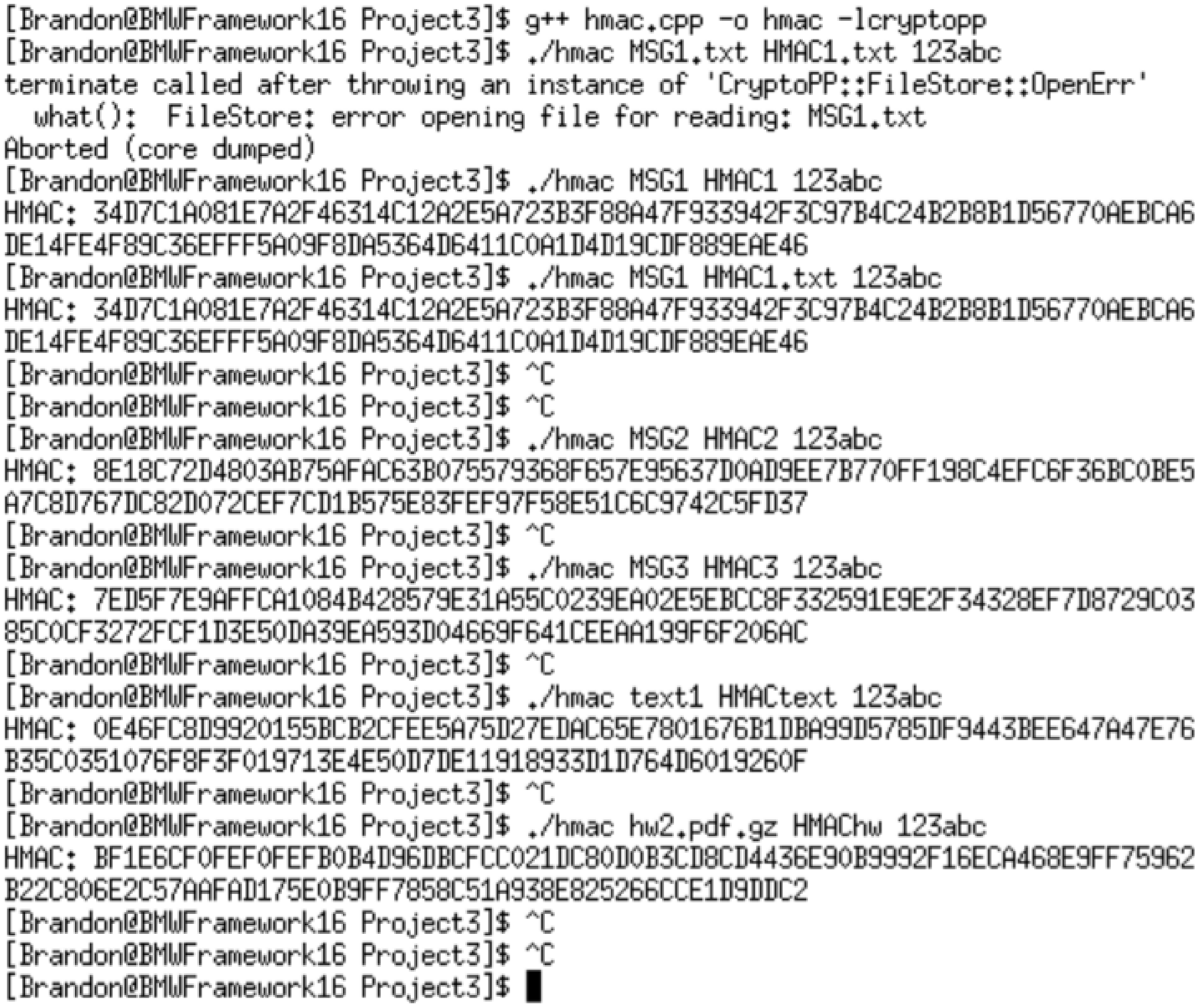
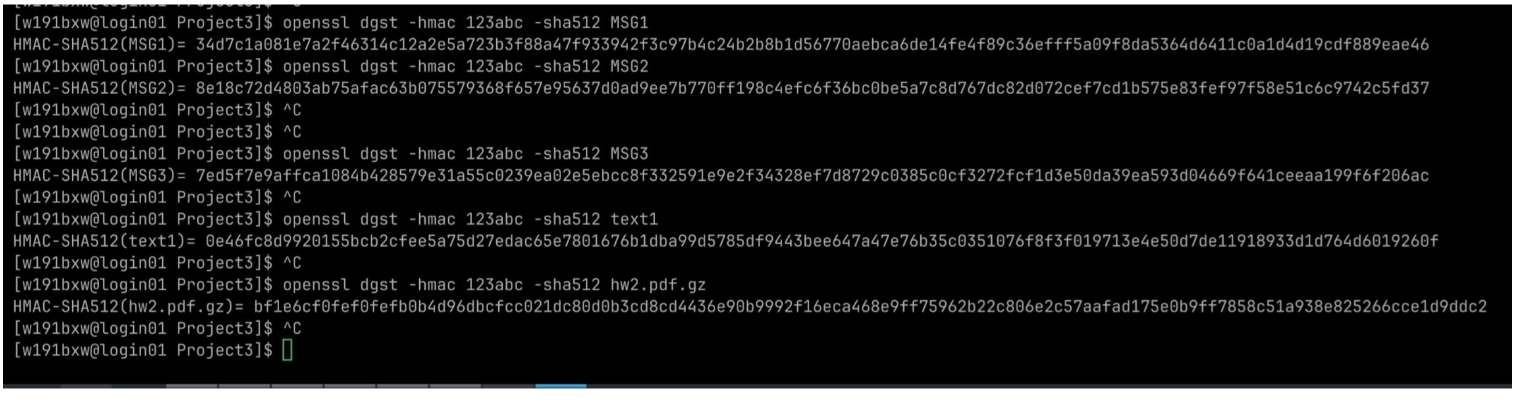
CEG-4751 Information Security
Brandon Walker
Meilin Liu
03/10/2024
Project 2

