IT 105 – Principles of Programming

Day 17

1. Signature Assignment.
2. Portfolium Instructions.
3. Look up an ISBN-10 number for a book, and share it, ***WITHOUT*** the last digit. "Find" the last digit with `ISBN.xlsx` and compare.
4. The last digit is a ***checksum***. It's used to try to avoid the most common errors that happen in reading a code:
    a. Misreading a single digit.
    b. Transposition of adjacent digits.
5. The checksum is calculated using modular arithmetic. Here, the remainder is "more important" than the quotient.
6. Modular arithmetic exercise:
   When N eggs in a basket are removed 5 at a time, ultimately none remain. However, if these N eggs are removed 2 at a time, then 1 remains. If removed 4 at a time, then 3 remain. What is the smallest possible value of N?

   N % 5 = 0 → ***N is a multiple of 5***
   N % 2 = 1 → ***N is odd***
   N % 4 = 3
   5 ~~***10***~~ ***15*** ~~***20***~~ ***25***
   5%4=1 ***15%4=3***

7. Modular arithmetic plays an important role in Cryptology.
8. Cryptology is the most general term:
    a. Cryptography – methods to make message secret.
    b. Cryptanalysis – attacking or finding weakness in ciphers.
9. When we make our messages secret, we have to be sure the process is invertible (can be undone), or the receiver won't be able to read them!
10. Caesar Square.
11. Caesar Cipher (using ASCII).
12. Caesar Cipher w/shift.
13. These cryptosystems require a private key, which could be problematic. *If I am sending you an encrypted message, how do I also get the private key to you securely, so you can unlock it?*
14. Public Key cryptosystem, such as RSA, do NOT use private keys.
15. Public Key cryptosystem example:
    a. Alice has a public key, P_A.

b. Alice has a secret key, S_A
c. If Bob wants to send Alice a message, he uses her freely available public key, P_A to encrypt the message.
d. This ciphertext is then sent to Alice.
e. When she receives the message, she decrypts it using her secret key, S_A.

$M \rightarrow \boxed{P_A} \rightarrow C = P_A(M) \rightarrow \boxed{S_A} \rightarrow M$

16. As opposed to the methods covered above, Steganography is “hiding in plain sight.”
17. Steganography slides.