CSCI 4230: Cryptography and Network Security I Homework #1b Q2

Colin Goldberg

Due Monday, September 24, 2018

Q2: [25pnts] Consider the crypto system below and compute H(K|C)

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

  $e_{k_1}(a) = 1$ $e_{k_1}(b) = 2$ $e_{k_1}(c) = 2$
  $e_{k_2}(a) = 2$ $e_{k_2}(b) = 3$ $e_{k_2}(c) = 1$
  $e_{k_3}(a) = 3$ $e_{k_3}(b) = 4$ $e_{k_3}(c) = 4$

Answers:

- $H(k_1|c_1) = \frac{P(k_1 \cap c_1)}{P(c_1)} = \frac{\frac{1}{2}\frac{1}{3}}{\frac{1}{2}\frac{1}{3}+\frac{1}{4}\frac{1}{2}} = \frac{4}{7}$
- $H(k_2|c_1) = \frac{\frac{1}{8}}{\frac{1}{8}+\frac{1}{6}} = \frac{3}{7}$
- $H(k_3|C_1) = 0$
- $H(k_1|C_2) = \frac{\frac{1}{12}+\frac{1}{4}}{\frac{1}{12}+\frac{1}{4}+\frac{1}{12}} = \frac{4}{5}$
- $H(k_2|C_2) = 1 - H(k_1|C_2) = \frac{1}{5}$
- $H(k_3|C_2) = 0$
- $H(k_1|C_3) = 0$
- $H(k_2|C_3) = \frac{\frac{1}{24}}{\frac{1}{24}+\frac{1}{12}} = \frac{1}{3}$
- $H(k_3|C_3) = 1 - H(k_2|C_3) = \frac{2}{3}$
- $H(k_1|C_4) = 0$
- $H(k_1|C_4) = 0$
- $H(k_1|C_4) = 1$