CNT5410 Assignment 2
Report

File encryption/decryption/transmission suite with OpenSSL

Submitted by Pankaj Nitin Warke

Abstract

The issue of theft of data is always a challenge in this internet connected life. The way information is shared between people has evolved a lot since the age of internet, which makes securing and protecting the data even more important. This assignment explores some of the ways and tools that help protect the data to a extent by encrypting it.

Contents

List of Figures

Chapter 1

Design Approach

The assignment expected a set of programs, ufsend and ufrec that work in local as well as network daemon mode. The programs are responsible for encryption and decryption of the file using the AES-256-GCM mode.

The design of the program is as per below steps

- PBKDF2 algorithm with SHA3-256(HMAC) and 4096 iterations for key generation.
- The salt is fixed in this, set to "SodiumChloride".
- IV is generated as random bytes using the RAND from OpenSSL, and is prepend to the encrypted file output.
- File encryption and decryption algorithm is AES256 in Galois Counter Mode(GCM).
- Network daemon is setup using TCP sockets, and with the help of arpa/inet.h header file.
- As per my tests program is capable of encrypting text files, image files, and machine code.
- make utility has been used to compile the programs.

Chapter 2

Introduction

2.1 Theory

2.1.1 PBKDF2

PBKDF2 is an algorithm used to derive key from given password by applying a HMAC function to the given password and additional salt. For randomised salt the same password from will have different derived key, thereby reducing the rainbow attacks.

2.1.2 AES256-GCM

AES256-GCM is an authenticated mode of encryption operation and is composed of two seperate functions, AES-CTR for encryption and GMAC for authentication. For optimal encryption it is expected that the KEY and IV pair is never reused.
The input received is

1. a Key
2. a unique IV
3. AAD, data to be processed only with authentication.
4. Data to be encrypted

It outputs the following

1. Encrypted data of input 4
2. Authentication tag

Chapter 3

Work Done

3.1 Implementation choices

3.1.1 Display patterns

- BIO_dump_fp is used at places to display encrypted and decrypted data in Hex format. The main reason was simplicity of its use.
- Error messages are printed using perror() and exit with 1 as return.
- If encrypted/decrypted file is already present the program returns 33 with appropriate message.

3.1.2 PBKDF2

- Password is taken as input from the user, whereas the salt for the purpose of this assignment is set as "SodiumChloride".
- The number of iterations is set to 4096.
- Key length is of 256 bits, and IV length is 96 bits.
- The IV is generated by using RAND_bytes() function from OpenSSL.
- Generated key is displayed in hex format.

3.1.3 Encryption AES256-GCM mode

- A total of four parameters are passed to gcm_encrypt function, key, iv and file pointers for input and output file.

- The IV is prepend to output of encrypted file.
- The number of bytes encrypted and encrypted text will be displayed after execution, however the output file will size will always be 12 bytes more than original file due to IV.

3.1.4 Decryption AES256-GCM mode

- A total of four parameters are passed to gcm_decrypt function, key, iv and file pointers for input and output file.
- The IV is extracted from the file's first 12 bytes, however it's also sent in the function call just to keep it consistent with the encrypt function.
- The number of bytes decrypted and decrypted text will be displayed after execution.

3.1.5 Network Daemon mode

- Server(ufrec) listens on the port specified from CLI argument.
- Client(ufsend) sends the encrypted file to specified IP:PORT after setting up the connection.

3.2 How to run

3.2.1 Local mode

1. Use make utility to compile both C files.

   ```
   $ make
   ```

   Refer figure 3.1.

2. Run ufsend with *filename* to be encrypted along with *-l* flag.

   ```
   $ ./ufsend filename -l
   ```

   Refer figure 3.2.

3. Enter the password for encryption. A file with the same filename as input but with *.ufsec* extension will be generated in the working directory e.g. *filename.ufsec*. Refer figure 3.2. Refer figure 3.3.

4. Remove the original plaintext file.

```
$ rm filename
```

   Refer figure 3.4.

5. Run ufrec with the filename, e.g. *filename.ufsec*, to be decrypted along with *-l* flag.

```
$ ./ufrec filename.ufsec -l
```

   Refer figure 3.5

6. Enter the password for decryption. Refer figure 3.5

7. The decrypted file will be stored without the *.ufsec* extension. Refer figure 3.6

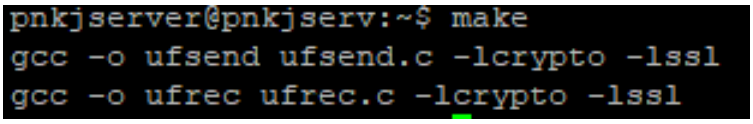

Figure 3.1: make command

```
thunder:~/cns> ./ufsend example.txt -l

Password: google
Hex password is 33A657D7B8E3514C199C673DC2A912945B689F74CAAE7077AB8085656A7CC43D
0000 - d1 9d 58 7a 12 ad ea 20-11 56 d4 be 2f b7 e1 3b   ..Xz... .V../..;
0010 - 05 49 eb 9c f3 8f b0 cc-e5 2c 7e f5 0c 39 d8 9e   .I.......,~..9..
0020 - 20 cb 0e 24 96 ef 0d ab-c1 6b 02 bd 06 d0 61 ca    ..$.....k....a.
0030 - 41 82 90 74 69 53 e3 25-f6 e4 c7 86 3a c4 47 99   A..tiS.%....:.G.
0040 - b2 16 4e 42 c7 87 2e 7e-3d 69 ae 4d 58 b8 da 88   ..NB...~=i.MX...
0050 - e9 ce 59 54 54 f3 d8 fd-ab 91 8b b5 ca 7c df bf   ..YTT........|..
0060 - 3c 6d 15 2f 67 c9 bb 49-76 75 cf 41 7d de 5c 5f   <m./g..Ivu.A}.\_
0070 - 93 72 f8 6e 39 66 53 91-10 ff d6 0a 0d e3 3a cf   .r.n9fS.......:.
0080 - 0b c3 a6 ba 49 47 93 23-74 44 dd 56 38 09 a3 0d   ....IG.#tD.V8...
0090 - 3c 8e 6d 71 ee c9 c6 b7-33 eb 7e 10 79 c8 a2 00   <.mq....3.~.y...
00a0 - 65 bd ee 92 7c c4 74 19-53 20 ed 73 9d 5e 46 b7   e...|.t.S .s.^F.
00b0 - 3c e8 65 e5 8b ee f2 f6-22 7b b2 80 5f 49 33 df   <.e....."{.._I3.
00c0 - 82 c2 58 ff 0b 32 ea a1-1d 41 d3 2d 1a 03 07 85   ..X..2...A.-....
00d0 - c0 55 06 85 6c 0d 65 ce-c2 b0 4c 48 c3 35 c8 b3   .U..l.e...LH.5..
00e0 - 00 5d 85 da a6 51 12 6b-dd 13 0b 3b 3f 70 eb 88   .]...Q.k...;?p..
00f0 - 64 ad b8 b0 13 93 29 be-8f e4 bb a6 11 51 1d 88   d.....).....Q..
0100 - 24 7a 52 27 19 8a 50 6e-53 0e d7 45 29 21 4d 62   $zR'..PnS..E)!Mb
0110 - 20 f2 18 55 02 42 f3 a4-9e f1 cb 5e 61 d2 b3 13    ..U.B.....^a...
0120 - 7a 94 23 b3 cb b5 13 df-df 42 fc 15 97 89 65 b4   z.#......B....e.
0130 - c4 7d ee 44 0c 7c 67 f8-ed 16 c8 5a 1a c8 56 b1   .}.D.|g....Z..V.
0140 - 98 0e cb c6 e6 5e cc aa-97 84 0f 81 2e 66 cc 9a   .....^.......f..
0150 - 85 15 ea f3 01 a9 c3 3d-80 27 0a 0c 6b 2e 90 f4   .......=.'..k...
0160 - 13 26 d5 79 2e f1 c3 ba-8b 1d 00 1b 14 37 91 61   .&.y.........7.a
0170 - ef 99 1f 55 26 28 6a 91-3f 60 64 2d 75 d8 0a c6   ...U&(j.?`d-u...
0180 - fb 96 73 94 8b ad 0a 05-af 74 16 5f ed 52 57 c9   ..s......t._.RW.
0190 - 8e 9e 6b 8d b1 d4 c2 62-42 97 4c 05 0a 76 f3 e5   ..k....bB.L..v..
01a0 - 1b d5 08 4e 67 c1 f7 fe-cc 8b 56 5c 8d 21 7e 8b   ...Ng.....V\.!~.
01b0 - 88 cf d5 da 34 5a 8e 87-4f 93 66 09 c2 3a a8 b8   ....4Z..O.f..:..
01c0 - c4 d4 9b 0a b2 9d 12 52-18 ea 35 10 59 ce e5 97   .......R..5.Y...
01d0 - a1 f7 22 f0 fa 14 8f ac-62 6f 83 74 f5 6a 8b 09   ....."....bo.t.j..
01e0 - c7 1c e3 31 ce e3 9a 78-8f 8f 2d 48 97 97 ee 0f   ...1...x..-H....
01f0 - 75 22 52 72 ad b4 03 1d-d8 7d d8 e7 0b c1 81 16   u"Rr.....}......
0200 - d2 9e da 2a 04 4a 82 ed-fb b3 18 15 40 18 88 e1   ...*.J......@...
0210 - 35 92 03 96 0a 5c 64 7e-2c 0b 7c 0e 2c 4a 0b 8a   5....\d~,.|.,J..
0220 - 0c c8 39 22 f0 9e 97 02-f0 b2 5f 82 08 38 01 be   ..9"......_..8..
0230 - 7f 6f ff 86 aa f4 ed ca-ed fd 97 52 31 fb 7c 2c   .o........R1.|,
0240 - d4 5d 73 fe b0 47 b7 de-b0 87 f0 c9 48 5b 61 7a   .]s..G......H[az
0250 - a1 a6 82 57 33 5e 3b a3-17 02 36 37 9f a8 3b bd   ...W3^;...67..;.
0260 - 4c 41 bf da d3 2f 6b 04-c9 f1 d9 af 36 d7 1a bb   LA.../k.....6...
0270 - f1 62 fb dd 60 57 db fd-3a 92 1a b9 1c c1 e4 25   .b..`W..:......%
0280 - f4 b9 35 4f 34 4e 3d fb-16 33 41 70 30 03 73 12   ..5O4N=..3Ap0.s.
0290 - 30 87 f0 f7 5b ff ab 61-0c ee 85 41 02 ef 13 a0   0...[..a...A....
02a0 - 09 72 72 14 1b 76 43 55-c3 b3 26 01 88 2e 9d f0   .rr..vCU..&.....
02b0 - ee 93 c3 1f 51 df f5 2f-1e 88 5a bb 86 de 77 21   ....Q../..Z...w!
02c0 - 0f de 07 11 2d e3 ef 35-22 77 14 7a 29 9e fb 7e   ....-..5"w.z)..~
02d0 - 39 2c 3d a0 e5 24 dc 08-35 c1 ed 59 80 35 65 e6   9,=..$..5..Y.5e.
02e0 - 47 60 44 6e 30 8f 80 45-ba 1a 33 05 47 e3 6d 03   G`Dn0..E..3.G.m.
02f0 - 27 f9 3f a7 81 d8 bd 75-09 87 69 0d 37 e0 e4 f0   '.?....u..i.7...
0300 - 73 fa f0 8c 9c 0a 9a 33-94 7b 6d 07 37 0c 25 7b   s......3.{m.7.%{
0310 - 52 9c b7 ec 26 ad a9 f4-b5 81 6c a0 7a bb 27 be   R...&.....l.z.'.
0320 - 25 f8 89 f6 a2 f2 e8 9e-5f e3 01 4a 54 6d 24 ee   %......._..JTm$.
0330 - d1 de bd b9 75 eb 65 bd-94 ff 4b 8e ff 03 d4 31   ....u.e...K....1
0340 - 43 58 7d 8d 32 bd 9c a7-94 46 f7 06 51 ec 21 39   CX}.2....F..Q.!9
0350 - d6 27 fb 99 b1 4c b8 0d-d4 a2 9d 02 db 7e d5 5d   .'...L.......~.]
0360 - 88 f6 b3 ea cf 31 6f d4-fe 67 3d d2 ce b6 d8 77   .....1o..g=....w
0370 - 89 0d 93 bb e9 ce 4d c8-eb 6b 67 e7 72 28 ee 27   ......M..kg.r(.'
0380 - e0 ce 53 1a dd 95 74 20-5c e0 fe ff 9f 72 ff b1   ..S...t \....r..
0390 - 6e 55 da 89 63 99 75 2c-b1 5f e9 41 6a 6e c8 dc   nU..c.u,._.Ajn..
03a0 - b5 9e 73 b9 89 24 f2 bd-00 1d 7b 79 ae cc ec 7d   ..s..$....{y...}
03b0 - db a2 f3 37 9a c6 f9 5b-8b 9d a4 d3 2f 72 69 01   ...7...[...../ri.
03c0 - ed d8 7a c4 16 9b 57 3e-d9 8b d4 d3 5a 15 ed dc   ..z...W>....Z...
03d0 - 2d 96 a6 92 bc 26 97 96-1b 5f 2a ee 9e 57 72 d3   -....&..._*..Wr.
03e0 - 95 c9 f1 22 1a ed 8e 2d-32 22 dc 30 83 bd 3c 7b   ..."...-2".0..<{
03f0 - 3e b9 57 2c 98 b0 20 0f-c8 d4 c2 87 6e a0 c9 6b   >.W,.. .....n..k
0000 - 74 8a 82 34 a1 c7 64 17-bc 1d 4e 82 30 0f f6 c8   t..4..d...N.0...
0010 - 53 0a a4 e5 c9 07 25 6b-dd c6 ba da e7 e0 3b 60   S.....%k......;`
0020 - 78 98 1e 73 0d 82 21 28-fc 09 85 f8 9d 4e e7 70   x..s..!(.....N.p
0030 - 1c e7 f2 2b 47 88 05 96-0f 5f 71 5f f1 ac 2f 38   ...+G...._q_../8
0040 - 6a 63 f4 af cf d3 01 46-09 e6 be 85 7e ef 45 93   jc.....F....~.E.
0050 - bd c6 46 4a 83 c3 f8 d3-a9 4c 4d d0 0e 75 48 1d   ..FJ.....LM..uH.
0060 - c8 51 a7 06 03 8d 89 e1-fb dd a1 06 c0 21 c4 9e   .Q...........!..
0070 - 3a 4c ad 4f 85 49 00 bc-78 c6 09 cb 52 0d 26      :L.O.I..x...R.&
1151 bytes encrypted.
thunder:~/cns>
```

