# ECE4802/CS4801 Assignment #2

- \* Due: 11:59 pm on April 4, 2023
- \* This assignment does not require any programming.

#### 1- DES

#### Input:

bit#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
bit	1	0	1	1	0	0	1	1	0	0	0	0	1	1	1	1	1	1	0	0	1	0	0	0	1	0	1	0	0	1	1	0

### Round Key:

bit#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
bit	0	0	1	1	0	1	1	1	0	0	0	1	1	0	1	0	1	1	0	1	1	1	1	1
bit#	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

## Permutation table

			F	)			
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

## **DES Expansion Table**

		Е	Ξ		
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

- a- Extend the input to 48 bits using DES expansion function
- b- Add (XOR) the given round key to the expanded input bits.
- c- Using 8 DES S-boxes, find the 32-bit output of substitution step. DES S-boxes are presented in the DES paper, appendix 1 (pages 17-18).
- d- Permute the S-box output using the given permutation table.

#### 2- AES

Compute the given steps below. You can use AES specification for more explanation. Show your work and present the results in a table to make it easy to follow.

- a- Convert the given 128-bit input to Hexadecimal form.
- b- Write the input in a state diagram (4 by 4 matrix).
- c- Apply SubBytes Step: use AES S-box to substitute the input.
- d- Apply ShiftRows Step.
- e- Apply Mixcolumns Step: use Irreducible polynomial  $P(x) = x^8 + x^4 + x^3 + x + 1$ .
- f- Apply AddRoundKey Step: use the given round key.

