Assignment 1: COMP90043
Due Date: **9AM, August 21, 2017**

1. Submit the answers to Part A. You should also work out a solution to Part B, which will not be marked.

2. A Discussion forum thread Assignment 1 has been created on LMS. Any clarification offered on this forum will be considered as a part of the specification of the Assignment.

3. All questions in Part A carries equal weight. The assignment contributes to 7.5% of the total.

4. Answers must be submitted as a PDF file via the comp90043 Assignment 1 Turnitin submission form on LMS by the due date. Late submissions will attract a penalty of 10% per day (or part thereof). Please ensure your name and login name are presented.

5. **I suggest all of you to enroll "Academic Integrity Module" on your LMS home and take the Quiz in the module. You will be submitting your work on Turnitin, so do not share your answers with others. You are welcome to discuss strategies to answer the questions, but not to share the work.**

Part A: Questions

1. Euclids's algorithm and Divisibility properties.

   (a) Implement the extended Euclid's algorithm in a language of your choice and submit the code here. Note: It is sufficient you only provide the function here and the language used in the implementation. You are at free to employ any underlying integer arithmetic library.

   (b) Explain how you can determine the inverse of a number $a \mod n$, where $a < n$ and n a positive integer, using the extended gcd algorithm. It is sufficient you sketch the algorithm.
   Note: Inverse of a number a mod n is a number x such that $xa = 1 \bmod n$.

   (c) Let a, b, c, d be integers and $(a, b) = 1$. If $c|a$ and $d|b$, then prove that $(c, d) = 1$.

2. General Security and Classical Ciphers.

   (a) Explain with an example how security risks and attacks are different. Name a security attack that has happened on computer systems in recent years. Describe how the attack took place in no more than half a page.

   (b) Consider the following version of a classical cipher where plain text and cipher text elements are from integers 0 to 28. Note that this alphabet may be used when the plaintexts are 26 English characters and three punctuation symbols, viz: “,” “.” and “ ” (Blank). The encryption function, which takes any plain text p to a cipher text c, is given by

$$c = E_{(a,b)}(p) = (ap + b) \bmod 29,$$

   where a and b are integers less than 29.

      i. What is the decryption function for the scheme?

      ii. How many different non-trivial keys are possible for the scheme?

      iii. What are the complexities of Cipher Text only Attack and Chosen Plain Attack on the scheme?

3. Polyalphabetic Cipher.

   We consider the Hill cipher given in the textbook defined for English text. Here the plain text (mod 26 characters)is processed successively in blocks of size m, $m > 1$ digits at a time. The encryption algorithm takes a block with m plain text digits and transforms into a cipher block of size m using a key matrix of size $m \times m$ by the linear transformation is given by:

$$\begin{aligned} c_1 &= (k_{1,1}p_1 + k_{1,2}p_2 + \cdots + k_{1,m}p_m) \bmod 26 \\ c_2 &= (k_{2,1}p_1 + k_{2,2}p_2 + \cdots + k_{2,m}p_m) \bmod 26 \\ &\cdots \\ c_m &= (k_{m,1}p_1 + k_{m,2}p_2 + \cdots + k_{m,m}p_m) \bmod 26 \end{aligned}$$

   Note: For this question, assume the familiar correspondence between English alphabets and number modulo 26, i.e. $A \leftrightarrow 0, B \leftrightarrow 1, C \leftrightarrow 2, \ldots Z \leftrightarrow 25$.

   (a) How many different keys are possible in the system?

   (b) The “cipher text only attack” on the system ’s hard to mount for the cipher. However, the cipher is easily broken with a known plain text attack. Illustrate the steps for the attack.

(c) An adversary discovers the following cipher text encrypted using teh Hill cipher with $m = 3$:

UJVEPWRBEWGFKOSDHJGRMWUPQPEEPMCHUUCFLFHCA
QWZHXAVVTDGRMWUPQPEEPMCHUNNALZCOMYGBJ

If the following plaintext and ciphertext blocks are given, decrypt the cipher by giving the plaintext and the key used in the encipherment. Show your workings, and if you have used a package or a program you need to include the details of the package, functions used, and any programs developed.

Plaintext	Ciphertext
PHI	UJV
LOS	EPW
OPH	RBE

Part B: Questions for Self Study (No need to submit answers for this part)

1. State any two differences and any two similarities between symmetric and asymmetric key cryptographic schemes.

2. This question pertains to five Block Cipher modes of operation defined by the NIST(National Institute of Standards and Technology).(4 points)

Mode	encryption Function	Decryption Function
ECB	$C_j = E_K[P_j], j = 1, \cdots, N$	$P_j = D_K[C_j], j = 1, \cdots, N$
CBC	$C_1 = E_K[P_1 \oplus IV]$ $C_j = E_K[P_j \oplus C_{j-1}], j = 2, \cdots, N$	$P_1 = D_K[C_1] \oplus IV$ $P_j = D_K[C_j] \oplus C_{j-1}, j = 2, \cdots, N$
CFB		
OFB		

Table 1:

(a) Complete the encryption and decryption functions for the Cipher Feedback (CFB) mode and the Output Feedback Mode (OBC).

(b) Compare the feedback mechanisms of the CFB and OBC modes.

(c) Which of the above modes in the table is naturally suited to realize a stream cipher?

(d) For each of the modes considered in the table:

- Identify which decrypted plaintext blocks P_x will be corrupted if there is an error in block C_4 of the transmitted ciphertext.

3. Questions related to Classical Ciphers(7 points)):

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

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

Similarly the decryption of C with the key K is given by

```
for i:=0 to n-1 do
M’[i] = C[i] - K[i] mod 26.
end for;
```

i. If the size of the key is n, how many different possible keys are in a Vernam cipher?

ii. Encrypt ”unimelb” with the key “enzymes”.

iii. Modify the cipher text in (2) to be the ciphertext for “rmituni”.