Figure 3.2: ufsend local command

```
thunder:~/cns> ls
example.txt  example.txt.ufsec  makefile  ufrec  ufrec.c  ufsend  ufsend.c  warke-assign2.tgz
thunder:~/cns>
```

Figure 3.3: ufsend local files

```
thunder:~/cns> rm example.txt
```

Figure 3.4: ufsend local remove

```
thunder:~/cns> ./ufrec example.txt.ufsec -l
Password: google
Hex password is 33A657D7B8E3514C199C673DC2A912945B689F74CAAE7077AB8085656A7CC43D
0000 - 53 74 75 64 65 6e 74 73-20 77 68 6f 20 73 74 61   Students who sta
0010 - 72 74 20 74 68 65 69 72-20 68 6f 6d 65 77 6f 72   rt their homewor
0020 - 6b 20 65 61 72 6c 79 20-74 65 6e 64 20 74 6f 20   k early tend to
0030 - 64 6f 20 77 65 6c 6c 2e-0a 54 68 6f 73 65 20 77   do well..Those w
0040 - 68 6f 20 64 6f 6e 27 74-2e 2e 2e 20 77 65 6c 6c   ho don't... well
0050 - 2e 2e 2e 0a 48 61 76 65-20 79 6f 75 20 73 74 61   ....Have you sta
0060 - 72 74 65 64 20 74 68 69-6e 6b 69 6e 67 20 61 62   rted thinking ab
0070 - 6f 75 74 20 70 72 6f 6a-65 63 74 73 3f 0a 53 74   out projects?.St
0080 - 75 64 65 6e 74 73 20 77-68 6f 20 73 74 61 72 74   udents who start
0090 - 20 74 68 65 69 72 20 68-6f 6d 65 77 6f 72 6b 20    their homework
00a0 - 65 61 72 6c 79 20 74 65-6e 64 20 74 6f 20 64 6f   early tend to do
00b0 - 20 77 65 6c 6c 2e 0a 54-68 6f 73 65 20 77 68 6f    well..Those who
00c0 - 20 64 6f 6e 27 74 2e 2e-2e 20 77 65 6c 6c 2e 2e    don't... well..
00d0 - 2e 0a 48 61 76 65 20 79-6f 75 20 73 74 61 72 74   ..Have you start
00e0 - 65 64 20 74 68 69 6e 6b-69 6e 67 20 61 62 6f 75   ed thinking abou
00f0 - 74 20 70 72 6f 6a 65 63-74 73 3f 0a 53 74 75 64   t projects?.Stud
0100 - 65 6e 74 73 20 77 68 6f-20 73 74 61 72 74 20 74   ents who start t
0110 - 68 65 69 72 20 68 6f 6d-65 77 6f 72 6b 20 65 61   heir homework ea
0120 - 72 6c 79 20 74 65 6e 64-20 74 6f 20 64 6f 20 77   rly tend to do w
0130 - 65 6c 6c 2e 0a 54 68 6f-73 65 20 77 68 6f 20 64   ell..Those who d
0140 - 6f 6e 27 74 2e 2e 2e 20-77 65 6c 6c 2e 2e 2e 0a   on't... well....
0150 - 48 61 76 65 20 79 6f 75-20 73 74 61 72 74 65 64   Have you started
0160 - 20 74 68 69 6e 6b 69 6e-67 20 61 62 6f 75 74 20    thinking about
0170 - 70 72 6f 6a 65 63 74 73-3f 0a 53 74 75 64 65 6e   projects?.Studen
0180 - 74 73 20 77 68 6f 20 73-74 61 72 74 20 74 68 65   ts who start the
0190 - 69 72 20 68 6f 6d 65 77-6f 72 6b 20 65 61 72 6c   ir homework earl
01a0 - 79 20 74 65 6e 64 20 74-6f 20 64 6f 20 77 65 6c   y tend to do wel
01b0 - 6c 2e 0a 54 68 6f 73 65-20 77 68 6f 20 64 6f 6e   l..Those who don
01c0 - 27 74 2e 2e 2e 20 77 65-6c 6c 2e 2e 2e 0a 48 61   't... well....Ha
01d0 - 76 65 20 79 6f 75 20 73-74 61 72 74 65 64 20 74   ve you started t
01e0 - 68 69 6e 6b 69 6e 67 20-61 62 6f 75 74 20 70 72   hinking about pr
01f0 - 6f 6a 65 63 74 73 3f 0a-53 74 75 64 65 6e 74 73   ojects?.Students
0200 - 20 77 68 6f 20 73 74 61-72 74 20 74 68 65 69 72    who start their
0210 - 20 68 6f 6d 65 77 6f 72-6b 20 65 61 72 6c 79 20    homework early
0220 - 74 65 6e 64 20 74 6f 20-64 6f 20 77 65 6c 6c 2e   tend to do well.
0230 - 0a 54 68 6f 73 65 20 77-68 6f 20 64 6f 6e 27 74   .Those who don't
0240 - 2e 2e 2e 20 77 65 6c 6c-2e 2e 2e 0a 48 61 76 65   ... well....Have
0250 - 20 79 6f 75 20 73 74 61-72 74 65 64 20 74 68 69    you started thi
0260 - 6e 6b 69 6e 67 20 61 62-6f 75 74 20 70 72 6f 6a   nking about proj
0270 - 65 63 74 73 3f 0a 53 74-75 64 65 6e 74 73 20 77   ects?.Students w
0280 - 68 6f 20 73 74 61 72 74-20 74 68 65 69 72 20 68   ho start their h
0290 - 6f 6d 65 77 6f 72 6b 20-65 61 72 6c 79 20 74 65   omework early te
02a0 - 6e 64 20 74 6f 20 64 6f-20 77 65 6c 6c 2e 0a 54   nd to do well..T
02b0 - 68 6f 73 65 20 77 68 6f-20 64 6f 6e 27 74 2e 2e   hose who don't..
02c0 - 2e 20 77 65 6c 6c 2e 2e-2e 0a 48 61 76 65 20 79   . well....Have y
02d0 - 6f 75 20 73 74 61 72 74-65 64 20 74 68 69 6e 6b   ou started think
02e0 - 69 6e 67 20 61 62 6f 75-74 20 70 72 6f 6a 65 63   ing about projec
02f0 - 74 73 3f 0a 53 74 75 64-65 6e 74 73 20 77 68 6f   ts?.Students who
0300 - 20 73 74 61 72 74 20 74-68 65 69 72 20 68 6f 6d    start their hom
0310 - 65 77 6f 72 6b 20 65 61-72 6c 79 20 74 65 6e 64   ework early tend
0320 - 20 74 6f 20 64 6f 20 77-65 6c 6c 2e 0a 54 68 6f    to do well..Tho
0330 - 73 65 20 77 68 6f 20 64-6f 6e 27 74 2e 2e 2e 20   se who don't...
0340 - 77 65 6c 6c 2e 2e 2e 0a-48 61 76 65 20 79 6f 75   well....Have you
0350 - 20 73 74 61 72 74 65 64-20 74 68 69 6e 6b 69 6e    started thinkin
0360 - 67 20 61 62 6f 75 74 20-70 72 6f 6a 65 63 74 73   g about projects
0370 - 3f 0a 53 74 75 64 65 6e-74 73 20 77 68 6f 20 73   ?.Students who s
0380 - 74 61 72 74 20 74 68 65-69 72 20 68 6f 6d 65 77   tart their homew
0390 - 6f 72 6b 20 65 61 72 6c-79 20 74 65 6e 64 20 74   ork early tend t
03a0 - 6f 20 64 6f 20 77 65 6c-6c 2e 0a 54 68 6f 73 65   o do well..Those
03b0 - 20 77 68 6f 20 64 6f 6e-27 74 2e 2e 2e 20 77 65    who don't... we
03c0 - 6c 6c 2e 2e 2e 0a 48 61-76 65 20 79 6f 75 20 73   ll....Have you s
03d0 - 74 61 72 74 65 64 20 74-68 69 6e 6b 69 6e 67 20   tarted thinking
03e0 - 61 62 6f 75 74 20 70 72-6f 6a 65 63 74 73 3f 0a   about projects?.
03f0 - 53 74 75 64 65 6e 74 73-20 77 68 6f 20 73 74 61   Students who sta
0000 - 72 74 20 74 68 65 69 72-20 68 6f 6d 65 77 6f 72   rt their homewor
0010 - 6b 20 65 61 72 6c 79 20-74 65 6e 64 20 74 6f 20   k early tend to
0020 - 64 6f 20 77 65 6c 6c 2e-0a 54 68 6f 73 65 20 77   do well..Those w
0030 - 68 6f 20 64 6f 6e 27 74-2e 2e 2e 20 77 65 6c 6c   ho don't... well
0040 - 2e 2e 2e 0a 48 61 76 65-20 79 6f 75 20 73 74 61   ....Have you sta
0050 - 72 74 65 64 20 74 68 69-6e 6b 69 6e 67 20 61 62   rted thinking ab
0060 - 6f 75 74 20 70 72 6f 6a-65 63 74 73 3f 0a 54 69   out projects?.Ti
0070 - 6d 65 20 74 6f 20 73 74-61 72 74 20 3a 29 0a      me to start :).

1151 bytes decrypted.
```

