

Introduction

1. **Goal of this assignment** : The Goal of this assignment is to create a SCP using openssl libraries.

2. **Design Explanation**

1. **ufsend input_filename [-d ipaddr:port] [-l]**

The ufsend takes a file name as a input and an IP address and PORT number if it is to be run in the -d(dumps) mode. After taking these details the user is prompted to enter his password and then using the function `get_key_using_pbkdf2` which is defined in the file `pbkdf2_extract.c` in the source code a 32 byte KEY is generated, this function uses the openssl implementation of PBKDF2 to generate the KEY. Now we read the entire input file into a buffer and then generate a IV using the `rand_bytes` function provided by openssl. Now we encrypt the data that is loaded into the buffer using the generated KEY and IV and produce the cipher text. If we are running the process in -d mode then this data along with the IV and the TAG are sent separately to the ufrec network daemon which is running on the specified ip address and port number. The final step of the process is to create a file with an extension of ".ufsec" and terminate the process, In the file that has been created we will be storing the IV, cipher text and tag data into the file so that when we are retrieving this file in the local mode on ufrec we will have access to the IV, ciphertext and the TAG and since we already know that the size of the IV and TAG is going to be 16 bytes it is going to be easy to recover these from the ".ufsec" file which will be given as an input for ufrec when it is run locally.

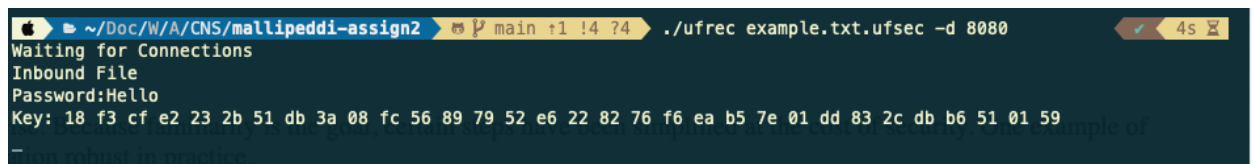
2. **ufrec filename [-d port] [-l]**

The ufrec works as a network daemon when it is run with -d option then it prompts the user for their password and waits for incoming data from ufsend. Once it recieved the IV, encrypted data and TAG in that order it decrypts the file and then prints the decrypted text on to the screen. Then it writes the plain text to the filename and exits. When we are running this in local mode (-l) we will simply decrypt the file which is given as input and then produce a file without the ".ufsec" extension

Rubric results and explanations

1. **With password "Hello", print the hexadecimal value of the symmetric key derived by PBKDF2** : *REFER to Figure 1 for output screenshots*

This PKCS5_PBKDF2_HMAC function is provided by the openssl library which is used in the `get_key_using_pbkdf2` function in the `pbkdf2_extract.c` file.



```
~/Doc/W/A/CNS/mallipeddi-assign2 main +1 !4 ?4 ./ufrec example.txt.ufsec -d 8080
Waiting for Connections
Inbound File
Password:Hello
Key: 18 f3 cf e2 23 2b 51 db 3a 08 fc 56 89 79 52 e6 22 82 76 f6 ea b5 7e 01 dd 83 2c db b6 51 01 59
```

The image shows a terminal window with a dark background. The title bar at the top indicates the current directory is ~/Doc/W/A/CNS/mallipeddi-assign2 and the active process is main +1 !4 ?4. The command being executed is ./ufrec example.txt.ufsec -d 8080. The terminal output shows 'Waiting for Connections', followed by 'Inbound File'. Then, a password 'Hello' is entered. Finally, a 32-byte hexadecimal key is displayed: 18 f3 cf e2 23 2b 51 db 3a 08 fc 56 89 79 52 e6 22 82 76 f6 ea b5 7e 01 dd 83 2c db b6 51 01 59.

