CS/MATH111 ASSIGNMENT 2

Problem 1:

Let $n = p_1 p_2 ... p_k$, where $p_1, p_2, ..., p_k$ are different primes. Prove that n has exactly 2^k different divisors. For example, if $n = 105$, then n $= 3 \cdot 5 \cdot 7$, so $k = 3$, and thus n has $2^3 = 8$ divisors. These divisors are: $1, 3, 5, 7, 15, 21, 35, 105$. Hint. You can reduce the problem to counting other objects that we already know how to count. Alternatively, this can be proved by induction on k.

Problem 2: Alice's RSA public key is $P = (e, n) = (13, 77)$. Bob sends Alice the message by encoding it as follows. First he assigns numbers to characters: A is 2, B is 3, ..., Z is 27, and blank is 28. Then he uses RSA to encode each number separately.

Bob's encoded message is:

10	7	58	30	23	62
7	64	62	23	62	61
7	41	62	21	7	49
75	7	69	53	58	37
37	41	10	64	50	7
10	64	21	62	61	35
62	61	62	7	52	10
21	58	7	49	75	7
62	26	22	53	30	21
10	37	64			

Decode Bob's message. Notice that you don't have Bob's secrete key, so you need to "break" RSA to decrypt his message.

For the solution, you need to provide the following:

- Describe step by step how you arrived at the solution. In particular, explain how you determined p, q, $\phi(n)$, and d.
- Show the calculation that determines the first letter in the message from the first number in ciphertext.
- Give Bob's message in plaintext. The message is a quote. Who said it?
- If you wrote a program, attach your code to the hard copy. If you solved it by hand (not recommended), attach your scratch paper with calculations for at least 5 first letters.

Suggestion: this can be solved by hand, but it will probably be faster to write a short program.

Problem 3: (a) Compute $13^{-1} \pmod{19}$ by enumerating multiples of the number and the modulus. Show your work.

(b) Compute $13^{-1} \pmod{19}$ using Fermat's theorem. Show your work.

(c) Compute $13^{-40} \pmod{19}$ using Fermat's theorem. Show your work.

(d) Find a number $x \in \{1, 2, ..., 36\}$ such that $8x \equiv 3 \pmod{37}$. Show your work. (You need to follow the method covered in class; brute-force checking all values of x will not be accepted.)

Submission. To submit the homework, you need to upload the pdf file into gradescope by Friday, May 4 (noon).