Figure 3.5: ufsend local decrypted

```
thunder:~/cns> ls -l
total 79
-rw-r--r-- 1 pwarke grad  1151 Sep 21 13:03 example.txt
-rw-r--r-- 1 pwarke grad  1163 Sep 21 12:32 example.txt.ufsec
-rw-r--r-- 1 pwarke grad    86 Sep 21 10:14 makefile
-rwxr-xr-x 1 pwarke grad 26280 Sep 21 12:32 ufrec
-rw-r--r-- 1 pwarke grad  8158 Sep 21 10:00 ufrec.c
-rwxr-xr-x 1 pwarke grad 26248 Sep 21 12:32 ufsend
-rw-r--r-- 1 pwarke grad  7066 Sep 21 11:40 ufsend.c
-rw-r--r-- 1 pwarke grad  4032 Sep 21 12:15 warke-assign2.tgz
```

Figure 3.6: ufsend local resulting files

3.2.2 Network mode

1. Use make utility to compile both C files.

```
$ make
```

2. Run ufrec with the filename, e.g. *filename.ufsec*, to be decrypted along with *-d* flag and the *PORT*. Enter the password for encryption at client side. Refer figure 3.7

```
$ ./ufrec filename.ufsec -d 9999
```

3. Run ufsend with *filename* to be encrypted along with *-d* flag and *IP:PORT*. Refer figure 3.8

```
$ ./ufsend filename -d 192.168.0.13:9999
```

4. A file with the same filename as input but with *.ufsec* extension will be displayed in terminal and generated in the working directory e.g. *filename.ufsec*. The encrypted file along with iv bytes will be transmitted over the network to receiver/server. Refer figure 3.10

5. The encrypted file will be displayed and stored at server side. Refer figure 3.10

6. Enter the password for decryption at server side. Refer figure 3.10

7. The decrypted file will be displayed and stored without the *.ufsec* extension on the server. Refer figure 3.11

```
pnkjserver@pnkjserv:~/CN5_Assign2$ ./ufrec example.txt.ufsec -d 9999
Server socket created.
Waiting for connections.
Inbound file.
0000 - ad 0b 99 0c 40 18 cf 67-40 63 6e 70 75 5c e4 80   ....@..g@cnpu\..
0010 - 4f aa dc 80 e7 2f e1 17-b4 0e 56 d0 b1 04 1f 19   O..../....V.....
0020 - e9 a9 36 79 d7 a2 c1 c1-a0 f4 8c d3 97 be 40 2a   ..6y.........@*
0030 - 14 a3 eb 7e 27 1a 8c 04-14 78 9d 62 8c 6e 97 99   ...~'....x.b.n..
0040 - a5 b0 51 35 36 ae 83 b7-25 2a 13 80 e3 df 62 c8   ..Q56...%*....b.
0050 - 05 3b d1 cb 8f 01 44 ba-11 88 32 3e d7 63 dd 2a   .;....D...2>.c.*
0060 - 80 c2 f9 f7 5e f3 dd a7-6f 82 4f 93 1a 70 7a ef   ....^...o.O..pz.
0070 - d6 10 1b d0 0e a2 12 91-b4 1c f0 4c 44 f1 b5 5a   ...........LD..Z
0080 - fe e1 5d e2 d9 b5 e6 0c-0e 1c 8a 53 5f 82 2f aa   ..]........S_./.
0090 - a1 1a 98 58 76 0c 2c b8-44 d2 84 be 2b 85 5b c6   ...Xv.,.D...+.[.
00a0 - 07 08 2c 1e 1b 2b 7f 9f-8a ae 11 f6 0d 6f 33 b8   ..,..+.......o3.
00b0 - ac 73 07 b1 72 19 d4 25-ee 58 50 74 f9 32 76 04   .s..r..%.XPt.2v.
00c0 - 34 52 dc 09 7a d4 dd c7-0b 65 cc 46 08 39 97 95   4R..z....e.F.9..
00d0 - e9 95 64 14 6e 4e 5a e9-78 bd a1 de 16 aa aa c2   ..d.nNZ.x.......
00e0 - dc 03 05 d7 d9 66 d6 9c-32 54 da 23 b6 d6 f6 de   .....f..2T.#....
00f0 - da 5c 3a 71 59 45 71 3d-7b 9e fd b3 5d e4 c1 f4   .\:qYEq={...]...
0100 - fb fc 61 13 af 2d e1 70-88 ff 07 af 3e c5 4f 32   ..a..-.p....>.O2
0110 - 66 26 e2 e0 6c 25 57 cf-3a 38 27 31 c8 ec 19 61   f&..l%W.:8'1...a
0120 - 57 16 84 bd 30 5e aa 2e-dd 90 36 93 2b 30 59 e0   W...0^....6.+0Y.
0130 - 95 db 72 b8 72 e3 ab f4-75 a0 75 7f 1f 99 13 da   ..r.r...u.u.....
0140 - f0 49 10 dd f2 17 9f 3b-9f d8 15 02 9f db 2f c2   .I.....;....../.
0150 - e7 0e 13 6b 11 bf 01 00-41 32 a2 2f 7f 51 98 49   ...k....A2./.Q.I
0160 - 21 17 80 92 f1 fa dc e9-a5 cd 08 c5 75 f3 8e 65   !...........u..e
0170 - 9a 45 1a 88 8c ff ca b9-3b 99 a7 ce f5 5f 04 f8   .E......;....._..
0180 - 0f 84 70 77 af e0 21 9d-a4 41 9f 84 87 81 59 1a   ..pw..!..A....Y.
0190 - 72 b3 8c d2 1a d9 cb 42-95 75 9e 8e cf 02 de 82   r......B.u......
01a0 - 24 18 af 32 0d 4c 7f 28-0d 32 5c 81 c4 e5 04 44   $..2.L.(.2\....D
01b0 - 07 89 b1 3a 94 07 e8 c6-aa a4 96 82 52 2f 65 4a   ...:........R/eJ
01c0 - 42 3e e4 4e 22 9f 54 2c-c6 a9 47 9c 9c c4 4c 90   B>.N".T,..G...L.
01d0 - 93 4f 3a 3e 1d 15 3f 59-7c 4d af 78 44 8f 86 cc   .O:>..?Y|M.xD...
01e0 - 53 f9 68 8a b6 40 35 05-28 c1 41 09 bc b8 10 a6   S.h..@5.(.A.....
01f0 - fd 0d 67 25 4e ec 5a 28-6b a3 02 13 08 8d 1d 9e   ..g%N.Z(k.......
0200 - 86 91 02 ac 20 11 22 1b-e5 db 50 ad 38 41 0d 5b   .... ."...P.8A.[
0210 - e0 2d 12 ac 1d 2e 9a 9e-ef 2b a4 f6 24 b7 ca 0b   .-.......+..$...
0220 - d6 d1 ac 1b 27 aa 88 71-77 76 fc 7b 57 0b 39 3b   ....'..qwv.{W.9;
0230 - 2e 52 10 6e 7e ca d1 d1-24 d8 f0 de 96 a9 51 f2   .R.n~...$.....Q.
0240 - 77 2c 4e c9 b4 09 82 df-b3 3e 3e a2 62 8f 86 16   w,N......>>.b...
0250 - e7 93 f4 04 05 48 6d 56-6d c8 9d 72 6d 84 ef cf   .....HmVm..rm...
0260 - 3b 55 55 66 29 72 e2 9c-d4 90 8f df e9 e1 28 46   ;UUf)r........(F
0270 - 75 1b 97 7d e1 4e c6 df-cd 29 f4 09 29 56 ae 8e   u..}.N...)..)V..
0280 - 00 8c e4 16 bc 08 7c 47-f5 d2 f9 f1 ab 49 e7 40   ......|G.....I.@
0290 - a6 01 25 85 73 7d 20 6c-ce fd e2 60 2d 03 02 35   ..%.s} l...`-..5
02a0 - 9e ea 5a 0c e9 31 86 d5-cf 3f e0 64 86 03 09 f3   ..Z..1...?.d....
02b0 - 45 1e 96 9c 10 57 eb 87-af 42 97 df 5d ff 45 84   E....W...B..].E.
02c0 - 90 10 3d 9f d3 c1 a4 be-a6 a3 2c ae fe 3a a1 9a   ..=.......,..:..
02d0 - a7 6c 6a 4b 99 64 ce 78-44 11 a3 e1 61 bf 83 11   .ljK.d.xD...a...
02e0 - 1f 2f 8d 06 b1 19 bb d4-14 e6 f6 1b 7f d7 6c 87   ./............l.
02f0 - 86 ea 1b 86 9a 24 67 98-74 d5 a4 c7 0c d3 53 b7   .....$g.t.....S.
0300 - 0f 4e 97 55 3f 59 69 0d-13 f6 73 64 69 31 d2 22   .N.U?Yi...sdil."
0310 - 2b 75 26 ab 34 fc 70 45-de f4 7c 0f 08 4a b1 68   +u&.4.pE..|..J.h
0320 - f5 29 5b 5f 67 84 49 22-8a 8f c1 31 a6 6f bf c9   .)[_g.I"...1.o..
0330 - 04 8b 69 d1 53 56 61 c4-ef 0d 0a 3c e5 7c c7 35   ..i.SVa....<.|.5
0340 - 19 6b 98 c7 31 d8 3e 76-bd e8 cb cc a2 36 5b 7c   .k..1.>v.....6[|
0350 - 93 86 69 2c 7c 99 03 5a-b1 ce 9a 1e 0e 3b 9c 38   ..i,|..Z.....;.8
0360 - 7e a6 42 dd 83 d8 10 2b-02 87 17 e4 3a b6 a6 b1   ~.B....+....:...
0370 - 49 35 42 28 a2 78 fb 53-e4 62 02 b9 97 0d 7f cd   I5B(.x.S.b......
0380 - a1 42 dc 80 14 a5 10 58-1a bb b3 b7 16 18 42 77   .B.....X......Bw
0390 - 21 07 19 c9 71 9a ee b2-b4 44 73 77 75 1b 3e 30   !...q....Dswu.>0
```