128-bit input

. 2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
. 1	0	0	0	0	0	0	0	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	0	1	1	1
3 34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
1	0	1	1	1	0	0	0	0	1	0	0	1	0	0	0	1	1	1	0	0	1	1	1	0	1	0	1	1	1	1
5 66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
0	1	1	1	0	0	1	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	1	1	1	0	1	1	0	1
7 98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
. 1	1	0	1	1	0	1	1	0	1	1	0	0	1	0	0	1	0	0	1	1	0	1	1	0	1	0	0	0	0	1
)	1 3 34 1 5 66 0	1 0 3 34 35 1 0 6 66 67 0 1	34 35 36 1 0 1 6 66 67 68 0 1 1	1 0 0 0 0 0 3 34 35 36 37 1 0 1 1 1 5 66 67 68 69 0 1 1 1 1 1 7 98 99 100 101	1 0 0 0 0 0 0 0 3 34 35 36 37 38 1 0 1 1 1 1 0 5 66 67 68 69 70 0 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 1	1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	1 0 0 0 0 0 0 0 0   3 34 35 36 37 38 39 40 41 42   1 0 1 1 1 0 0 0 0   6 66 67 68 69 70 71 72 73 74   0 1 1 1 0 0 1 1 0   7 98 99 100 101 102 103 104 105 106	1 0 0 0 0 0 0 0 0 1   3 34 35 36 37 38 39 40 41 42 43   1 0 1 1 1 0 0 0 0 1   6 66 67 68 69 70 71 72 73 74 75   0 1 1 1 0 0 1 1 0 1   7 98 99 100 101 102 103 104 105 106 107	1 0 0 0 0 0 0 0 1 1   3 34 35 36 37 38 39 40 41 42 43 44   1 0 1 1 1 0 0 0 0 1 0   6 66 67 68 69 70 71 72 73 74 75 76   0 1 1 1 0 0 1 1 0 1 0   7 98 99 100 101 102 103 104 105 106 107 108	1 0 0 0 0 0 0 0 1 1 0   3 34 35 36 37 38 39 40 41 42 43 44 45   1 0 1 1 1 0 0 0 0 1 0 0   6 66 67 68 69 70 71 72 73 74 75 76 77   0 1 1 1 0 0 1 1 0 1 1   7 98 99 100 101 102 103 104 105 106 107 108 109	1 0 0 0 0 0 0 0 1 1 0 1   3 34 35 36 37 38 39 40 41 42 43 44 45 46   1 0 1 1 1 0 0 0 0 1 0 0 1   6 66 67 68 69 70 71 72 73 74 75 76 77 78   0 1 1 1 0 0 1 1 0 1 0   7 98 99 100 101 102 103 104 105 106 107 108 109 110	1   0   0   0   0   0   0   0   1   1   0   1   0     3   34   35   36   37   38   39   40   41   42   43   44   45   46   47     1   0   1   1   1   0   0   0   0   1   0   0   1   0     6   66   67   68   69   70   71   72   73   74   75   76   77   78   79     0   1   1   1   0   0   1   1   0   1   0   0     7   98   99   100   101   102   103   104   105   106   107   108   109   110   111	1 0 0 0 0 0 0 1 1 0 1 0 1   3 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48   1 0 1 1 1 0 0 0 0 1 0 0 1 0 0   66 67 68 69 70 71 72 73 74 75 76 77 78 79 80   0 1 1 1 0 0 1 1 0 1 0 0 1   7 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112	1   0   0   0   0   0   0   1   1   0   1   0   1   1   0   1   1   0   1   1   1   1   0   1   1   1   0   1   1   0   1   0   1   0   1   0   0   0   0   1   0   0   0   0   0   0   1   0	1   0   0   0   0   0   0   1   1   0   1   0   1   1   0   1   1   0   1   1   0   1   1   0   1   1   0   1   1   0   1   1   0   1   0   0   1   0   0   0   1   0   0   0   0   1   0   0   0   0   1   0   0   0   0   1   0   0   0   0   0   1   0	1   0   0   0   0   0   0   1   1   0   1   0   1   0   1   1   0   1   1   0   0   1   1   0   1   0   1   0   1   1   0   0   1   1   0   1   0   0   0   0   1   0   0   0   0   1   0   0   0   0   1   0   0   0   0   1   0   0   0   0   1   0   0   0   0   1   1   0   0   0   1   1   0   0   0   0   1   0   0   0   0   1   1   0   0   0   0   1   0	1   0   0   0   0   0   0   0   1   1   0   1   0   1   1   0   0   1   1   0   0   1   1   0   0   1   1   0   0   1   1   0   0   0   1     3   34   35   36   37   38   39   40   41   42   43   44   45   46   47   48   49   50   51   52     1   0   1   1   0   0   0   0   1   0   0   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1 </td <td>1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 1 0</td> <td>1   0   0   0   0   0   0   1   1   0   1   0   1   1   0   1   1   0   0   1   1   0   1   1   0   0   1   0   1   0   1   1   0   0   1   0   0   1   0   0   1   0   0   0   1   0   0   0   1   0   0   0   0   1   0   0   0   0   1   0   0   0   0   0   1   0   0   0   0   1   0   0   0   0   1   0   0   0   0   0   1   0   0   0   0   1   1   0</td> <td>1   0   0   0   0   0   0   0   1   1   0   1   1   0   1   1   0   0   1   1   0   1   1   1   0   1   1   0   0   1   1   1   1   1   0   0   1   1   1   0   0   1   1   1   0   0   1   1   1   0   0   1   1   1   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   0   0   1   1   0   0   0   0   0   0   0   0   0</td> <td>1 0 0 0 0 0 0 0 0 0 1 1 1 0 1 0 1 0 1 0</td> <td>1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 1 0</td> <td>1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 0 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 1 0</td> <td>1   0   0   0   0   0   0   1   1   0   1   1   0   1   1   0   1   1   0   0   1   1   0   1   1   0   0   1   1   0   0   1   1   0   0   1   1   0   0   1   1   0   0   1   1   0   0   1   1   1   0   0   1   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   1   1   0   0   0   1   1   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0</td> <td>1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 0 1 1 0 0 1 1 0 0 1 0 0 1 1 0 0 1 1 0 0 0 1 0 0 1 1 0 0 0 1 0</td> <td>1 0 0 0 0 0 0 0 0 0 0 1 1 1 0 1 0 1 0 1</td> <td>1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 1 0</td> <td>1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 1 0</td>	1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 1 0	1   0   0   0   0   0   0   1   1   0   1   0   1   1   0   1   1   0   0   1   1   0   1   1   0   0   1   0   1   0   1   1   0   0   1   0   0   1   0   0   1   0   0   0   1   0   0   0   1   0   0   0   0   1   0   0   0   0   1   0   0   0   0   0   1   0   0   0   0   1   0   0   0   0   1   0   0   0   0   0   1   0   0   0   0   1   1   0	1   0   0   0   0   0   0   0   1   1   0   1   1   0   1   1   0   0   1   1   0   1   1   1   0   1   1   0   0   1   1   1   1   1   0   0   1   1   1   0   0   1   1   1   0   0   1   1   1   0   0   1   1   1   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   0   0   1   1   0   0   0   0   0   0   0   0   0	1 0 0 0 0 0 0 0 0 0 1 1 1 0 1 0 1 0 1 0	1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 1 0	1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 0 0 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 0 1 1 0 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 1 0	1   0   0   0   0   0   0   1   1   0   1   1   0   1   1   0   1   1   0   0   1   1   0   1   1   0   0   1   1   0   0   1   1   0   0   1   1   0   0   1   1   0   0   1   1   0   0   1   1   1   0   0   1   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   0   1   1   0   0   1   1   0   0   0   1   1   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0	1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 0 1 1 0 0 1 1 0 0 1 0 0 1 1 0 0 1 1 0 0 0 1 0 0 1 1 0 0 0 1 0	1 0 0 0 0 0 0 0 0 0 0 1 1 1 0 1 0 1 0 1	1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 1 0	1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 0 1 0 1 0

