Cavell Teng
Crypto 1
Homework 1 Part 2

Q1. A

S_0

	00	01	10	11
00	1	0	3	2
01	3	2	1	0
10	0	2	1	3
11	3	1	3	2

$S(0000) \oplus S(1111)$

$01 \oplus 10 = 11$

$0011 \oplus x^* = 0110$

$S(0011) \oplus S(0101)$

$10 \oplus 01 = 11$

$S(1110) \oplus S(1111) = 0001$ (x^*)

$11 \oplus 10 = 01$

x'

x	y	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	01	00	10	01	11	10	00	11	01	01	10	11	00	00	10	10	11
0001	11	00	10	01	11	10	00	11	01	00	11	10	01	00	10	01	00
0010	00	00	10	01	11	10	00	11	01	10	01	00	11	11	10	01	11
0011	10	00	11	01	11	10	00	11	01	11	00	01	10	00	01	01	11
0100	11	00	11	01	11	10	00	11	01	10	00	00	01	11	00	01	10
0101	01	00	10	01	11	10	00	11	01	10	00	11	10	10	01	00	11
0110	10	00	10	01	11	10	00	11	01	01	00	11	01	00	11	10	01
0111	00	00	10	01	11	10	00	11	01	10	11	11	01	01	10	11	00
1000	00	00	11	10	01	01	11	11	10	01	11	00	10	11	01	10	00
1001	11	00	11	10	01	00	01	01	00	00	10	01	11	10	00	11	01
1010	10	00	11	10	01	01	00	11	01	10	00	11	01	00	10	01	11
1011	01	00	11	10	01	11	10	10	00	11	01	10	00	01	11	00	10
1100	01	00	10	10	11	01	10	11	00	10	00	11	01	00	10	01	11
1101	11	00	10	01	00	00	11	10	01	10	00	11	01	00	10	01	11
1110	11	00	01	10	00	01	10	11	00	01	11	00	10	11	01	10	00
1111	10	00	01	01	11	11	00	01	10	10	00	11	01	00	10	01	11

B.

y'

x'	00	01	10	11
0000	16	0	0	0
0001	0	2	10	4
0010	0	10	6	0
0011	2	4	0	10
0100	2	4	8	2
0101	10	0	4	2
0110	0	2	2	12
0111	4	10	2	0
1000	2	4	8	2
1001	8	2	2	4
1010	4	2	2	8
1011	2	8	4	2
1100	8	2	2	4
1101	2	4	8	2
1110	2	8	4	2
1111	4	2	2	8

$x = 1110, 1111$ $x^* = 1111, 1110$

$x \oplus x^* = 0001$

$S(x) \oplus S(x^*) = 01$

(x, x^*) such that $x \oplus x^* = x'$

Decide on an x' with multiple input pairs. Run that input pair through to determine the output of the input pair. Look through table A to create a list of inputs of x' that generates the received output. XOR x and x^* with each value on that list to generate a list of possible keys. Repeat process and ... keys until there is only possible key left.

Q2. $P = \{a, b, c\}$ w/ $P_p(a) = 1/3$ $P_p(b) = 1/6$ $P_p(c) = 1/2$

$K = (k_1, k_2, k_3)$ w/ $P_k(k_1) = 1/2$ $P_k(k_2) = 1/4$ $P_k(k_3) = 1/4$

$C = (1, 2, 3, 4)$

$e_{k_1}(a) = 1$ $e_{k_1}(b) = 2$ $e_{k_1}(c) = 2$

$e_{k_2}(a) = 2$ $e_{k_2}(b) = 3$ $e_{k_2}(c) = 1$

$e_{k_3}(a) = 3$ $e_{k_3}(b) = 4$ $e_{k_3}(c) = 4$

$H(K|C) = ???$

$= H(K) + H(P) - H(C)$

$H(P) = \frac{1}{3}\log_2 3 + \frac{1}{6}\log_2 6 + \frac{1}{2}\log_2 2 = 1.459$

$H(K) = \frac{1}{2}\log_2 2 + \frac{1}{4}\log_2 4 + \frac{1}{4}\log_2 4 = 1.5$

$P_r(y=1) = \frac{1}{2}\cdot\frac{1}{3} + \frac{1}{4}\cdot\frac{1}{2} = \frac{1}{6} + \frac{1}{8} = \frac{7}{24}$

$P_r(y=2) = \frac{1}{2}\left(\frac{1}{6} + \frac{1}{2}\right) + \frac{1}{4}\left(\frac{1}{3}\right) = \frac{1}{3} + \frac{1}{12} = \frac{5}{12}$

$P_r(y=3) = \frac{1}{4}\left(\frac{1}{6}\right) + \frac{1}{4}\left(\frac{1}{3}\right) = \frac{1}{24} + \frac{1}{12} = \frac{1}{8}$

$P_r(y=4) = \frac{1}{4}\left(\frac{1}{6} + \frac{1}{2}\right) = \frac{1}{6}$

$H(C) = -\frac{7}{24}\log_2\left(\frac{7}{24}\right) - \frac{5}{12}\log\left(\frac{5}{12}\right) - \frac{1}{8}\log\left(\frac{1}{8}\right) - \frac{1}{6}\log(1/6)$

$H(K|C) = 1.108$