ECE4802/CS4801 Assignment #2

* Due: 11:59 pm on Nov 16, 2018 (submit a soft copy via Canvas)
* 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	1	0	0	1	0	0	0	1	0	1	0	0	1	1	0	1	0	1	1	0	0	1	1	0	0	0	0	1	1	1	1

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	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
bit	1	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	0	1	0	1	1	0	1	1	0	0	1	0	1	1	1	0	0	1	1	1	0	1	1	1	1	0	0	0	1	0	1	1

Permutation table

P							
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

E					
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

128-bit 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	1	0	0	0	0	0	1	0	0	0	1	1	0	0	1	1	1	0	0	1	1	0	0	0	0	0	1	0	0	0	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	0	1	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	1	1	1	0	0

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	0	0	1	1	1	1	0	1	0	0	0	0	0	1	1	0	1	0	1	1	0	1	1	1	0	0	1	1	1	0	0	0

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	0	1	0	0	1	1	1	0	0	1	1	0	1	0	0	1	0	1	0	1	0	1	0	0	0	0	0	1	1	1	0

AES S-box Table

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
x	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

a- Write the given input to Hexadecimal form.
b- Write the input in a state diagram (4 by 4 matrix)
c- Use AES S-box to substitute the given input.

4-

a- Find $17^{-1}\ mod\ 43$ using Extended Euclidean Algorithm.
b- Find the inverse of x^2+1 in $GF(2^3)$ with $P(x)=x^3+x^2+1$ using Extended Euclidean Algorithm.
c- Multiply x^2+1 by x^2+x+1 in $GF(2^3)$ with $P(x)=x^3+x^2+1$.