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 $P = (e, n) = (23, 55)$. 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:

51	12	51	39	31	21
14	10	20	17	7	25
14	26	33	52	15	7
27	51	7	49	8	15
51	7	8	25	7	25
10	49	18	52	51	7
8	25	7	18	26	25
25	10	27	52	51	7
27	33	21	7	20	26
21	7	25	10	49	18
52	51	39			

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:

- (a) Describe step by step how you arrived at the solution.
- (b) Show your work (the computation) for the first three numbers in the message.
- (c) Give Bob's message in plaintext (also, what does it mean and who said it?).
- (d) Show (attach) your code or computations for the remaining numbers. The code can be written in any programming language. If all computations are done by hand, please attach your work as well.

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

Problem 3: (a) Compute $11^{-1} \pmod{19}$ by enumerating multiples. Show your work.
(b) Compute $11^{-5} \pmod{19}$ using Fermat's Little Theorem. Show your work.
(c) Use Fermat's Little Theorem to compute $5^{1209640} \pmod 7$. Show your work.
(d) Find an integer x, $0 \leq x \leq 40$, that satisfies $31x = 3 \pmod{41}$. Show your work.

Submission. To submit the homework, you need to upload the pdf file into ilearn and Gradescope.

Reminders. Remember that only $\LaTeX$ papers are accepted.