# CS 411/507

**Homework 4**

**Ataberk Asil Karaman**

**28945**

**Question 1:** In this question, way of attacking was “chosen cyphertext attack”. The method I used to solve this question was basically: First pick a random number that has no other common divisor other than one. Then, I get the corresponding text of that number from the query function. Finally, with the mathematical implementation in the question\_1.py, I extracted the message from the text. The secret code is: 43411

**Question 2:** In this question, the problem of the system is the span of R value; it is smaller than it should be. Therefore, using brute-force (trying each case in loops) we can solve it even though it takes some time. R = 246, m = 5718

**Question 3:** For this question the flaw of the program is the limits of k value. It can be found by exhaustive search method. After the we find k value, only thing left to do is traceback the mathematical formulas in the previous functions to get message. In this question, k value is 24397 and message is: b'It begins, as most things begin, with a song.’

**Question 4:** The method I followed for this question is similar to previous one; I checked the given equations on given functions and found what I need, the public key h. Again, trace backed the formulas with help on modular inverse function to get the message. After finding the numerical value of message I simply converted it to string output. The second message was: “In sorrow, seek happiness.”