Figure 3.7: Remote ufrec Inbound file

```
pnkjwrk@pnkj-virtual-machine:~/CNS_TEST_RAND$ ./ufsend example.txt -d 192.168.0.13:9999

Password: google
Hex password is 33A657D7B8E3514C199C673DC2A912945B689F74CAAE7077AB8085656A7CC43D
0000 - 75 5c e4 80 4f aa dc 80-e7 2f e1 17 b4 0e 56 d0   u\..O..../....V.
0010 - b1 04 1f 19 e9 a9 36 79-d7 a2 c1 a0 f4 8c d3   ......6y........
0020 - 97 be 40 2a 14 a3 eb 7e-27 1a 8c 04 14 78 9d 62   ..@*...~'....x.b
0030 - 8c 6e 97 99 a5 b0 51 35-36 ae 83 b7 25 2a 13 80   .n....Q56...%*..
0040 - e3 df 62 c8 05 3b d1 cb-8f 01 44 ba 11 88 32 3e   ..b..;....D...2>
0050 - d7 63 dd 2a 80 c2 f9 f7-5e f3 dd a7 6f 82 4f 93   .c.*....^...o.O.
0060 - 1a 70 7a ef d6 10 1b d0-0e a2 12 91 b4 1c f0 4c   .pz...........L
0070 - 44 f1 b5 5a fe e1 5d e2-d9 b5 e6 0c 0e 1c 8a 53   D..Z..]........S
0080 - 5f 82 2f aa a1 1a 98 58-76 0c 2c b8 44 d2 84 be   _./....Xv.,.D...
0090 - 2b 85 5b c6 07 08 2c 1e-1b 2b 7f 9f 8a ae 11 f6   +.[...,..+......
00a0 - 0d 6f 33 b8 ac 73 07 b1-72 19 d4 25 ee 58 50 74   .o3..s..r..%.XPt
00b0 - f9 32 76 04 34 52 dc 09-7a d4 dd c7 0b 65 cc 46   .2v.4R..z....e.F
00c0 - 08 39 97 95 e9 95 64 14-6e 4e 5a e9 78 bd a1 de   .9....d.nNZ.x...
00d0 - 16 aa aa c2 dc 03 05 d7-d9 66 d6 9c 32 54 da 23   .........f..2T.#
00e0 - b6 d6 f6 de da 5c 3a 71-59 45 71 3d 7b 9e fd b3   .....\:qYEq={...
00f0 - 5d e4 c1 f4 fb fc 61 13-af 2d e1 70 88 ff 07 af   ].....a..-.p....
0100 - 3e c5 4f 32 66 26 e2 e0-6c 25 57 cf 3a 38 27 31   >.O2f&..l%W.:8'1
0110 - c8 ec 19 61 57 16 84 bd-30 5e aa 2e dd 90 36 93   ...aW...0^....6.
0120 - 2b 30 59 e0 95 db 72 b8-72 e3 ab f4 75 a0 75 7f   +0Y...r.r...u.u.
0130 - 1f 99 13 da f0 49 10 dd-f2 17 9f 3b 9f d8 15 02   .....I.....;....
0140 - 9f db 2f c2 e7 0e 13 6b-11 bf 01 00 41 32 a2 2f   ../....k....A2./
0150 - 7f 51 98 49 21 17 80 92-f1 fa dc e9 a5 cd 08 c5   .Q.I!...........
0160 - 75 f3 8e 65 9a 45 1a 88-8c ff ca b9 3b 99 a7 ce   u..e.E......;...
0170 - f5 5f 04 f8 0f 84 70 77-af e0 21 9d a4 41 9f 84   ._....pw..!..A..
0180 - 87 81 59 1a 72 b3 8c d2-1a d9 cb 42 95 75 9e 8e   ..Y.r......B.u..
0190 - cf 02 de 82 24 18 af 32-0d 4c 7f 28 0d 32 5c 81   ....$..2.L.(.2\.
01a0 - c4 e5 04 44 07 89 b1 3a-94 07 e8 c6 aa a4 96 82   ...D...:........
01b0 - 52 2f 65 4a 42 3e e4 4e-22 9f 54 2c c6 a9 47 9c   R/eJB>.N".T,..G.
01c0 - 9c c4 4c 90 93 4f 3a 3e-1d 15 3f 59 7c 4d af 78   ..L..O:>..?Y|M.x
01d0 - 44 8f 86 cc 53 f9 68 8a-b6 40 35 05 28 c1 41 09   D...S.h..@5.(.A.
01e0 - bc b8 10 a6 fd 0d 67 25-4e ec 5a 28 6b a3 02 13   ......g%N.Z(k...
01f0 - 08 8d 1d 9e 86 91 02 ac-20 11 22 1b e5 db 50 ad   ........ ."...P.
0200 - 38 41 0d 5b e0 2d 12 ac-1d 2e 9a 9e ef 2b a4 f6   8A.[.-.......+..
0210 - 24 b7 ca 0b d6 d1 ac 1b-27 aa 88 71 77 76 fc 7b   $.......'..qwv.{
0220 - 57 0b 39 3b 2e 52 10 6e-7e ca d1 d1 24 d8 f0 de   W.9;.R.n~...$...
0230 - 96 a9 51 f2 77 2c 4e c9-b4 09 82 df b3 3e 3e a2   ..Q.w,N......>>.
0240 - 62 8f 86 16 e7 93 f4 04-05 48 6d 56 6d c8 9d 72   b........HmVm..r
0250 - 6d 84 ef cf 3b 55 55 66-29 72 e2 9c d4 90 8f df   m...;UUf)r.....
0260 - e9 e1 28 46 75 1b 97 7d-e1 4e c6 df cd 29 f4 09   ..(Fu..}.N...)..
0270 - 29 56 ae 8e 00 8c e4 16-bc 08 7c 47 f5 d2 f9 f1   )V........|G....
0280 - ab 49 e7 40 a6 01 25 85-73 7d 20 6c ce fd e2 60   .I.@..%.s} l...`
0290 - 2d 03 02 35 9e ea 5a 0c-e9 31 86 d5 cf 3f e0 64   -..5..Z..1...?.d
02a0 - 86 03 09 f3 45 1e 96 9c-10 57 eb 87 af 42 97 df   ....E....W...B..
02b0 - 5d ff 45 84 90 10 3d 9f-d3 c1 a4 be a6 a3 2c ae   ].E...=.......,.
02c0 - fe 3a a1 9a a7 6c 6a 4b-99 64 ce 78 44 11 a3 e1   .:...ljK.d.xD...
02d0 - 61 bf 83 11 1f 2f 8d 06-b1 19 bb d4 14 e6 f6 1b   a..../..........
02e0 - 7f d7 6c 87 86 ea 1b 86-9a 24 67 98 74 d5 a4 c7   ..l......$g.t...
02f0 - 0c d3 53 b7 0f 4e 97 55-3f 59 69 0d 13 f6 73 64   ..S..N.U?Yi...sd
0300 - 69 31 d2 22 2b 75 26 ab-34 fc 70 45 de f4 7c 0f   i1."+u&.4.pE..|.
0310 - 08 4a b1 68 f5 29 5b 5f-67 84 49 22 8a 8f c1 31   .J.h.)[_g.I"...1
0320 - a6 6f bf c9 04 8b 69 d1-53 56 61 c4 ef 0d 0a 3c   .o....i.SVa....<
0330 - e5 7c c7 35 19 6b 98 c7-31 d8 3e 76 bd e8 cb cc   .|.5.k..1.>v....
0340 - a2 36 5b 7c 93 86 69 2c-7c 99 03 5a b1 ce 9a 1e   .6[|..i,|..Z....
0350 - 0e 3b 9c 38 7e a6 42 dd-83 d8 10 2b 02 87 17 e4   .;.8~.B....+....
0360 - 3a b6 a6 b1 49 35 42 28-a2 78 fb 53 e4 62 02 b9   :...I5B(.x.S.b..
0370 - 97 0d 7f cd a1 42 dc 80-14 a5 10 58 1a bb b3 b7   .....B.....X....
0380 - 16 18 42 77 21 07 19 c9-71 9a ee b2 b4 44 73 77   ..Bw!...q....Dsw
0390 - 75 1b 3e 30 4b 12 f7 de-d0 34 85 30 b8 02 4a ac   u.>0K....4.0..J.
03a0 - eb e4 20 f2 ea f1 8d 3d-83 72 40 c4 6e 9a ac c0   .. ....=.r@.n...
```

Figure 3.8: Remote ufsend send file encrypted text

```
03b0 - f4 37 1a 2c cb a9 2d cc-3c a9 87 01 2f ee 40 56   .7.,..-.<.../.@V
03c0 - f8 35 e4 b1 cb 72 3a bc-b7 01 a9 50 58 84 90 7b   .5...r:....PX..{
03d0 - fb 26 97 df 6e 17 dc 8a-c9 26 8f fc 95 51 2d 62   .&..n....&...Q-b
03e0 - 33 b5 71 de 9e 6c 48 37-d0 27 04 db b6 18 89 5a   3.q..lH7.'.....Z
03f0 - ca 93 58 8b 00 19 23 a0-b3 53 6e 63 2d a7 5f 7f   ..X...#..Snc-._.
0000 - e4 27 bf 71 5c 3a fb 5a-64 d2 ea f8 33 f5 df 87   .'.q\:.Zd...3...
0010 - 0d ca 82 ae d9 b0 83 50-ee a3 4c d0 25 99 77 a6   .......P..L.%.w.
0020 - 04 1c 69 70 41 88 9c d7-fc 39 87 f6 09 0d 98 c0   ..ipA....9......
0030 - d7 aa f7 40 31 cd 69 de-e7 db 5f 16 a5 93 2e 10   ...@1.i..._.....
0040 - e8 fe 3c 0c 0d 08 ba f3-82 b9 e3 54 bb cf 64 a7   ..<........T..d.
0050 - de 4a 4f 11 8a c7 e6 9a-c3 e9 93 fa 1a 8b 1b 3e   .JO...........>
0060 - 04 d4 2b 42 81 f3 0d 8c-b4 34 ed 10 97 af b2 53   ..+B.....4.....S
0070 - 33 df ba 7b 2d 91 69 cf-2c 07 86 01 46 24 a5      3..{-.i.,...F$.
1151 bytes encrypted.
Transmitting to 192.168.0.13:9999
File sent successfully.
```

