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

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?

$$\begin{aligned} C_1 &= M_1 \oplus K \\ C_2 &= M_2 \oplus K \\ C_1 \oplus C_2 &= (M_1 \oplus K) \oplus (M_2 \oplus K) \\ &= M_1 \oplus M_2 \oplus K \oplus K \\ &= M_1 \oplus M_2 \end{aligned}$$

   Ciphertext can be decrypted by using another pair of plaintext and ciphertext encrypted using the same key.

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?
   The decryption of C with the key K can be given by

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

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

   (c) Encrypt "unimelb" with the key "tuesday".
   u(20) + t(19) = n(13)
   n(13) + u(20) = h(7)
   i(8) + e(4) = m(12)
   m(12) + s(18) = e(4)
   e(4) + d(3) = h(7)
   l(11) + a(0) = l(11)
   b(1) + y(24) = z(25)

(d) What should be the key that decrypts the ciphertext in (c) to "rmituni"?
n(13) - r(17) = w(22)
h(7) - m(12) = v(21)
m(12) - i(8) = e(4)
e(4) - t(19) = l(11)
h(7) - u(20) = n(13)
l(11) - n(13) = y(24)
z(25) - i(8) = r(17)

3. State the condition for perfect secrecy.

$\mathbf{Pr}[\mathbf{M} = \mathbf{x}|\mathbf{C} = \mathbf{y}] = \mathbf{Pr}[\mathbf{M} = \mathbf{x}]$

Part B: Block Cipher Modes

(see next page)