* Exercise $\underline{5}$

Problem $\underline{1}$: K_0 64 bits $\rightarrow C_0, D_0$

1	2	3	4	5	6	7	b_1
9	10	11	12	13	14	15	b_2
17	18	19	20	21	22	23	b_3
25	26	27	28	29	30	31	b_4
33	34	35	36	37	38	39	b_5
41	42	43	44	45	46	47	b_6
49	50	51	52	53	54	55	b_7
57	58	~~7~~59	60	61	62	63	b_8

C_0

$\rightarrow$ 000 1111 1 000 1 1 1 1 D_0

You can see that C_0 is all zero and D_0 is all $\underline{1}$.

$K_1 = K_2 = \dots = K_{16}$ all round keys are equal.

Encryption $DES_K(M)$ is identical to decryption

$\Rightarrow DES_K(DES_K(M)) = M$.

$K_1 = 0X\ 0101\ 0101\ 0101\ 0101$ $(C_0 = D_0 = 0)$

$K_2 = 0X\ 1F1F\ 1F1F\ 0E0E\ 0E0E$
$(C_0 = 0, D_0 = 1)$

$K_3 = 0X\ E0E0\ E0E0\ F1F1\ F1F1$
$(C_0 = 1, D_0 = 0)$

$K_4 = 0X\ FEFE\ FEFE\ FEFE\ FEFE$
$(C_0 = D_0) = 1$

Problem 2: (AES mix column)

$r = Tc$ $\qquad c = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} \in \mathbb{F}_{2^8}^4$

$r = \begin{pmatrix} r_0 \\ \vdots \\ r_3 \end{pmatrix} \in \mathbb{F}_{2^8}^4$

$$\mathbb{F}_{2^8} = \mathbb{F}_2[X] / (x^8 + x^4 + x^3 + x + 1)\, \mathbb{F}_2[X].$$

$$T = \begin{pmatrix} x & (x+1) & 1 & 1 \\ 1 & x & (x+1) & 1 \\ 1 & 1 & x & (x+1) \\ (x+1) & 1 & 1 & x \end{pmatrix}$$

$$(c_3 u^3 + c_2 u^2 + c_1 u + c_0) \cdot X$$
$$((x+1) u^3 + u^2 + u + x) \mod (u^4 + 1)$$

$$= (r_3 u^3 + r_2 u^2 + r_1 u + r_0)$$

$$-P(u) = P(u) \mod (u^4+1)$$

$$u^4 = 1 \mod (u^4+1)$$

$$\Rightarrow \quad u^5 = u \mod (u^4+1)$$

$$u^6 = u^2 \ (\mathrm{mod})(u^4+1)$$

$$(c_3u^3 + c_2u^2 + c_1u + c_0)\left((x+1)u^3 + u^2 + u + x\right)$$

$$= c_3(x+1)u^6 + c_3u^5 + c_3u^4 + c_3x\,u^3$$

$$+ c_2(x+1)u^5 + c_2u^4 + c_2u^3 + c_2x\,u^2$$

$$+ c_1(x+1)u^4 + c_1u^3 + c_1u^2 + c_1x\,u$$

$$+ c_0(x+1)u^3 + c_0u^2 + c_0u + c_0x$$

$$= u^3\big(\overbrace{c_0(x+1) + c_1 + c_2 + c_3x}^{r_3}\big)$$

$$+ u^2\big(\overbrace{c_3(x+1) + c_2x + c_1 + c_0}^{r_2}\big)$$

$$+ u\big(\overbrace{c_3 + c_2(x+1) + c_1x + c_0}^{r_1}\big)$$

$$+ \big(\overbrace{c_3 + c_2 + c_1(x+1) + c_0x}^{r_0}\big)$$