COMP90043: Cryptography and security
Week 3: Workshop Questions

Preparation:

(1) Please revise the Extended Euclid's algorithm before going to the workshop (ExtendedEuclid.pdf).

Questions: Part A

(1) What is a cipher? What does it do? And, in general, how does it go about doing this?

(2) What is a block cipher and a stream cipher?

(3) What is a one time pad? Discuss the practical applicability of the scheme in security?

(4) Now that we have defined our definitions, lets apply this in a more practical setting:

  (a) What is a symmetric cipher? What are the essential components of a symmetric cipher?

  (b) What is an asymmetric cipher? How does it different from a symmetric cipher? Cite at least two differences.

(5) Lets consider cryptographic keys.

  (a) What is it and why do we need one?

  (b) List some of the different types of cryptographic keys used in practice?

  (c) What are some of the security requirements for storing keys? How is this different when considering both symmetric ciphers and asymmetric ciphers?

Questions: Part B

(1) Solve the following problems using Extended Euclid's algorithm using first principles. Make sure that you understand the process.

  (a) $3^{-1} \bmod 7 =$ ....

  (b) $5^{-1} \bmod 13 =$ ....

  (c) $1473^{-1} \bmod 1562 =$ ....

  (d) $73^{-1} \bmod 127 =$ ....

(2) Try the above questions uisng any online Extended GCD function (XGCD on magma).
(http://magma.maths.usyd.edu.au/calc/)

(3) Any number $a \geq 1$ has a unique factorization given by: $a = {p_1}^{a_1}{p_2}^{a_2}\cdots{p_n}^{a_n}$, where $p_1, p_2, \cdots p_n$ are the first n primes in the representation of a. Give an expression for the gcd of two numbers using the above representation of numbers.

(4) Classical Ciphers

- (a) What is a Caesar Cipher?
- (b) Explain differences between mon and poly alphabetic cipehrs.
- (c) If you have a Caesar Cipher with key $k = 4$. Encrypt "MELBOURNE" using the key.
- (d) Consider the affine Caesar cipher defined as follows. The encryption function is defined as: $C = E_{[a,b]}(p) = (ap + b) \bmod 26$, where p is the plain text and the tuple $[a, b]$ is the key.
  - (i) How many different keys are possible with the system?
  - (ii) Derive a decryption function and determine what values of a and b are allowed, if this function exists.

Part C: Homework

The following are a list of questions for students to attempt at home to get a better grasp of the concepts discussed during the workshop.

(1) Complete any questions which were not completed during the workshop.

(2) List at least six vulnerabilities listed in www.cert.org.

(3) There are also a number of Internet sites dedicated to information security, including www.cert.org, www.securityfocus.com, and others Using these sites, find one vulnerability of each of the following types:

- (a) Buffer overflow
- (b) Unintended program function caused by unexpected input
- (c) Cryptographic weakness
- (d) Back door / trojan programs

(4) What is a CVE number?