Submission guidelines:

1. Please submit your write-up as a single PDF file. That file should be named in the following manner: Lastname_2.pdf   (For example: Vadrevu_2.pdf)
2. All additional scripts/programs that you write as part of your analysis should also be included. These can be given any suitable names that you like.
3. Finally put all these files into a directory that should be named as follows: Lastname_2. Please compress this directory and upload it to Moodle.
4. No submissions are allowed after the deadline.

The deadline for this assignment is 11:55 PM on March 28th, 2023 (Tuesday)

Question-1 [60 points] (Chapter-4)

¡Vamos!

After her last encryption attempt ended up as a fiasco, Alice has now learnt her lesson. She vowed not to use such weak ciphers again.

Now, Alice has another need for encryption. She needs to send some confidential material to Bob. After we covered Chapter 4, she was impressed by AES and decided to use it for this task. She knew that Oscar or for that matter, anyone isn't rich enough to be able to brute force AES-128. So, she decided to use AES-128 to keep the secret away from Bob. She did the following things:

1. Alice and Bob have already agreed upon a 128 bit secret key. (Note that this can be represented by 32 Hexadecimal characters)
2. She converted her sensitive plain text to a hexadecimal string using this encoding tool: https://codebeautify.org/string-hex-converter
3. She input the 32 digit hexadecimal key and her hexadecimal encoded text (which is the sensitive plain text) into an AES encryption system to get the encrypted text and then sent it to Bob (She used the "ECB" mode for this purpose).

Oscar who was keenly spying on Alice's network got to find out that this was the ciphertext that Alice sent to Bob:

```
E0ECE8BFB0C9854BC9916246DC1E7EC42994C78EBC0796690E7E0385FA49EA367CD829
E046538A205A27B6848E26C274FD1494A930F64E0E7BE70DDCEC6DB9CAED505D4E8F77
5E4AB8920E02B1010869A96EBBB65B6BA6D78A733735A0D890D6AF11586CB504FDCAD9
8CB1D1BAF7DA4A0F205304D1F7596AE23E9414FD2B56458CC1961C131C52524BF7B2A1
5140E943D61AA53F280340693612F8A9551D2406CE6CF66FCAB6F925BD5EB76CFB25945
740D229F0D125E6DADDFA1FACA411E93AE56DFD27F186F30DB22BC79C17594F16FE414
57D2C769EF08201B0FF91D482BF92EAA0AEE4991009C8717EFB6DC0CD0B535E38EB13E
E4AC65FCE00E82C6587FECBC9EC550DDB66587D5735B1DB78BFB8AF54F1F237D2A2EE
```

AB2B61D195105CBB6557644B2474ED96DBB918DE09D0B17DED901BE61C97A1CD3B200
A3678369FF4

But, unfortunately for Alice, there was a small security bug in the software that Alice used. The authors of the software forgot to wipe out the variables that are used for storing the sub-keys during encryption. As a result, Oscar was able to log into the same computer that Alice used and obtain the last couple of AES subkeys that were used from unused system memory. These are the keys that Oscar got:

k_{10} = F6FA49F03DBF50565D152248ABC2E463
k_{11} = E593B292D82CE2C48539C08C2EFB24EF

Given this info, will Oscar be able to find the key to decrypt Alice's cipher text? Pretend you are Oscar and try to decrypt the text. What is the text that Alice sent to Bob?

Hint: The goal should be to first obtain the key that was used. For this, you can either try to code this or do this manually. Either way, you should try to retrace the steps of the key schedule. But, it might be easier and less error-prone if you code this. Note that you don't really need two sub-keys for this problem. The tenth one is given just as a check to make sure that you are on the right path.

Hint 2: Snippets of this code might serve you as hints for you - https://gist.github.com/raullenchai/2920069 (Note that this is for AES-256 though)

Question 2. [40 points] (Chapter-5)

Chris is another friend of Alice. He began to use DES to send messages to Alice and Bob. He sent these 2 messages using all the 5 different block cipher modes.
Hello there!!!

Oops! I just realized that I am talking to Privateers. I shouldn't say 'Hello there!'. I'll say 'Ahoy, Mateys!!'
(Note that there's no new line character in the above message. It's just one long string with only spaces as the separators between words)

Unfortunately though for all the messages, Chris used the **same IV**. (Of course, ECB uses no IV and CTR uses only the first half of the IV). The key he used is also the same. Based on this information, can you figure out which of the following cipher texts corresponds to **which mode** and **which plain text message**?

