

MCS 425: Codes and Cryptography (Fall 2020)

Homework 4

Due at 12:00pm CST, Monday, Nov 30

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?
2. Suppose a function $h : \{0, 1\}^n \rightarrow \{0, 1\}^n$ is strongly collision-free. Let $h' : \{0, 1\}^n \rightarrow \{0, 1\}^n$ be the function defined as $h'(x) = h(h(x))$. Prove that h' is strongly collision-free.
3. In a 3-out-of-5 Shamir's 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.
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? Justify your answer.
 - c) Calculate the entropy $H(X)$ of X .
 - d) Calculate $H(X, Y)$ and $H(X|Y)$.
 - e) Calculate $H(X, Y, Z)$ and $H(Z|X, Y)$.

(Hint: the chain rule of conditional entropy $H(Y|X) = H(X, Y) - H(X)$ could be useful for questions (d) and (e).)

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