Fall 2025 CIS 3362 Homework #4: DES, AES Solutions

1) Solution is attached as question1sol.c. In general, the key to the solution is to go bit by bit and turn on the appropriate bits in the output as needed. For question 4, the solution is stored in question4sol.c

2) (6 pts) The input to the expansion matrix E in DES, expressed in hexadecimal, is 3F6BD297. What is the output? Please express your answer in hexadecimal and put a little space between each group of 2 hex characters.

Convert hexadecimal to binary:

3	F	6	B	D	2	9	7
0011	1111	0110	1011	1101	0010	1001	0111

Permute bits:

32	1	2	3	4	5
1	0	0	1	1	1

4	5	6	7	8	9
1	1	1	1	1	0

8	9	10	11	12	13
1	0	1	1	0	1

12	13	14	15	16	17
0	1	0	1	1	1

16	17	18	19	20	21
1	1	1	0	1	0

20	21	22	23	24	25
1	0	0	1	0	1

24	25	26	27	28	29
0	1	0	0	1	0

28	29	30	31	32	1
1	0	1	1	1	0

Convert binary to hexadecimal:

1001	1111	1110	1011	0101	0111	1110	1010	0101	0100	1010	1110
9	F	E	B	5	7	E	A	5	4	A	E

9F EB 57 EA 54 AE

3) (8 pts) Consider a portion of a single DES round where the input (expressed in HEX) to S boxes S1, S2, S3, S4 S5, S6, S7, and S8 is 13579BDFC840. What are the 32 bits of output from the S-boxes? Express your result in binary (so 32 separate bits). (Note: Partial credit on this question will be limited for obvious reasons, so double check your answers.)

Convert hexadecimal to binary:

1	3	5	7	9	B	D	F	C	8	4	0
0001	0011	0101	0111	1001	1011	1101	1111	1100	1000	0100	0000

Group bits into groups of six:

000100 110101 011110 011011 110111 111100 100001 000000

Index into S-boxes (row, column):

S1(000100) = 13
S2(110101) = 7
S3(011110) = 8
S4(011011) = 10
S5(110111) = 9
S6(111100) = 11
S7(100001) = 6
S8(000000) = 13

Convert decimal to binary:

13	7	8	10	9	11	6	13
1101	**0111**	**1000**	**1010**	**1001**	**1011**	**0110**	**1101**

5) (8 pts) Let the state matrix to AES right before the SubBytes step be the matrix shown below. Show the state of the matrix right AFTER the SubBytes step:

Substitute bytes using S-box table:

29	76	0A	1B
8C	3D	4E	5F
A3	B7	C2	D9
E0	F5	14	68

A5	**38**	**67**	**AF**
64	**27**	**2F**	**CF**
0A	**A9**	**25**	**35**
E1	**E6**	**FA**	**45**

6) (4 pts) Let the state matrix to AES right before the ShiftRows step be your answer from problem 5. Show the state of the matrix right AFTER the ShiftRows step. (This will be graded solely based on what your answer to problem 5 was. You can get this one correct even if you got problem 5 incorrect.)

Cyclically shift each row i left i bytes:

A5	38	67	AF	Shift left 0
64	27	2F	CF	Shift left 1
0A	A9	25	35	Shift left 2
E1	E6	FA	45	Shift left 3

A5	**38**	**67**	**AF**
27	**2F**	**CF**	**64**
25	**35**	**0A**	**A9**
45	**E1**	**E6**	**FA**

7) (10 pts) Consider the process of AES Key Expansion. Imagine that we have:
w[28] = B5 2F 3C 97 (in hex)
w[31] = 1E 06 A8 4D (in hex)
Calculate w[32], showing each of the following intermediate results: RotWord(temp), SubWord(RotWord(temp)), Rcon[i/4], and the result of the XOR with Rcon[i/4].

RotWord - Cyclic shift left by one byte:

1E 06 A8 4D
06 A8 4D 1E

SubWord - Substitute bytes using S-box table:

06 A8 4D 1E
6F C2 E3 72

Rcon[i/4] - Obtain Rcon[8] from given Rcon table:

80 00 00 00

XOR - XOR result of SubWord with Rcon[8]:

  6F C2 E3 72
^ 80 00 00 00
= EF C2 E3 72

FinalResult - XOR result with w[28]:

```
  EF C2 E3 72
^ B5 2F 3C 97
= 5A ED DF E5
```

RotWord	SubWord	Rcon[i/4]	XOR	FinalResult
06 A8 4D 1E	**6F C2 E3 72**	**80 00 00 00**	**EF C2 E3 72**	**5A ED DF E5**

8) (12 pts) In class we discussed multiplication in the AES field GF(2^8) with the irreducible polynomial x^8 + x^4 + x^3 + x + 1. Based on this discussion, derive the answer for the calculation of 14 x E6. Display your final result with two hexadecimal characters.

```
  14 x E6
= 0001 0100 x 1110 0110


0000 0100 x 1110 0110
     =      1110 0110 << 2
     = 0011 1001 1000
     ^ 0010 0011 0110 (mod << 1)
     = 0001 1010 1110
     ^ 0001 0001 1011 (mod << 0)
     =      1011 0101


0001 0000 x 1110 0110
     =      1110 0110 << 4
     = 1110 0110 0000
     ^ 1000 1101 1000 (mod << 3)
     = 0110 1011 1000
     ^ 0100 0110 1100 (mod << 2)
     = 0010 1101 0100
     ^ 0010 0011 0110 (mod << 1)
     =      1110 0010
```

  1011 0101
^ 1110 0010
= 0101 0111
= **57**

9) (10 pts) Let the input to the MixCols (during AES encryption) be:

B5	34	29	06
A6	19	79	97
63	F5	4C	C2
DB	D2	FD	A3

What's the output in row 4 col 1? (The matrix by which to "multiply" is:

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

x

B5	34	29	06
A6	19	79	97
63	F5	4C	C2
DB	D2	FD	A3

= 03 x B5 + 01 x A6 + 01 x 63 + 02 x DB

```
  03 x B5
= 0011 x 1011 0101

  0001 x 1011 0101
       = 1011 0101

  0010 x 1011 0101
  =      1011 0101 << 1
  = 0001 0110 1010
  ^ 0001 0001 1011 (mod << 0)
  =      0111 0001

  1011 0101
^ 0111 0001
= 1100 0100


  01 x A6
= A6
= 1010 0110


  01 x 63
= 63
= 0110 0011


  02 x DB
= 0010 x 1101 1011
=        1101 1011 << 1
=   0001 1011 0110
^   0001 0001 1011 (mod << 0)
=        1010 1101


  1100 0100
^ 1010 0110
^ 0110 0011
^ 1010 1101
= 1010 1100
= AC
```