Advanced Topics in Cryptography – Exercise Set 5

Handed out on June 26, 2013

To be handed in on July 3, 2013

Exercise 1

Let X be a random variable taking values in a finite set $\mathcal{X}$.

Prove that $H_2(X) \leq H(X)$, with equality if X is uniform over $\mathcal{X}$.

Exercise 2

Consider a random variable X taking values in the finite set $\{1, \ldots, 2^k\}$, $k \in \mathbb{Z}^+$, according to the following probability distribution:

$$P_X[x] = \begin{cases} 2^{-k/4} & \text{if } X = 1 \\ \frac{1-2^{-k/4}}{2^k-1} & \text{if } X \neq 1 \end{cases}$$

Show that $\lim_{k\to\infty} \frac{1}{k} H(X) = 1$ and $\lim_{k\to\infty} \frac{1}{k} H_2(X) = \frac{1}{2}$.

Exercise 3

This question is about designing a "physical" secret sharing system as a box with locks. Let there be $n = 11$ participants in this system. Any subset with 6 (or more) participants must be able to access the secret (which is locked in the box), while any subset with $t < 6$ participants must not be able to do so.

What is the minimal number of locks and the minimal number of keys (per participant) needed for this system?

Write a general formula for this numbers of keys, for any n and t, where $t < n$.

Exercise 4

Consider Shamir (t, n)-threshold scheme over the field $\mathbb{Z}_p$, where p is prime. Suppose that $p = n$, where n is the number of participants.

Explain why this scheme is not t-private?