COSC 4P03 – Advanced Algorithms
Winter 2019
Assignment #3

Due Date: April 12th, noon **Late Date: April 15th, noon**
This assignment accounts for 10% of your final grade and is worth a total of 100 marks.

In this assignment you will be performing cryptanalysis on 3 different pieces of ciphertext. In each case, you are to determine the plaintext and give a clear description of the steps you follow in your cryptanalysis. You must also submit any programs you used.

You will be marked not only on obtaining the correct answer, but also on **the methods, and explanation of the methods**, used to achieve that answer.

1. [30 marks] The following ciphertext was encrypted using a Substitution Cipher.

```
HJTXRKRQVTNKVHJTXRKRTYTGGZFBTQEDJXVFEVXH
YKBUKVSTKYTQGQZWZFIZVVXVFETITKQVJZSTYYUF
ZTMRVJZBTQGRXBZTFZIKWZQTHJTQHZVXHYKBUULV
VJZEFZSLRZVJZEHYKQIVXVJZFZTYBXFVJZIXGRXF
YXWZKYYLRKXQRXQYEVJZYTGGZFKRFZTYVJZHYKBU
KRTYYVJZFZKR
```

2. [35 marks] The following ciphertext was encrypted using a Vigenere Cipher.

```
TRZBTEHKPVGGEJBJYANRSGKRGRPDLDFFQEJXPEOE
SGFAYCFILAYVSZIFMLCZGLWLLCZFAGKKKCXMDEAY
SBXZXYKKBAZHSZJRWSGKNVBHAXZNVBAAESKVRWOH
YUGZEFHIVMVXKTYZRQPWPPKVBYLTURBFAWKVIFNX
ZXYKCBQSGFRBFAWKZRZYHWILERFSFMOVANROBAYH
UIKPVIRCSOXYISFMVXZNVRVWFLEPRPAXCVWGVWLP
USFRGFVISNRVGVCSFWKHWFKRVALHDIZQWKZKFVGC
TZYOQSOHUKVRASESMOECKFBIAHVWWFVHFLSWVNGP
EFDPCZNRVHMKHVQWLHMSECKFHCZZEFVHEQNWLTCV
FLPSKNVGUEVHD
```

3. [35 marks] The following ciphertext was encrypted using RSA with public key (*n*=20701,*b*=4525).
   Each character of the plaintext was first converted into numerical format by mapping a→0, b→1, …, z→25. The plaintext was then divided into sets of 3 characters. Each set of 3 characters $c_0c_1c_2$ was converted to the value $x = c_0*26^2 + c_1*26 + c_2$: for example, the word "the" would be converted to x = 13030. Each value x was then encrypted as ciphertext $y = x^{4525} \bmod 20701$. The total number of characters in the plaintext is divisible by 3.

```
12217 11047  5883 10968 15048  7532  3576  6924 10069 16656
10878  8083  6996 15349 20338  2773 16453  5072  7141 13101
 7144  3902 10965  4270  1354  9645 13101  2409  3400 17343
 2700  4097  9348 17112 20235  7382  1185  3008  5100  8323
13730  7829  7420 20463 16088  3342  6930  5133 17294  3342
 7866 11743 16470  6611  6846  2773  3342  4514 13730 12614
14852  3914  9006 10903  5883  7955  9427 15322  7331 11778
 9917 16954 18357 18340   276  7917   725  8066  8576  3029
 1597  3011  6698  9834 18322  5533  4678 16948  8374  1969
 8643  2751 20596  3576 15559  5883 11345  6361  6788 17802
11622 10966  5900 17571   851
```

Submission Requirements:
All of the following must be placed in a sealed envelope in the 4P03 assignment box:

1. A cover sheet, available from http://www.cosc.brocku.ca/forms/cover, completely filled out. Your assignment will not be marked unless one is submitted with the assignment.
2. Commented and properly documented listings for all source code for your programs.
3. Full and complete explanations of the methods used to decipher the messages.
4. Any information required to run your programs.

You must also submit your assignment electronically so that it can be checked for plagiarism using `MOSS`. To do this, create a directory on Sandcastle containing all files for this assignment, and run the script `submit4p03` from this directory.