Figure 1: Result of "Hello" as a password using PBKDF2

2. Encrypt `example.txt` and display hexadecimal value of encrypted file on screen *REFER to Figure 2 and 3 for output screenshots*

```

~/Doc/W/A/CNS/mallipeddi-assign2 main +1 !3 72 ./ufsend example.txt -d 127.0.0.1:8080
Connection to server successful
Password:Hello
Key: 18 f3 cf e2 23 2b 51 db 3a 08 fc 56 89 79 52 e6 22 82 76 f6 ea b5 7e 01 dd 83 2c db b6 51 01 59
Ciphertext is:
0000 - 62 4c b5 1b 60 c1 16 56-6a d8 ad 3b 18 bc 58 9e bL..`Vj...X.
0010 - bd a6 fb a1 29 b7 f9 c2-63 94 39 2c 5a 42 51 00 ....)...c.9,ZBQ.
0020 - 02 1c 3a 29 fc e4 2a ef-7a 97 c4 23 0c 6e 7f b4 ...:)*.z...#.n..
0030 - e3 a5 d3 65 66 51 1c a1-cd 49 ab c6 0a b6 3b e3 ...efQ...I....;
0040 - b4 b6 04 4c e4 51 c1 cb-7b e5 33 ab 3a ec 10 17 .k.L.Q...{.3....
0050 - 7a f1 ed af 94 c5 68 e3-ee 5f 09 f4 06 ec a4 81 z....h..._.
0060 - 3e 4a d3 a9 72 d1 41 d1-f4 23 a9 54 4f 87 87 c5 >J...r.A.#.T0...
0070 - 2f e9 7b c8 b7 49 33 26-17 ac 8e 48 0e e0 5c 83 /.{..I3&...H.\.
0080 - 86 33 5a a5 53 3d b3 df-44 71 31 d4 3d 93 ab d9 .3Z.S=.Dq1.=...
0090 - f2 57 93 c9 3e f0 04 3e-fd 20 c8 88 ef 7b 8e 8f .W...>...>. ...{.
00a0 - bc 60 e6 c6 5e e1 43 9e-5c be c2 ae b0 11 bf 58 .`..^..C.\.....X
00b0 - 03 18 c5 ed 30 3a 18 53-ab 3a a1 7f f8 91 8c 5a ....0:..S:.....Z
00c0 - 01 d5 25 ea b2 ff 8b fe-c4 e1 2a fa ba 21 34 e6 .%......*...!4.
00d0 - 7c da 26 b1 be 36 5b c7-31 75 b6 21 7e de db f1 |.&..6[.lu.!...
00e0 - 51 b5 f9 cc 0c 8c 99 0b-65 de 8e 07 64 43 fc 8f Q.....e...dC..
00f0 - a7 69 28 57 6a 14 b6 6f-cf a5 9a d1 96 1c 71 d5 .i(Wj..o.....q.
0100 - 94 69 f1 f6 68 87 db d3-b4 d6 cc c5 5c eb ac 65 .i..h.....\..e
0110 - 2d bd 1c fd fa 02 09 05-9f ff 4a ab 33 f2 25 38 -. ....J.3.%8
0120 - 9f 10 b5 02 37 74 da 6d-29 8c db 5c 4b 44 f6 62 ....7t.m)..KD.b
0130 - 90 e7 53 44 9b f0 4d b1-ee a1 41 4f 11 00 33 e5 ..SD..M...A0..3.
0140 - 6e d1 c5 4c 7e 7e ec 3d-99 ab a9 2d dc 66 70 96 n..L~.=...-fp.
0150 - a8 45 15 34 a9 96 97 c7-43 54 a3 7b 60 fb a5 a8 .E.4....CT.{'...
0160 - 09 ae fe b4 26 96 74 bb-50 5e 60 d3 28 1d ec c3 ...&.t.P^'(..(
0170 - 35 ab e4 19 a3 9d b7 83-14 fe 8d b0 d7 aa 54 2a 5.....T*
0180 - 41 5a f4 8a 77 70 9f ab-a4 ed a1 c0 fb ae 1d f2 AZ..wp.....
0190 - 2f 5c 7c 61 f5 2c 0c 2a-6a 61 2d f5 94 08 0c 5e /\|a.,*ja-....^
01a0 - c5 1d f9 c1 48 e6 9e 7f-ad a1 f0 b1 e1 fb 7a 8d ....H.....Z.
01b0 - 0a 52 f2 df d7 f3 61 9a-be 6a 6a 61 74 80 73 4a .R...a..jjat.sj
01c0 - e9 e9 30 73 5f 12 05 12-3c cd 63 6d 59 89 96 21 ..0s_...<.cmY...!
01d0 - 99 d6 5d 5c cb a1 c0 78-ac 8b 34 44 71 00 48 b8 ..\...x...40q.H.
01e0 - b2 60 4e 84 41 a0 ec a2-05 71 69 fe a4 2d 92 f7 .N.A....qi1.-..
01f0 - bd 04 78 e5 ac b8 da 11-24 73 9d 38 11 83 8d 06 .x.....$s.8....
0200 - 58 bf a0 f4 d2 2f a5 80-c6 06 71 93 2b 82 df 5d X.../.....q.+..]
0210 - b0 42 68 4b c5 ce 24 db-1d 5a 4d 18 bb 2e 2c 04 .BhK..$.ZM....
0220 - 1d f1 51 fc b8 93 15 1b-93 32 f7 67 e5 c4 2a 97 ..Q.....2.g..*.
0230 - 33 b3 f6 12 a7 8e 6d c9-3c 9b 88 b3 b0 95 3e 49 3.....m.<.....>I
0240 - 53 96 b9 55 d6 2f f6 1f-e6 03 ae 40 20 77 a9 bf S..U./.....@ w..
0250 - 3e e5 5f 0c b1 59 21 8b-4b ae 22 55 7d 8f 4d 38 >...Y!..K."U).M8
0260 - a7 43 65 83 38 c3 5e 18-64 a8 39 3e fb 1a 31 04 .Ce.8..<d.9>..1.
0270 - 51 99 cb b7 74 0f 28 54-ec 4a 57 4f ec e4 bc 51 Q...t.(.JWO...Q
0280 - a8 f3 06 05 b4 6f 3a 1a-48 08 1b b8 b6 1c 1c aa .....0:..H.....
0290 - 3d 27 c4 cf 56 e8 89 97-7b 88 29 e8 bb cb 6f 7a ='...V...{.)...oz
02a0 - 9c cf 40 63 70 8f 0a 2f-3d 64 95 eb 9f 1b dc 86 ..@cp../=d.....
02b0 - 0e 5c a7 d7 fe ba a4 e3-a0 04 c1 13 08 8e 38 47 .\.....8G
02c0 - ee 35 24 fc b6 50 dd 70-a2 6e 40 0f 63 8e 61 0d .5$..P.p.n@c.a.
02d0 - b0 e2 d8 57 2a bb 40 ee-2e 1f 26 df 07 1b 3b 7d ...W*..@...&...;
02e0 - cd 53 48 32 bb 10 2d 66-2d 8e de eb 37 11 35 23 .SH2..-f-...7.5#
02f0 - 85 d5 26 12 bc 9b 21 dc-4b 53 42 47 06 3a c4 79 ..&...!..KSBG.:y
  
```

Figure 2: Encrypted Text after encrypting `example.txt` using the KEY and IV (Rubric 2)

