ECE 3170 Cryptographic Hardware for Embedded Systems

Fall 2024

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

Homework 3 SOLUTION

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,

S Box																
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	14	8	12	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Given a 6-bit binary string, the two outer bits choose the row, and then the middle 4 bits choose the column. The following shows the answer to the substitutions requested.

Input (HEX)	Input (Binary)	Row value	Column Value	S-Box value	Output (Binary)	Output (HEX)
0x0F	001111	01	0111	1	0001	0x1
0x37	110111	11	1011	14	1110	0xE
0x25	100101	11	0010	8	1000	0x8
0x10	010000	00	1000	3	0011	0x3

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.

Confusion is the principle of obscuring the relationship between the plaintext and the ciphertext. DES uses S-boxes to perform confusion through substitution algorithm. The substitution algorithm in DES obscures the relationship of the 6-bit input and 4-bit output.

To clarify the difference between confusion and diffusion, confusion obscures the relationship between plaintext and ciphertext, often through some form of substitution, while diffusion specifically refers to the property that changing a single bit of either the key or the plaintext will change roughly half of the bits of the ciphertext.

The following comparison chart may be helpful:

Comparison Chart

BASIS FOR COMPARISON	CONFUSION	DIFFUSION
Basic	Utilized to generate vague cipher texts.	No bits of ciphertext should be independent from plaintext
Seeks to	Make a relation between statistics of the ciphertext and the value of the encryption key as complicated as possible.	The statistical relationship between the plaintext and ciphertext is made as complicated as possible.
Achieved through	Substitution algorithm	Transposition algorithm
Used by	Stream cipher and block cipher	Block cipher only.
Result in	Increased vagueness	Increased redundancy

Source for above figure (note top right entry reworded):
https://techdifferences.com/difference-between-confusion-and-diffusion.html

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.

A simple relation is any property of a block cipher which can effectively reduce the search space that an attacker must traverse.

The textbook cites a property of DES such that if DES is defined as some $F(K, P) = C$, and the inverse were defined as $F^{-1}(K, C) = P$, then the simple relation exbited by DES can be stated as $F^{-1}(K', C') = P'$, where each element is complemented.

As a practical example, a simple relation reduces the search size of an attacker by an order of two because now each iteration of inverse-DES (considered a computationally "heavy" operation) can be used to see two solutions (P and P') through bit-flipping (a comparably "lightweight" operation).

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) 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.

The run time for radix sort is O(nw), where "w" is the maximum length of a name, "n" is the number of names in the list. If "w" is significantly smaller than "n", then radix sort can be considered to be linear time O(n).

b. (5) 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.

Yes. Selection sort has O(n^2)

c. (5) 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.

Yes, bubble sort is one answer for this problem. There can be many correct answers.

Please also note that "Big-O" notation provides an upper bound for the algorithm. An algorithm that is linear time will complete within exponential time, and an algorithm with a $O(n^2)$ complexity will satisfy $O(n^3)$, even though the former is more specific and will usually be expected.

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!)

Using 512 bits, there are approximately 10^{151} prime numbers (see Lecture 6 Number Theory I, slide 19).

6) (10 pts.) In practical prime number generation, one of the steps is to set a high order bit to one and the lowest order bit to one.

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

Setting a high order bit to one ensures that the prime will be sufficiently large.

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

A prime number cannot be even (except the number 2). Thus, setting the low order bit to 1 ensures that the number is an odd number.

c. (5) 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.

The MSB should be set to 0. Setting the MSB of p or q to 1 will result in their product, n=pq, having >2048 bits and overflowing.

However, if the student mentioned that the p and q both need to be 1024 bits, then credit is awarded – as the most significant but of a 1024 bit number should be 1 to allow for a full 2048 bit n.

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

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

From a few trial and error process below:

$$3^1 mod\ 17 = 3$$
$$3^2 mod\ 17 = 9$$
$$3^3 mod\ 17 = 10$$
$$3^4 mod\ 17 = 13$$
$$3^5 mod\ 17 = 5$$

X = 5

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

From trial and error process below:

$$3^1 mod\ 13 = 3$$
$$3^2 mod\ 13 = 9$$
$$3^3 mod\ 13 = 1$$
$$3^4 mod\ 13 = 3$$
$$3^5 mod\ 13 = 9$$
$$3^6 mod\ 13 = 1$$

You start to see the pattern above, which means no solution exists. Some students had solutions which were very large (x > 40). This most likely returned a correct answer in python or matlab due to rounding. In general, if a solution exists it will be found before you reach x > n.

8) (5 pts.) Read the following article and listen to the follow 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=mYShybwfcd