CS111 W'24 ASSIGNMENT 2

Problem 1:

Prove the following statement:
If $p > 5$ and $gcd(p, 20) = 1$, then $(p^2 - 21)(p^2 + 16) \equiv 0 \pmod{20}$.

Hint: The product of any k consecutive integers is divisible by k.

Problem 2:

Alice's RSA public key is $P = (e, n) = (7, 4453)$. Bob sends Alice the message by encoding it as follows. First he assigns numbers to characters: A is 8, B is 9, ..., Z is 33, a blank is 34, quotation marks: 35, a coma: 36, a period: 37, an apostrophe: 38. Then he uses RSA to encode each number separately.

Bob's encoded message is:

```
1400 2218   99 2088 4191   84  843   99 4191 3780  764 4191 2979 2269   99  764
2218 2269 2088  843 3015   99 2970 1443 1655   99 3237 2979   99  447 1443 3237
1032 2382  871  843 1655   99  871 1443   99 4242  843   99 4191 2269   99  843
4191 2269 2979   99  871 1443   99 2382 2269  843   99 4191 2269   99 3237 2979
  99  871  843 3780  843 1032 2088 1443 2962  843 2916   99 3237 2979   99  764
2218 2269 2088   99 2088 4191 2269   99  447 1443 3237  843   99  871 1655 2382
 843   99 4242  843  447 4191 2382 2269  843   99 2218   99  447 4191 2962   99
2962 1443   99 3780 1443 2962 1294  843 1655   99 2970 2218 1294 2382 1655  843
  99 1443 2382  871   99 2088 1443  764   99  871 1443   99 2382 2269  843   99
3237 2979   99  871  843 3780  843 1032 2088 1443 2962  843 2916 1400
```

Decode Bob's message. Notice that you only know Alice's public key, but don't know the private key. So you need to "break" RSA to decrypt Bob's message. For the solution, you need to provide the following:

(a) Describe step by step how you arrived at the solution: show how to find p and q, $\phi(n)$ and d.

(b) Show your work for one integer in the message (M = 2218): the expression, the decrypted integer, the character that it is mapped to.

(c) To decode the remaining numbers, you need to write a program in C++ (see below), test it in Gradescope, and append the code to HW 2, Problem 2 solutions.

(d) Give the decoded message (in integers).

(e) Give Bob's message in plaintext. What does it mean and who said it?

For part (c). Your program should :

(i) Take three integers, e, n (the public key for RSA), and m (the number of characters in the message) as input to your program. Next, input the ciphertext.

(ii) Test whether the public key is valid. If not, output a single line "Public key is not valid!" and quit the program.

(iv) If the public key is valid, decode the message.

(v) Output p and q, $\phi(n)$ and d.

(vi) On a new line, output the decoded message in integers.

(vii) On a new line, output the decoded message in English. The characters should be all uppercase. You can assume that the numbers will be assigned to characters according to the mapping above.

More information and specifications will be provided separately.

Upload your code to Gradescope to test. There will be 15-16 (open and hidden) test cases. Your score for the RSA code will be based on the score that you received in Gradescope. If you have any questions, post them on Slack.

Problem 3:

(a) Compute $5^{1627} \pmod{12}$. Show your work.

(b) Compute $8^{-1} \pmod{17}$ by listing the multiples. Show your work.

(c) Compute $8^{-1} \pmod{17}$ using Fermat's Little Theorem. Show your work.

(d) Compute $8^{-11} \pmod{17}$ using Fermat's Little Theorem. Show your work.

(e) Find an integer x, $0 \leq x \leq 40$, that satisfies the following congruence: $31x + 54 \equiv 16 \pmod{41}$. Show your work. You should not use brute force approach.

Academic integrity declaration. The homework papers must include at the end an academic integrity declaration. This should be a brief paragraph where you state *in your own words* (1) whether you did the homework individually or in collaboration with a partner student (if so, provide the name), and (2) whether you used any external help or resources.

Submission. To submit the homework, you need to upload the pdf and cpp files to Gradescope. If you submit with a partner, you need to put two names on the assignment and submit it as a group assignment.

Reminders. Remember that only LaTeX papers are accepted.