CSCE 222: Discrete Structures for Computing
Section 502 & 503
Fall 2020

YOUR NAME HERE

Homework 4

Due: 11 October (Sunday) before 11:59 p.m..
You must show your work in order to recieve credit.

Aggie Honor Statement: On my honor as an Aggie, I have neither given nor received any unauthorized aid on any portion of the academic work included in this assignment.

Checklist: Did you...

1. abide by the Aggie Honor Code?
2. solve all problems?
3. start a new page for each problem?
4. show your work clearly?
5. type your solution?
6. submit your solutions as a PDF unless otherwise specified?

Problem 1.
Show the sequence of numbers generated by a linear congruential random number generator with the following characteristic: How many numbers do you get without repeats?

$$\begin{aligned} X_{n+1} &= (aX_n + c) \mod m \\ m &= 7 \\ a &= 3 \\ c &= 1 \\ x_0 &= 1 \end{aligned}$$

Problem 2.
Let $P(n)$ be the statement that $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$ for positive integer n.

a. Show that $P(1)$ is true, completing the basis step of the proof.
b. What is the inductive hypothesis?
c. Complete the inductive step, identifying where you use the inductive hypothesis.

Problem 3.
One form of private key encryption uses an exclusive OR (XOR) to encrypt and decrypt messages. It uses the principle that $(M \oplus k) \oplus k = M$, where M a message and k is the encryption key.

Suppose, for instance, that your plaintext message is "Gig 'em!" and the numeric key you have chosen is 0x0F (15 in base 10). Each character in the message will be processed XORing it with the key. For instance, 'G' has an ASCII code of 0x47 ($= 71_{10}$), $0x47 \oplus$ 0x0F = 0x48 = 'H'; 'i' has an ASCII code of 0x69 ($= 105_{10}$), $0x69 \oplus$ 0x0F = 0x66 = 'f', etc.

Continuing the process, we obtain the ciphertext message "Hfh/(jb.". In the same way, we can apply the same key to decrypt our ciphertext back to the original plaintext message "Gig 'em!".

Write a computer program (in the language of your choice, C, C++, Java, Python, Ada, assembly language, etc. ...) that will accept a plaintext string and a numeric key in the range in the range 0-31, apply the the key character by character, and display the resulting ciphertext. Turn in a screenshot of your program encrypting a text and giving its output, followed by you inputting the ciphertext result and showing that the same program can be used to decrypt back to the original plaintext. Also, submit a text file containing your source code.

Problem 4.
Use mathematical induction to prove that $3^n > 2n^2 + 3n$ whenever n is an integer greater than or equal to 4.

a. What is the basis?
b. Complete the basis step of the proof.
c. What is the inductive hypothesis?
d. Complete the inductive step, identifying where you use the inductive hypothesis.

Problem 5. Bonus:
(Recall what you have learned about the binary number system.) Use strong induction to show that every positive integer n can be written as a sum of distinct powers of two, that is, as a sum of a subset of the integers $2^0 = 1, 2^1 = 2, 2^2 = 4$, and so on. (Hint: For the inductive step, separately consider the case where $k + 1$ is even and where it is odd. When $k + 1$ is even, note that $(k + 1)/2$ is an integer.)