Task 1: I wrote a program to calculate the HMAC of an input file using the cryptopp libraries following the guidelines.



```
[Brandon@BMWFramework16 Project3]$ g++ hmac.cpp -o hmac -lcryptopp
[Brandon@BMWFramework16 Project3]$ ./hmac MSG1.txt HMAC1.txt 123abc
terminate called after throwing an instance of 'CryptoPP::FileStore::OpenErr'
  what():  FileStore: error opening file for reading: MSG1.txt
Aborted (core dumped)
[Brandon@BMWFramework16 Project3]$ ./hmac MSG1 HMAC1 123abc
HMAC: 34D7C1A081E7A2F46314C12A2E5A723B3F88A47F933942F3C97B4C24B2B8B1D56770AEBCA6
DE14FE4F89C36EFFF5A09F8DA5364D6411C0A1D4D19CDF889EAE46
[Brandon@BMWFramework16 Project3]$ ./hmac MSG1 HMAC1.txt 123abc
HMAC: 34D7C1A081E7A2F46314C12A2E5A723B3F88A47F933942F3C97B4C24B2B8B1D56770AEBCA6
DE14FE4F89C36EFFF5A09F8DA5364D6411C0A1D4D19CDF889EAE46
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ./hmac MSG2 HMAC2 123abc
HMAC: 8E18C72D4803AB75AFAC63B075579368F657E95637D0AD9EE7B770FF198C4EFC6F36BC0BE5
A7C8D767DC82D072CEF7CD1B575E83FEF97F58E51C6C9742C5FD37
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ./hmac MSG3 HMAC3 123abc
HMAC: 7ED5F7E9AFFCA1084B428579E31A55C0239EA02E5EBCC8F332591E9E2F34328EF7D8729C03
85C0CF3272FCF1D3E50DA39EA593D04669F641CEEAA199F6F206AC
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ./hmac text1 HMACtext 123abc
HMAC: 0E46FC8D9920155BCB2CFEE5A75D27EDAC65E7801676B1DBA99D5785DF9443BEE647A47E76
B35C0351076F8F3F019713E4E50D7DE11918933D1D764D6019260F
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ./hmac hw2.pdf.gz HMAChw 123abc
HMAC: BF1E6CF0FEF0FEFB0B4D96DBCFCC021DC80D0B3CD8CD4436E90B9992F16ECA468E9FF75962
B22C806E2C57AAFAD175E0B9FF7858C51A938E825266CCE1D9DDC2
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ █
```

