CS 2050 Spring 2023 Homework 7

Due: March 17th

Released: March 10th

i. This assignment is due on **11:59 PM EST, Friday, March 17, 2023**. Early submissions (24+ hours in advance) receive 2.5 points of extra credit. You may turn it in one day late for a 10 point penalty or two days late for a 25 point penalty. Assignments more than two days late will NOT be accepted. We will prioritize on-time submissions when grading before an exam.

ii. You will submit your assignment on **Gradescope**. Solutions must be recorded on a typeset (e.g. using LaTeX) or *neatly* written PDF.

iii. Ensure that all questions are correctly assigned on Gradescope. Questions that take up multiple pages should have all pages assigned to that question. Incorrect page assignments will lead to point deductions.

iv. You may collaborate with other students, but any written work should be your own. Write the names of the students you work with on the top of your assignment.

v. Always justify your work, even if the problem doesn't specify it. It can help the TA's to give you partial credit.

Author(s): David Teng and Ronnie Howard

1. Show your work. You may not bruteforce by checking x values until you find one that works. Use the Chinese Remainder Theorem to find all values x such that: (20 points)
   $x \equiv 2 \pmod{5}$
   $x \equiv 3 \pmod{7}$
   $x \equiv 4 \pmod{8}$

   1. Check if 5,7,8 are coprimes

   $$\gcd(5,7) = 1$$

   $$\gcd(5,8) = 1$$

   $$\gcd(7,8) = 1$$

   5,7,8 are coprimes.

   2. $M = 5 * 7 * 8 = 280$
   3.

m_i	a_i	$\bar{m_i} = \frac{M}{m_i}$	u_i	$a_i * m_i * u_i$
5	2	$\frac{280}{5} = 56$	$56 \equiv_5 1 \rightarrow u_i = 1$	112
7	3	$\frac{280}{7} = 40$	$40 \equiv_7 5 \rightarrow u_i = 3$	360
8	4	$\frac{280}{8} = 35$	$35 \equiv_8 3 \rightarrow u_i = 3$	420

   $$x \equiv (112 + 360 + 420) \mod 280$$

   $$\equiv 892 \mod 280$$

   $$\equiv 52 \mod 280$$

2. The following statement was put through a Caeser cipher using a shift of 13. Decrypt the bolded portions of the statement: (10 points)

   "Cvarnccyr cvmmn vf fvzcyl fhcrevbe guna abezny cvmmn"

   Pineapple pizza is simply superior than normal pizza

3. Encrypt the following statement using a shift cipher of 17: RONNIE MADE THIS QUESTION (10 points)

   YVUUPL THKL AOPZ XBLZAPVU

4. Encrypt the plaintext message **"I ALSO MADE THIS ONE"** using the transposition cipher with blocks of five, based on the permutation σ of $\{1, 2, 3, 4, 5\}$ defined by $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 5$, $\sigma(4) = 1$, and $\sigma(5) = 4$. (10 points)

IALSOMADETHISONE
IALSO MADET HISON EXXXX

SIAOL EMATD OHINS XEXXX

5. Decrypt the ciphertext message **“wettyniffyxt”** which was produced using the transposition cipher with blocks of three, based on the permutation σ of $\{1, 2, 3\}$ defined by $\sigma(2) = 1, \sigma(3) = 2, \sigma(1) = 3$. (10 points)

   wettyniffyxt
   wet tyn iff yxt
   twe nty fif tyx

   twentyfiftyx

6. Encrypt the message “MATHISFUN” using the RSA system with n = 77 and e = 17. (15 points)

$$C(M) = M^e \mod N = M^{17} \mod 77$$

$$\begin{aligned}
C(\text{"M"}) = C(12) = 12^{17} \mod 77 = 45 \\
C(\text{"A"}) = C(00) = 0^{17} \mod 77 = 0 \\
C(\text{"T"}) = C(19) = 19^{17} \mod 77 = 24 \\
C(\text{"H"}) = C(07) = 7^{17} \mod 77 = 28 \\
C(\text{"I"}) = C(08) = 8^{17} \mod 77 = 57 \\
C(\text{"S"}) = C(18) = 18^{17} \mod 77 = 72 \\
C(\text{"F"}) = C(05) = 5^{17} \mod 77 = 3 \\
C(\text{"U"}) = C(20) = 20^{17} \mod 77 = 48 \\
C(\text{"N"}) = C(13) = 13^{17} \mod 77 = 62
\end{aligned}$$

