ECE: Information and Network Security
Homework 5 Solutions
Spring 2006

Chapter 15:

2. (a) There are four possible outcomes: HH, HT, TH, and TT. The probabilities are

$$\begin{aligned} p(HH) &= p^2 \\ p(HT) &= p(1-p) \\ p(TH) &= p(1-p) \\ p(TT) &= (1-p)^2 \end{aligned}$$

(b) The entropy is

$$-\left(p^2 \log_2 p^2 + 2p(1-p)\log_2(p(1-p)) + (1-p)^2 \log_2(1-p)^2\right).$$

By expanding and manipulating this can be expressed as $-2p\log_2 p - 2(1-p)\log_2(1-p)$. This could have been calculated easier using the fact that $H(X,Y) = H(X) + H(Y)$ when X and Y are independent. Now observe that when X and Y are independent flips of the unfair coin, that $H(X,Y) = 2H(X) = -2p\log_2 p - 2(1-p)\log_2(1-p)$.

5. (a) $Y = 2^X$, so the possible outcomes for Y are 1/4, 1/2, 0, 2, and 4. The probabilities for Y are the same as the probabilities for X. Since the entropy only uses the probabilities, $H(X) = H(Y)$.

(b) Observe that the possible outcomes for Y are 4, 1, and 0. In particular, two elements of X get mapped to $Y = 4$ and two elements get mapped to $Y = 1$. Since x^2 is not a one-to-one function, we have $H(Y) \leq H(X)$.

9. (a) The plaintext entropy is

$$H(P) = -\left(\frac{1}{3}\log_2\frac{1}{3} + \frac{2}{3}\log_2\frac{2}{3}\right).$$

(b) Observe that this system matches up with the one-time pad, and hence $H(P|C) = H(P)$.

10. (a) $H(P,K) = H(C,P,K)$ since knowledge of the plaintext and the key determine the ciphertext. $H(P,K) = H(P) + H(K)$ since the keys are chosen independently of the plaintext in a cryptosystem.

(b) $H(C,P) = H(C) + H(P|C)$ by the Chain Rule. Since we have perfect secrecy, $H(P|C) = H(P)$, and thus $H(C,P) = H(C) + H(P)$. For the last part, refer to the solution to problem 14.11 to get $H(C|P) = H(K) - H(K|C,P)$. We must show that in a system with perfect secrecy, that $H(C|P) = H(C)$. To see this, observe that $H(C,P) = H(C) + H(P|C) = H(P) + H(C|P)$. Since $H(P) = H(P|C)$, we have $H(C) = H(C|P)$.

(c) Use the last part of (b) and observe that the stated condition implies that $H(K|C,P) = 0$.