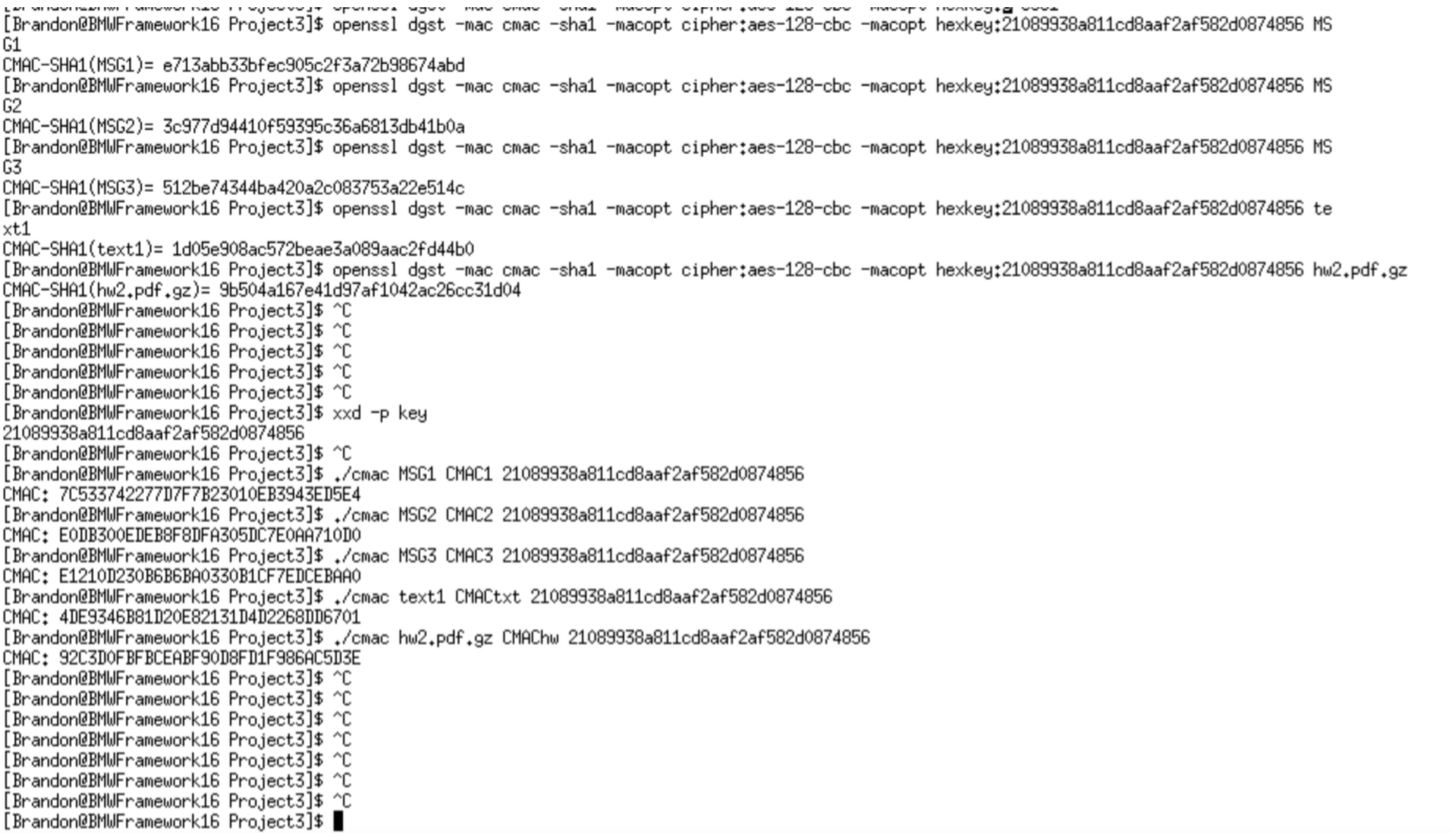
Task 2: I misunderstood and first ran my hmac program on fry, but then realized I was supposed to use the openssl command to perform the function. So I kept my useless output to just show my process, and then did it the right way and have that as well. My hmac's matched which is what I expected because they are hash functions, and that is the point of hash functions, given the same input, you should always get the same output.



```
[w191bxw@login01 Project3]$ openssl dgst -hmac 123abc -sha512 MSG1
HMAC-SHA512(MSG1)= 34d7c1a081e7a2f46314c12a2e5a723b3f88a47f933942f3c97b4c24b2b8b1d56770aebca6de14fe4f89c36efff5a09f8da5364d6411c0a1d4d19cdf889eae46
[w191bxw@login01 Project3]$ openssl dgst -hmac 123abc -sha512 MSG2
HMAC-SHA512(MSG2)= 8e18c72d4803ab75afac63b075579368f657e95637d0ad9ee7b770ff198c4efc6f36bc0be5a7c8d767dc82d072cef7cd1b575e83fef97f58e51c6c9742c5fd37
[w191bxw@login01 Project3]$ ^C
[w191bxw@login01 Project3]$ ^C
[w191bxw@login01 Project3]$ openssl dgst -hmac 123abc -sha512 MSG3
HMAC-SHA512(MSG3)= 7ed5f7e9affca1084b428579e31a55c0239ea02e5ebcc8f332591e9e2f34328ef7d8729c0385c0cf3272fcf1d3e50da39ea593d04669f641ceeaa199f6f206ac
[w191bxw@login01 Project3]$ ^C
[w191bxw@login01 Project3]$ openssl dgst -hmac 123abc -sha512 text1
HMAC-SHA512(text1)= 0e46fc8d9920155bcb2cfee5a75d27edac65e7801676b1dba99d5785df9443bee647a47e76b35c0351076f8f3f019713e4e50d7de11918933d1d764d6019260f
[w191bxw@login01 Project3]$ ^C
[w191bxw@login01 Project3]$ openssl dgst -hmac 123abc -sha512 hw2.pdf.gz
HMAC-SHA512(hw2.pdf.gz)= bf1e6cf0fef0fefb0b4d96dbcfcc021dc80d0b3cd8cd4436e90b9992f16eca468e9ff75962b22c806e2c57aafad175e0b9ff7858c51a938e825266cce1d9ddc2
[w191bxw@login01 Project3]$ ^C
[w191bxw@login01 Project3]$ ▯
```

