Introduction to Modern Cryptography, Fall 2020
Homework 7 - due December 29

December 8, 2020

This assignment deals with signatures based on hash functions. For more information about the construction of such signatures see lecture 8 and the recommended reading.

1. You are given a Python 3 script *ver.py* implementing the signature's verification algorithm and your goal is to implement the signing algorithm. In more detail, you are given a signing key and verification key pair (in the files *sk1* and *vk1*) and you should submit two valid signatures: one on your first name and one on your last name. Your signatures must be both correct (pass verification) and secure. See Part 2 for an example of signatures that are correct but not secure.

2. You are given a verification key (in the file *vk2*) and 5 signatures: for $x \in \{a, b, c, d, e\}$ the signature on the message x is given in the file *x.sig*. The signatures are correct but not secure. Your goal is find the security flaw and use it to sign your 9-digit ID. Your signature must verify under *vk2*.

3. If we used the hash function sha512 instead of sha256, what would be the size of the resulting signatures? (No need to submit your answer.)

What to submit. Submit a single zip file named "solution.zip" that contains:

- For Part 1 submit the two signatures in two files: "#FIRST.sig" and "#LAST.sig" (replace #FIRST and #LAST with your first and last name respectively).
- For Part 2 submit the signature the file: "#ID.sig" (replace #ID with your ID number).
- A folder named "code" containing all the source code you used to get to your solution.