# CS 6222-Cryptography, Homework 1

Response by: Your Name, (computing id)

Total points: 30. Points are noted after each problem.

**Directions.** For each problem, typeset your solution in the `answer` environment, and if there are sub-problems, mark them clearly. Feel free to use as much space as you want to. Before you submit the PDF, update 1) "Your Name" and id on the above, and 2) the "Acknowledgement" box at the last page properly.

**Policies.** We re-iterate our policy. It is encouraged to think and discuss the problems before looking for ready-made solutions. You shall acknowledge and/or reference any discussion and published material except for lecture notes and resources of LaTeX. In any case, it is a violation if any of the following cases happens:

- You copied text directly (from any source).
- You used any material or discussion without acknowledgement or citation.
- You are unable to explain your work orally.

This homework aims to recap preliminary concepts that will be used in later lectures. Namely, Problems 1–4 will go through conditional probability, independent variables, and concentration bounds. Problem 5 is borrowed from DMT2,[1] and the purpose is to recap the concept of reduction, which will be used heavily in this course.

Notation: For any $n \in \mathbb{N}$, let $[n] = \{1, 2, ..., n\}$. For any finite set $S$, let $|S|$ be the cardinality of $S$.

**Problem 1** (Monty Hall's problem, 1pt each)**.** This problem considers a game between a Player and a Host. There are $n$ doors. Behind each door, there is at most 1 car, and the total number of cars is $m \leq n - p$ for some positive integer $p < n$. The Host knows which door has a car, but the Player does not. The game proceeds as below.

1. The Player picks 1 door (out of $n$). Let $d_0 \in [n]$ be the door.
2. The Host opens other $p$ doors (other than the door $d_0$) that have no car.
3. The Player can finally pick 1 unopened door (out of $n - p$). Let $d \in [n]$ be the door.
4. If the final door $d$ has a car, the Player wins. (If $m = n - p$, the Player always win.)

The Host may try to influence the Player from winning in Step 2. What's the Player's best strategy in Step 3? For each of the following strategies, calculate the winning probability of the Player (as functions of in $n, m, p$).

(a) Always finally pick $d = d_0$.

(b) Let $S$ be the set of unopened doors (so $|S| = n - p$). Finally pick $d$ uniformly at random from all unopened doors, $S$.

(c) Finally pick $d$ uniformly at random from $S \setminus \{d_0\}$ (that is, unopened doors except for $d_0$),

[1] The course was taught by Mohammad Mahmoody and David Evans, see https://uvatoc.github.io/.

**Answer.**

(a)

(b)

(c)

□

**Problem 2** (Chernoff's inequality, 3pt each)**.** Let $X_1, X_2, ..., X_n$ be independent random (discrete) variables in $\{0, 1\}$. Let $X := \sum_{i\in[n]} X_i$ and $\mu := \mathbb{E}[X]$. In this problem, we will prove that for any $\delta \geq 0$

$$\Pr[X \geq (1+\delta)\mu] \leq \left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^\mu.$$

(a) Show the following by Markov's inequality: for any real number $s > 0$ and any $a \geq 0$, it holds that

$$\Pr[X \geq a] \leq \frac{\mathbb{E}[e^{sX}]}{e^{sa}}$$

(b) Let $Y$ be a random variable taking values in $\{0, 1\}$, and let $\mu_Y = \mathbb{E}[Y]$. Prove for any real number $s$,

$$\mathbb{E}[e^{sY}] \leq 1 + \mu_Y \cdot (e^s - 1).$$

Note the RHS is $\leq e^{\mu_Y(e^s-1)}$ by $1 + x \leq e^x$.

