Simple SHA-3: A small endeavor into cryptographic hashing

Implementation based on: https://github.com/mjosaarinen/tiny_sha3/blob/master/sha3.c

Authors: Patrick Tibbals and Ian McLean

Our application is command line based and will offer four functions listed as follows. The prompts simple require the correct letter,[a-eA-E], and the return key to continue through the menu. Completing a valid operation will return you to the main menu any incorrect inputs will continue to ask for valid input until entered. Encryption function will ask for file input and a desired password, function will return message "Encoded successfully" when complete. For the decryption function you must encrypt a file first. This encrypted data is stored within the program and will be accessed by the decryption function. Passwords must be same as password used for file encryption.

Encryption Security for all functions: 256 bits

A) Compute plain cryptographic hash:

– This function will allow file loading or user input.

B) Compute MAC authentication tag:

– This function will allow file loading or user input.

C) Encryption a data file:

– Function will ask for a file path to the desired file if provided with invalid input it will ask again for valid input.

– Provided sample is accessed with: "test1.txt"

D) Decrypt symmetric cryptogram:

– Function will ask only for password for previously encrypted file

– Program will access previous computed cryptogram compare the t, t' returning accepted or rejected input message.

E) Exit

---

cSHAKE and KMACXOF algorithms functionality was verified according to the test cases:

cSHAKE256 - https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards-and-Guidelines/documents/examples/cSHAKE_samples.pdf

KMACXOF256 - https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Standards-and-Guidelines/documents/examples/KMACXOF_samples.pdf