Advanced Topics in Cryptography – Exercise Set 3

Handed out on June 5, 2013

To be handed in on June 12, 2013

Exercise 1

Let X and Y be the Bernoulli random variables, which take values in $\{0, 1\}$.

Prove that $\Delta[X; Y] = |P_X[1] - P_Y[1]|$.

Exercise 2

Let X and Y be the random variables taking values in the finite set $\mathcal{X}$, and let Z be the random variable taking values in the finite set $\mathcal{Z}$. Suppose that X and Z are independent, and also Y and Z are independent.

Define the statistical distance between the random variables (X, Z) and (Y, Z) as follows:

$$\Delta[(X, Z); (Y, Z)] = \frac{1}{2} \sum_{x \in \mathcal{X}, z \in \mathcal{Z}} \big| P_{XZ}[x, z] - P_{YZ}[x, z] \big|.$$

Prove that $\Delta[(X, Z); (Y, Z)] = \Delta[X; Y]$.