45 00 24 28 57 72 03 48 62

7. Suppose you intercept the message “09 11 49 52 49 33 52 02 00 10 17 39 08 13 09 52 02 17 52 10” that has been encrypted using the RSA algorithm. You know that the public key used for encryption is (55, 23). Decrypt the message to determine what was said. Use the process shown in lecture to complete this problem. You must show all work. (15 points)

   (*Note*: If your calculator is unable to calculate $a^d mod n$ where a is one of the numbers in the message above and d is the decryption key, then you can just show $a^d mod n$ for each value of a. Note that this is the final step in decryption so you won't show what the message actually was. You must still show the work for calculating the decryption key d).

   To find decryption key, we know e is relatively prime to $\phi(n)$

$$p = 11, \quad q = 5, \quad e = 23$$

$$ed = 1 \mod \phi(n)$$

$$\phi(n) = (p-1)(q-1) = (10)(4) = 40$$

$$23d \equiv 1 \mod 40$$

$$1, 41, 81, 121, 161$$

$$23(7) = 161$$

$$d = 7$$

   Determine blocksizes 25 < 55, $N = 1$
   Decrypt $p = c^d \mod n$

$$09^7 \mod 55 = 4 = \text{E}$$

$$11^7 \mod 55 = 11 = \text{L}$$

$$49^7 \mod 55 = 14 = \text{O}$$

$$52^7 \mod 55 = 13 = \text{N}$$

$$49^7 \mod 55 = 14 = \text{O}$$

$$33^7 \mod 55 = 22 = \text{W}$$

$$52^7 \mod 55 = 13 = \text{N}$$

$$02^7 \mod 55 = 18 = \text{S}$$

$$00^7 \mod 55 = 0 = \text{A}$$

$$10^7 \mod 55 = 10 = \text{K}$$

$$17^7 \mod 55 = 8 = \text{I}$$

$$39^7 \mod 55 = 19 = \text{T}$$

$$08^7 \mod 55 = 2 = \text{C}$$

$$13^7 \mod 55 = 7 = \text{H}$$
$$09^7 \mod 55 = 4 = \text{E}$$
$$52^7 \mod 55 = 13 = \text{N}$$
$$02^7 \mod 55 = 18 = \text{S}$$
$$17^7 \mod 55 = 8 = \text{I}$$
$$52^7 \mod 55 = 13 = \text{N}$$
$$10^7 \mod 55 = 10 = \text{K}$$

ELONOWNSAKITCHENSINK
ELON OWNS A KITCHEN SINK

8. Use mathematical induction, prove that $3+7+11+\cdots+(4n-1) = n(2n+1)$ for all positive integers n. (10 points)

Proof through mathematical induction that Let $\mathrm{P}(n) = 3+7+11+\cdots+(4n-1) = \sum_{j=1}^{1} 4n-1 = n(2n+1)$ through mathematical induction that $\forall n \in \mathbb{Z}^+, \mathrm{P}(n)$

Base Step: $\mathrm{P}(1)$ because $(4(1)-1=3) = ((1)(2(1)+1)=3) = 3$. This completes basis step.

Induction Hypothesis: Assume $\mathrm{P}(k) = 3+7+11+\cdots+(4k-1) = k(2k+1)$ is true for fixed arbitary integer $k \geq 1$.

Induction Step

1. $3+7+11+\cdots+(4k-1) = k(2k+1)$ (Induction Hypothesis)
2. $3+7+11+\cdots+(4k-1)+(4(k+1)-1) = k(2k+1)+(4(k+1)-1)$ (Add $4(k+1)-1$ to both sides (1))
3. $3+7+11+\cdots+(4k-1)+(4(2k)-1) = 2k^2+5k+3$ (Simplify (2))
4. $3+7+11+\cdots+(4k-1)+(4(2k)-1) = (2k+3)(k+1)$ (Factorize (3))
5. $3+7+11+\cdots+(4k-1)+(4(2k)-1) = (k+1)(2(k+1)+1)$ (Expand $2k+3$ (4))

By (5), we now see that $\mathrm{P}(k+1) : 3+7+11+\cdots+(4k-1)+(4(k+1)-1) = k(2k+1)+(4(k+1)-1)$ is true whenever $\mathrm{P}(k)$ is true. This completes the induction step.

By mathematical induction, $\mathrm{P}(n)$ is true $n \in \mathbb{Z}^+$