## COMP90043: Cryptography and security
## Week 2: Workshop Questions - with solutions

### 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) $73 \bmod 23 = 4$
  (b) $-11 \bmod 7 = 3$
  (c) $(-13)^2 \bmod 9 = 7$
  (d) $32 \bmod 19 = 13$
  (e) $(-2)^3 \bmod 17 = 9$
  (f) $(-1) \bmod 19 = 18$

(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) $GCD(60, 24) = 12$
  (b) $GCD(30, 105) = 15$
  (c) $GCD(1473, 1562) = 1$

(3) When considering Data, stored digitally, how would you determine the satisfaction of the following criteria:
  (a) Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
  (b) Integrity: Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.
  (c) Availability: Ensuring timely and reliable access to and use of information.

(d) Authentication: Is the property of being genuine and being able to be verified and trusted.

(e) Accountability: Is a security goal that requires all actions of an entity to be traced uniquely to that entity.

(f) Which one of the three (Confidentiality, Integrity or Availability) do you think is the MOST important? Depends on the circumstances but some examples to discuss include (these examples are also relevant to the next question):

  (i) students at University of Melbourne and their personal data and marks

  (ii) wifi-enabled pacemaker or other critical medical device

  (iii) online banking and/or buying/selling stock

  (iv) physical security at an airport (not data but useful to think about threats and attacks)

(4) Security Attacks and Threats:

(a) Define a Security Threat and a Security Attack: A Security Threat is a possible danger that might exploit a vulnerability A Security Attack is an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

(b) Define the following attacks:

  (i) Denial of Service: is an attack which prevents of inhibits the normal use or management of communications facilities.

  (ii) Release of Message Contents: is an attack in which the contents of a message or transmission are either directly or indirectly released.

  (iii) Message Modification: Is an attack which aims to alter a part or whole of a legitimate message as a means of delaying or reordering in order to produce an unauthorized effect.

  (iv) Masquerade: A masquerade takes place when one entity pretends to be a different entity.

  (v) Traffic Analysis: is an attack which aims to analyse data and information going across the network in order to infer the details of the message and/or communication.

(vi) Replay: Is an attack that passively captures a data unit and subsequently retransmits it to produce an unauthorized effect.

(c) From the above, identify which constitute as active attacks and which constitute as passive attacks?

An active attack is one that involves some modification of the data stream or the creation of a false stream. From the above, the following constitute as active attacks:

(i) Denial of Service
(ii) Message Modification
(iii) Masquerade
(iv) Replay

A passive attack involves the eavesdropping or monitoring of transmissions with the goal of obtaining information that is being transmitted. From the above, the following constitute as passive attacks:

(i) Release of Message Contents
(ii) Traffic Analysis