Advanced Topics in Cryptography – Exercise Set 1

April 26, 2011

Exercise 1

Show that $P[\mathcal{A} \cap \mathcal{B}]P[\mathcal{A} \cup \mathcal{B}] \leq P[\mathcal{A}]P[\mathcal{B}]$ for all events $\mathcal{A}, \mathcal{B}$.

Exercise 2

Suppose $\mathcal{A}, \mathcal{B}, \mathcal{C}$ are events such that $\mathcal{A} \cap \bar{\mathcal{C}} = \mathcal{B} \cap \bar{\mathcal{C}}$. Show that $|P[\mathcal{A}] - P[\mathcal{B}]| \leq P[\mathcal{C}]$.

Exercise 3

Three fair coins are tossed. Let $\mathcal{A}$ be the event that at least two coins are *heads*. Let $\mathcal{B}$ be the event that the number of *heads* is odd. Let $\mathcal{C}$ be the event that the third coin is *heads*.
a) Are $\mathcal{A}$ and $\mathcal{B}$ independent?
b) Are $\mathcal{A}$ and $\mathcal{C}$ independent?
c) Are $\mathcal{B}$ and $\mathcal{C}$ independent?

Remark: Do not only answer “yes” or “no”, but also *argue your answer formally.*