Task 3: I am not a graduate student but I made a pass at this task, and documented it below.

Task 4: Same here, but my output doesn’t seem to match, and I am not sure if that is because I am doing something wrong, or something about how CMAC works or the way openssl performs the function, though I suspect it is down to me having the openssl command wrong, or my program wrong.



```
[Brandon@BMWFramework16 Project3]$ openssl dgst -mac cmac -sha1 -macopt cipher:aes-128-cbc -macopt hexkey:21089938a811cd8aaf2af582d0874856 MS
G1
CMAC-SHA1(MSG1)= e713abb33bfec905c2f3a72b98674abd
[Brandon@BMWFramework16 Project3]$ openssl dgst -mac cmac -sha1 -macopt cipher:aes-128-cbc -macopt hexkey:21089938a811cd8aaf2af582d0874856 MS
G2
CMAC-SHA1(MSG2)= 3c977d94410f59395c36a6813db41b0a
[Brandon@BMWFramework16 Project3]$ openssl dgst -mac cmac -sha1 -macopt cipher:aes-128-cbc -macopt hexkey:21089938a811cd8aaf2af582d0874856 MS
G3
CMAC-SHA1(MSG3)= 512be74344ba420a2c083753a22e514c
[Brandon@BMWFramework16 Project3]$ openssl dgst -mac cmac -sha1 -macopt cipher:aes-128-cbc -macopt hexkey:21089938a811cd8aaf2af582d0874856 te
xt1
CMAC-SHA1(text1)= 1d05e908ac572beae3a089aac2fd44b0
[Brandon@BMWFramework16 Project3]$ openssl dgst -mac cmac -sha1 -macopt cipher:aes-128-cbc -macopt hexkey:21089938a811cd8aaf2af582d0874856 hw2.pdf.gz
CMAC-SHA1(hw2.pdf.gz)= 9b504a167e41d97af1042ac26cc31d04
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ xxd -p key
21089938a811cd8aaf2af582d0874856
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ./cmac MSG1 CMAC1 21089938a811cd8aaf2af582d0874856
CMAC: 7C533742277D7F7B23010EB3943ED5E4
[Brandon@BMWFramework16 Project3]$ ./cmac MSG2 CMAC2 21089938a811cd8aaf2af582d0874856
CMAC: E0DB300EDEB8F8DFA305DC7E0AA710D0
[Brandon@BMWFramework16 Project3]$ ./cmac MSG3 CMAC3 21089938a811cd8aaf2af582d0874856
CMAC: E1210D230B6B6BA0330B1CF7EDCEBAA0
[Brandon@BMWFramework16 Project3]$ ./cmac text1 CMACtxt 21089938a811cd8aaf2af582d0874856
CMAC: 4DE9346B81D20E82131D4D2268DD6701
[Brandon@BMWFramework16 Project3]$ ./cmac hw2.pdf.gz CMAChw 21089938a811cd8aaf2af582d0874856
CMAC: 92C3D0FBFBCEABF90D8FD1F986AC5D3E
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ ^C
[Brandon@BMWFramework16 Project3]$ █
```