Figure 3.9: Remote ufsend bytes encrypted and file transmission

```
03a0 - 4b 12 f7 de d0 34 85 30-b8 02 4a ac eb e4 20 f2   K....4.0..J... .
03b0 - ea f1 8d 3d 83 72 40 c4-6e 9a ac c0 f4 37 1a 2c   ...=.r@.n....7.,
03c0 - cb a9 2d cc 3c a9 87 01-2f ee 40 56 f8 35 e4 b1   ..-.<.../.@V.5..
03d0 - cb 72 3a bc b7 01 a9 50-58 84 90 7b fb 26 97 df   .r:....PX..{.&..
03e0 - 6e 17 dc 8a c9 26 8f fc-95 51 2d 62 33 b5 71 de   n....&...Q-b3.q.
03f0 - 9e 6c 48 37 d0 27 04 db-b6 18 89 5a ca 93 58 8b   .lH7.'.....Z..X.
0000 - 00 19 23 a0 b3 53 6e 63-2d a7 5f 7f e4 27 bf 71   ..#..Snc-._..'.q
0010 - 5c 3a fb 5a 64 d2 ea f8-33 f5 df 87 0d ca 82 ae   \:.Zd...3.......
0020 - d9 b0 83 50 ee a3 4c d0-25 99 77 a6 04 1c 69 70   ...P..L.%.w...ip
0030 - 41 88 9c d7 fc 39 87 f6-09 0d 98 c0 d7 aa f7 40   A....9........@
0040 - 31 cd 69 de e7 db 5f 16-a5 93 2e 10 e8 fe 3c 0c   1.i..._.......<.
0050 - 0d 08 ba f3 82 b9 e3 54-bb cf 64 a7 de 4a 4f 11   .......T..d..JO.
0060 - 8a c7 e6 9a c3 e9 93 fa-1a 8b 1b 3e 04 d4 2b 42   ...........>..+B
0070 - 81 f3 0d 8c b4 34 ed 10-97 af b2 53 33 df ba 7b   .....4.....S3..{
0080 - 2d 91 69 cf 2c 07 86 01-46 24 a5                  -.i.,...F$.
1163 bytes downloaded.
Data written in the file example.txt.ufsec successfully.
Password: google
Hex password is 33A657D7B8E3514C199C673DC2A912945B689F74CAAE7077AB8085656A7CC43D
0000 - 53 74 75 64 65 6e 74 73-20 77 68 6f 20 73 74 61   Students who sta
0010 - 72 74 20 74 68 65 69 72-20 68 6f 6d 65 77 6f 72   rt their homewor
0020 - 6b 20 65 61 72 6c 79 20-74 65 6e 64 20 74 6f 20   k early tend to
0030 - 64 6f 20 77 65 6c 6c 2e-0a 54 68 6f 73 65 20 77   do well..Those w
0040 - 68 6f 20 64 6f 6e 27 74-2e 2e 2e 20 77 65 6c 6c   ho don't... well
0050 - 2e 2e 2e 0a 48 61 76 65-20 79 6f 75 20 73 74 61   ....Have you sta
0060 - 72 74 65 64 20 74 68 69-6e 6b 69 6e 67 20 61 62   rted thinking ab
0070 - 6f 75 74 20 70 72 6f 6a-65 63 74 73 3f 0a 53 74   out projects?.St
0080 - 75 64 65 6e 74 73 20 77-68 6f 20 73 74 61 72 74   udents who start
0090 - 20 74 68 65 69 72 20 68-6f 6d 65 77 6f 72 6b 20    their homework
00a0 - 65 61 72 6c 79 20 74 65-6e 64 20 74 6f 20 64 6f   early tend to do
00b0 - 20 77 65 6c 6c 2e 0a 54-68 6f 73 65 20 77 68 6f    well..Those who
00c0 - 20 64 6f 6e 27 74 2e 2e-2e 20 77 65 6c 6c 2e 2e    don't... well..
00d0 - 2e 0a 48 61 76 65 20 79-6f 75 20 73 74 61 72 74   ..Have you start
00e0 - 65 64 20 74 68 69 6e 6b-69 6e 67 20 61 62 6f 75   ed thinking abou
00f0 - 74 20 70 72 6f 6a 65 63-74 73 3f 0a 53 74 75 64   t projects?.Stud
0100 - 65 6e 74 73 20 77 68 6f-20 73 74 61 72 74 20 74   ents who start t
0110 - 68 65 69 72 20 68 6f 6d-65 77 6f 72 6b 20 65 61   heir homework ea
0120 - 72 6c 79 20 74 65 6e 64-20 74 6f 20 64 6f 20 77   rly tend to do w
0130 - 65 6c 6c 2e 0a 54 68 6f-73 65 20 77 68 6f 20 64   ell..Those who d
0140 - 6f 6e 27 74 2e 2e 2e 20-77 65 6c 6c 2e 2e 2e 0a   on't... well....
0150 - 48 61 76 65 20 79 6f 75-20 73 74 61 72 74 65 64   Have you started
0160 - 20 74 68 69 6e 6b 69 6e-67 20 61 62 6f 75 74 20    thinking about
0170 - 70 72 6f 6a 65 63 74 73-3f 0a 53 74 75 64 65 6e   projects?.Studen
0180 - 74 73 20 77 68 6f 20 73-74 61 72 74 20 74 68 65   ts who start the
0190 - 69 72 20 68 6f 6d 65 77-6f 72 6b 20 65 61 72 6c   ir homework earl
01a0 - 79 20 74 65 6e 64 20 74-6f 20 64 6f 20 77 65 6c   y tend to do wel
01b0 - 6c 2e 0a 54 68 6f 73 65-20 77 68 6f 20 64 6f 6e   l..Those who don
01c0 - 27 74 2e 2e 2e 20 77 65-6c 6c 2e 2e 2e 0a 48 61   't... well....Ha
01d0 - 76 65 20 79 6f 75 20 73-74 61 72 74 65 64 20 74   ve you started t
01e0 - 68 69 6e 6b 69 6e 67 20-61 62 6f 75 74 20 70 72   hinking about pr
01f0 - 6f 6a 65 63 74 73 3f 0a-53 74 75 64 65 6e 74 73   ojects?.Students
0200 - 20 77 68 6f 20 73 74 61-72 74 20 74 68 65 69 72    who start their
0210 - 20 68 6f 6d 65 77 6f 72-6b 20 65 61 72 6c 79 20    homework early
0220 - 74 65 6e 64 20 74 6f 20-64 6f 20 77 65 6c 6c 2e   tend to do well.
0230 - 0a 54 68 6f 73 65 20 77-68 6f 20 64 6f 6e 27 74   .Those who don't
0240 - 2e 2e 2e 20 77 65 6c 6c-2e 2e 2e 0a 48 61 76 65   ... well....Have
0250 - 20 79 6f 75 20 73 74 61-72 74 65 64 20 74 68 69    you started thi
0260 - 6e 6b 69 6e 67 20 61 62-6f 75 74 20 70 72 6f 6a   nking about proj
0270 - 65 63 74 73 3f 0a 53 74-75 64 65 6e 74 73 20 77   ects?.Students w
0280 - 68 6f 20 73 74 61 72 74-20 74 68 65 69 72 20 68   ho start their h
0290 - 6f 6d 65 77 6f 72 6b 20-65 61 72 6c 79 20 74 65   omework early te
02a0 - 6e 64 20 74 6f 20 64 6f-20 77 65 6c 6c 2e 0a 54   nd to do well..T
02b0 - 68 6f 73 65 20 77 68 6f-20 64 6f 6e 27 74 2e 2e   hose who don't..
```

Figure 3.10: Remote ufrec downloaded bytes and password

```
02c0 - 2e 20 77 65 6c 6c 2e 2e-2e 0a 48 61 76 65 20 79   . well....Have y
02d0 - 6f 75 20 73 74 61 72 74-65 64 20 74 68 69 6e 6b   ou started think
02e0 - 69 6e 67 20 61 62 6f 75-74 20 70 72 6f 6a 65 63   ing about projec
02f0 - 74 73 3f 0a 53 74 75 64-65 6e 74 73 20 77 68 6f   ts?.Students who
0300 - 20 73 74 61 72 74 20 74-68 65 69 72 20 68 6f 6d    start their hom
0310 - 65 77 6f 72 6b 20 65 61-72 6c 79 20 74 65 6e 64   ework early tend
0320 - 20 74 6f 20 64 6f 20 77-65 6c 6c 2e 0a 54 68 6f    to do well..Tho
0330 - 73 65 20 77 68 6f 20 64-6f 6e 27 74 2e 2e 2e 20   se who don't...
0340 - 77 65 6c 6c 2e 2e 2e 0a-48 61 76 65 20 79 6f 75   well....Have you
0350 - 20 73 74 61 72 74 65 64-20 74 68 69 6e 6b 69 6e    started thinkin
0360 - 67 20 61 62 6f 75 74 20-70 72 6f 6a 65 63 74 73   g about projects
0370 - 3f 0a 53 74 75 64 65 6e-74 73 20 77 68 6f 20 73   ?.Students who s
0380 - 74 61 72 74 20 74 68 65-69 72 20 68 6f 6d 65 77   tart their homew
0390 - 6f 72 6b 20 65 61 72 6c-79 20 74 65 6e 64 20 74   ork early tend t
03a0 - 6f 20 64 6f 20 77 65 6c-6c 2e 0a 54 68 6f 73 65   o do well..Those
03b0 - 20 77 68 6f 20 64 6f 6e-27 74 2e 2e 2e 20 77 65    who don't... we
03c0 - 6c 6c 2e 2e 2e 0a 48 61-76 65 20 79 6f 75 20 73   ll....Have you s
03d0 - 74 61 72 74 65 64 20 74-68 69 6e 6b 69 6e 67 20   tarted thinking
03e0 - 61 62 6f 75 74 20 70 72-6f 6a 65 63 74 73 3f 0a   about projects?.
03f0 - 53 74 75 64 65 6e 74 73-20 77 68 6f 20 73 74 61   Students who sta
0000 - 72 74 20 74 68 65 69 72-20 68 6f 6d 65 77 6f 72   rt their homewor
0010 - 6b 20 65 61 72 6c 79 20-74 65 6e 64 20 74 6f 20   k early tend to
0020 - 64 6f 20 77 65 6c 6c 2e-0a 54 68 6f 73 65 20 77   do well..Those w
0030 - 68 6f 20 64 6f 6e 27 74-2e 2e 2e 20 77 65 6c 6c   ho don't... well
0040 - 2e 2e 2e 0a 48 61 76 65-20 79 6f 75 20 73 74 61   ....Have you sta
0050 - 72 74 65 64 20 74 68 69-6e 6b 69 6e 67 20 61 62   rted thinking ab
0060 - 6f 75 74 20 70 72 6f 6a-65 63 74 73 3f 0a 54 69   out projects?.Ti
0070 - 6d 65 20 74 6f 20 73 74-61 72 74 20 3a 29 0a      me to start :).

1151 bytes decrypted.
pnkjserver@pnkjserv:~/CNS_Assign2$
```

Figure 3.11: Remote ufrec decrypted file size

Chapter 4

Rubrics

4.1 ”Hello” HEX symmetric key from PBKDF2

```
pnkjserver@pnkjserv:~/CNS_Assign2$ ./ufsend example.txt -l

Password: Hello
Hex password is 18F3CFE2232B51DB3A08FC56897952E6228276F6EAB57E01DD832CDBB6510159
```

