Tcsss487

Prof. Paulo Barreto

5/6/2024

Cryptographic Project Part 1

Ahmed Mohamed , Louis John Lomboy, and Shu-Ren Shen

Our project interacts with the user through the console. The user will be given a prompt to choose whether to compute a plain cryptographic hash of a given file or input, compute an authentication tag (MAC), use a passphrase, and be able to encrypt a file symmetrically and decrypt the same file. The user selects which operation to perform at the beginning of the program. The program will loop once the operation is finished and the user can exit by entering “Exit” at the end of each operation. The program arguments include the input file, output file, and the password to be used to perform these operations. In a command line, it will look like “java Main inputFile.txt outputFile.txt password”.

Solution for Part 1:

We have implemented a Java version of SHA-3 based on Markku-Juhani Saarinen’s C version (https://github.com/mjosaarinen/tiny_sha3/blob/master/sha3.c). This project follows the specification in the NIST Special Publication 800-185 (https://dx.doi.org/10.6028/NIST.SP.800-185) for implementing the KMACXOF256 primitive.

Getting inputFile name will then use input file as bytes and call cShake256 as input and store the data. In cShake256, it will call init() which will Initializes the state to zero, sets the message digest length and rate size, and resets the pointer.

Known Bugs:

- There are trailing zeros when it comes to the output of the encrypted file.
- The case for symmetric encryption and decryption are not implemented yet.