COMP90043 Cryptography and Security
Semester 2, 2021, Workshop Week 4

Preparation:
Please revise OneTimePad.pdf and BlockCipherModes.pdf before coming to workshop.

Part A

1. Let C_1 and C_2 be two n-bit ciphertexts obtained by encrypting using one-time pad key K on plaintexts M_1 and M_2 respectively. Show that $M_1 \oplus M_2 = C_1 \oplus C_2$. What is the consequence of Known Plaintext attack on the one-time pad encryption?

2. The Vernam cipher can be considered as a one-time pad where message and cipher space are English text treated as sequences of integers between 0 and 25 and the $\oplus$ operation is replaced by sum modulo 26. Let $M[i], K[i] \in \{0, 1, \cdots, 25\}, 0 \leq i < n$, then the encryption function can be implemented as:

```
for i = 0 to n-1 do
    C[i] = M[i] + K[i] mod 26
```

   (a) What's the decryption function?

   (b) If the length of the key is n, how many different possible keys are there in Vernam cipher?

   (c) Encrypt "unimelb" with the key "tuesday".

   (d) What should be the key that decrypts the ciphertext in (c) to "rmituni"?

3. State the condition for perfect secrecy.

Part B: Block Cipher Modes

1. If a bit error occurs in the transmission of a ciphertext character in OFB mode, how far does the error propagate?

2. Why do some block cipher modes of operations only use encryption while others use both encryption and decryption?

3. You want to build a hardware device to do block encryption in the cipher block chaining (CBC) mode using an algorithm stronger than DES. 3DES is a good candidate. Figure below shows two possibilities, both of which follow from the definition of CBC. Which of the two would you choose:

   (a) For security?

   (b) For performance?

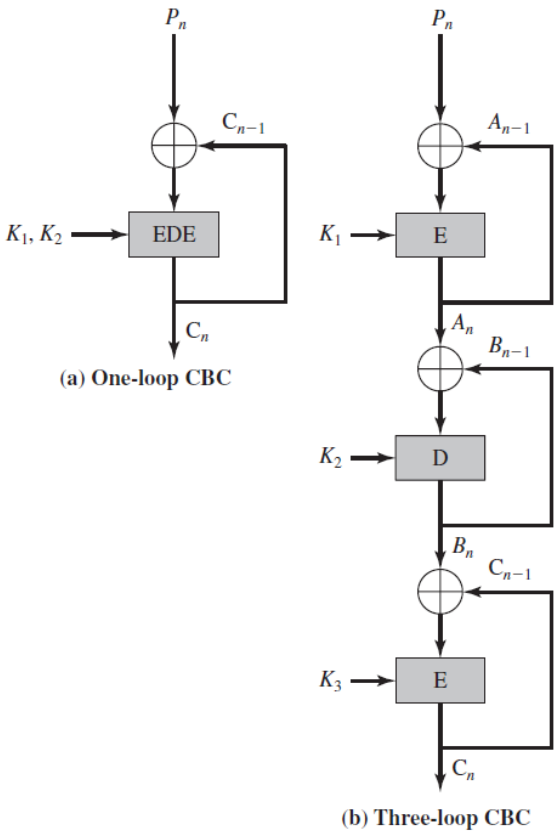

Figure 1: Use of Triple DES in CBC Mode

Part C: Homework

The following are a list of questions for you to get a better grasp of the concepts discussed during the workshop.

1. What is reversible mapping? What is irreversible mapping? Think about why Fiestels algorithm works for any function F, even for the irreversible ones.
2. What is the difference between a block cipher and a stream cipher?
3. What is the difference between diffusion and confusion? How diffusion and confusion is achieved in Fiestels encryption algorithm?
4. What parameters and design choices determine the actual algorithm of a Feistel Cipher?
5. What is avalanche effect? Why it is desired in encryption algorithms?
6. Write the block diagram for DES decryption algorithm.