**COM S 6830 – Cryptography** Due Sep 6, 2011

# Homework 1

*Instructor: Rafael Pass* *TA: Eleanor Birrell*

You may collaborate with other students on the homework but you must submit your own individually written solution and you must identify your collaborators. If you make use of any other external source, you must acknowledge it. You are not allowed to submit a problem solution which you cannot explain orally to the course staff.

**Problem 1.** *Expectation and Variance*

Let $X$ and $Y$ be two independent random variables. Prove the following facts.

(a) $\mathbb{E}[XY] = \mathbb{E}[X]\,\mathbb{E}[Y]$

(b) $\mathrm{Var}[X+Y] = \mathrm{Var}[X] + \mathrm{Var}[Y]$

Give examples when $X$ and $Y$ are not independent and equalities (a) and (b) do not hold.

**Problem 2.** *Pairwise Independence*

Let $r_1, r_2, \ldots, r_k$ be $n$-bit strings picked uniformly at random. For any subset $S$ of $\{1, 2, \ldots, k\}$, define a random variable $z_S = \oplus_{i \in S} r_i$. Prove that the set of random variables $\{z_S \mid S \subseteq \{1, 2, \ldots, k\}\}$ are pairwise independent.

**Problem 3.** *Sum of Pairwise Independent Variables*

Let $X_1, X_2, \ldots, X_n$ be random variables that are pairwise independent. Further, for all $i$, let $\mathbb{E}[X_i] = \mu$ and $\mathrm{Var}[X_i] = \sigma^2$

(a) Show that,

$$\Pr\left[\left|\frac{\sum X_i}{n} - \mu\right| \geq \epsilon\right] \leq \frac{\sigma^2}{n\epsilon^2}$$

Note that this is a Chernoff like bound when the random variables are only pairwise independent. (Hint: Use Chebyshev's inequality)

(b) Suppose further that the random variables assume only the values 1 and -1. Show that the inequality can be simplified to,

$$\Pr\left[\left|\frac{\sum X_i}{n} - \mu\right| \geq \epsilon\right] \leq \frac{1-\mu^2}{n\epsilon^2}$$

**Problem 4.** *Secure Encryption*

The cryptographers at secure-encryption.com have come up with an encryption scheme using secret keys. This scheme has a known vulnerability that an attacker, given a random message $m \in \mathcal{M}$ and its encryption, can guess for *any* $i$, the $i^{th}$ bit of the secret key with probability $\frac{1}{2} + \epsilon$.

Let us suppose the attacker gains access to $k$ such messages $m_1, m_2, \ldots, m_k$ with its encryption.

(a) If the messages $m_1, \ldots, m_k$ are known to be independent, show that the attacker can find any bit of the secret key with very high probability (Hint: Use Chernoff bound). Using the union bound, find a lower bound on the probability of the attacker guessing the entire secret key, if the key is made up of $n$ bits.

(b) Find the number of messages required to guess the entire key with 99% probability when $\epsilon = 0.0001$ and $n = 1024$.

(c) In real life, it is hard for the messages to be independent. Repeat parts (a) and (b) if the messages are known to be only pairwise independent (Hint: Use Problem 3).

**Problem 5.** *Match-making*

Try to formalize what it means for the "match-making" card game presented in class to be secure. Decide on what properties are desired. Provide explicit assumptions and prove that the game satisfies the desired properties under your assumptions.