After generating the KEY using PBKDF2 and using a cryptographically pseudorandom number as an IV, we encrypt the contents of the input text file using AES encryption in GCM mode. The displayed text is hexadecimal value of the encrypted file.

```
0160 - 09 ae fe b4 26 96 74 bb-50 5e 60 d3 28 1d ec c3 ....&.t.P^`.(...
0170 - 35 ab e4 19 a3 9d b7 83-14 fe 8d b0 d7 aa 54 2a 5.....T*
0180 - 41 5a f4 8a 77 70 9f ab-a4 ed a1 c0 fb ae 1d f2 AZ..wp.....
0190 - 2f 5c 7c 61 f5 2c 0c 2a-6a 61 2d f5 94 08 0c 5e /\|a.,.*ja-....^
01a0 - c5 1d f9 c1 48 e6 9e 7f-ad a1 f0 b1 e1 fb 7a 8d ....H.....Z.
01b0 - 0a 52 f2 df d7 f3 61 9a-be 6a 6a 61 74 80 73 4a .R....a..jjat.sJ
01c0 - e9 e9 30 73 5f 12 05 12-3c cd 63 6d 59 89 96 21 ..0s....<.cmY..!
01d0 - 99 d6 5d 5c cb a1 c0 78-ac 8b 34 44 71 00 48 b8 ..l\...x..4Dq.H.
01e0 - b2 60 4e 84 41 a0 ec a2-05 71 69 fe a4 2d 92 f7 .`N.A.....qi.-..
01f0 - bd 04 78 e5 ac b8 da 11-24 73 9d 38 11 83 8d 06 ..X.....$s.8....
0200 - 58 bf a0 f4 d2 2f a5 80-c6 06 71 93 2b 82 df 5d X..../....q.+..]
0210 - b0 42 68 4b c5 ce 24 db-1d 5a 4d 18 bb 2e 2c 04 .BhK..$.ZM....,
0220 - 1d f1 51 fc b8 93 15 1b-93 32 f7 67 e5 c4 2a 97 ..Q.....2.g..*.
0230 - 33 b3 f6 12 a7 8e 6d c9-3c 9b 88 b3 b0 95 3e 49 3.....m.<.....>I
0240 - 53 96 b9 55 d6 2f f6 1f-e6 03 ae 40 20 77 a9 bf S..U./.....@ w..
0250 - 3e e5 5f 0c b1 59 21 8b-4b ae 22 55 7d 8f 4d 38 >.,.Y!<K."U}.M8
0260 - a7 43 65 83 38 c3 5e 18-64 a8 39 3e fb 1a 31 04 .Ce.8.^<d.9>..1.
0270 - 51 99 cb b7 74 0f 28 54-ec 4a 57 4f ec e4 bc 51 Q...t.(T.JW0...Q
0280 - a8 f3 06 05 b4 6f 3a 1a-48 08 1b b8 b6 1c 1c aa .....o:.H.....
0290 - 3d 27 c4 cf 56 e8 89 97-7b 88 29 e8 bb cb 6f 7a ='.V....(.)...oz
02a0 - 9c cf 40 63 70 8f 0a 2f-3d 64 95 eb 9f 1b dc 86 ..@cp../=d.....
02b0 - 0e 5c a7 d7 fe ba a4 e3-a0 04 c1 13 08 8e 38 47 .\.....8G
02c0 - ee 35 24 fc b6 50 dd 70-a2 6e 40 0f 63 8e 61 0d .5$.P.p.n@c.a.
02d0 - b0 e2 d8 57 2a bb 40 ee-2e 1f 26 df 07 1b 3b 7d ...W*..@...&...; }
02e0 - cd 53 48 32 bb 10 2d 66-2d 8e de eb 37 11 35 23 .SHZ..-f....7.5#
02f0 - 85 d5 26 12 bc 9b 21 dc-4b 53 42 47 06 3a c4 79 ..&...!<KSBG...y
0300 - 86 be 7c 08 fd 03 71 34-de 3c 17 11 47 90 e3 40 ..|...q4.<..G..@
0310 - 68 ea 19 c6 7c cd 09 53-26 27 c8 e6 6e 0a 30 28 h...|..5&'..n.0(
0320 - 45 1e ed 28 47 60 e6 a2-33 1c a8 74 8c 31 15 61 E..(G`..3..t.1.a
0330 - 4c 3f cc 6e 1b 64 b8 45-b6 db 39 84 39 68 7a fc L?.n.d.E..9.9hz.
0340 - ca 06 32 83 9b f6 18 c9-4a 42 0c 0b b9 55 7e 02 ..2.....J8...U~.
0350 - c6 dd e2 ac cb 8a a9 27-b6 bd 78 5b 94 fc 60 06 .....'.x[...'
0360 - 1d f2 a0 bb f6 c7 80 3a-6a 15 7e 35 fb b7 98 c2 .....j..~5....
0370 - ed d7 8f c2 f0 30 59 8d-35 53 46 ce ff ee e0 6e .....0Y.55F....n
0380 - 77 24 2f 94 f2 ac af 51-fd 53 4c a3 64 b6 32 86 w$/....Q.SL.d.2.
0390 - ac 5a d4 f3 3e ac 7a 70-d8 f7 f1 79 ab fb 22 2c .Z..>.zp...y...".
03a0 - 3a 9a a7 2c 59 13 f7 fa-93 80 33 68 11 9f 4b 85 :..Y.....3h..K.
03b0 - 6c 5e 6a 0f 0a bb bf 6d-74 90 97 00 dc c0 d1 29 l^j.....mt.....)
03c0 - 4a 61 16 f6 2c c8 95 e7-2e b2 26 22 1d df 5b 11 Ja.,....&".[.
03d0 - 9c d9 df 09 7b d7 7a 1e-d7 7f e9 cc 4e 9a 3f 9b ....{.z.....N.?.
03e0 - c9 8f 9b ab 10 f6 38 44-29 a3 bd 7f 74 7f ab 42 .....8D)...t..B
03f0 - af 0b de bc d3 83 36 d6-e3 3c d8 8d d3 a1 76 96 .....6..<....V.
0400 - 03 c3 2b d0 20 c2 2e 0a-2a 1b 87 42 a2 32 52 ae .+. ...*.B.2R..
0410 - a1 7f 49 a6 12 95 95 59-d5 ee 56 4f 80 d2 48 ed ..I....Y..V0..H.
0420 - 95 2d 2e 58 be 46 2b d4-95 76 8a 00 14 ba 63 61 .-X.F+.v....ca
0430 - b4 59 c4 20 fb 5e 94 bd-22 59 14 14 91 ca 8d 99 .Y. .^..Y.....
0440 - 42 2c eb 73 53 f9 5d 33-28 81 de 49 38 75 e8 99 B,.sS.]3(..I8u..
0450 - 42 ad 60 00 ec d6 ba e2-d6 30 2d 32 e2 64 41 72 B.`.....0-2.dAr
0460 - 91 af b7 18 bb 3a 22 01-33 23 8e 40 a3 f6 08 48 .....".3#.e...H
0470 - 76 39 7b d8 4b c7 78 60-b8 c5 b1 38 08 cd e4 v9{.K.x`...8...
Transmitting to 127.0.0.1:8080
Successfully Encrypted data and sent 1151 bytes
```

Figure 3: Encrypted Text after encrypting example.txt using the KEY and IV(Cont'd) (Rubric 2)

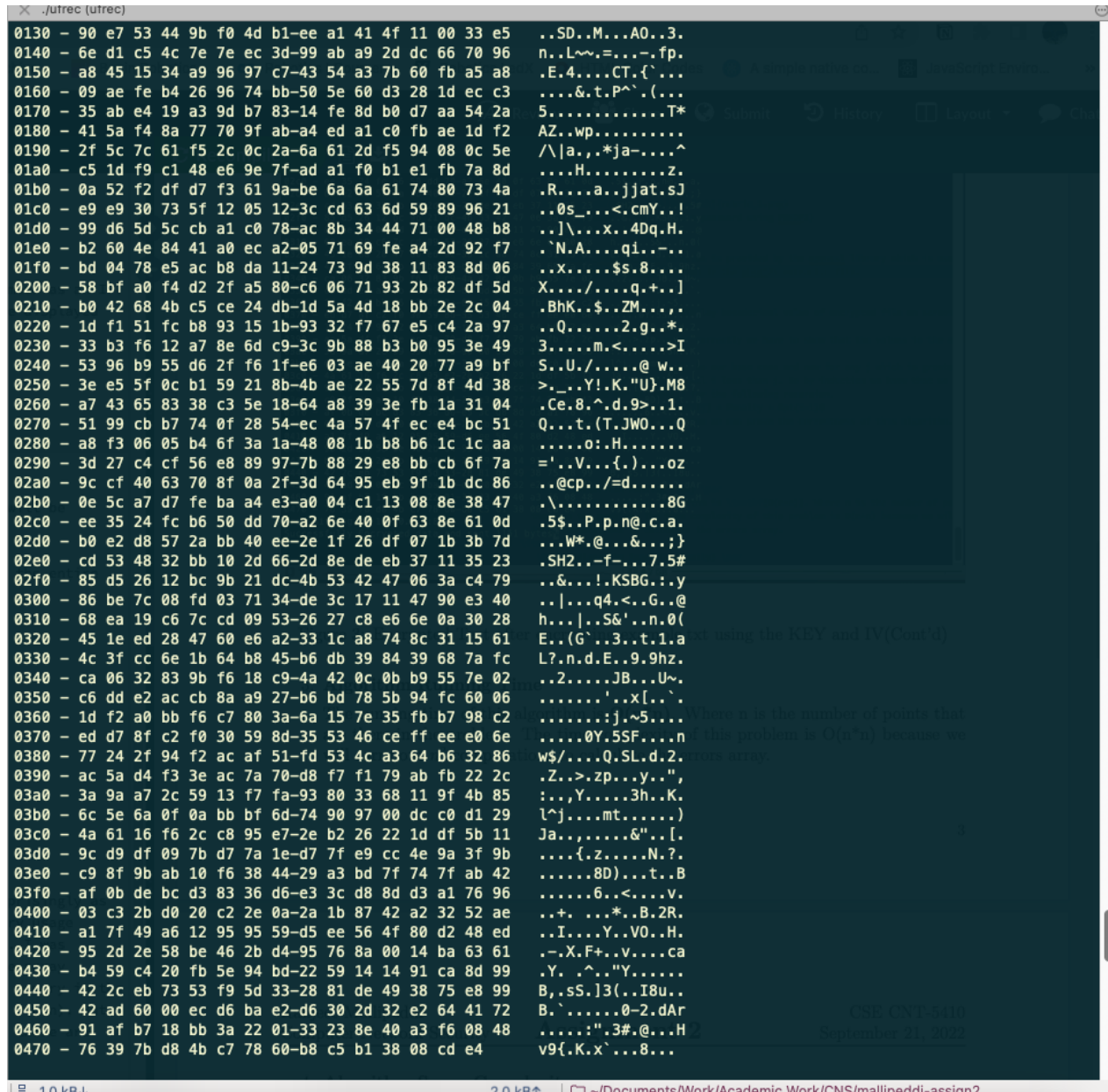
3. Display encrypted text received by ufrec REFER to Figure 4 and 5 for output screenshots

