Virtual Class, Week 8

MATH 601, Spring 2020

Algebraic Topics in Computing: Cryptography

Welcome to our first week of Virtual MATH 601! Please follow these instructions:

1. **Read** 11.1 in the Savin **text**.
2. **Read the full lecture notes** for Week 8 in the **Daily Update**.
3. Access Blackboard, and **watch the instructional videos** entitled
   (a) Miller Rabin Example
   (b) Parity of Discrete Log Solution
4. Complete the following **homework problems** and submit your solutions to Gradescope by **next Tuesday** (3/31) at midnight.

   Instructions for homework submission:

   (a) You should have received an email from Gradescope telling you that you are enrolled in their MATH 601 roster. Use the link provided to set up an account, using your KU email address.
   (b) If you use the typesetting program `LaTeX`, compile your homework as a PDF.
   (c) If you handwrite your solutions, either scan your homework, or follow the instructions here to turn your homework into a PDF.
   (d) Follow the instructions on the last page of this same document to submit your homework PDF on Gradescope.

   Homework Problems: As usual, show all your steps in each problem. If you use *fast exponentiation*, point this out and omit the actual calculation.

   Problems #1 and #3 apply material covered before Spring Break; see Daily Update 2/25 and Savin 10.3 for details of the *Baby-step, giant step method* for solving discrete logarithms, and see Daily Update 3/5 and Savin 11.1 for *Carmichael numbers* and *Korselt's criterion*.

   1. (10 points) A key k is exchanged using the Diffie-Hellman method with $p = 421$ and $g = 2$. The numbers exchanged over a public channel are $X = 229$ and $Y = 247$. Compute k using the baby-step giant-step method.
   2. (5 points) It can be checked that 5 is a primitive root modulo the prime 1223. You are interested in the discrete logarithm problem $5^x \equiv 3 \mod 1223$. Given that $3^{611} \equiv 1 \mod 1223$, determine whether a solution x is odd or even *without finding a solution.*

3. (15 points) Use Korselt's criterion to determine which of the following are Carmichael numbers:

   (a) 1517 (b) 6601 (c) 41041

4. (15 points) Use the Miller-Rabin test to show that the following numbers are composite:

   (a) 899 (b) 3599 (c) 38200901201

5. Download the **Extended Euclidean Algorithm/RSA** Programming Investigation Module and get started. This module is **due on Friday, April 10**. It is more involved that the first programming assignment, so please start early! After completing the assignment, upload the full file with *.ipynb* extension to Gradescope.

6. Access **Virtual Office Hours** on Blackboard with any questions. You can submit a question by clicking *Add your own* and uploading a picture of a piece of paper, a PDF, or even just a voice recording. If you upload a visual, click *Comment* to explain your question vocally! (*Please do not share your full answer to a question, since some students may have not finished the problem when they check out Virtual Office Hours.*)

   Though I will respond to submissions frequently, students can also reply to any other student's question, or ask follow-up questions. Check out the **example question and answer** that I uploaded on Blackboard.

7. Interested in delving deeper into this week's topics?

   - For the proof that over 75% of integers $1 < a < n-1$ are witnesses to the fact that an odd composite n is is in fact composite using Miller-Rabin appears is Theorem 2.9 in this document.
   - You might also check out out this article on modern primality tests
   - Try the following challenge problem for fun: Assuming k is an integer such that each of the three factors below is prime, prove that

     $$(60k + 41)(90k + 61)(150k + 101)$$

     is a Carmichael number.