University at Albany, SUNY

College of Engineering and Applied Sciences, Computer Science

ICEN/ICSI-210: Discrete Structures

Spring 2019

Homework Set 7

Chengjiang Long

Assigned Date: Mar 11, 2019 (Monday).
Due Date: Mar 25, 2019 (Monday), 11:59 PM.
Collaboration Policy. Homeworks will be done individually: each student must hand in their own answers. Use of partial or entire solutions obtained from others or online is strictly prohibited.
Late Policy. If urgent or unusual circumstances prohibit you from submitting a homework assignment in time, please e-mail the instructor explaining the situation to get exempt from late penalty. Otherwise, any late submissions without consent from the instructor will result in exponential penalty – late for one day loses 25%, two days loses 50%, and so on and so forth. **Those submissions $\geq$ 3 hours after the deadline will be considered as "late submission" with no exemption.**
Submission Format. Electronic submission as a PDF file to blackboard is mandatory.

- You can write your solution in Word and save it as a PDF file.
- You also can write it on any physical papers and scan them to a PDF file.
- If you don't have condition to scan, you still can take pictures by your smart phone and convert images to a PDF file by the online tool (https://imagetopdf.com).
- If you have multiple PDF files, please combine them to a PDF file by the online tool (https://www.pdfmerge.com) or (https://www.ilovepdf.com/merge_pdf).

Problem 1: Prime and Composite (15 points)

(a) [5 points] Determine whether 119 is prime with detailed explanation.

(b) [10 points] Determine whether the integers in the set $\{17, 18, 19, 23\}$ are pairwise relatively prime.

Problem 2: GCD and LCM (45 points)

(a) [5 points] What are the greatest common divisor and the least common multiple for $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$.

(b) [10 points] Find gcd(1000, 625) and lcm(1000, 625) and verify that gcd(1000, 625) · lcm(1000, 625) = 1000 · 625.

(c) [10 points] Show that if a and b are positive integers, then ab = gcd(a,b) · lcm(a,b). [**Hint***: Use the prime factorizations of a and b and the formulae for gcd(a,b) and lcm(a,b) in terms of these factorizations.*]

(d) [10 points] Use the Euclidean algorithm to find gcd(12345, 54321).

(e) [10 points] Use the Euclidean algorithm and the conclusion in (c) to find lcm(1529, 14038).

Problem 3: Integer Representations (30 points)

Encrypt the message "WATCH YOUR STEP" by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

(a) $f(p) = (p + 14)$ **mod** 26.

(b) $f(p) = (14p + 21)$ **mod** 26.

(c) $f(p) = (-7p + 1)$ **mod** 26.

Problem 4: Modular Exponentiation (20 points)

Decrypt these messages encrypted using the shift cipher $f(p) = (p+10)$ **mod** 26.

(a) CEBBOXNOB XYG

(b) LO WI PBSOXN

(c) DSWO PYB PEX

[Optional] Extra Points (20 points)

In the RSA cryptosystem, each individual has an encryption key (n, e) where $n = pq$, the modulus is the product of two large primes p and q, say with 200 digits each, and an exponent e that is relatively prime to $(p - 1)(q - 1)$. To produce a usable key, two large primes must be found. This can be done quickly on a computer using probabilistic primality tests, referred to earlier in this section. However, the product of these primes $n = pq$, with approximately 400 digits, cannot, as far as is currently known, be factored in a reasonable length of time. As we will see, this is an important reason why decryption cannot, as far as is currently known, be done quickly without a separate decryption key.

(a) [10 points] Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers.

(b) [10 points] What is the original message encrypted using the RSA system with $n = 43 \cdot 59$ and $e = 13$ if the encrypted message is 0667 1947 0671?

[**Hint**: *To decrypt, first find the decryption exponent d which is the inverse of $e = 13$ modulo $42 \cdot 58$.*]