ECE 3170 Cryptographic Hardware for Embedded Systems

Fall 2025

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

Homework 3, 85 pts.

Due Friday Sept. 5 prior to 11:55pm

(please turn in homework electronically on Canvas)

1) (5 pts.) In the Media Gallery on Canvas, listen to the lecture "Lecture10TheoryCiphers."

2) (10 pts.) Consider S-box 1 of DES. Below is Table 12.6 from the course text. Give the results for the following substitutions: 0x0F, 0x37, 0x25 and 0x10. Give your answers in both decimal as well as hexadecimal. Please use your lab 1 code for DES in C and in VHDL to help in answering this question.

Table 12.6
S-Boxes

S-box 1:

14,	4,	13,	1,	2,	15,	11,	8,	3,	10,	6,	12,	5,	9,	0,	7,
0,	15,	7,	4,	14,	2,	13,	1,	10,	6,	12,	11,	9,	5,	3,	8,
4,	1,	14,	8,	13,	6,	2,	11,	15,	12,	9,	7,	3,	10,	5,	0,
15,	12,	8,	2,	4,	9,	1,	7,	5,	11,	3,	14,	10,	0,	6,	13,

3) (20 pts.) This question covers some of the principles behind the construction of block ciphers.

a. (10 pts.) Use your own words to describe how the Data Encryption Standard (DES) implements the principle of *confusion*. Give one example of an operation in DES which illustrates this principle and explain the illustration.

b. (10 pts.) Why is it a problem for a block cipher to exhibit a *simple relation*? Give one example of a drawback due to a *simple relation* holding true for a block cipher.

4) (15 pts.) Suppose you are given a list of n names in no order at all (or in a random order). Is it possible to sort the list in linear, polynomial or exponential time?

a. (5 pts.) Is it possible to sort the list in linear time (or faster) using a known algorithm (e.g., bubble sort, radix sort or quicksort)? If so, please name at least one algorithm which is able to sort a list in $O(n)$ time and explain any necessary assumptions; if not, simply stating that no such algorithm exists is sufficient to answer this question.

b. (5 pts.) Is it possible to sort the list of n names in polynomial time (or faster) using a known algorithm (e.g., bubble sort, radix sort or quicksort)? If so, please name at least one algorithm which is able to sort a list in at most $O(n^c)$ time and give a value for the constant c (e.g., you could say that $c = 4$); if not, simply stating that no such algorithm exists is sufficient to answer this question.

c. (5 pts.) Is it possible to sort the list of n names in exponential time (or faster) using a known algorithm (e.g., bubble sort, radix sort or quicksort)? If so, please name at least one algorithm which is able to sort a list in exponential time or faster; if not, simply stating that no such algorithm exists is sufficient to answer this question.

5) (5 pts.) Approximately how many prime numbers exist using 512 bits or less to represent the prime number? (Hint: the answer is in the lecture notes as well as in the assigned reading!)

6) (15 pts.) In practical prime number generation, one of the steps is to set a higher order bit to one and the lowest order bit to one.

a. (5 pts.) What is the purpose of setting a higher order bit to one?

b. (5 pts.) What is the purpose of setting the lowest order bit to one?

c. (5 pts.) Consider RSA with 2048 bits and the search for two prime numbers p and q such that $n = pq$. For generation of prime numbers p and q, does it make sense to set the most significant bit to a 1 or a 0 and why? Please note that a correct answer (1 or 0) without a correct reason will receive zero points.

7) (10 pts.) Consider the inverse modular exponentiation: find x where $a^x \equiv b \pmod{n}$.

a. (5 pts.) If $3^x \equiv 5 \pmod{17}$, then $x = ?$ Give an answer for x or state that no solution exists.

b. (5 pts.) If $3^x \equiv 7 \pmod{13}$, then $x = ?$ Give an answer for x or state that no solution exists.

8) (5 pts.) Read the following article and listen to the following two youtube videos (the two videos are intended to provide "pro" and "con" arguments about the article). Please indicate that you have read the article and listened to the two videos by writing an appropriate sentence, e.g., "I hereby certify under the Georgia Tech Honor Code that I have read the Big Hack article and have listened to the two associated youtube videos assigned in this homework for problem 8." There is no partial credit; you must read the article and listen to both videos to receive any points.

a. J. Robertson and M. Riley, "The Big Hack," Bloomberg, 4 October 2018, available https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

b. China Global Television Network (CGTN): Dialogue, available https://www.youtube.com/watch?v=aHRtx3oCVlc

c. Bloomberg News: Digital Defense, available https://www.youtube.com/watch?v=mYShybwfcdo

YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES. ALL LABORATORY 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!).