

# ECE/CS 578 Assignment #2

\* Due: 11:59 pm on October 8, 2025 (submit via Canvas)

## 1. DES

- i. 64 bits DES input and 56-bit key are given. Apply two rounds reduced DES and find the related ciphertext. You can find the related permutation tables and S-boxes from the lecture notes or DES Standardization document (shared on Canvas - DES-fips46-3.pdf).

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

DES Key (Parity bits are removed):

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

- ii. Use the same DES key from part I and use the input below (only the red bit is different) and solve part I again. Compare the output differences from part i and part ii.

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

- iii. Use the same DES key from part I and use the input below (only the red bit is different) and solve part I again. Compare the output differences from part i, part ii and part iii.

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

## 2. AES

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

- i.
- Convert the given 128-bit input to Hexadecimal form.
  - Write the input in a state diagram (4 by 4 matrix). Hint: pay attention to the order when converting to a table.
  - Apply SubBytes Step: use AES S-box to substitute the input.
  - Apply ShiftRows Step.
  - Apply Mixcolumns Step: use Irreducible polynomial  $P(x) = x^8 + x^4 + x^3 + x + 1$ . Hint: You can use shift and XOR approach explained in class if you do not want to use finite field arithmetic.
  - Apply AddRoundKey Step: Generate and use round keys.

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

AES S-box Table

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	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
	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

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

ii. Solve part i with the following input and the same round key. Compare the output bits.

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