I have the hmac.cpp that I used to make the hmac script in this folder, but the versions of cryptopp on my laptop and fry are different so there are 2 compiled versions, one named fryhmac and then the cmac.cpp for running that. I attached the screenshots here and everything else will be in the zipped folder with this report, and all the outputs are in text format and named right below this

HMAC1:

34D7C1A081E7A2F46314C12A2E5A723B3F88A47F933942F3C97B4C24B2B8B1D56770AEBCA6DE14FE4F89C36EFFF5A09F8DA5364D6411C0A1D4D19CDF889EAE46

opensslHMAC1:

34d7c1a081e7a2f46314c12a2e5a723b3f88a47f933942f3c97b4c24b2b8b1d56770aebca6de14fe4f89c36efff5a09f8da5364d6411c0a1d4d19cdf889eae46

CMAC1: 9679628C8EA94807F8936042AE6C970E

opensslCMAC1: e713abb33bfec905c2f3a72b98674abd

HMAC2:

8E18C72D4803AB75AFAC63B075579368F657E95637D0AD9EE7B770FF198C4EFC6F36BC0BE5A7C8D767DC82D072CEF7CD1B575E83FEF97F58E51C6C9742C5FD37

opensslHMAC2:

8e18c72d4803ab75afac63b075579368f657e95637d0ad9ee7b770ff198c4efc6f36bc0be5a7c8d767dc82d072cef7cd1b575e83fef97f58e51c6c9742c5fd37

CMAC2: 724075857C50B45081B24A117E6CF0E6

opensslCMAC2: 3c977d94410f59395c36a6813db41b0a

HMAC3: 7ED5F7E9AFFCA1084B428579E31A55C0239EA02E5EBCC8F332591E9E2F343CMAC-SHA1(MSG1)= e713abb33bfec905c2f3a72b98674abd28EF7D8729C0385C0CF3272FCF1D3E50DA39EA593D04669F641CEEAA199F6F206AC

opensslHMAC3:
7ed5f7e9affca1084b428579e31a55c0239ea02e5ebcc8f332591e9e2f34328ef7d8729c0385c0cf3272fcf1d3e50da39ea593d04669f641ceeaa199f6f206ac
CMAC3: FA2DB5E92BDEC1276C995B622559DD48
opensslCMAC3: 512be74344ba420a2c083753a22e514c

HMACtxt:
0E46FC8D9920155BCB2CFEE5A75D27EDAC65E7801676B1DBA99D5785DF9443BEE647A47E76B35C0351076F8F3F019713E4E50D7DE11918933D1
D764D6019260F
opensslHMACtxt:
0e46fc8d9920155bcb2cfee5a75d27edac65e7801676b1dba99d5785df9443bee647a47e76b35c0351076f8f3f019713e4e50d7de11918933d1d764d6019260f
CMACtxt: 53F548EDAA266CE332AEDFB282B2C0B0
opensslCMACtxt: 1d05e908ac572beae3a089aac2fd44b0

HMAChw:
BF1E6CF0FEF0FEFB0B4D96DBCFCC021DC80D0B3CD8CD4436E90B9992F16ECA468E9FF75962B22C806E2C57AAFAD175E0B9FF7858C51A938E8
25266CCE1D9DDC2
opensslHMAChw:
bf1e6cf0fef0fefb0b4d96dbcfcc021dc80d0b3cd8cd4436e90b9992f16eca468e9ff75962b22c806e2c57aafad175e0b9ff7858c51a938e825266cce1d9ddc2
CMAChw: DC3273609BBEDC9D4249596DDDCFE3E5
opensslCMAChw: 9b504a167e41d97af1042ac26cc31d04