ECE404 Introduction to Computer Security: Homework 07

Spring 2024
Due Date: 5:59pm, March 5, 2024

1 Introduction

In this homework assignment, we will dive into the practical side of cryptography by implementing the Secure Hash Algorithm 512 (SHA-512) in Python. SHA-512 is a widely used crytographic hash function that generates a fixed-sized message digest from input data as large as 2^{128} bits. Furthermore, the algorithm is part of the SHA family developed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST).

As always, please read the homework document in its entirety before coming to office hours with your questions. The teaching staff have spent a long time writing the assignment to cover many common questions you might have.

2 Problem 1: SHA-512

Write a **Python script** that implements the SHA-512 algorithm. More specifically, your program should have the following call syntax:

```
python3 sha512.py input.txt hashed.txt
```

An explanation of the syntax and some key points to note are mentioned below:

- Using the logic described in Lecture 17.5.2, hash the ASCII text in `input.txt` and write the resulting message digest to `hashed.txt`
- Note that the resulting message digest should be written in **hexstring format**
- You can check the correctness of your work by comparing the message digest your implementation produces with that produced by this online tool
- For those of you that I know for a fact will skip over the previous bullet, the message digest for the given input represented as a one-line hexstring is:

```
84f353348a552229554fba7ba822005edcb6bca2fac8cf1735d53ae9e
2915aa2e625f6d3cfa0106c8707ff0004d3ce95281b47b851b380ef91
c86d2fb0e58b28
```

Submission Instructions

- Make sure to follow program requirements specified above. **Failure to follow these instructions may result in loss of points!**.
- You must turn in a single zip file on Brightspace with the following naming convention: HW07_<last name>_<first name>.zip . Your submission must include:
  - A PDF titled `hw07_<last_name>_<first_name>.pdf` containing:
    - a brief explanation of your code.
    - The input and the output of the sha12.py.
  - The file `sha512.py` containing your code for your SHA-512 implementation.