Cryptography & Blockchain – 5IF, INSA Lyon

SHA-512

Attempt the following exercises. Describe your analysis results in a report. Upload your report and source code to the course's Moodle website.

1. Implement the SHA-512 cryptographic hashing function. You may use any programming language.

2. Verify the correctness of your implementation using the examples discussed in class.

3. *Search puzzle:* Let H be the cryptographic hash function that you have implemented. Consider the equation: $h = H(id \,||\, x)$, where h is the output hash value, and id concatenated with x is the input of the hash function. Generate and assign a random value to id. Search for a value of x such that the first bit of the output hash value h is 0.

4. Search again for a value of x such that the first p bits of h are 0, where $p = 2, 3, 4, \ldots$, until it becomes too time-consuming to find a solution. Analyze the results.