# AES S-box Table

	1								7	7							
_		0	1	2	3	4	5	6	7	8	9	a	ь	С	d	e	f
	0	63	7c	77	7ь	f2	6Ъ	6f	с5	30	01	67	2ъ	fe	d7	ab	76
	1	ca	82	с9	7d	fa	59	47	f0	ad	<b>d4</b>	a2	af	9c	a4	72	c0
	2	ь7	fd	93	26	36	3f	f7	C	34	a5	e5	f1	71	d8	31	15
	3	04	с7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	Ъ2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3Ъ	<b>d6</b>	Ъ3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5Ъ	6a	ф	be	39	4a	4c	58	cf
	6	<b>d</b> 0	ef	aa	fЪ	43	4d	33	85	45	f9	02	7f	50	3с	9f	a8
١.,	7	51	a3	40	8f	92	9d	38	f5	bc	ъ6	da	21	10	ff	f3	d2
x	8	cd	0c	13	ec	5f	97	44	17	С4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	Ъ8	14	de	5e	0Ъ	ф
	a	e0	32	3a	0a	49	06	24	5c	c2	<b>d</b> 3	ac	62	91	95	e4	79
	Ъ	e7	с8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	С	ba	78	25	2e	1c	a6	Ъ4	с6	e8	dd	74	1f	4b	bd	8Ъ	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	Ъ9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9Ъ	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	Ъ0	54	bb	16

## Round Key

bit#	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
bit	0	0	1	1	0	1	0	0	0	0	0	0	1	0	0	1	1	0	1	0	0	1	1	0	1	1	0	1	0	1	1	0
bit#	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
bit	0	1	1	1	0	1	1	0	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	1	1
bit#	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
bit	1	1	0	1	0	1	0	1	0	0	0	0	0	1	0	0	1	1	0	0	1	0	0	0	1	1	0	0	1	1	0	1
bit#	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
bit	1	1	1	1	0	0	0	1	1	0	1	1	0	1	0	1	0	1	1	1	0	0	1	0	0	1	1	1	0	0	1	0