Figure 4.1: hex of Hello

4.2 Hex value of encrypted file

```
pnkjwrk@pnkj-virtual-machine:~/CNS_TEST_RAND$ ./ufsend example.txt -d 192.168.0.
13:9999

Password: Hello
Hex password is 18F3CFE2232B51DB3A08FC56897952E6228276F6EAB57E01DD832CDBB6510159
0000 - 1d d7 17 73 d8 57 8a ff-24 02 4e d0 af 67 b0 29   ...s.W..$.N..g.)
0010 - fa ec 30 9d a1 fd 06 41-dd c5 94 8c 87 bf a8 72   ..0....A.......r
0020 - b2 95 28 82 fe c5 aa ea-b3 f7 7b aa d7 8f 84 f2   ..(.......{.....
0030 - 22 28 20 32 fd 3d ff a2-19 cb 25 3f 0d 72 cc 14   "( 2.=....%?.r..
0040 - 33 b1 dd 04 a4 b3 4f 5c-44 2e 04 c1 47 b0 a2 34   3.....F\D...G..4
0050 - 8e 43 d2 1d e8 b2 fc fb-02 59 77 13 2d 1d 7d 95   .C.......Yw.-.}..
0060 - 49 90 4a 34 72 4e 63 a3-c8 e2 5e bf 22 5b 06 3f   I.J4rNc...^."[.?
0070 - e9 49 27 9c 44 44 58 8d-d2 78 fd 9f 2e 74 4f d7   .I'.DDX..x...tO.
0080 - 83 12 25 97 ca 06 cb 38-2e 00 75 4d c4 b8 27 a5   ..%....8..uM..'.
0090 - df 25 71 f6 29 1e 53 4e-bc e9 01 b9 0a 0c 96 7f   .%q.).SN........
00a0 - 4d 6c 99 2f 36 6b 6c 69-e0 11 49 d8 33 66 81 eb   Ml./6kli..I.3f..
00b0 - da 35 92 a2 60 42 fb a9-10 44 e9 c4 04 ce 3e 68   .5..`B...D....>h
00c0 - 97 9a 0f 58 7f ef 0e 9d-ec 5c 53 e4 8c 54 51 d0   ...X.....\S..TQ.
00d0 - 60 c6 6b e1 c4 4e a8 10-f4 d5 22 a4 18 3d 67 c2   `.k..N...."..=g.
00e0 - 07 bb 34 b8 92 c2 33 7f-56 42 73 a5 72 b7 1f 96   ..4...3.VBs.r...
00f0 - 01 95 fb 4f 71 75 17 70-50 6c 55 57 be f9 02 e0   ...Oqu.pPlUW....
0100 - db 6a 98 b9 11 c6 05 f0-c4 83 a4 9d e3 3f 5b 7c   .j...........?[|
0110 - 1f e7 72 74 c3 2d a6 c0-e3 87 cc 20 1d cb 85 0d   ..rt.-..... ....
0120 - 16 24 40 75 0f 3e 13 0d-aa 53 50 36 57 ab ff 86   .$@u.>...SP6W...
0130 - a1 54 ec 78 fb 8e 1b e7-6d 72 38 32 20 9d 2c 42   .T.x....mr82 .,B
0140 - f6 fe 52 8b c7 1d c2 3f-2b ac 64 0d ef e5 fb fd   ..R....?+.d.....
0150 - d6 01 01 39 4e 9d 7a 16-35 df 01 c2 25 a3 c2 20   ...9N.z.5...%..
0160 - 39 5c 96 cc 5f ce f6 3c-d8 35 b9 9e 21 a7 d1 2c   9\.._..<.5..!..,
0170 - ef 81 1e 25 f5 90 0e b6-91 fb d7 f0 34 4f 1a 78   ...%........4O.x
0180 - 99 51 de 43 f0 92 a6 74-bd 6d 02 a2 4b c8 83 c7   .Q.C...t.m..K...
0190 - da f2 f2 e0 3b cd 58 3e-13 1d d4 33 e4 5d 19 ee   ....;.X>...3.]..
01a0 - a8 7f 60 55 10 a5 a9 6c-a5 fe c4 5c 57 30 b4 03   ..`U...l...\W0..
01b0 - 19 8f 72 cc 83 4f 33 b4-38 14 c8 17 9f 0e 42 24   ..r..O3.8.....B$
01c0 - 8b c4 22 ab cc 9a 2d 0b-e5 e5 8f 1c e4 01 b3 41   ..".."..-.......A
01d0 - c2 f3 32 90 76 34 18 58-5c 13 03 c8 da 56 3b 5a   ..2.v4.X\....V;Z
01e0 - c1 6d 27 4e 75 e7 19 56-1f 80 73 a6 a0 48 12 b5   .m'Nu..V..s..H..
01f0 - 5d e2 df d1 67 9d 5f c5-1f 92 fc 1b 3d ca 00 0c   ]...g._.....=...
0200 - 88 a6 ed 08 5b 33 54 7c-84 c6 63 cb 61 45 e3 8f   ....[3T|..c.aE..
0210 - 00 5e 35 b4 85 50 d2 10-2e 6e d0 62 72 5c 1c d2   .^5..P...n.br\..
0220 - 9d 96 3d ef d6 4d 06 0d-71 b7 23 df 16 a3 09 d9   ..=..M..q.#.....
0230 - c4 4f d8 98 22 f1 f1 e3-6a 3a 7a bf 08 23 b7 c4   .O.."...j:z..#..
0240 - 2b e4 bb 88 4a 1d ae 33-c2 f1 23 88 93 d3 2c 08   +...J..3..#...,.
0250 - b7 5d 3d 1b a8 26 34 41-8c fc f5 37 de 8c 70 1a   .]=..&4A...7..p.
0260 - 2a 54 d4 66 54 98 e7 0e-9c 34 ae 31 72 7b b6 6e   *T.fT....4.1r{.n
0270 - ec 7e 86 ff b9 1a 06 75-eb 2a f3 3a df 6d 00 de   .~.....u.*.:.m..
0280 - e4 1d 3f dc e9 8c 58 2f-0c be 5b 49 8a 6c 3e c8   ..?...X/..[I.l>.
0290 - 33 c4 68 87 74 8c 33 7a-89 d5 a7 5f 5d 11 4b 09   3.h.t.3z...]_K.
02a0 - 70 3f 83 c3 d3 bd 42 e3-a7 c6 58 75 ce b6 26 0c   p?....B...Xu..&.
02b0 - ab 64 2f 34 e5 1c 08 28-11 2e d2 14 86 a1 aa a5   .d/4...(........
02c0 - 40 ad b2 b2 c4 1a 4f 51-bc 6d 23 fb 7d 1b 28 b7   @.....OQ.m#.}.(.
02d0 - 01 2f 9a 86 9e 4e 4a 16-37 9f 06 42 71 31 62 45   ./...NJ.7..Bq1bE
02e0 - e2 10 71 7f b4 b7 de 73-1e a8 ea d2 b4 5f 70 07   ..q....s.....p.
02f0 - b8 75 2e b6 e1 fe c0 35-af 37 bc 30 3d d3 c8 8d   .u.....5.7.0=...
0300 - ed 6e 99 75 b2 36 db f6-9e 47 0a b3 3f 0b ee ea   .n.u.6...G..?...
0310 - fa ee 7a 70 1a 85 1a c3-c8 dd 73 a0 e7 8d 87 a2   ..zp......s.....
0320 - 77 75 73 c0 2c 71 41 e6-78 18 24 50 ae 9c 73 40   wus.,qA.x.$P..s@
0330 - 07 02 5c e6 ae d8 b1 2a-68 96 f4 b5 85 5c 5a 66   ..\....*h....\Zf
0340 - a1 ef e1 f8 b2 d5 b7 32-f9 9b c3 f2 30 a1 ad a5   .......2....0...
0350 - bc 85 99 d9 7a 06 ca 39-91 ce 6d 98 a6 f8 3e ae   ....z..9..m...>.
0360 - f1 33 62 11 15 ca 4c b9-f4 d3 35 c3 92 d5 c8 dd   .3b...L.....5.....
0370 - ec b3 3c c7 2a 61 b8 b2-ff 61 66 72 5c be ca 9a   ..<.*a...afr\...
0380 - 54 c8 4e d9 7e 43 0e 27-0a d1 83 31 dc 08 1b fd   T.N.~C.'...1....
0390 - e2 6e d2 98 31 43 c7 72-0e 7a 27 05 ae 3b 4b 97   .n..1C.r.z'..;K.
03a0 - 49 0e 1e 29 85 29 64 31-b8 02 99 01 5e e8 7d a5   I..).)d1....^.}.
03b0 - f3 ae 4d 86 ce 8f 86 f0-dd 59 2b 81 45 ab 76 e4   ..M.....Y+.E.v.
03c0 - d5 71 10 13 2d 0c 74 c9-7d 96 c3 b7 e9 ce 18 35   .q..-.t.}......5
03d0 - 6e 51 b0 55 3f 69 31 63-b7 68 dc 6b 0e 2e 50 cb   nQ.U?i1c.h.k..P.
03e0 - cb 44 60 5c 1d e8 ff 99-9c b6 76 0e 27 f7 5c 1f   .D`\......v.'.\.
03f0 - 9f c2 50 9a e5 4a 73 bd-a9 6f 31 42 3a 55 3c 5d   ..P..Js..o1B:U<]
0000 - 97 fb 84 77 88 96 20 3a-63 09 e2 28 73 a7 8a 03   ...w.. :c..(s...
0010 - 4c ad cb 0c e8 95 da 15-fe 9d c0 7f 5d 67 e2 9d   L...........]g..
0020 - bd 20 f2 0b 37 6c ea 0f-21 ee 05 35 d9 54 69 3f   . ..7l..!..5.Ti?
0030 - 07 3f f5 00 d1 df 7c b7-f7 76 f5 e3 d2 dd 80 36   .?....|..v.....6
0040 - 6d 0f 00 30 57 95 60 07-bb 59 e0 10 1b be 5a cf   m..0W.`..Y....Z.
0050 - 44 ff 8e 9b e5 05 0b b6-18 46 d2 ea d2 69 52 2c   D.......F...iR,
0060 - cf 2e d6 ef 3c 1f 78 4c-ca ae 25 c7 df 9c 8c 42   ....<.xL..%....B
0070 - 4a c2 1d 2a 24 79 57 50-e4 93 c7 55 56 b6 f5      J..*$yWP...UV..
1151 bytes encrypted.
Transmitting to 192.168.0.13:9999
File sent successfully.
pnkjwrk@pnkj-virtual-machine:~/CNS_TEST_RAND$
```

