CS 4801: Assignment 2

Adam Camilli (aocamilli@wpi.edu)

Friday 16th November, 2018

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
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

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
bit	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

Using expansion table, we populate a new 48-bit string:

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

This extends input to

111001010001010101001101010110100110100001011111

(b) Add (XOR) the given round key to the expanded input bits.

111001010001010101001101010110100110100001011111 (Expanded input)

$\oplus$

100010110100000001011011001011100111011110001011 (Key)

011011100101010100010110011101000001111111010100

(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).

Note S-rows and columns start at zero.

Box	**Input**	**Row**	**Col**	**Sub**
S_1	011011	01 (R2)	1101 (C14)	5 (0101)
S_2	100101	11 (R4)	0010 (C3)	8 (1000)
S_3	010100	00 (R1)	1010 (C11)	6 (0110)
S_4	010110	00 (R1)	1011 (C12)	12 (1100)
S_5	011101	01 (R2)	1110 (C15)	3 (0011)
S_6	000001	01 (R2)	0000 (C1)	0 (0000)
S_7	111111	11 (R4)	1111 (C16)	13 (1101)
S_8	010100	00 (R1)	1010 (C11)	6 (0110)

This reduces output to

01011000011011000011000011010110

(d) Permute the S-box output using the given permutation table.

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

00100010000110111001000011100111

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
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

11000001 00011001 11001100 00010000 01010110 01010000 00001010 01011100
00111101 00000110 10110111 00111000 10100111 00110100 10101010 00001110

(a) Write the given input to Hexadecimal form.

> $11000001\ 00011001 \ldots 00001110_2 =$
> 0C 11 9C C1 01 59 42 97 3D 06 B7 32 29 CD 2A $8E_{16}$

(b) Write the input in a state diagram (4 by 4 matrix)

$$\begin{bmatrix} 0C & 01 & 3D & 29 \\ 11 & 59 & 06 & CD \\ 9C & 42 & B7 & 2A \\ C1 & 97 & 32 & 8E \end{bmatrix}$$

(c) Use AES S-box to substitute the given input.

$$\begin{bmatrix} 0C & 01 & 3D & 29 \\ 11 & 59 & 06 & CD \\ 9C & 42 & B7 & 2A \\ C1 & 97 & 32 & 8E \end{bmatrix} = \begin{bmatrix} S'_{0,C} & S'_{0,1} & S'_{3,D} & S'_{2,9} \\ S'_{1,1} & S'_{5,9} & S'_{0,6} & S'_{C,D} \\ S'_{9,C} & S'_{4,2} & S'_{B,7} & S'_{2,A} \\ S'_{C,1} & S'_{9,7} & S'_{3,2} & S'_{8,E} \end{bmatrix}$$

$$= \begin{bmatrix} FE & 7C & 27 & A5 \\ 82 & CB & 6F & BD \\ DE & 83 & A9 & E5 \\ BA & 88 & 23 & 19 \end{bmatrix}$$

3. -

(a) Find $17^{-1} \bmod 43$ using Extended Euclidean Algorithm

During each step s_i, recursively calculate

$$p_i = p_{i-2} - p_{i-1}q_{i-2} \bmod n$$

q_i is equal to the coefficient on the left side (bolded). Repeat until remainder is 0 and iterate right side (p calcuation) one more time.

$$\texttt{gcd}(17, 43) = 1$$

$$\therefore \exists \text{ integers } (p, n) \mid 17p = 43n + 1$$

$$\begin{array}{ll}
s_0 : \; 43 = \mathbf{2}(17) + 9 & p_0 = 0 \text{ (given)} \\
s_1 : \; 17 = \mathbf{1}(9) + 8 & p_1 = 1 \text{ (given)} \\
s_2 : \; 9 = \mathbf{1}(8) + 1 & p_2 = p_0 - p_1(q_0) \bmod 43 \\
 & \quad = 0 - 1(2) \bmod 43 = 41 \\
s_3 : \; 8 = \mathbf{8}(1) + 0 & p_3 = p_1 - p_2(q_1) \bmod 43 \\
 & \quad = 1 - 41(1) \bmod 43 = 3 \\
 & p_4 = p_2 - p_3(q_2) \bmod 43 \\
 & \quad = 41 - 3(1) \bmod 43 = \mathbf{38}
\end{array}$$

Modular inverse is **38**

(b) Find the inverse of $Q(x) = x^2 + 1$ in $GF(2^3)$ with $P(x) = x^3 + x^2 + 1$ using Extended Euclidean Algorithm.

We want to find the inverse of $Q(x)$ in the field $\dfrac{GF(2^3)}{P(x)}$, which is the same as finding a polynomial $F(x)$ such that

$$QF \equiv 1 (\mathrm{mod}\ P)$$

or equivalently

$$QF + PG = 1, G(x) \in \frac{GF(2^3)}{P(x)}$$

Using the extended Euclidean algorithm, we can back-substitute from a greatest common divisor calculation (if and only if the result is 1):

$$\begin{aligned} x^3 + x^2 + 1 &= (x+1)(x^2+1) - x \\ x^2 + 1 &= (-x)(-x) + 1 \end{aligned}$$

$$\begin{aligned} 1 &= (x^2+1) - (-x)(-x) \\ &= (x^2+1) - (-x)((x^3+x^2+1) - (x+1)(x^2+1)) \\ &= Q - (-x)(F - (x+1)(Q)) \\ &= Q - (x)(x+1)(Q) - (-x)P \\ &= (1 - (x)(x+1))Q + (x)P \\ &= (-x^2 - x + 1)Q + (x)P \\ &= (x^4 - x^4 + x^3 - x^3 + x^2 - x^2 + x - x + 1) = 1 \end{aligned}$$

This is verified by the final equation as well as the fact that the coefficient of $P(x)$ $G = x \in \dfrac{GF(2^3)}{P(x)}$.

The inverse of $Q(x)$ is therefore $\boldsymbol{-x^2 - x + 1}$.

(c) Multiply $x^2 + 1$ by $x^2 + x + 1$ in $GF(2^3)$ with $P(x) = x^3 + x^2 + 1$

Given that the multiplication is performed in a Galois field of form (2^n), this can be performed by binary multiplication of the coefficients:

$$(1)x^2 + (0)x^1 + (1)x^0 \rightarrow 101$$

$$(1)x^2 + (1)x^1 + (1)x^0 \rightarrow 111$$

$$\begin{aligned} 101 \cdot 111 &= 101 + 101 \cdot 10 + 10101 \cdot 10 \cdot 10 \\ &= 101 + 1010 + 10101 \\ &= \mathbf{11011} \end{aligned}$$

The result is

$$\mathbf{1}x^4 + \mathbf{1}x^3 + \mathbf{0}x^2 + \mathbf{1}x^1 + \mathbf{1}x^0$$