# MCS 425: Codes and Cryptography (Spring 2020)
# Homework 4

Due at 11:00am, Wednesday, Apr 15

Submission instructions:

- Email a single file to `yucheng2@uic.edu` (PDF format only).
- Name your file `<Lastname><Firstname>.pdf`, e.g., `ChengYu.pdf`.

**Digital signatures:**

1) Alice uses RSA signatures with the following parameters: $n = 55$ and $e = 3$. Bob receives a signed document $(m, s) = (47, 53)$ from Alice. How does Bob verify that the message is signed by Alice?

**Hash functions:**

2) Suppose a function $h : \{0,1\}^n \to \{0,1\}^n$ is strongly collision-free. Let $h' : \{0,1\}^n \to \{0,1\}^n$ be the function defined as $h'(x) = h(h(x))$. Prove that $h'$ is strongly collision-free.

**Secret sharing:**

3) In a 3-out-of-5 Shamir secret sharing scheme with modulus $p = 7$, the following were given to Alice, Bob, and Charlie: $(1, 4)$, $(2, 6)$, $(3, 5)$. Identify the secret.

**Information theory:**

4) (2 points) A bag contains 2 red, 2 green, and 2 blue marbles that are identical to each other except color. Choose 2 marbles at random from the bag (without replacement).

   Let $X$, $Y$, and $Z$ be the number of red, green, and blue marbles chosen respectively.

   a) Calculate the expected value $\mathbb{E}[X]$.
   b) Are $X$ and $Y$ independent random variables?
   c) Calculate the entropy $H(X)$ of $X$.
   d) Calculate $H(X, Y)$ and $H(X|Y)$.
   e) Calculate $H(X, Y, Z)$ and $H(Z|X, Y)$.

   You may leave your answer as the sum of logarithms for the entropy-related questions.

   (Hint: the chain rule of conditional entropy could be useful for questions (d) and (e).)