Advanced Topics in Cryptography – Exercise Set 1

Handed out on April 24, 2013

To be handed in on May 1, 2013

Exercise 1

Three coins are tossed uniformly and independently. 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.*

Exercise 2

Show how to compute the probability $\Pr[a|3]$ in Example 1.1 (Lecture #2).

Exercise 3

Write a proof of the converse part of Theorem 1.2 (Lecture #2), i.e. prove that if for some cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ it holds that $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$, every key is used with probability $\frac{1}{|\mathcal{K}|}$, and $\forall x \in \mathcal{P}$, $y \in \mathcal{C}$ there exists a unique key K such that $e_K(x) = y$, then such the cryptosystem is perfectly secure.

Exercise 4

Suppose that the key $(K_1, \ldots, K_n) \in \mathbb{Z}_2^n$ in a one-time pad was re-used.

More precisely, suppose that an adversary received
$y = (y_1, \ldots, y_n) = (x_1 + K_1, \ldots, x_n + K_n)$ and
$y' = (y'_1, \ldots, y'_n) = (x'_1 + K_1, \ldots, x'_n + K_n)$, where summation is "mod 2",
for some plaintexts $x = (x_1, \ldots, x_n) \in \mathbb{Z}_2^n$ and $x' = (x_1, \ldots, x'_n) \in \mathbb{Z}_2^n$.

Show that perfect security will not hold in this case.

Hint: The adversary is allowed to make computations on the given ciphertexts.

Remark: This shows that in perfectly secure encryption
the key *cannot be re-used.*