Problem Set #4

CMSC/Math 456
Instructor: Daniel Gottesman

Due on Gradscope, Thursday, Oct. 6, noon (before start of class)

General instructions: You can solve these problems by hand or with the assistance of a computer or calculator. However, when the problem asks you to "show your work," a single integer arithmetic operation (+, -, *, or /) or a single modular reduction (e.g., $45 = 6 \bmod 13$) counts as a single step that you should show.

There are three problems (remember to look at page 2).

Problem #1. Substitution Permutation Networks (20 points)

In this problem, consider a substitution permutation network composed of $8n$ bits, with $n = 2^s$, s a positive integer. The bits are labelled $j \in \{0, \ldots, 8n-1\}$, and j_i is the ith bit of the number j written in binary, with $i = 0$ corresponding to the least significant bit (the 1's place) and $i = s+2$ corresponding to the most significant bit (the $4n$'s place).

In the substitution permutation network, the bits are mixed with a key via XOR, then divided up into groups of 8 and passed through S-boxes. Bits whose labels agree on the most significant s places go into the same S-box. That is, bits 0–7 go into the first S-box, bits 8–15 go into the second S-box, and so on. The S-boxes take 8-bit inputs and produce 8-bit outputs.

Then the bits are passed to one of the following transformations, which relabel bit number j as bit number j' (for all j), completing one round. The same sequence of steps is repeated for many rounds.

Only one of the transformations below is a possible candidate to produce a substitution permutation network with an avalanche effect. Identify which one and for each of the candidates, describe your reasoning for why it is or is not the correct choice. (5 points for each candidate.)

a) $j \to j'$ with $j'_i = j_i$ except for $i = 0$, $j'_0 = 1 \oplus j_0$.

b) $j \to j'$ with $j'_i = j_i$ for i even and $j'_i = 1 \oplus j_i$ for i odd.

c) $j \to j'$ with $j' = 3j \bmod (8n)$.

d) $j \to j'$ with $j' = 4j \bmod (8n)$.

Problem #2. Modular Arithmetic Practice (20 points)

Calculate the following in modular arithmetic. Show your work (an integer operation or modular reduction counts as one step).

a) (3 points) $(15 + 23) \bmod 31$

b) (3 points) $(15 - 23) \bmod 31$

c) (3 points) $(15 * 23) \bmod 31$

d) (5 points) $(15/23) \bmod 31$

e) (6 points) $15^{23} \bmod 31$

Problem #3. Mathemagician Trick (20 points)

A mathemagician is giving a cryptography class. He writes on the board:

$$N = 12d + 31m,$$

and asks his students to think about their own birthdays and calculate N, where $d \in \{1, ..., 31\}$ corresponds to the day, and $m \in \{1, .., 12\}$ to the month. (For instance, if the birthday is May 15, then $N = 12(15)+31(5) = 335$). Then he asks them to tell their N, but not their birthdays. One by one he tells them their own birthdays: "$N = 136$," says one student. "April 1st," the mathemagician replies. "$N = 265$," proclaims another student. "You must have a lot of fun in your birthday, because you were born on July 4th," the mathemagician replies. And so on.

a) (5 points) If $N = 465$, compute its corresponding birthday (d, m). Show your work.

Hint:(for parts a and b) Try considering N mod q for useful values of q to simplify the formula for N.

b) (5 points) Suppose this were taking place in a world where there were 12^s months in the year and 31^s days in a month, and the formula was instead $N = 12^s d + 31^s m$. Describe an algorithm (in words, pseudocode, or if you prefer Python code) that will compute (d, m) given N. Your algorithm should run in a time polynomial in s. Give a basic explanation for why your algorithm works.

If you are presenting your algorithm in words or pseudocode, you may invoke subroutines for algorithms we described in class, such as Euclid's algorithm, without further detail about how those algorithms work.

c) (5 points) Prove for the original version of the problem (with $N = 12d + 31m$ and months and days as in our world) that there cannot be two (day, month) pairs (d, m) that produce the same number N.

Note: This is not quite the same as part b, besides the difference in the formula. In part b, you need to justify why your algorithm produces one of the correct answers, even if there are multiple possibilities. In part c, you must prove that there is only ever at most one possibility.

d) (5 points) If we change the formula, is it possible to have

$$N = 12d + 30m$$

for $N = 256$ and some integers d, m? If yes, find some pair (d, m). If not, explain why.