COMP90043 Cryptography and Security
Semester 2, 2020, Workshop Week 2
Lecturer: Prof. Udaya Parampalli

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 $(p \bmod n) = (q \bmod n)$. 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) 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. When considering Data, stored digitally, how would you determine the satisfaction of the following criteria:
   (a) Confidentiality make sure the sending information is not captured by others
   (b) Integrity ensure message not to be modified by intruder
   (c) Availability assure the service is not denied by other unauthorized users
   (d) Authentication guarantee the identity of sender
   (e) Accountability system can trace back to historical data

   Which one of the three (Confidentiality, Integrity and Availability) do you think is the MOST important?
4. Security Attacks and Threats:
   (a) Define a Security Threat and a Security Attack.
   (b) Define the following attacks:
      i. Denial of Service active attack; the server receives so many requests from attacker that cannot handle normal requests
      ii. Release of Message Contents passive attack; intercept one's information and share with others
      iii. Message Modification active attack; tamper one user's message
      iv. Masquerade active attack; pretend one user's identity and communicate with others
      v. Traffic Analysis passive attack; analyze pattern of network traffic
      vi. Replay active attack; hijack a request from one entity, and send it to another one later for unauthorized effect
   (c) From the above, identify which constitute as active attacks and which constitute as passive attacks?