Figure 4.2: Hex of encrypted example.txt

4.3 ufdec receipt and hex of encrypted file

```
pnkjserver@pnkjserv:~/CNS_Assign2$ ./ufrec example.txt.ufsec -d 9999
Server socket created.
Waiting for connections.
Inbound file.
0000 - a8 02 29 bc cd 69 8a ea-d5 4d 21 b9 1d d7 17 73   ..)..i...M!....s
0010 - d8 57 8a ff 24 02 4e d0-af 67 b0 29 fa ec 30 9d   .W..$.N..g.)..0.
0020 - a1 fd 06 41 dd c5 94 8c-87 bf a8 72 b2 95 28 82   ...A.......r..(.
0030 - fe c5 aa ea b3 f7 7b aa-d7 8f 84 f2 22 28 20 32   ......{.....".( 2
0040 - fd 3d ff a2 19 cb 25 3f-0d 72 cc 14 33 b1 dd 04   .=....%?.r..3...
0050 - a4 b3 46 5c 44 2e 04 c1-47 b0 a2 34 8e 43 d2 1d   ..F\D...G..4.C..
0060 - e8 b2 fc fb 02 59 77 13-2d 1d 7d 95 49 90 4a 34   .....Yw.-.}.I.J4
0070 - 72 4e 63 a3 c8 e2 5e bf-22 5b 06 3f e9 49 27 9c   rNc...^."[.?.I'.
0080 - 44 44 58 8d d2 78 fd 9f-2e 74 4f d7 83 12 25 97   DDX..x...tO...%.
0090 - ca 06 cb 38 2e 00 75 4d-c4 b8 27 a5 df 25 71 f6   ...8..uM..'..%q.
00a0 - 29 1e 53 4e bc e9 01 b9-0a 0c 96 7f 4d 6c 99 2f   ).SN........Ml./
00b0 - 36 6b 6c 69 e0 11 49 d8-33 66 81 eb da 35 92 a2   6kli..I.3f...5..
00c0 - 60 42 fb a9 10 44 e9 c4-04 ce 3e 68 97 9a 0f 58   `B...D....>h...X
00d0 - 7f ef 0e 9d ec 5c 53 e4-8c 54 51 d0 60 c6 6b e1   .....\S..TQ.`.k.
00e0 - c4 4e a8 10 f4 d5 22 a4-18 3d 67 c2 07 bb 34 b8   .N....".=g...4.
00f0 - 92 c2 33 7f 56 42 73 a5-72 b7 1f 96 01 95 fb 4f   ..3.VBs.r......O
0100 - 71 75 17 70 50 6c 55 57-be f9 02 e0 db 6a 98 b9   qu.pPlUW.....j..
0110 - 11 c6 05 f0 c4 83 a4 9d-e3 3f 5b 7c 1f e7 72 74   .........?[|..rt
0120 - c3 2d a6 c0 e3 87 cc 20-1d cb 85 0d 16 24 40 75   .-..... .....$@u
0130 - 0f 3e 13 0d aa 53 50 36-57 ab ff 86 a1 54 ec 78   .>...SP6W....T.x
0140 - fb 8e 1b e7 6d 72 38 32-20 9d 2c 42 f6 fe 52 8b   ....mr82 .,B..R.
0150 - c7 1d c2 3f 2b ac 64 0d-ef e5 fb fd d6 01 01 39   ...?+.d........9
0160 - 4e 9d 7a 16 35 df 01 c2-25 a3 c2 20 39 5c 96 cc   N.z.5...%.. 9\..
0170 - 5f ce f6 3c d8 35 b9 9e-21 a7 d1 2c ef 81 1e 25   _..<.5..!.,...%
0180 - f5 90 0e b6 91 fb d7 f0-34 4f 1a 78 99 51 de 43   ........4O.x.Q.C
0190 - f0 92 a6 74 bd 6d 02 a2-4b c8 83 c7 da f2 f2 e0   ...t.m..K.......
01a0 - 3b cd 58 3e 13 1d d4 33-e4 5d 19 ee a8 7f 60 55   ;.X>...3.]....`U
01b0 - 10 a5 a9 6c a5 fe c4 5c-57 30 b4 03 19 8f 72 cc   ...l...\W0....r.
01c0 - 83 4f 33 b4 38 14 c8 17-9f 0e 42 24 8b c4 22 ab   .O3.8.....B$..".
01d0 - cc 9a 2d 0b e5 e5 8f 1c-e4 01 b3 41 c2 f3 32 90   ..-........A..2.
01e0 - 76 34 18 58 5c 13 03 c8-da 56 3b 5a c1 6d 27 4e   v4.X\....V;Z.m'N
01f0 - 75 e7 19 56 1f 80 73 a6-a0 48 12 b5 5d e2 df d1   u..V..s..H..]...
0200 - 67 9d 5f c5 1f 92 fc 1b-3d ca 00 0c 88 a6 ed 08   g._.....=.......
0210 - 5b 33 54 7c 84 c6 63 cb-61 45 e3 8f 00 5e 35 b4   [3T|..c.aE...^5.
0220 - 85 50 d2 10 2e 6e d0 62-72 5c 1c d2 9d 96 3d ef   .P...n.br\....=.
0230 - d6 4d 06 0d 71 b7 23 df-16 a3 09 d9 c4 4f d8 98   .M..q.#......O..
0240 - 22 f1 f1 e3 6a 3a 7a bf-08 23 b7 c4 2b e4 bb 88   "...j:z..#..+...
0250 - 4a 1d ae 33 c2 f1 23 88-93 d3 2c 08 b7 5d 3d 1b   J..3..#...,..]=.
0260 - a8 26 34 41 8c fc f5 37-de 8c 70 1a 2a 54 d4 66   .&4A...7..p.*T.f
0270 - 54 98 e7 0e 9c 34 ae 31-72 7b b6 6e ec 7e 86 ff   T....4.1r{.n.~..
0280 - b9 1a 06 75 eb 2a f3 3a-df 6d 00 de e4 1d 3f dc   ...u.*.:.m....?.
0290 - e9 9c 58 2f 0c be 5b 49-8a 6c 3e c8 33 c4 68 87   ..X/..[I.l>.3.h.
02a0 - 74 8c 33 7a 89 d5 a7 5f-5d 11 4b 09 70 3f 83 c3   t.3z...]_].K.p?..
02b0 - d3 bd 42 e3 a7 c6 58 75-ce b6 26 0c ab 64 2f 34   ..B...Xu..&..d/4
02c0 - e5 1c 08 28 11 2e d2 14-86 a1 aa a5 40 ad b2 b2   ...(........@...
02d0 - c4 1a 4f 51 bc 6d 23 fb-7d 1b 28 b7 01 2f 9a 86   ..OQ.m#.}.(../..
02e0 - 9e 4e 4a 16 37 9f 06 42-71 31 62 45 e2 10 71 7f   .NJ.7..Bq1bE..q.
02f0 - b4 b7 de 73 1e a8 ea d2-b4 5f 70 07 b8 75 2e b6   ...s....._p..u..
0300 - e1 fe c0 35 af 37 bc 30-3d d3 c8 8d ed 6e 99 75   ...5.7.0=....n.u
0310 - b2 36 db f6 9e 47 0a b3-3f 0b ee ea fa ee 7a 70   .6...G..?.....zp
0320 - 1a 85 1a c3 c8 dd 73 a0-e7 8d 87 a2 77 75 73 c0   ......s.....wus.
0330 - 2c 71 41 e6 78 18 24 50-ae 9c 73 40 07 02 5c e6   ,qA.x.$P..s@..\.
0340 - ae d8 b1 2a 68 96 f4 b9-85 5c 5a 66 a1 ef e1 f8   ...*h....\Zf....
0350 - b2 d5 b7 32 f9 9b c3 f2-30 a1 ad a5 bc 85 99 d9   ...2....0.......
0360 - 7a 06 ca 39 91 ce 6d 98-a6 f8 3e ae f1 33 62 11   z..9..m...>..3b.
0370 - 15 ca 4c b9 f4 d3 35 c3-92 d5 c8 dd ec b3 3c c7   ..L...5.......<.
0380 - 2a 61 b8 b2 ff 61 66 72-5c be ca 9a 54 c8 4e d9   *a...afr\...T.N.
0390 - 7e 43 0e 27 0a d1 83 31-dc 08 1b fd e2 6e d2 98   ~C.'...1.....n..
03a0 - 31 43 c7 72 0e 7a 27 05-ae 3b 4b 97 49 0e 1e 29   1C.r.z'..;K.I..)
03b0 - 85 29 64 31 b8 02 99 01-5e e8 7d a5 f3 ae 4d 86   .)d1....^.}...M.
03c0 - ce 8f 86 f0 dd 59 2b 81-45 ab 76 e4 d5 71 10 13   .....Y+.E.v..q..
03d0 - 2d 0c 74 c9 7d 96 c3 b7-e9 ce 18 35 6e 51 b0 55   -.t.}......5nQ.U
03e0 - 3f 69 31 63 b7 68 dc 6b-0e 2e 50 cb cb 44 60 5c   ?i1c.h.k..P..D`\
03f0 - 1d e8 ff 99 9c b6 76 0e-27 f7 5c 1f 9f c2 50 9a   ......v.'.\...P.
0000 - e5 4a 73 bd a9 6f 31 42-3a 55 3c 5d 97 fb 84 77   .Js..o1B:U<]...w
0010 - 88 96 20 3a 63 09 e2 28-73 a7 8a 03 4c ad cb 0c   .. :c..(s...L...
0020 - e8 95 da 15 fe 9d c0 7f-5d 67 e2 9d bd 20 f2 0b   ........]g... ..
0030 - 37 6c ea 0f 21 ee 05 35-d9 54 69 3f 07 3f f5 00   7l..!..5.Ti?.?..
0040 - d1 df 7c b7 f7 76 f5 e3-d2 dd 80 36 6d 0f 00 30   ..|..v.....6m..0
0050 - 57 95 60 07 bb 59 e0 10-1b be 5a cf 44 ff 8e 9b   W.`..Y....Z.D...
0060 - e5 05 0b b6 18 46 d2 ea-d2 69 52 2c cf 2e d6 ef   .....F...iR,....
0070 - 3c 1f 78 4c ca ae 25 c7-df 9c 8c 42 4a c2 1d 2a   <.xL..%....BJ..*
0080 - 24 79 57 50 e4 93 c7 55-56 b6 f5                  $yWP...UV..
1163 bytes downloaded.
Data written in the file example.txt.ufsec successfully.
```

Figure 4.3: Hex of received file with 12B IV

4.4 Decrypted file and value

```
Password: Hello
Hex password is 18F3CFE2232B51DB3A08FC56897952E6228276F6EAB57E01DD832CDBB6510159
0000 - 53 74 75 64 65 6e 74 73-20 77 68 6f 20 73 74 61   Students who sta
0010 - 72 74 20 74 68 65 69 72-20 68 6f 6d 65 77 6f 72   rt their homewor
0020 - 6b 20 65 61 72 6c 79 20-74 65 6e 64 20 74 6f 20   k early tend to
0030 - 64 6f 20 77 65 6c 6c 2e-0a 54 68 6f 73 65 20 77   do well..Those w
0040 - 68 6f 20 64 6f 6e 27 74-2e 2e 2e 20 77 65 6c 6c   ho don't... well
0050 - 2e 2e 2e 0a 48 61 76 65-20 79 6f 75 20 73 74 61   ....Have you sta
0060 - 72 74 65 64 20 74 68 69-6e 6b 69 6e 67 20 61 62   rted thinking ab
0070 - 6f 75 74 20 70 72 6f 6a-65 63 74 73 3f 0a 53 74   out projects?.St
0080 - 75 64 65 6e 74 73 20 77-68 6f 20 73 74 61 72 74   udents who start
0090 - 20 74 68 65 69 72 20 68-6f 6d 65 77 6f 72 6b 20    their homework
00a0 - 65 61 72 6c 79 20 74 65-6e 64 20 74 6f 20 64 6f   early tend to do
00b0 - 20 77 65 6c 6c 2e 0a 54-68 6f 73 65 20 77 68 6f    well..Those who
00c0 - 20 64 6f 6e 27 74 2e 2e-2e 20 77 65 6c 6c 2e 2e    don't... well..
00d0 - 2e 0a 48 61 76 65 20 79-6f 75 20 73 74 61 72 74   ..Have you start
00e0 - 65 64 20 74 68 69 6e 6b-69 6e 67 20 61 62 6f 75   ed thinking abou
00f0 - 74 20 70 72 6f 6a 65 63-74 73 3f 0a 53 74 75 64   t projects?.Stud
0100 - 65 6e 74 73 20 77 68 6f-20 73 74 61 72 74 20 74   ents who start t
0110 - 68 65 69 72 20 68 6f 6d-65 77 6f 72 6b 20 65 61   heir homework ea
0120 - 72 6c 79 20 74 65 6e 64-20 74 6f 20 64 6f 20 77   rly tend to do w
0130 - 65 6c 6c 2e 0a 54 68 6f-73 65 20 77 68 6f 20 64   ell..Those who d
0140 - 6f 6e 27 74 2e 2e 2e 20-77 65 6c 6c 2e 2e 2e 0a   on't... well....
0150 - 48 61 76 65 20 79 6f 75-20 73 74 61 72 74 65 64   Have you started
0160 - 20 74 68 69 6e 6b 69 6e-67 20 61 62 6f 75 74 20    thinking about
0170 - 70 72 6f 6a 65 63 74 73-3f 0a 53 74 75 64 65 6e   projects?.Studen
0180 - 74 73 20 77 68 6f 20 73-74 61 72 74 20 74 68 65   ts who start the
0190 - 69 72 20 68 6f 6d 65 77-6f 72 6b 20 65 61 72 6c   ir homework earl
01a0 - 79 20 74 65 6e 64 20 74-6f 20 64 6f 20 77 65 6c   y tend to do wel
01b0 - 6c 2e 0a 54 68 6f 73 65-20 77 68 6f 20 64 6f 6e   l..Those who don
01c0 - 27 74 2e 2e 2e 20 77 65-6c 6c 2e 2e 2e 0a 48 61   't... well....Ha
01d0 - 76 65 20 79 6f 75 20 73-74 61 72 74 65 64 20 74   ve you started t
01e0 - 68 69 6e 6b 69 6e 67 20-61 62 6f 75 74 20 70 72   hinking about pr
01f0 - 6f 6a 65 63 74 73 3f 0a-53 74 75 64 65 6e 74 73   ojects?.Students
0200 - 20 77 68 6f 20 73 74 61-72 74 20 74 68 65 69 72    who start their
0210 - 20 68 6f 6d 65 77 6f 72-6b 20 65 61 72 6c 79 20    homework early
0220 - 74 65 6e 64 20 74 6f 20-64 6f 20 77 65 6c 6c 2e   tend to do well.
0230 - 0a 54 68 6f 73 65 20 77-68 6f 20 64 6f 6e 27 74   .Those who don't
0240 - 2e 2e 2e 20 77 65 6c 6c-2e 2e 2e 0a 48 61 76 65   ... well....Have
0250 - 20 79 6f 75 20 73 74 61-72 74 65 64 20 74 68 69    you started thi
0260 - 6e 6b 69 6e 67 20 61 62-6f 75 74 20 70 72 6f 6a   nking about proj
0270 - 65 63 74 73 3f 0a 53 74-75 64 65 6e 74 73 20 77   ects?.Students w
0280 - 68 6f 20 73 74 61 72 74-20 74 68 65 69 72 20 68   ho start their h
0290 - 6f 6d 65 77 6f 72 6b 20-65 61 72 6c 79 20 74 65   omework early te
02a0 - 6e 64 20 74 6f 20 64 6f-20 77 65 6c 6c 2e 0a 54   nd to do well..T
02b0 - 68 6f 73 65 20 77 68 6f-20 64 6f 6e 27 74 2e 2e   hose who don't..
02c0 - 2e 20 77 65 6c 6c 2e 2e-2e 0a 48 61 76 65 20 79   . well....Have y
02d0 - 6f 75 20 73 74 61 72 74-65 64 20 74 68 69 6e 6b   ou started think
02e0 - 69 6e 67 20 61 62 6f 75-74 20 70 72 6f 6a 65 63   ing about projec
02f0 - 74 73 3f 0a 53 74 75 64-65 6e 74 73 20 77 68 6f   ts?.Students who
0300 - 20 73 74 61 72 74 20 74-68 65 69 72 20 68 6f 6d    start their hom
0310 - 65 77 6f 72 6b 20 65 61-72 6c 79 20 74 65 6e 64   ework early tend
0320 - 20 74 6f 20 64 6f 20 77-65 6c 6c 2e 0a 54 68 6f    to do well..Tho
0330 - 73 65 20 77 68 6f 20 64-6f 6e 27 74 2e 2e 2e 20   se who don't...
0340 - 77 65 6c 6c 2e 2e 2e 0a-48 61 76 65 20 79 6f 75   well....Have you
0350 - 20 73 74 61 72 74 65 64-20 74 68 69 6e 6b 69 6e    started thinkin
0360 - 67 20 61 62 6f 75 74 20-70 72 6f 6a 65 63 74 73   g about projects
0370 - 3f 0a 53 74 75 64 65 6e-74 73 20 77 68 6f 20 73   ?.Students who s
0380 - 74 61 72 74 20 74 68 65-69 72 20 68 6f 6d 65 77   tart their homew
0390 - 6f 72 6b 20 65 61 72 6c-79 20 74 65 6e 64 20 74   ork early tend t
03a0 - 6f 20 64 6f 20 77 65 6c-6c 2e 0a 54 68 6f 73 65   o do well..Those
03b0 - 20 77 68 6f 20 64 6f 6e-27 74 2e 2e 2e 20 77 65    who don't... we
03c0 - 6c 6c 2e 2e 2e 0a 48 61-76 65 20 79 6f 75 20 73   ll....Have you s
03d0 - 74 61 72 74 65 64 20 74-68 69 6e 6b 69 6e 67 20   tarted thinking
03e0 - 61 62 6f 75 74 20 70 72-6f 6a 65 63 74 73 3f 0a   about projects?.
03f0 - 53 74 75 64 65 6e 74 73-20 77 68 6f 20 73 74 61   Students who sta
0000 - 72 74 20 74 68 65 69 72-20 68 6f 6d 65 77 6f 72   rt their homewor
0010 - 6b 20 65 61 72 6c 79 20-74 65 6e 64 20 74 6f 20   k early tend to
0020 - 64 6f 20 77 65 6c 6c 2e-0a 54 68 6f 73 65 20 77   do well..Those w
0030 - 68 6f 20 64 6f 6e 27 74-2e 2e 2e 20 77 65 6c 6c   ho don't... well
0040 - 2e 2e 2e 0a 48 61 76 65-20 79 6f 75 20 73 74 61   ....Have you sta
0050 - 72 74 65 64 20 74 68 69-6e 6b 69 6e 67 20 61 62   rted thinking ab
0060 - 6f 75 74 20 70 72 6f 6a-65 63 74 73 3f 0a 54 69   out projects?.Ti
0070 - 6d 65 20 74 6f 20 73 74-61 72 74 20 3a 29 0a      me to start :).

1151 bytes decrypted.
pnkjserver@pnkjserv:~/CNS_Assign2$
```