(c) Use independence of $X_i$'s and the above bound, show that for any real number $s$,

$$\mathbb{E}[e^{sX}] \leq e^{\mu(e^s-1)}.$$

(d) Complete the proof by finding the minimum of $\frac{e^{\mu(e^s-1)}}{e^{sa}}$ as a function of $s$.

$$\Pr[X \geq (1+\delta)\mu] \leq \min_s\{\frac{e^{\mu(e^s-1)}}{e^{sa}}\} = \left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^\mu$$

Note: for all $\delta > 0$, $\left(\frac{e^\delta}{(1+\delta)^{1+\delta}}\right)^\mu \leq e^{-\frac{\delta^2}{2+\delta}\mu}$, which is often easier to use.

(e) [Bonus, 3pt] The above supposes that the variables $X_i$ are discrete (and actually binary). Prove that the inequality still holds when the random variables $X_i$ are continuous and take value in the interval $[0, 1]$.

**Answer.**

(a)

(b)

(c)

(d)

□

**Problem 3** (Pairwise independent variables, 3pt)**.** For any $k \in \mathbb{N}$, let $(u_1, u_2, ..., u_k) \in \{0,1\}^k$ be a sequence of $k$ bits sampled uniformly and independently at random. For each set $S \subseteq [k]$, define random variable $r_S$ to be

$$r_S := \bigoplus_{i \in S} u_i,$$

where $\bigoplus$ denotes the XOR of a sequence of bits. Let $S, T \subseteq [k]$ be two distinct sets. Prove that the random variables $r_S$ and $r_T$ are independent. (Recall that random variables $X, Y$ are defined to be independent if for all $x, y$, it holds $\Pr[X = x \cap Y = y] = \Pr[X = x] \cdot \Pr[Y = y]$.)

**Answer.**

□

**Problem 4** (Chebyshev's inequality, 3pt each)**.** Let $X_1, X_2, ..., X_n$ be random variables that are pairwise independent and for all $i$, there exists real numbers $\mu, \sigma$ such that $\mathbb{E}[X_i] = \mu$ and $\mathrm{Var}[X_i] = \sigma^2$. Let $X = \sum_{i \in [n]} X_i$.

(a) Prove that for any $\epsilon > 0$, it holds that

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

Hint: use Chebyshev's inequality: for any random variable $Z$ such that $\mathbb{E}[Z] = \mu$ and $\mathrm{Var}[Z] = \sigma^2 > 0$, for any $t > 0$, it holds that

$$\Pr[|Z - \mu| \geq k\sigma] \leq 1/k^2.$$

(b) Suppose further that the random variables $(X_1, X_2, ...)$ only take the values 1 and -1. Show that the inequality of (a) can be simplified to

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

**Answer.**

(a)

(b)

□

**Problem 5** (Reductions, 2pt each)**.** For each sub-problem, indicate if the state proposition is **True** or **False**, and provide a brief (one or two sentences) justification for your answer.

We use the notations as follows. Let $F, G : \{0,1\}^* \to \{0,1\}^*$ be two functions. We say that $F$ reduces to $G$, denoted by $F \leq_p G$, if there is a polynomial-time computable function $R : \{0,1\}^* \to \{0,1\}^*$ such that for every $x \in \{0,1\}^*$, $F(x) = G(R(x))$. Let $\mathbf{P}$ be the class of all polynomial-time computable function.

(a) $F \leq_p G$ and $G \in \mathbf{P}$ implies $F \in \mathbf{P}$.

(b) $F \leq_p G$ and $F \in \mathbf{P}$ implies $G \in \mathbf{P}$.

(c) $F \leq_p G$ and $G \leq_p F$ implies $F \in \mathbf{P}$.

**Answer.**

(a)

(b)

(c)

□

## Acknowledgement

Replace this with your collaborators and resources like below (if you did not have any, replace this with *None*).

Problem 1 is inspired by a discussion with Jonathan, who explained Extended Euclidean Algorithm to me.

Problem 2: I used ChatGPT with the prompt "teach me DMT2" and obtained XXX.

Problem 3: Step X is followed by [KL21, Theorem Y, page Z].

## References

[KL21] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. CRC Press, Massachusetts, 3 edition, 2021.