The ufrec network daemon keeps waiting for data after there has been a connection then it receives the IV, encrypted text and tag data from ufsend and then it displays

```
./ufrec (ufrec)
~/Doc/W/A/CNS/mallipeddi-assign2 main +1 !3 72 ./ufrec example3.txt -d 8080
Waiting for Connections
Inbound File
Password:Hello
Key: 18 f3 cf e2 23 2b 51 db 3a 08 fc 56 89 79 52 e6 22 82 76 f6 ea b5 7e 01 dd 83 2c db b6 51 01 59
Recieved Cipher is:
0000 - 62 4c b5 1b 60 c1 16 56-6a d8 ad 3b 18 bc 58 9e bL...Vj...X.
0010 - bd a6 fb a1 29 b7 f9 c2-63 94 39 2c 5a 42 51 00 ....).c.9,ZBQ.
0020 - 02 1c 3a 29 fc e4 2a ef-7a 97 c4 23 0c 6e 7f b4 ...).*.z.#.n..
0030 - e3 a5 d3 65 66 51 1c a1-cd 49 ab c6 0a b6 3b e3 ...efQ...I....;
0040 - b4 b6 04 4c e4 51 c1 cb-7b e5 33 ab 3a ec 10 17 .k.L.Q..{.3....
0050 - 7a f1 ed af 94 c5 68 e3-ee 5f 09 f4 06 ec a4 81 z....h.....
0060 - 3e 4a d3 a9 72 d1 41 d1-f4 23 a9 54 4f 87 87 c5 >J..r.A..#.T0...
0070 - 2f e9 7b c8 b7 49 33 26-17 ac 8e 48 0e e0 5c 83 /.{..I3&...H..\
0080 - 86 33 5a a5 53 3d b3 df-44 71 31 d4 3d 93 ab d9 .3Z.S=..Dq1.=...
0090 - f2 57 93 c9 3e f0 04 3e-fd 20 c8 88 ef 7b 8e 8f .W..>..>. ...{..
00a0 - bc 60 e6 c6 5e e1 43 9e-5c be c2 ae b0 11 bf 58 .`..^..C..\.....X
00b0 - 03 18 c5 ed 30 3a 18 53-ab 3a a1 7f f8 91 8c 5a ....0:.S:.....Z
00c0 - 01 d5 25 ea b2 ff 8b fe-c4 e1 2a fa ba 21 34 e6 ..%......*..!4.
00d0 - 7c da 26 b1 be 36 5b c7-31 75 b6 21 7e de db f1 |.&..6[.1u.!~...
00e0 - 51 b5 f9 cc 0c 8c 99 0b-65 de 8e 07 64 43 fc 8f Q.....e...dC..
00f0 - a7 69 28 57 6a 14 b6 6f-cf a5 9a d1 96 1c 71 d5 .i(Wj..o.....q.
0100 - 94 69 f1 f6 68 87 db d3-b4 d6 cc c5 5c eb ac 65 .i..h.....\..e
0110 - 2d bd 1c fd fa 02 09 05-9f ff 4a ab 33 f2 25 38 ~\.....J.3.%8
0120 - 9f 10 b5 02 37 74 da 6d-29 8c db 5c 4b 44 f6 62 ....7t.m)..KQD.b
0130 - 90 e7 53 44 9b f0 4d b1-ee a1 41 4f 11 00 33 e5 ..SD..M...A0..3.
0140 - 6e d1 c5 4c 7e 7e ec 3d-99 ab a9 2d dc 66 70 96 n..L~=-...-.fp.
0150 - a8 45 15 34 a9 96 97 c7-43 54 a3 7b 60 fb a5 a8 .E.4....CT.{'...
0160 - 09 ae fe b4 26 96 74 bb-50 5e 60 d3 28 1d ec c3 ....&.t.P^`.(...
0170 - 35 ab e4 19 a3 9d b7 83-14 fe 8d b0 d7 aa 54 2a 5.....T*
0180 - 41 5a f4 8a 77 70 9f ab-a4 ed a1 c0 fb ae 1d f2 AZ..wp.....
0190 - 2f 5c 7c 61 f5 2c 0c 2a-6a 61 2d f5 94 08 0c 5e /\|a.,.*ja-....^
01a0 - c5 1d f9 c1 48 e6 9e 7f-ad a1 f0 b1 e1 fb 7a 8d ....H.....Z.
01b0 - 0a 52 f2 df d7 f3 61 9a-be 6a 6a 61 74 80 73 4a .R....a..jjat.sJ
01c0 - e9 e9 30 73 5f 12 05 12-3c cd 63 6d 59 89 96 21 ..0s....<.cmY..!
01d0 - 99 d6 5d 5c cb a1 c0 78-ac 8b 34 44 71 00 48 b8 ..]...x...4Dq.H.
01e0 - b2 60 4e 84 a1 a0 ec a2-05 71 69 fe a4 2d 92 f7 .N.A....qi1-...
01f0 - bd 04 78 e5 ac b8 da 11-24 73 9d 38 11 83 8d 06 ...X.....$s.8....
0200 - 58 bf a0 f4 d2 2f a5 80-c6 06 71 93 2b 82 df 5d X..../....q+..]
0210 - b0 42 68 4b c5 ce 24 db-1d 5a 4d 18 bb 2e 2c 04 .BhK..$.ZM....,
0220 - 1d f1 51 fc b8 93 15 1b-93 32 f7 67 e5 c4 2a 97 ..Q.....2.g..*.
0230 - 33 b3 f6 12 a7 8e 6d c9-3c 9b 88 b3 b0 95 3e 49 3.....m.<.....>I
0240 - 53 96 b9 55 d6 2f f6 1f-e6 03 ae 40 20 77 a9 bf S..U./.....@ w..
0250 - 3e e5 5f 0c b1 59 21 8b-4b ae 22 55 7d 8f 4d 38 >._.Y!.K."U}.M8
0260 - a7 43 65 83 38 c3 5e 18-64 a8 39 3e fb 1a 31 04 .Ce.8.^..d.9>..1.
0270 - 51 99 cb b7 74 0f 28 54-ec 4a 57 4f ec e4 bc 51 Q...t.(T.JW0...Q
0280 - a8 f3 06 05 b4 6f 3a 1a-48 08 1b b8 b6 1c 1c aa .....0:.H.....
0290 - 3d 27 c4 cf 56 e8 89 97-7b 88 29 e8 bb cb 6f 7a ='...V....{.)...oz
02a0 - 9c cf 40 63 70 8f 0a 2f-3d 64 95 eb 9f 1b dc 86 ..@cp../=d.....
02b0 - 0e 5c a7 d7 fe ba a4 e3-a0 04 c1 13 08 8e 38 47 .\.....8G
02c0 - ee 35 24 fc b6 50 dd 70-a2 6e 40 0f 63 8e 61 0d .5$.P.p.n@.c.a.
02d0 - b0 e2 d8 57 2a bb 40 ee-2e 1f 26 df 07 1b 3b 7d ...W*.*@...&...; }
02e0 - cd 53 48 32 bb 10 2d 66-2d 8e de eb 37 11 35 23 .SH2..-f-...7.5#
```

