ECE 3170 Cryptographic Hardware for Embedded Systems

Fall 2025
Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology
Homework 2, 100 pts.
Due Friday Aug. 29 prior to 11:55pm
(please turn in homework electronically on Canvas)

This homework will focus on the RSA asymmetric encryption algorithm described in class. You should have enough information in the RSA lecture notes and book chapter to solve this homework, therefore you are **not** allowed to look for answers to these questions using the internet. You also may **not** consult anyone else except for the GTA (Kareem Ahmad) or professor for the course. The goal is for you to find your own RSA keys and use them to encrypt and decrypt.

Special “consulting” notes for this homework, homework #2 of the class Cryptographic Hardware for Embedded Systems, ECE 3170 A & LA, Fall 2025, are as follows:

> Explicitly NOT counted as “consulting” is help received regarding how to calculate with large numbers, e.g., asking a friend about on-line calculators. As long as assistance is not received for the specific math calculations for your homework answer, generic questions about how to use calculators or other on-line or software based mathematics able to deal with ranges of number values exceeding typical floating point precision is NOT considered “consulting” on this homework.

Part I (10 pts.)

(1) From the Media Gallery in Canvas, listen to the lectures “Lecture4DES” and “Lecture5RSA” if you have not already done so (if you have done so, this viewing will be indicated in the statistics available to the instructor).

(2) Choose two prime numbers p and q each of which is larger than seven. Do not choose numbers that are too large as you will need to perform a lot of operations with these numbers in Part II. You may not pick 47 or 71 as these were used in the RSA lecture (but you really want smaller numbers anyway).

(3) Send an email to ccarpenter38@gatech.edu stating you have completed item (1) and with the prime numbers specified in (2); if your prime numbers have already been used by another student that sent an email earlier than yours, the Graduate Teaching Assistant (GTA), Chauncey Carpenter, will respond to let you know that you have to reselect item (2).

(4) Once the GTA confirms via email that you have a unique pair of prime numbers, respond to his email with the value of $n = p*q$ and proceed to step (5).

Part II (90 pts.)

(5) Select encryption key e such that e and $(p - 1)(q - 1)$ have only 1 as a factor in common.

(6) Find a value for d such that d is the multiplicative inverse of e in modular arithmetic. Show your work for this and explain how you found d. You are not required to write a program to help you find d, but if you do, please provide a printout of the code and a brief explanation.

(7) Given message m = 3655802389472199, divide m into multiple blocks m_i where each block has size less than 2^s where 2^s is less than $n = p*q$. In other words, each can be expression in binary using s bits. (However, we will not be using any binary expressions in this homework assignment.)

(8) Consider the second block only. This block is m_2. You are going to encrypt m_2. However, the first step is the exponentiation step (m_i^e). Show the result for m_2^e and explain how you carried out the calculation.

(9) Complete the encryption of m_2 to c_2 using the RSA formula $c_i = m_i^e \bmod n$. Explain all of your calculations.

(10) Take your answer to the previous item (9): c_2. Use c_2 to calculate the exponentiation step c_i^d of RSA decryption. Show the result for c_2^d and explain how you carried out the calculation.

(11) Complete the decryption of c_2 using the RSA decryption formula $m_i = c_i^d \bmod n$. Explain all of your calculations.

(12) Verify that your result (11) matches the input m_2 found in (7).

When you have successfully completed the above, you will have (i) found your own RSA keys and will have used the keys for (ii) encryption and (iii) decryption.

In summary, you must provide the following individual answers (including explanations) in your final submission for this assignment (even if already contained in emails sent), please repeat the information:

(1) Verify you have listened to the lecture recordings especially “Lecture5RSA.”

(2) Two prime numbers p and q.

(3) Email sent to ccarpenter38@gatech.edu with p and q.

(4) The value of n.

(5) Encryption key e.

(6) Decryption key d.

(7) Message m = 3655802389472199 divided into multiple blocks m_i.

(8) The result for m_2^e.

(9) The result for c_2.

(10) The result for c_2^d.

(11) The result for $m_2 = c_2^d$ with all of your calculations explicitly shown and explained.

(12) Verification that result (11) matches m_2 found in (7); if there are any issues, please explain in detail.

YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES. ALL HOMEWORK SUBMISSIONS MUST INCLUDE YOUR NAME, COURSE NUMBER, SECTION, AND THE HOMEWORK SET NUMBER. ALL SHEETS MUST BE STAPLED TOGETHER. ALL WRITING MUST BE EASY TO READ (FOR EXAMPLE, YOU MAY HAVE TO WRITE ONLY ON ONE SIDE OF EACH SHEET OF PAPER THAT YOU SUBMIT AND MAY NOT BE ABLE TO USE RECYCLED PAPER). FAILURE TO FOLLOW INSTRUCTIONS MAY RESULT IN ZERO POINTS. ALL WORK MUST BE YOUR OWN. NO PLAGIARISM IS ALLOWED, AND YOU MUST PROPERLY REFERENCE ALL SOURCES OF YOUR INFORMATION – ALTHOUGH YOU SHOULD NOT LOOK FOR AND MAY NOT CONSULT "SOLUTIONS" AVAILABLE FROM OTHER SOURCES (TO REPEAT, YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES!).