Samad Farooqui 1/23/2018 Crypto HW1

Q1: We are following the dc. tex to get possible values of the key from S_0. Our inputs are chosen to be 0 and 3 that XOR's to 3 and also outputs XOR to 3.

$3' \to 3: 0, 1, 2, 3$

Using the fact that $S1'_I = S1_I \oplus S1^*_I$

$= (S1_E \oplus S1_k) \oplus (S1^*_E \oplus S1_k)$

$= S1_E \oplus S1^*_E$

$= S1'_E$

$S1_I = S1_E \oplus S1_k$

$0 \oplus 0 = 0$	$0 \oplus 3 = 3$
$1 \oplus 0 = 1$	$1 \oplus 3 = 2$
$2 \oplus 0 = 2$	$2 \oplus 3 = 1$
$3 \oplus 0 = 3$	$3 \oplus 3 = 0$

So the possible keys are $\{0, 1, 2, 3\}$.

The other inputs are 2, 1 that XOR to 3, and that produces the same possible key values.

Therefore, the possible keys are $\{0, 1, 2, 3\}$

Q2 : $H(K|C) = H(K) + H(P) - H(C)$

- $P = \{a, b, c\}$ w/ $P_p(a) = 1/3$ $P_p(b) = 1/6$, $P_p(c) = 1/2$
- $K = (k_1, k_2, k_3)$ with $P_K(k_1) = 1/2$ $P_K(k_2) = 1/4$ $P_K(k_3) = 1/4$
- $C = \{1, 2, 3, 4\}$

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

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

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

We can compute prob. dist P_C.

$P_C(1) = 1/6 + 1/8 = 7/24$

$P_C(2) = 1/12 + 1/12 + 1/4 = 5/12$

$P_C(3) = 1/12 + 1/24 = 1/8$

$P_C(4) = 1/24 + 1/8 = 1/6$

We can now use the fact $H(X) = -\sum_{i=1}^{n} p(X = x_i) \log_2 p(X = x_i)$ to find $H(P)$, $H(K)$, and $H(C)$.

$H(P) = -(1/3 \log_2 1/3 + 1/6 \log_2 1/6 + 1/2 \log_2 1/2) = 1.459$

$H(K) = -(1/2 \log_2 1/2 + 1/4 \log_2 1/4 + 1/4 \log 1/4) = 1.5$

$H(C) = -(7/24 \log_2 7/24 + 5/12 \log_2 5/12 + 1/8 \log_2 1/8 + 1/6 \log_2 1/6) = 1.851$

According to the slides, $H(K|C) = H(K) + H(P) - H(C)$

$= 1.459 + 1.5 - 1.851 = \underline{1.108}$