Advanced Topics in Cryptography – Exercise Set 4

Handed out on June 12, 2013

To be handed in on June 19, 2013

Exercise 1

Let $p_1, \ldots, p_n \in \mathbb{R}$, such that $\sum_{i=1}^{n} p_i = 1$.

Prove that $\sum_{i=1}^{n} p_i^2 \geq \frac{1}{n}$.

Exercise 2

Let X and Y be the random variables taking values in the finite set $\{1, 2, 3, 4\}$, according to the following joint probability distribution:

Y \ X	1	2	3	4
1	$\frac{1}{8}$	$\frac{1}{16}$	$\frac{1}{32}$	$\frac{1}{32}$
2	$\frac{1}{16}$	$\frac{1}{8}$	$\frac{1}{32}$	$\frac{1}{32}$
3	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$	$\frac{1}{16}$
4	$\frac{1}{4}$	0	0	0

Compute $H(Y|X)$, and write down the calculations.

Exercise 3

Let X and Y be random variables.

Prove that $0 \leq H(X|Y) \leq H(X)$.

Exercise 4

Let X, Y and Z be random variables.

Prove that $H(X, Y|Z) = H(X|Z) + H(Y|X, Z)$.