COMP90043: Cryptography and security
Week 2: Workshop Questions

Preparation:

(1) Please revise Euclid's algorithm discussed in the lectures before going to the workshop.
(2) Please study the notes on Introduction security.

Questions:

(1) Modulo Arithmetic. Two integers p and q are said to be congruent modulo n, if $(p \bmod n) = (q \mod n)$. This is written as $p \equiv q \pmod{n}$. Solve the following pairs of numbers using modulo arithmetic:
   (a) $73 \bmod 23 =$ .....
   (b) $-11 \bmod 7 =$ .....
   (c) $(-13)^2 \bmod 9 =$ .....
   (d) $32 \bmod 19 =$ .....
   (e) $(-2)^3 \bmod 17 =$ .....
   (f) $(-1) \bmod 19 =$ .....
(2) Greatest Common Division (GCD) A GCD is defined as the largest number m which divides two numbers p, and q. Find the GCD for the following pairs of numbers using the Euclid's algorithm: Make sure that you understand the process. You should be able to carry out the computations on a new set of numbers. Try creating your examples.
   (a) $GCD(60, 24) =$ .....
   (b) $GCD(30, 105) =$ .....
   (c) $GCD(1473, 1562) =$ .....
(3) For each of sub questions in the above question, apply extended Euclidean algorithm and represent the gcd as a linear sum of the function operands.
(4) When considering Data, stored digitally, how would you determine the satisfaction of the following criteria:
   (a) Confidentiality
   (b) Integrity
   (c) Availability
   (d) Authentication
   (e) Accountability

(f) Which one of the three do you think is the MOST important?

(5) Security Attacks and Threats:
   (a) Define a Security Threat and a Security Attack.
   (b) Define the following attacks:
      (i) Denial of Service
      (ii) Release of Message Contents
      (iii) Message Modification
      (iv) Masquerade
      (v) Traffic Analysis
      (vi) Replay
   (c) From the above, identify which constitute as active attacks and which constitute as passive attacks?