**cmput210** **asn2** **due in class 930am feb 7** **40 marks**

Late assignments (under the door of Athabasca Hall 301 within 24 hours of the due date) will be docked 10%. Later assignments will not be marked: their weight will be transferred to the final exam.

Each group should hand in one (1) only assignment.

1. **If you leave any part of this question blank, your assignment will not be marked and its weight will be transferred to the final exam.** In alphabetic order by first name, print first name, last name, and ID number of each group member (at most 5) for this assignment:

   _____

   _____

   _____

   _____

   _____

   Acknowledge **all** sources, including all references and all people not in your group with whom you discussed any part of any question (for each discussion, list the relevant questions) (continue on the back of this page if there is insufficient space):

   Each group member must read, agree to, and sign this statement:

   **I am familiar with the Code of Student Behaviour. I understand that there are significant penalties for any infraction of this Code. Regarding the questions on this assignment, I have not shared or received any detailed information regarding any of these questions with anyone outside my group, and any non-detailed communications have been cited above by both parties.**

   _____

   _____

   _____

   _____

   _____

2. This ciphertext was created by starting with text from The Code Book, removing blanks and punctuation, and encrypting with a homophonic substitution cipher that replaces the 26 letter alphabet with 29 symbols.

```
jxyimzljxtiqctouzhjxzjjxeczifxtbyffulm
zlrhtqaydwjxtsyfxthevcqhogkutdevlsejl
```

a) [2] If you were designing such a cipher, which of these schemes would you prefer, and why?

Scheme A: 25 plaintext letters each have 1 homophone, 1 letter has 4 homophones.

Scheme B: 24 plaintext letters each have 1 homophone, 1 letter has 3 homophones, 1 letter has 2.

Scheme C: 23 plaintext letters each have 1 homophone, 3 letters each have 2 homophones.

b) [2] Here are the ciphertext frequencies. Which scheme was used? Explain briefly.

```
j t x l z e f h y c i q u d m o s v a b g k r w
7 7 7 5 5 4 4 4 4 3 3 3 3 2 2 2 2 2 1 1 1 1 1 1  75 chars
```

c) [6] Crack the cipher. Explain your methods in at most 200 words. (Hint: e, a, s have 2 homophones each. every other character has 1).

3. `{ a, a, a, a, a, b, b, c, c, c}`
   `{ a, a, a, b, b, c, c, d, d}`

   `show your work for each part of this question`

   i) [1] give the index of coincidence for the first multiset

   ii) [1] give the index of coincidence for the second multiset

   iii) [2] give the index of mutual coincidence of the two multisets

   iv) [2] give the index of mutual coincidence of the first multiset compared with typical English. for English, use the frequencies from the webnotes example on imc

4. i) [2] By hand, using this table, encrypt `vigenere cipher immune` using keyword `shift`. check your answer using program `vig/vig.py`

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

   ii) [2] you are asked to encrypt Vigenere ciphertext by hand with no encryption table. would you prefer keyword `babyface` or keyword `viginere`? Explain briefly.

5. `qomzartdpgtlsaxytremaeilbdeydprpevppmpca`
   `qmlleiropbrcoqalihppshxawhsuatilhoocnexzi`
   `tcmmmgphhzjwtiopflrhpgpcbzaeyicxshmfnxwwscq`

   i) [2] using program `freqs/kgram.py` from the class gitcode repository, using the Babbage/Kasiski method, give the most likely keyword length of the above Vigenere ciphertext. explain briefly

   ii) [2] using program `vig/friedman.py` from the class gitcode repository, what is the suggested keyword length? what evidence supports this?

   iii) [2] using program `vig/friedman.py` from the class gitcode repository, what is the suggested shift of the 2nd-last keyword character? what evidence supports this?

   iv) [2] give the keyword and the plaintext. check your answer using `vig/vig.py`. is this exactly the answer guessed by `fig/friedman.py`? explain briefly.

   v) [2] now that you know the plaintext, show exactly how the repeated ciphertext digram `ei`, offset 23 characters, is a false positive for the Kasiski method: give the plaintext and key fragments that yield the first occurrence, and the plaintext and key fragments that yield the first occurrence.