COMP90043: Cryptography and Security

Week 3 Workshop Activity

COMP90043: Cryptography and Security
Week 3 Workshop Activity

(Problems are from the text by Stallings, 5th & 6th edition)
Part A: (Please work at home before coming to the class)
Before we begin, take a few minutes to discuss the following:

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?

Now that we have defined our definitions, let's apply this in a more practical setting:

4. What is a symmetric cipher? What are the essential components of a symmetric cipher?

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

6. Let's 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?

Part B: (Discussion in the class)
7. Let us now consider the example of a Caesar Cipher:
a. What is a Caesar Cipher?

b. If you have a Caesar Cipher with key **k=4**. Encrypt

8. Consider the affine Caesar cipher defined as follows. The encryption function is defined as: C = E_[a,b](p) = (a p+ b) mod 26, where p is the plain text and the tuple [a,b] is the key.
a. How many different keys are possible with the system?

b. Derive decryption function and determine what values of a and b, this function exists.

9. Consider the affine Caesar cipher with a = 7, b= 5. Derive decryption equations by manually working with gcd and extended gcd algorithms.

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?