COMP90043: Cryptography and Security

Week 2 Workshop Activity

Semester 2, 2016

(Problems are from the text by Stallings, 5th & 6th edition)

Before we begin, take a few minutes to discuss the following:

1. 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?

2. Number Theory
   a) 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:
   i. 73 mod 23 = 4
   ii. -11 mod 7 = 3
   iii. $(-13)^2$ mod 9 = 7
   b) 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:
   i. GCD(60, 24) = 12
   ii. GCD(30, 105) = 15
   iii. GCD(1473, 1562) = 1

3. 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?

4. Homework
    On your own, please read up on the Euclidean Algorithm, and the Extended Euclidean algorithm to understand how the principles of modulo arithmetic are applied in order to obtain the GCD for two given integers. We will be applying these concepts in coming weeks.