Problem 6.1

a) $m = 01110001$

$k = (k_0, k_1, k_2) = (9, 5, 3)$

~~$l_0 = 0$~~

$m = l_0 \,||\, r_0$

$l_0 = 0110$, $r_0 = 0001$

$l_1 = r_0 = 0001$

$r_1 = l_0 \oplus F(r_0, k_0)$

$= 0110 \oplus (0001 + 9)$

$= 0110 \oplus 1010$

$r_1 = 1100$ ⇐ 1st round

$l_2 = r_1 = 1100$

$r_2 = l_1 \oplus F(r_1, k_1)$

~~$= 0001 \oplus (0100 + 5)$~~

$= 0001 \oplus (1100 + 5)$

$= 0001 \oplus 0007$

$r_2 = 0000$ ⇐ 2nd round

$l_3 = r_2 = 0000$

$r_3 = l_2 \oplus F(r_2, k_2)$

$= 1100 \oplus (0000 + 3)$

$= 1100 \oplus 0007$

$r_3 = 1111$ ⇐ 3rd round

ciphertext = ~~$l_0 || r_0$~~ $(l_3 || r_3) = 00001111$ or by flipping left & right, $(r_3 || l_3) = 11110000$

b) $c = (r_3 \| l_3) = 11110000$

$l_0 = 1111$

$r_0 = 0000$

~~$k = (k_0,$~~ $k = (3, 5, 9)$ (flip the keys direction also)

$l_1 = r_0 = 0000$

$r_1 = l_0 \oplus F(r_0, k_0)$

$= 1111 \oplus (0000 + 3)$

$= 1111 \oplus 0011$

$r_1 = 1100$ ⇐ 1st round

$l_2 = r_1 = 1100$

$r_2 = l_1 \oplus F(r_1, k_1)$

$= 0000 \oplus (1100 + 5)$

$= 0000 \oplus 0001$

$r_2 = 0001$ ⇐ 2nd round

$l_3 = r_2 = 0001$

$r_3 = l_2 \oplus F(r_2, k_2)$

$= 1100 \oplus (0001 + 9)$

$= 1100 \oplus 1010$

$r_3 = 0110$ ⇐ 3rd round

Flip the direction again,

$m = (r_3 \| l_3) = 01100001$