplomas issued in a certain time period. Design a process using hashing algorithms such that:

      1. The integrity of the diplomas is still ensured
      2. It is unknown to a third party how much diplomas are issued
      3. the administration still wants to publish some information, e.g., a database in the backend with a frontend should not be used

      Explain what additional information is required to properly validate a certificate.

   (b) The administration wants to extend the tool such that it is possible to invalidate hashes. It discusses if it should just publish the revoked hashes, however, this would reveal the number of certificates it has revoked (which can be sometimes embarrassing). First, explain why it is not possible to remove a hash out of a Merkle Tree. Further, explain why storing additional Merkle-Trees with revoked hashes still allows students with revoked certificates to validate their certificates.

(c) Explain why using Bloom filters is not suitable for validating certificates.

7. Why are public keys of identities hashed before they are used as an address? Name two reasons and explain.