Figure 4.4: Hex of decrypted file and plaintext

4.5 Modify ciphertext in local

4.5.1 Hex of encrypted file

```
pnkjserver@pnkjserv:~/CNS_Assign2$ ./ufsend example.txt -l

Password: Hello
Hex password is 18F3CFE2232B51DB3A08FC56897952E6228276F6EAB57E01DD832CDBB6510159
0000 - f7 02 10 cd 2f 6f fa 45-4f cd 2d 33 cf 33 0d cf   ..../o.EO.-3.3..
0010 - 86 8f 55 f3 f2 aa 04 e3-db 1f 3e aa 59 40 7d 9a   ..U.......>.Y@}.
0020 - b7 62 a1 db a4 f5 2d ee-65 b8 2d b2 39 b3 86 6c   .b....-.e.-.9..l
0030 - 26 94 26 d3 dc b5 8a cc-67 81 08 71 5a 72 a5 bf   &.&.....g..qZr..
0040 - 93 0d e9 87 01 b8 e3 09-ec 26 92 b2 5c b3 2a f5   .........&..\.*.
0050 - 3c 98 c4 5d ea 44 1c 93-26 77 89 2e d3 23 f4 c7   <..].D..&w...#..
0060 - 91 63 59 54 c2 41 ed a8-18 39 19 94 ba 99 80 ac   .cYT.A...9......
```

Figure 4.5: Hex of encrypted file

4.5.2 First byte of encrypted file

```
0060 - db b8 24 47 67 ac 49 50-f9 df 60 1d 03 bc e9 40   ..$Gg.IP..`....@
0070 - 4b fa 6d 4a 2a 7d c0 00-7d aa b6 d9 ab dc 2b      K.mJ*}..}.....+
1151 bytes encrypted.
pnkjserver@pnkjserv:~/CNS_Assign2$ head -c 1 example.txt.ufsec
apnkjserver@pnkjserv:~/CNS_Assign2$
```

Figure 4.6: first byte of enc file

4.5.3 Modified first byte of encrypted file

```
pnkjserver@pnkjserv:~/CNS_Assign2$ echo -ne \\xFF | dd conv=notrunc bs=1 count=1 of=example.txt.ufsec
1+0 records in
1+0 records out
1 byte copied, 6.7381e-05 s, 14.8 kB/s
pnkjserver@pnkjserv:~/CNS_Assign2$ head -c 1 example.txt.ufsec
ÿpnkjserver@pnkjserv:~/CNS_Assign2$ls
```

Figure 4.7: mod first byte of enc file

4.5.4 Attempting to decrypt

```
pnkjserver@pnkjserv:~/CNS_Assign2$ mv example.txt example.txt.bk
pnkjserver@pnkjserv:~/CNS_Assign2$ ./ufrec example.txt.ufsec -l
Password: Hello
Hex password is 18F3CFE2232B51DB3A08FC56897952E6228276F6EAB57E01DD832CDBB6510159
0000 - b1 5d df 93 9f 24 ab 49-66 1f c6 49 e2 40 a7 8b   .]...$.If..I.@..
0010 - e6 37 46 64 8a 58 11 18-62 5e 53 17 31 3d 27 f4   .7Fd.X..b^S.1='.
0020 - 92 5b 97 75 27 9e 7b 1c-33 90 36 00 cb d6 82 51   .[.u'.{.3.6....Q
0030 - 74 0f c5 17 42 16 87 18-84 78 17 b0 8e 18 84 3d   t...B....x.....=
0040 - 38 1f 7a df 2e 6c 70 86-57 28 c2 94 a7 ae 00 5e   8.z..lp.W(.....^
```

Figure 4.8: Attempt to decrypt

4.5.5 Running diff on decrypted file

```
03a0 - 6b 9e 5d 66 b1 e0 c7 a7-3b d9 2c d6 cf ac 98 d2   k.]f....;.,.....
03b0 - 7c 76 7d 15 e5 5a 7f 87-83 69 64 de a3 33 98 21   |v}..Z...id..3.!
03c0 - 64 ef 0a 9b 7c 7d aa da-1a 12 f2 df 7a 85 71 a5   d...|}......z.q.
03d0 - 8e 2a 8a 0c 3b ee d2 df-8d fa 17 65 25 c2 27 15   .*..;......e%.'.
03e0 - 73 00 4a b6 a1 42 8b f9-ac fc 24 2f f6 80 f1 d2   s.J..B....$/....
03f0 - 6e b5 72 8a c7 e4 34 14-00 ac d2 fb eb 09 42 ad   n.r...4.......B.
0000 - 2a 15 f5 30 78 d3 18 81-c0 1e db 8d af d3 a6 6a   *..0x..........j
0010 - 28 24 a1 0f 4b a1 c2 f5-59 a1 05 84 79 ba d2 42   ($..K...Y...y..B
0020 - 2c 74 df b4 5b 53 12 f3-95 c0 c0 48 ca 9f 87 68   ,t..[S.....H...h
0030 - 30 3e ad 0f bb 3d a8 da-e0 54 a0 38 b7 bd 61 5c   0>...=...T.8..a\
0040 - 53 5c 8a e2 47 50 76 ce-d1 a3 2d 7a 77 ea b7 dd   S\..GPv...-zw...
0050 - 0f f2 e6 af 2d c0 f2 47-a6 3a 2e 23 c5 76 be b1   ....-..G.:.#.v..
0060 - 00 ee f1 84 bc 61 b5 86-81 3c 0a f8 7c e2 82 fd   .....a...<..|...
0070 - 42 4a 31 95 81 17 a0 71-19 64 3d 32 de ed e4      BJ1....q.d=2...

1151 bytes decrypted.
pnkjserver@pnkjserv:~/CNS_Assign2$ diff example.txt example.txt.
diff: example.txt.: No such file or directory
pnkjserver@pnkjserv:~/CNS_Assign2$ diff example.txt example.txt.bk
Binary files example.txt and example.txt.bk differ
pnkjserver@pnkjserv:~/CNS_Assign2$
```

Figure 4.9: Decrypted gibberish

4.6 Show graceful exit codes

4.6.1 Sample output

```
pnkjwrk@pnkj-virtual-machine:~/CNS_TEST_RAND$ ls
example.txt  example.txt.ufsec  makefile  ufrec  ufrec.c  ufsend  ufsend.c
pnkjwrk@pnkj-virtual-machine:~/CNS_TEST_RAND$ ./ufrec example.txt.ufsec -l
Decrypted file exists.
: Success
pnkjwrk@pnkj-virtual-machine:~/CNS_TEST_RAND$ ./ufsend example.txt -l
Encrypted file exists.
: Success
pnkjwrk@pnkj-virtual-machine:~/CNS_TEST_RAND$
```

Figure 4.10: Exit when file already present

4.6.2 Code samples

```
        exit(1);
    }

    enc_file_fp = fopen(inFile, "r");

    int len1 = strlen(inFile);
    char* outFile = strndup(inFile, len1>=strlen(ext)?len1-strlen(ext):0);

    if(access(outFile, F_OK) == 0){
    perror("Decrypted file exists.\n");
    return 33;
}
```

Figure 4.11: Exit when decrypted already present

```
    FILE *toenc_file, *enc_file;
    toenc_file = fopen(inFile, "r");

    char *ext = ".ufsec";
    char *encfilename = strcat(inFile, ext);

    // check if encrypted file exists
    if(access(encfilename, F_OK) == 0){
        perror("Encrypted file exists.\n");
        return 33;
    }
```

Figure 4.12: Exit when encrypted file already present