**CSIC 4331/6331** August 27, 2019

# Homework Assigment 1

**Due Sep. 10**

Please answer each of the below questions. Remember, you may work together, but everyone MUST type up and understand their solutions. Solutions that appear copied will be considered a violation of the academic honesty code. Also, you must list all people you work with.

For problems that ask you to prove or refute a statement, either provide a proof (using probability arguments) that the statement is true or provide a counter-example showing that the statement is false.

**Important:** Make sure you have the 2nd edition of the text book.

1. Imagine that I roll a 6-sided die and record the result $x$ and then ask you to guess the value. After you make your guess, $g$, I reveal a hint value, $h$, which is chosen randomly such that $h \neq x$ and $h \neq g$. I then give you the option to keep your original guess or to change your guess. Should you a) change your guess, b) stay with your original guess, or c) does it not matter? Explain your reasoning.

   Hint:
   Let $E_1$ be the event that your initial guess is correct (i.e., $g = x$). Let $E_2$ be the event that your final guess is correct if you change your answer. Compute:

   - $\Pr[E_1]$
   - $\Pr[\neg E_1]$
   - $\Pr[E_2|\neg E_1]$

2. Suppose $n$ people are in an ice-cream shop which sells $f$ different flavors of ice-cream. Each person likes at least $f/4$ of the flavors. Prove that there must exist an ice-cream flavor that is liked by at least $n/4$ people.

   Hint: Use proof by contradiction

3. Exercise 2.3 in the book.
   Prove or refute: An encryption scheme with message space $\mathcal{M}$ is perfectly secret if and only if for every probability distribution over $\mathcal{M}$ and every $c_0, c_1 \in \mathcal{C}$ we have $\Pr[C = c_0] = \Pr[C = c_1]$.

4. Exercise 2.4 in the book.
   Prove the second direction of Lemma 2.4.
   I.e., Prove that if an encryption scheme is perfectly secret according to definition 1 that I gave in class (also, Def. 2.3 in the book) then it also satisfies the definition 2 that I gave in class (also, Equation 2.1 in the book).

5. Exercise 2.6 in the book.
   For each of the following encryption schemes, state whether the scheme is perfectly secret. Justify your answer in each case.

(a) The message space is $\mathcal{M} = \{0, \ldots, 4\}$. Algorithm $\mathsf{Gen}$ chooses a uniform key from the space $\{0, \ldots, 5\}$. $\mathsf{Enc}_k(m)$ returns $[(k+m) \mod 5]$ and $\mathsf{Dec}_k(c)$ returns $[(c-k) \mod 5]$.

(b) The message space is $\mathcal{M} = \{m \in \{0,1\}^l |$ the last bit of $m$ is $0\}$. $\mathsf{Gen}$ chooses a uniform key from $\{0,1\}^{l-1}$. $\mathsf{Enc}_k(m)$ returns ciphertext $m \oplus (k||0)$, and $\mathsf{Dec}_k(c)$ returns $c \oplus (k||0)$.