Assignment 1: COMP90043
Due Date: 9.30 Am, August 23, 2016

1. Answer all the questions.
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. The total number of points for this assignment is 30. This contributes to 7.5% of the total.
4. Answers must be submitted as a PDF file via the comp90043 Assignment 1 submission form on LMS by 9.30 Am, August 23, 2016. Late submissions will attract a penalty of 10% per day (or part thereof). Please ensure your name and login name are clearly presented.

Questions

1. Cryptanalysis of General Substitution Cipher:(12 points)
   This question is about cipher text only attack on Substitution cipher. Ciphertext from a mono alphabetic substitution cipher for this task will be made available on the departmental server dimefox individualy. You are not allowed to share or exchange the ciphertext with other students or any third party.

   You need to obtain ciphertext from

   `/home/subjects/COMP90043/Assignment1/login_id/ciphertext on dimefox.`

   (a) Decrypt the ciphertext given for you at the above address by following ciphertext only attack and determine the encryption and decryption keys.

   (b) You should elaborate on your selected approach to decode the ciphertext. In particular provide a detailed account on how you deducted the decryption mapping. You should include the sequence of guesses for the partial keys that you may have made using statistics such as relative frequency of letters and frequency of

digrams and trigrams in the cipher text. And also you might have decided partial keys based on trial and error, and also by guessing output words. You should enumerate all such steps.

(c) If you have used algorithms or code, please include and explain the relevant sections here and additional code segments can be included in the appendix.

For this question, assume the familiar correspondence between English alphabets and number modulo 26, i.e.
$A \leftrightarrow 0, B \leftrightarrow 1, C \leftrightarrow 2, \ldots Z \leftrightarrow 25$.
You are also given with the following table depicting single letter frequency count for English.

A	B	C	D	E	F	G	H	I	J	K	L	M
7.8	1.3	2.9	4.1	13.0	2.9	1.4	5.8	6.8	0.2	0.4	3.6	2.6
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7.3	8.2	2.1	0.1	6.6	6.5	9.0	2.8	1.0	1.5	0.3	1.5	0.1

Table 1: Single letter frequency count for English (percentages)

Points to Note:

(a) You will need some simple functions to compute letter, digram, trigram frequencies and for displaying partial decrypted text. Please refer to magma functions posted on "Lectures and Workshops" pages on LMS.

(b) Answers that do not show any supporting arguments for obtaining the correct decrypted text will not receive full marks.

2. Cryptanalysis of Affine Caesar Cipher:(3 points)

This question is about known plain text attack on Affine Caesar Cipher You are given below a ciphertext encrypted using an Affine Caesar Cipher.

SWXTJNPVYKLRUOLIEJDCXGLAXKSWXMHQZGLF

(a) Determine the complexity of brute force attack to break the cipher?

(b) Given that the plain text "THE" is mapped to the cipher text "SWX", can you break the above cipher text? If you can, decrypt the cipher text and describe how you break the code.

3. (4 points)

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

4. 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		
CTR		

Table 2:

(a) Complete the above table by filling missing details. Also expand the various terms used in the table.

(b) Compare the performances and relative advantages of the five modes of usage of block ciphers. You need to list only the important aspects in point form.

(c) For each of the modes ECB, CBC and OFB:

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

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

(a) Explain how you can determine 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 $amodn$ is a number x such that $xa = 1modn$.

(b) The polynomial cipher given below is a generalization of Affine cipher. The encryption function, which takes any plain text p to a cipher text c, is given by

$$c = E_{(a,b,c)}(p) = (ap^2 + bp + c) \bmod 26,$$

where a, b and c are integers less than 26. How many different non-trivial keys are possible for the scheme?

(c) 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".