Figure 4: Display the receipt of the file on ufrec and the hexadecimal value of the encrypted file (Rubric 3)

the encrypted text onto the screen.



```
0130 - 90 e7 53 44 9b f0 4d b1-ee a1 41 4f 11 00 33 e5 ..SD..M...A0..3.
0140 - 6e d1 c5 4c 7e 7e ec 3d-99 ab a9 2d dc 66 70 96 n..L~.=...-.fp.
0150 - a8 45 15 34 a9 96 97 c7-43 54 a3 7b 60 fb a5 a8 .E.4....CT.{'....
0160 - 09 ae fe b4 26 96 74 bb-50 5e 60 d3 28 1d ec c3 ....&.t.P^`.(...
0170 - 35 ab e4 19 a3 9d b7 83-14 fe 8d b0 d7 aa 54 2a 5.....T*
0180 - 41 5a f4 8a 77 70 9f ab-a4 ed a1 c0 fb ae 1d f2 AZ..wp.....
0190 - 2f 5c 7c 61 f5 2c 0c 2a-6a 61 2d f5 94 08 0c 5e /\|a.,.*ja-....^
01a0 - c5 1d f9 c1 48 e6 9e 7f-ad a1 f0 b1 e1 fb 7a 8d ....H.....Z.
01b0 - 0a 52 f2 df d7 f3 61 9a-be 6a 6a 61 74 80 73 4a .R....a..jjat.sJ
01c0 - e9 e9 30 73 5f 12 05 12-3c cd 63 6d 59 89 96 21 ..0s_...<.cmY.!
01d0 - 99 d6 5d 5c cb a1 c0 78-ac 8b 34 44 71 00 48 b8 ..|\....x..4Dq.H.
01e0 - b2 60 4e 84 41 a0 ec a2-05 71 69 fe a4 2d 92 f7 .`N.A....qi.-...
01f0 - bd 04 78 e5 ac b8 da 11-24 73 9d 38 11 83 8d 06 ..X....$s.8....
0200 - 58 bf a0 f4 d2 2f a5 80-c6 06 71 93 2b 82 df 5d X..../.....q.+..]
0210 - b0 42 68 4b c5 ce 24 db-1d 5a 4d 18 bb 2e 2c 04 .BhK..$.ZM....,
0220 - 1d f1 51 fc b8 93 15 1b-93 32 f7 67 e5 c4 2a 97 ..Q.....2.g.*.
0230 - 33 b3 f6 12 a7 8e 6d c9-3c 9b 88 b3 b0 95 3e 49 3.....m.<.....>I
0240 - 53 96 b9 55 d6 2f f6 1f-e6 03 ae 40 20 77 a9 bf S..U./.....@ w..
0250 - 3e e5 5f 0c b1 59 21 8b-4b ae 22 55 7d 8f 4d 38 >._.Y!.K."U}.M8
0260 - a7 43 65 83 38 c3 5e 18-64 a8 39 3e fb 1a 31 04 .Ce.8.^..d.9>..1.
0270 - 51 99 cb b7 74 0f 28 54-ec 4a 57 4f ec e4 bc 51 Q...t.(T.JW0...Q
0280 - a8 f3 06 05 b4 6f 3a 1a-48 08 1b b8 b6 1c 1c aa .....0:.H.....
0290 - 3d 27 c4 cf 56 e8 89 97-7b 88 29 e8 bb cb 6f 7a ='..V...{.)...oZ
02a0 - 9c cf 40 63 70 8f 0a 2f-3d 64 95 eb 9f 1b dc 86 ..@cp../=d.....
02b0 - 0e 5c a7 d7 fe ba a4 e3-a0 04 c1 13 08 8e 38 47 .\.....8G
02c0 - ee 35 24 fc b6 50 dd 70-a2 6e 40 0f 63 8e 61 0d .5$.P.p.n@c.a.
02d0 - b0 e2 d8 57 2a bb 40 ee-2e 1f 26 df 07 1b 3b 7d ...W*.*...&...;
02e0 - cd 53 48 32 bb 10 2d 66-2d 8e de eb 37 11 35 23 .SH2.-f-...7.5#
02f0 - 85 d5 26 12 bc 9b 21 dc-4b 53 42 47 06 3a c4 79 ..&...!.KSBG.:.y
0300 - 86 be 7c 08 fd 03 71 34-de 3c 17 11 47 90 e3 40 ..|...q4.<..G.@
0310 - 68 ea 19 c6 7c cd 09 53-26 27 c8 e6 6e 0a 30 28 h...|.S&'..n.(
0320 - 45 1e ed 28 47 60 e6 a2-33 1c a8 74 8c 31 15 61 E..(G`.3..t.1.a
0330 - 4c 3f cc 6e 1b 64 b8 45-b6 db 39 84 39 68 7a fc L?.n.d.E..9.9hz.
0340 - ca 06 32 83 9b f6 18 c9-4a 42 0c 0b b9 55 7e 02 ..2.....JB...U~.
0350 - c6 dd e2 ac cb 8a a9 27-b6 bd 78 5b 94 fc 60 06 .....'.x[...'.
0360 - 1d f2 a0 bb f6 c7 80 3a-6a 15 7e 35 fb b7 98 c2 .....:j~5....
0370 - ed d7 8f c2 f0 30 59 8d-35 53 46 ce ff ee e0 6e .....0Y.55F....n
0380 - 77 24 2f 94 f2 ac af 51-fd 53 4c a3 64 b6 32 86 w$/....Q.SL.d.2.
0390 - ac 5a d4 f3 3e ac 7a 70-d8 f7 f1 79 ab fb 22 2c .Z..>.zp...y..",
03a0 - 3a 9a a7 2c 59 13 f7 fa-93 80 33 68 11 9f 4b 85 :..Y.....3h..K.
03b0 - 6c 5e 6a 0f 0a bb bf 6d-74 90 97 00 dc c0 d1 29 l^j....mt.....)
03c0 - 4a 61 16 f6 2c c8 95 e7-2e b2 26 22 1d df 5b 11 Ja.....&"...[.
03d0 - 9c d9 df 09 7b d7 7a 1e-d7 7f e9 cc 4e 9a 3f 9b ....{z.....N.?.
03e0 - c9 8f 9b ab 10 f6 38 44-29 a3 bd 7f 74 7f ab 42 .....8D)...t..B
03f0 - af 0b de bc d3 83 36 d6-e3 3c d8 8d d3 a1 76 96 .....6..<....V.
0400 - 03 c3 2b d0 20 c2 2e 0a-2a 1b 87 42 a2 32 52 ae ..+. ...*.B.2R.
0410 - a1 7f 49 a6 12 95 95 59-d5 ee 56 4f 80 d2 48 ed ..I....Y..VO..H.
0420 - 95 2d 2e 58 be 46 2b d4-95 76 8a 00 14 ba 63 61 .-X.F+.v....Ca
0430 - b4 59 c4 20 fb 5e 94 bd-22 59 14 14 91 ca 8d 99 .Y. .^.."Y.....
0440 - 42 2c eb 73 53 f9 5d 33-28 81 de 49 38 75 e8 99 B,.sS.]3(..I8u..
0450 - 42 ad 60 00 ec d6 ba e2-d6 30 2d 32 e2 64 41 72 B.`.....0-2.dAr
0460 - 91 af b7 18 bb 3a 22 01-33 23 8e 40 a3 f6 08 48 .....:".3#.@...H
0470 - 76 39 7b d8 4b c7 78 60-b8 c5 b1 38 08 cd e4 v9{.K.x`...8...
```

