SCI 2000
Introduction to Encryption, Assignment 5
Due April 7 via upload to Crowdmark.

Questions will be marked both on correctness and clarity of presentation. Poor writing and sloppy/illegible presentation both impact the clarity of your work and so will be penalized. For this assignment, you can use Wolfram Alpha (https://www.wolframalpha.com/) to perform computations, however you must show all steps in your computations to get credit.

Question 1: You and Alice are communicating using RSA. Your keys are:

$$\text{Public key: } (17, 1769)$$
$$\text{Private key: } (593, 1769)$$

Alice's public key is $(5, 851)$. You receive the message $(398 \mod 851, 32 \mod 1769)$. What is the message? Is it from Alice? Show all your work and justify your conclusions.

Question 2: Bob's public key is $(17, 1769)$, Alice's public key is $(5, 851)$. They have agreed upon the following hash function:

The function, H, takes a contract C and returns the number $H(C)$ calculated as follows: If c is the number of consonants in the contract, and v is the number of vowels in the contract, then $H(C) = 2v^2 + c$.

Bob claims that Alice has signed the contract C below:

$$C = \text{I will mind Bob's kids while he gives online lectures}$$

However, now that all schools are closed, Alice claims that this is not true!

a) Bob presents the number 595 to you as evidence of her agreement to the contract. Based upon this evidence, is Bob's assertion that she signed the contract true or false?

b) Alice claims the contract was actually:

$$\text{Bob will give Alice one hundred five thousand dollars}$$

Based upon the available evidence, can you conclude who is correct? Why or why not?

c) If you CANNOT decide who is correct in part (b), suggest a new hash function that would've settled the dispute (had they used it). Given that Alice's private key is $(317, 851)$, compute the result of her signing the contract using your new hash function. Show all work.

If you CAN decide who is correct in the previous question, then show that there exists a contract C' such that $H(C) = H(C')$, meaning that there are instances where you would not have been able to settle their dispute.

Question 3: a) Show that the code

$$C = \{000, 011, 110\}$$

is 1 error-detecting.

b) How many 1 error-**correcting** fixed length binary codes having codewords of length three are there? Justify your conclusions.

Question 4: Suppose that r, s, t are binary strings of the same length. Explain why the Hamming distance between these strings (denoted by $d(a, b)$) obeys the inequality $d(r, t) \leq d(r, s) + d(s, t)$.