Message 1:

```
95 49 c3 87 bf ec 92 ec c7 f9 5d 5f 9a 8d
```

Message 2:

```
66 bd a4 a6 da 5b 7a 1b 2d 80 70 10 00 86 82 ae
```

Message 3:

```
95 49 c3 87 bf ec 92 ec a2 f5 06 4e f4 fa
```

Message 4:

```
92 43 df 98 f1 ec af a4 c8 fe 4b 0a 9b de 0e 8e 54 2c bc 2d 77 e8 d0 dc 94 70 66 23 44 7b 3c 16 45
75 d7 53 b0 cd cc 3c 5a 5f 30 25 b1 be 1a 31 01 4d 8c 2f 7c 68 9b e1 a3 43 f9 08 26 00 ac 2c 75 73
50 07 b8 70 6f 72 77 26 5a dd c2 11 47 42 ac e8 bf ba 41 77 37 8e 17 70 77 bd af 74 6b c7 ed 13 c2
12 db 06 ec 94 33 8e d3 99 fb fb 2a 32
```

Message 5:

```
01 7a 15 22 01 eb 04 d0 4f d2 02 9a da a6 6f cc d7 14 66 a1 ec a5 db 88 7f 86 23 af 6e 18 6b ff e7
d3 f4 f6 ee 6a 74 40 76 5b 79 46 fb 05 60 a5 e4 8b e1 6b 77 53 75 cc 3b f8 f8 50 55 73 e6 d1 6c 4b
a0 7a 05 81 e6 28 66 bd a4 a6 da 5b 7a 1b 67 f0 35 76 ad ec 43 48 09 b9 72 e9 10 4a bc 76 13 b4
56 a5 6c b8 77 da 15 65 bd 10 f0 72 66 ef 01 25 6c 26 6e 8f bb f7
```

Message 6:

```
06 f0 39 5c 3d c7 6a bd a4 30 b3 07 cb 94 15 7c
```

Message 7:

```
cb a4 45 d5 8b 8e 94 76 e1 cf 52 03 51 e5 d9 3d e7 d7 2f 49 98 46 36 ec dc 98 23 dc 78 a4 71 56
1c b2 0e 37 f8 93 49 08 e7 af 77 68 ea 57 f1 17 0c 33 b2 73 27 d2 d4 5f fc 16 32 55 c6 a6 94 e2 11
41 bd ee b5 1f c0 6d 97 70 0e 04 d2 6d 11 c9 ba 15 e6 00 77 01 a3 a6 ce 4a 02 10 45 df b2 ca 11
bc 63 f6 04 40 ce 35 15 9d 5e dd ad 7f 26 95
```

Message 8:

```
cc ae 59 ca c5 8e a9 3e ee c8 44 56 50 b6
```

Message 9:

```
74 bb de cf 11 40 bf 97 1e 6b ce b8 6d 72 7f 53 b9 e3 7b b5 a0 f4 bb 96 3d 41 1a ea c5 4b 38 77 2e
de 65 e5 27 c0 d2 4c 0a 02 eb 37 4f 87 3c 6f 02 45 7a 33 1f 56 89 39 74 b6 4f f4 09 92 42 76 59 2c
9e 93 c2 b2 00 fd fe 0b c8 6e a8 06 e2 b0 1a d3 09 e0 a6 b8 2f e8 30 74 43 15 47 5c e1 a0 75 06
0d d6 d8 39 d8 65 f3 fa fe c9 09 7d 5d 03 51 7b d4 38 4b 18 d8 12
```

Message 10:

```
92 43 df 98 f1 ec af a4 8a e0 8f 2a 6f 45 2d 6a 02 8c c7 93 e3 2c a2 6f 03 98 2d d9 25 6f b5 79 92
60 d4 27 cd 55 07 90 31 02 07 83 10 df 3a bb a0 d8 d9 78 86 e8 f0 be 4f ca b3 98 5d 52 d6 a6 5a
1c 35 1b c2 d8 90 db 38 69 31 1a 10 7d 76 6e 01 c2 c8 68 45 6c 4d f1 20 b1 2f 4d d9 7a e0 55 00
c6 d0 35 8c b6 6a 6f a2 82 63 37 ef 63 f1 b3
```