Figure 5: Display the receipt of the file on ufrec and the hexadecimal value of the encrypted file (Cont'd) (Rubric 3)

4. Decrypt File and display contents on the screen

REFER to Figure 6 for output screenshots

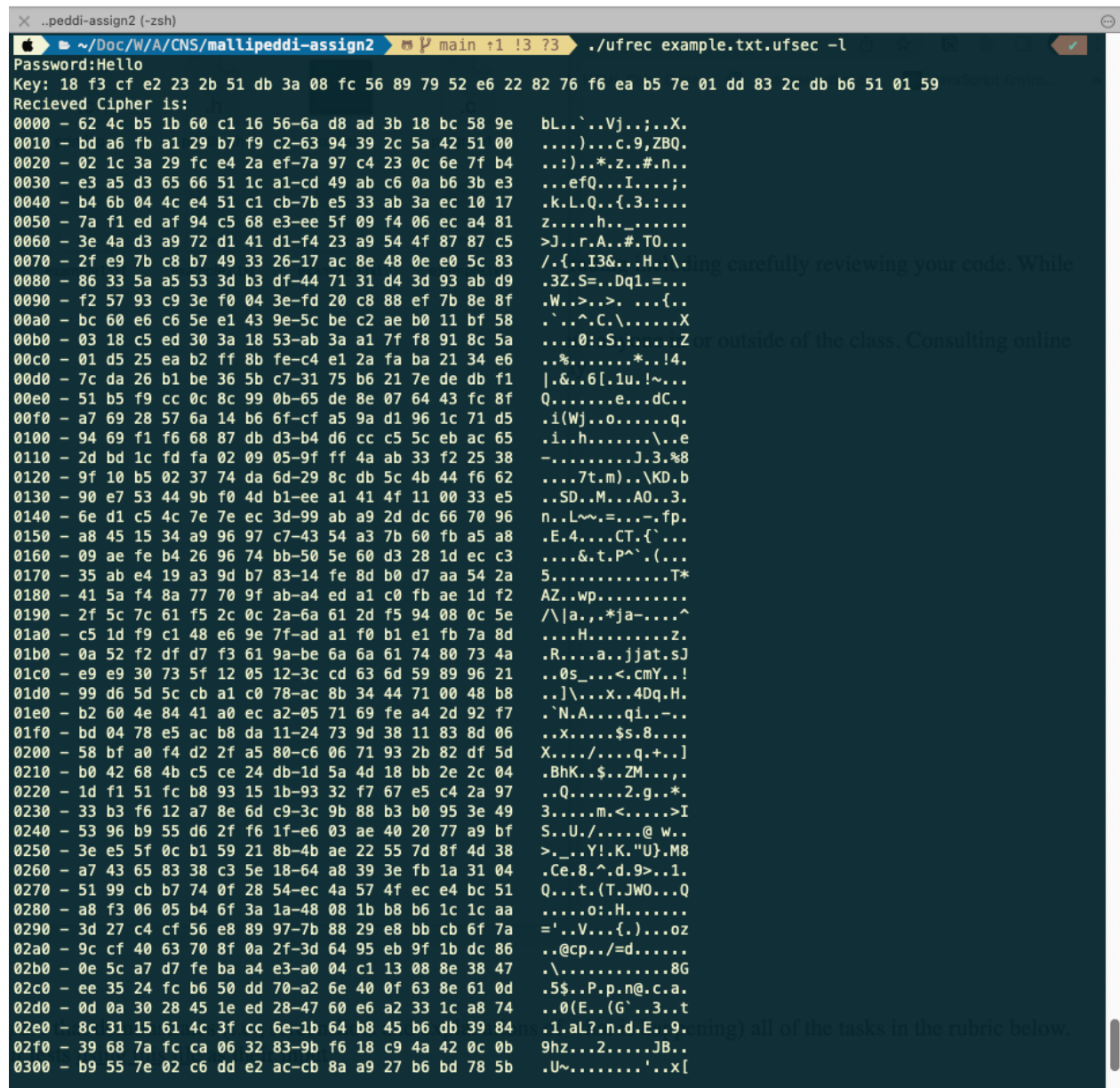
Once we get the IV, encrypted text data and the TAG we can now decrypt the file using the AES256 GCM mode to decrypt the contents of these files. Once the text is

```
0360 - 1d f2 a0 bb f6 c7 80 3a-6a 15 7e 35 fb b7 98 c2 .....:j.~5....
0370 - ed d7 8f c2 f0 30 59 8d-35 53 46 ce ff ee e0 6e .....0Y.5SF....n
0380 - 77 24 2f 94 f2 ac af 51-fd 53 4c a3 64 b6 32 86 w$/...Q.SL.d.2.
0390 - ac 5a d4 f3 3e ac 7a 70-d8 f7 f1 79 ab fb 22 2c .Z...>.zp...y..",
03a0 - 3a 9a a7 2c 59 13 f7 fa-93 80 33 68 11 9f 4b 85 :...Y.....3h..K.
03b0 - 6c 5e 6a 0f 0a bb bf 6d-74 90 97 00 dc c0 d1 29 l^j.....mt.....)
03c0 - 4a 61 16 f6 2c c8 95 e7-2e b2 26 22 1d df 5b 11 Ja.....&"..[.
03d0 - 9c d9 df 09 7b d7 7a 1e-d7 7f e9 cc 4e 9a 3f 9b ....{.z.....N.?.
03e0 - c9 8f 9b ab 10 f6 38 44-29 a3 bd 7f 74 7f ab 42 .....8D)...t..B
03f0 - af 0b de bc d3 83 36 d6-e3 3c d8 8d d3 a1 76 96 .....6..<....V.
0400 - 03 c3 2b d0 20 c2 2e 0a-2a 1b 87 42 a2 32 52 ae ..+. ...*..B.2R.
0410 - a1 7f 49 a6 12 95 95 59-d5 ee 56 4f 80 d2 48 ed ..I....Y..V0..H.
0420 - 95 2d 2e 58 be 46 2b d4-95 76 8a 00 14 ba 63 61 .-.X.F+..v....ca
0430 - b4 59 c4 20 fb 5e 94 bd-22 59 14 14 91 ca 8d 99 .Y. .^.."Y.....
0440 - 42 2c eb 73 53 f9 5d 33-28 81 de 49 38 75 e8 99 B,.sS.]3(..I8u..
0450 - 42 ad 60 00 ec d6 ba e2-d6 30 2d 32 e2 64 41 72 B.`.....0-2.dAr
0460 - 91 af b7 18 bb 3a 22 01-33 23 8e 40 a3 f6 08 48 .....:"3#.@...H
0470 - 76 39 7b d8 4b c7 78 60-b8 c5 b1 38 08 cd e4 v9{.K.x`...8...
Decrypted text is:
Students who start their homework early tend to do well.
Those who don't... well...
Have you started thinking about projects?
Students who start their homework early tend to do well.
Those who don't... well...
Have you started thinking about projects?
Students who start their homework early tend to do well.
Those who don't... well...
Have you started thinking about projects?
Students who start their homework early tend to do well.
Those who don't... well...
Have you started thinking about projects?
Students who start their homework early tend to do well.
Those who don't... well...
Have you started thinking about projects?
Students who start their homework early tend to do well.
Those who don't... well...
Have you started thinking about projects?
Students who start their homework early tend to do well.
Those who don't... well...
Have you started thinking about projects?
Students who start their homework early tend to do well.
Those who don't... well...
Have you started thinking about projects?
Students who start their homework early tend to do well.
Those who don't... well...
Have you started thinking about projects?
Time to start :)
Successfully recieved encrypted file and decrypted the text. 1151 bytes written%
diff example.txt example3.txt
./ufrec example.txt.ufsec -l
```

