Fall 2020 CIS 3362 Quiz #4 Part B: Miller-Rabin, Factoring, Fast Mod Expo

Date: 10/26/2020

Directions: Please use your course notes and a calculator as aids for this exam. Do NOT attempt to look up information online. Even if you use a calculator, show each step of your calculations that you would do by hand. The role of the calculator will simply be to speed up individual calculations (13 x 29, for example), not to skip whole steps, as these steps are typically awarded points in the grading criteria.

Please either type your answers. The accepted file types for submission will be .doc, .docx, .txt and .pdf. I recommend that you directly type into the posted document to save time.

Please look at Webcourses to see when your due time and late due time are. It's recommended that you stop working at the due time and start uploading at that time. Anything turned in before the late due time will be accepted for full credit. Anything that doesn't make it in by the late due time will earn a 0. A 10 minute buffer will be provided after both due times. Please don't take advantage of these buffers as it's an unnecessary risk.

1) (8 pts) In the Miller-Rabin primality test, when testing if a positive integer n is prime or not, instead of calculating a^{n-1} mod n only, where a is a randomly selected integer in between 2 and n-1, a raised to several different powers mod n are potentially calculated. If n = 1281, what are all of the possible exponents for which the Miller-Rabin primality test might raise a randomly chosen a?

2) (8 pts) Using Fermat Factoring, determine the factorization of 1541. Please build a table similar to the one shown in class to show your work.

3) (8 pts) Write a function, in C, that determines the maximum integer k for which an integer n is divisible by p^k, where p is a given integer greater than 1. For example, numTimesDivide(48, 2) should return 4, numTimesDivide(243000, 3) should return 5, and numTimesDivide(100, 7) should return 0.) The function prototype is provided below:

```
int numTimesDivide(int n, int p);
```

4) (1 pt) After what mathematician are Catalan numbers named?