Information Theoretic Security

Fall semester, 2013

Assignment 1

Assigned: Thursday, September 19, 2013

Due: Wednesday, October 2, 2013

Somayeh Salimi, Tobias Oechtering

Problems

Problem 1.1: Cover & Thomas 2.25 (p. 49)

Problem 1.2: Cover & Thomas 3.8 (p. 66)

Problem 1.3: Cover & Thomas 3.9 (p. 67)

Problem 1.4: Cover & Thomas 4.10 (p. 92)

Problem 1.5:

Suppose that X, Y and Z are three arbitrary random variables with joint pmf P_{XYZ}. Show that:

a) $I(X;Y) - H(Z) \leq I(X;Y|Z) \leq I(X;Y) + H(Z)$

b) $I(X;Y|Z) = I(X,T;Y|Z)$ for every random variable T which is a function of (X,Z)

c) $H(X|Z) \leq H(X|Y) + H(Y|Z)$

d) if Z is a function of (X,Y), and X is independent of Z, then $H(Z) \leq H(Y)$

e) if Z is independent of (X,Y), then show correctness or incorrectness of the following equalities:

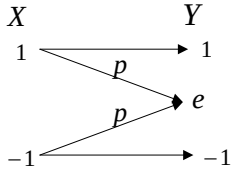
- $I(X;Y) = I(X;Y|Z)$
- $I(X;Y|T) = I(X;Y|TZ)$ where T is an arbitrary random variable with joint pmf P_{XYZT}.

Problem 1.6:

Consider the random variable X which takes ± 1 with equal probability. Then $Y = X.E$ is an erased version of X where erasure happens with probability p according to the following figure (in $Y = X.E$, . has the usual meaning of multiplication, i.e., E makes erasure with probability p and equals 1 with probability $1-p$). Show that:

a) $H(Y) = h(p) + 1 - p$ where $h(p) = -p\log p - (1-p)\log(1-p)$ is the binary entropy function

b) $H(Y|X) = h(p)$



Problem 1.7:

Explain the packing lemma and the covering lemma and the differences between them.