Figure 6: Display the decrypted file on to the screen (Rubric 4)

decrypted it is displayed and then written to the filename given as a argument. Also as you can see on the screenshot there is a diff check performed which shows that the output file from ufrec and the original example.txt file are the same.

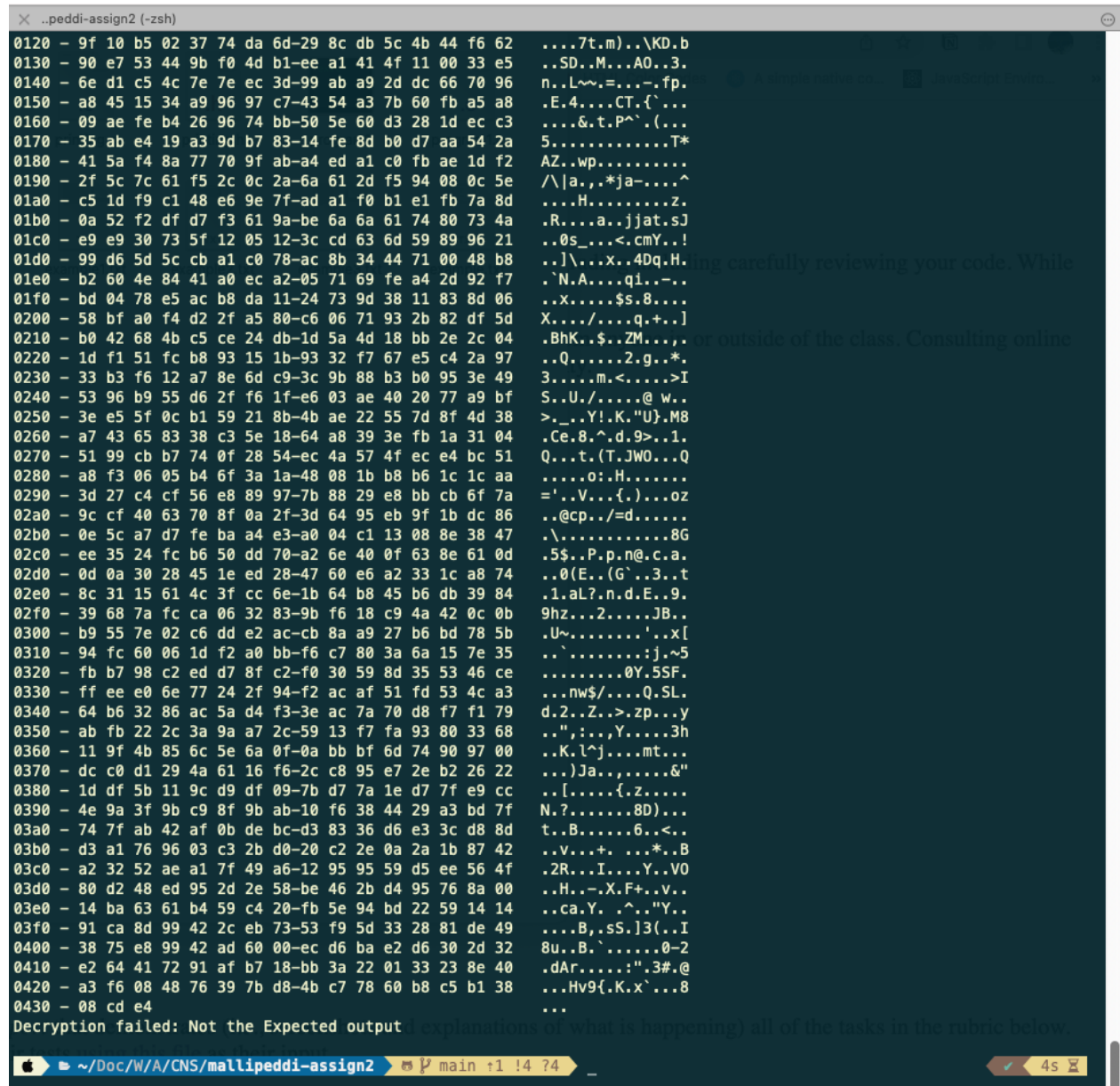
5. Manually modify the ciphertext and attempt to decrypt it locally. *REFER to Figure 7 and 8 for output screenshots*



```
..peddi-assign2 (-zsh)
~/Doc/W/A/CNS/mallipeddi-assign2 main +1 !3 ?3 ./ufrec example.txt.ufsec -l
Password:Hello
Key: 18 f3 cf e2 23 2b 51 db 3a 08 fc 56 89 79 52 e6 22 82 76 f6 ea b5 7e 01 dd 83 2c db b6 51 01 59
Recieved Cipher is:
0000 - 62 4c b5 1b 60 c1 16 56-6a d8 ad 3b 18 bc 58 9e bL...Vj...;X.
0010 - bd a6 fb a1 29 b7 f9 c2-63 94 39 2c 5a 42 51 00 ....).c.9,ZBQ.
0020 - 02 1c 3a 29 fc e4 2a ef-7a 97 c4 23 0c 6e 7f b4 ..:)*.z..#.n..
0030 - e3 a5 d3 65 66 51 1c a1-cd 49 ab c6 0a b6 3b e3 ...efQ...I....;
0040 - b4 6b 04 4c e4 51 c1 cb-7b e5 33 ab 3a ec 10 17 .k.L.Q..{.3:....
0050 - 7a f1 ed af 94 c5 68 e3-ee 5f 09 f4 06 ec a4 81 Z.....h.....
0060 - 3e 4a d3 a9 72 d1 41 d1-f4 23 a9 54 4f 87 87 c5 >J..r.A..#.T0...
0070 - 2f e9 7b c8 b7 49 33 26-17 ac 8e 48 0e e0 5c 83 /.{..I3&...H..\.
0080 - 86 33 5a a5 53 3d b3 df-44 71 31 d4 3d 93 ab d9 .3Z.S=..Dq1.=...
0090 - f2 57 93 c9 3e f0 04 3e-fd 20 c8 88 ef 7b 8e 8f .W..>..>. ...{..
00a0 - bc 60 e6 c6 5e e1 43 9e-5c be c2 ae b0 11 bf 58 .^..C..\.....X
00b0 - 03 18 c5 ed 30 3a 18 53-ab 3a a1 7f f8 91 8c 5a ....0:..S:.....Z
00c0 - 01 d5 25 ea b2 ff 8b fe-c4 e1 2a fa ba 21 34 e6 .%......*..!4.
00d0 - 7c da 26 b1 be 36 5b c7-31 75 b6 21 7e de db f1 |.&..6[.1u.!~...
00e0 - 51 b5 f9 cc 0c 8c 99 0b-65 de 8e 07 64 43 fc 8f Q.....e...dC..
00f0 - a7 69 28 57 6a 14 b6 6f-cf a5 9a d1 96 1c 71 d5 .i(Wj..o.....q.
0100 - 94 69 f1 f6 68 87 db d3-b4 d6 cc c5 5c eb ac 65 .i..h.....\..e
0110 - 2d bd 1c fd fa 02 09 05-9f ff 4a ab 33 f2 25 38 -.....J.3.%8
0120 - 9f 10 b5 02 37 74 da 6d-29 8c db 5c 4b 44 f6 62 ....7t.m)..KD.b
0130 - 90 e7 53 44 9b f0 4d b1-ee a1 41 4f 11 00 33 e5 ..SD..M...A0..3.
0140 - 6e d1 c5 4c 7e 7e ec 3d-99 ab a9 2d dc 66 70 96 n..L~..=...-.fp.
0150 - a8 45 15 34 a9 96 97 c7-43 54 a3 7b 60 fb a5 a8 .E.4....CT.{^...
0160 - 09 ae fe b4 26 96 74 bb-50 5e 60 d3 28 1d ec c3 ....&.t.P^^(...
0170 - 35 ab e4 19 a3 9d b7 83-14 fe 8d b0 d7 aa 54 2a 5.....T*
0180 - 41 5a f4 8a 77 70 9f ab-a4 ed a1 c0 fb ae 1d f2 AZ..wp.....
0190 - 2f 5c 7c 61 f5 2c 0c 2a-6a 61 2d f5 94 08 0c 5e /\|a.,.*ja-....^
01a0 - c5 1d f9 c1 48 e6 9e 7f-ad a1 f0 b1 e1 fb 7a 8d ....H.....z.
01b0 - 0a 52 f2 df d7 f3 61 9a-be 6a 6a 61 74 80 73 4a .R.....a..jjat,sJ
01c0 - e9 e9 30 73 5f 12 05 12-3c cd 63 6d 59 89 96 21 ..0s_...<.cmY..!
01d0 - 99 d6 5d 5c cb a1 c0 78-ac 8b 34 44 71 00 48 b8 .)]...x...4Dq.H.
01e0 - b2 60 4e 84 41 a0 ec a2-05 71 69 fe a4 2d 92 f7 .N.A....qi..-..
01f0 - bd 04 78 e5 ac b8 da 11-24 73 9d 38 11 83 8d 06 .x.....$s.8....
0200 - 58 bf a0 f4 d2 2f a5 80-c6 06 71 93 2b 82 df 5d X.../....q.+..]
0210 - b0 42 68 4b c5 ce 24 db-1d 5a 4d 18 bb 2e 2c 04 .BhK..$.ZM....,
0220 - 1d f1 51 fc b8 93 15 1b-93 32 f7 67 e5 c4 2a 97 ..Q.....2.g.*.
0230 - 33 b3 f6 12 a7 8e 6d c9-3c 9b 88 b3 b0 95 3e 49 3.....m.<.....>I
0240 - 53 96 b9 55 d6 2f f6 1f-e6 03 ae 40 20 77 a9 bf S..U./.....@ w..
0250 - 3e e5 5f 0c b1 59 21 8b-4b ae 22 55 7d 8f 4d 38 >...Y!..K."U}.M8
0260 - a7 43 65 83 38 c3 5e 18-64 a8 39 3e fb 1a 31 04 .Ce.8.^..d.9>..1.
0270 - 51 99 cb b7 74 0f 28 54-ec 4a 57 4f ec e4 bc 51 Q...t.(T.JW0...Q
0280 - a8 f3 06 05 b4 6f 3a 1a-48 08 1b b8 b6 1c 1c aa .....0:..H.....
0290 - 3d 27 c4 cf 56 e8 89 97-7b 88 29 e8 bb cb 6f 7a ='..V...{.)...oz
02a0 - 9c cf 40 63 70 8f 0a 2f-3d 64 95 eb 9f 1b dc 86 ..@cp.../d.....
02b0 - 0e 5c a7 d7 fe ba a4 e3-a0 04 c1 13 08 8e 38 47 .\.....8G
02c0 - ee 35 24 fc b6 50 dd 70-a2 6e 40 0f 63 8e 61 0d .5$.P.p.n@.c.a.
02d0 - 0d 0a 30 28 45 1e ed 28-47 60 e6 a2 33 1c a8 74 .0(E..(G`..3..t
02e0 - 8c 31 15 61 4c 3f cc 6e-1b 64 b8 45 b6 db 39 84 .1.aL?.n.d.E..9.
02f0 - 39 68 7a fc ca 06 32 83-9b f6 18 c9 4a 42 0c 0b 9hz...2.....JB..
0300 - b9 55 7e 02 c6 dd e2 ac-cb 8a a9 27 b6 bd 78 5b .U~.....'..x[
```

