HW 3 FEEDBACK

(1) **Question 7 of Sec. 6.8** Many of you wrote answers like *"divide the expression* $2m \pmod n$ *by* 2 *" or "divide by* 2 $\pmod n$*"*. We think that this is not ideal for conceptual understanding but at the same time we understand that in Textbook Sec. 3.3.1- 3.3.2, the authors really use the word 'divide'.

Later in the course, you will learn the elementary theory of groups. We almost never say 'divide' in this setting. Going back to the question, it is more appropriate to say '**multiply** $2^{-1} \pmod n$ to the expression $2m \pmod n$' instead. Here $2^{-1} \pmod n$ is the inverse of 2 $\pmod n$ and is defined by $2 \cdot 2^{-1} \equiv 1 \pmod n$.

(2) **Question 9 (b) of Sec. 6.8**. Most of you mention that it follows from part (a) and the Chinese Remainder Theorem. We would say this is acceptable. Nonetheless for your reference, we would like to point out that you are actually using the statement of the intermediate lemma in pp. 76 of the Textbook.

(3) **Question 9 (b) of Sec. 6.8**. There are inaccuracies in some of your argument. For example, a number of you wrote something like:

"Consider the system of congruence

$$\begin{cases} x^{\frac{\phi(n)}{2}} \equiv 1 \pmod p \\ x^{\frac{\phi(n)}{2}} \equiv 1 \pmod q. \end{cases} \tag{0.1}$$

There exists a unique solution $\pmod n$ *. . . "*

First of all, there is **no** equation here to solve as x is already **given** to you by the question! Moreover, this system is not linear and thus may **not** have unique solution $x \pmod n$.

Some of you try to write "there is unique solution $x^{\frac{\phi(n)}{2}} \pmod n$ to the system (0.1)". However, this is ambiguous and improper. When you talk about solutions to (0.1), it always means $x \pmod n$.

(4) **Question 9 (b) of Sec. 6.8** Some of you needed to handle the equation $\alpha p = \beta q$ in the argument, where p, q are the distinct odd primes given by the question, but wrongly concluded that $\alpha = q$ and $\beta = p$. In fact, the correct conclusion is that $\alpha = qk$ and $\beta = pk$ for some integer k.

(5) **Question 16**. Some of you say *"Eve can find the message* m *by computing* $m^{e_A x + e_B y} \pmod n$*, where* $e_A x + e_B y = 1$*"*. However, this is unreasonable in practice. It is important to keep in mind that right now you want to decrypt and you should have no knowledge about the original message "m". The correct and reasonable (both mathematically and practically) answer is $c_A^x c_B^y \pmod n$.

Date: October 3, 2018.