Hardware-Oriented Security and Trust
ECE 4156 A / ECE 6156 A
Spring 2025

Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology

Homework 6, 110 pts. (ECE 4156) 110 pts. (ECE 6156)
Due Friday March 7 prior to 11:55pm

Problems 2 and 3 on this homework cover the RSA asymmetric encryption algorithm. You should have enough information in the RSA lecture notes and textbooks for the course to solve this homework, therefore you are **not** allowed to look for direct answers to these questions using the internet (but you may use a calculator with a modulus function). You also may **not** consult anyone else except for the professor and teaching assistant for the course. The goal is for you to find your own RSA keys and use them to encrypt and decrypt.

1) (25 pts.) Consider the Needham-Schroeder protocol as presented in the lecture notes where A is an identifier for Alice, B is an identifier for Bob, $E_A()$ is encryption with a symmetric key held by Alice, $E_B()$ is encryption with a symmetric key held by Bob, K is a symmetric key, and both N_A and N_B are nonces:

1) Alice to Trent: A,B,N_A
2) Trent to Alice: $E_A(N_A,B,K,E_B(K,A))$
3) Alice to Bob: $E_B(K,A)$
4) Bob to Alice: $E_K(N_B)$
5) Alice to Bob: $E_K(N_B-1)$

Please note that we are using **symmetric** keys! Now suppose that for "efficiency" the identifiers A and B are omitted from encryption in steps 2 and 3 of the protocol with the result as follows:

1) Alice to Trent: A,B,N_A
2) Trent to Alice: $E_A(N_A,K,E_B(K))$
3) Alice to Bob: $A,E_B(K)$
4) Bob to Alice: $E_K(N_B)$
5) Alice to Bob: $E_K(N_B-1)$

Without breaking any keys (i.e., none of the symmetric keys of others held by Trent are discovered by Mallory), is it possible for Mallory to carry out a Man-in-the-Middle (MitM) attack on the "efficient" modified protocol above? If so, show the steps in detail. If not, give at least one clear reason why not and show some attempted steps which fail to successfully carry out a MitM attack. Some assumptions are likely to be needed for your answer; if so, please clearly state any assumption you require.

2) (10 pts.) 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).

Send an email to the TA, Arman Allahverdi, at aallahverdi3@gatech.edu and then check the course webpage for homeworks

http://mooney.gatech.edu/Courses/ECE4823/hwlabexam/index.html

to see if your number pair has already been taken or not. You need to make a first attempt to choose two prime numbers p and q prior to 2pm on Tuesday March 4. If your first name, first letter of your last name, and selected pair of numbers appear under homework 6, you are done. Otherwise, prior to 2pm on Wednesday March 5, you need to make a second attempt to choose your two prime numbers and send another email to another email to the TA. Again, if your first name and number appears under homework 6, you are done. Otherwise, prior to 2pm on Thursday March 6, you need to try again. Please note that if your prime numbers have already been used by another student that sent an email earlier than yours, the TA will respond to let you know that you have to reselect.

Once your unique pair of prime numbers has been posted on the homeworks web page, send another email with the value of $n = p*q$ and proceed to problem 3 below.

3) (75 pts.) Perform the following after completing problem 2 above.

a. (10 pts.) Select encryption key e such that e and $(p - 1)(q - 1)$ have only 1 as a factor in common.

b. (15 pts.) 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. You may also use a calculator with modulus functionality, but please specify which calculator you use if special modulus capability is utilized (e.g., with an on-line calculator).

c. (10 pts.) Given message m = 3855209917429573, 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 expressed in binary using s bits. (However, we will not be using any binary expressions in this homework assignment; instead, please answer all questions using a decimal representation.)

d. (10 pts.) 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.

e. (10 pts.) 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.

f. (10 pts.) Take your answer to the previous item (e): 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.

g. (10 pts.) Complete the decryption of c_2 using the RSA decryption formula $m_i = c_i^d \bmod n$. Explain all of your calculations. Verify that your result matches the input m_2 found in (c).

YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES, INCLUDING OTHER/PREVIOUS SECTIONS OF ECE COURSES TAUGHT BY PROFESSOR MOONEY SUCH AS THOSE WITH NAMES INCLUDING HARDWARE ORIENTED SECURITY AND TRUST AS WELL AS CRYPTOGRAPHIC HARDWARE FOR EMBEDDED SYSTEMS. ALL HOMEWORK SUBMISSIONS MUST INCLUDE YOUR NAME, COURSE NUMBER, SECTION, AND THE HOMEWORK SET NUMBER. ALL SUBMISSIONS MUST BE DONE ONLINE. ALL WRITING MUST BE EASY TO READ (FOR EXAMPLE, YOU MAY HAVE TO WRITE WITH THICK INK AND MAY NOT BE ABLE TO USE LOW RESOLUTION PHOTOS OF HANDWRITTEN DIAGRAMS). FAILURE TO PROVIDE CLEAR AND LEGIBLE ANSWERS 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!).