Figure 7: Running ufrec locally after editing the encrypted text file (Rubric 5)

For this I have manually edited the encrypted text file "example.txt.ufsec". I have removed a line from the encrypted data. As you can see in the first image that the user prompt and input file name are taken and then the cipher text from the file is displayed



The screenshot shows a terminal window titled '..peddi-assign2 (-zsh)'. The terminal displays a large block of hexadecimal data (ciphertext) on the left side, starting with '0120 - 9f 10 b5 02 37 74 da 6d-29 8c db 5c 4b 44 f6 62' and ending with '0430 - 08 cd e4'. On the right side, there is a large block of garbled, non-readable text, likely the result of an attempted decryption. At the bottom of the terminal, a red error message is displayed: 'Decryption failed: Not the Expected output'. Below this message, there is a line of text that reads: 'Explanations of what is happening) all of the tasks in the rubric below.' The terminal window also shows a file explorer at the bottom with the path '~/Doc/W/A/CNS/mallipeddi-assign2' and a status bar indicating 'main +1 !4 ?4' and '4s'.

Figure 8: Displaying error message that the decryption has failed after manually changing the ciphertext locally (Rubric 5).

on to the screen.

In the second image you can see that instead of the decrypted text being printed we have a message that says "Decryption Failed: Not the Expected output". This is because the encrypted text has been changed.

6. **Show Graceful error messages** As you can see on all these screenshots there are messages for every operation that is being performed.

How to Run the Code and workflow

1. A make file has been used to develop this project so run "make" on your terminal and then ufsend and ufrec are created then use the object files as you wish.

If you wish to use the -d mode then please use the following workflow:

1. Run the ./ufrec command with the desired arguments which will keep the daemon running on the specified port number.
2. Then run the ./ufsend command with the desired arguments along with the IP address and PORT number on which ./ufrec is running.
3. Please enter your password on ./ufrec.
4. Then enter your password on ./ufsend.
5. Then you can see the file being encrypted on ./ufsend and being sent to ./ufrec and it will be displayed there and it will get decrypted and ends with the plain text being displayed on the screen and writing the plain text to a file.