Last Name:_____ **First Name:**_____

- **CMPUT 396 Midterm** (50 minutes)
- March 6, 2019.
- Instructor: G. Kondrak
- Do not open this exam until you are instructed to do so. Read the instructions.
- Fill in your name above, and your name and ID on the last page. Print clearly.
- Be prepared to show your Student ID Card to the proctor.
- There are 4 questions (32 marks in total).
- Use space below the questions to write your answers.
- Add comments as appropriate to help clarify the intent of your code.
- Closed book except one handwritten page. No electronics allowed.
- All programming questions refer to Python 3.

---

1. (**8 marks**) Write a function *keyAccuracy* that returns the key accuracy of a decipherment attempt, as described in Problem 2 of Assignment 5. It takes two strings as arguments: the plaintext, and the decipherment.

   For example, the following function call:
   `keyAccuracy("TURING WAS A CRYPTANALYST", "TYRINF WAS A CRUPTANALUFT"))`
   should return the value of $10/13 = 0.77$.

   Assume that the cipher used for encryption is monoalphabetic substitution, and that the strings contain only uppercase letters and spaces.

   Note: coding style matters.

```
LETTERS = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

def keyAccuracy(txt,dec):
```

2. (**6 marks**)

Suppose that a long secret message has been enciphered using two methods:

- the autokey cipher that you implemented in Problem 4 of Assignment 2,
- the Vigenere cipher from Chapter 18

In both cases, a 4-letter dictionary word has been used as the key.

Discuss the relative security of the two ciphertexts with respect to the following codebreaking techniques:

(a) brute-force decryption

(b) dictionary attack

(c) frequency analysis

(d) Kasiski examination

3. (**6 marks**) For each of the following program segments, write the output as it would be displayed.

(a)
```
s = "ABCDEF"
print(s[s.find('J')])
```

(b)
```
print((3,6) + (2019,))
```

(c)
```
y = ['ABC','DEF','GHI']
print(y[1][2])
```

(d)
```
x = (17 // 6) + (17 % 6)
print(x)
```

(e)
```
spam = ham = [1,2,3]
spam[ham.index(1)] = 99
print(ham)
```

(f)
```
print(3 * [6] + [2])
```

---

4. (**12 marks**) Short answers. Show your work.

   (a) Decode the following ciphertext that has been encrypted using the Caesar cipher. (The letter indices can be found at the bottom of this page.)

   `PDA AJZ EO JEYA`

   (b) Encipher the message "BELA" using the Affine cipher with the key $(5, 25)$.

   (c) Decode the ciphertext "EVEEVMN" that was enciphered using the substitution cipher with a key generated from a pass-phrase "vexed nymphs go for quick waltz job".

   (d) Decode the ciphertext "GOAVS" that was enciphered using the Vigenere ciphertext with the key "BAY". (The Vigenere square can be found on the next page.)

   (e) Compute the approximate value (2 significant digits) of the index of coincidence for the string: `ADDBADCABDAD`

   (f) Complete the code for the Python function that calculates the greatest common divisor of integers a and b.

```
def gcd(a,b):
    while
        a, b =
    return
```

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Last Name:_____ **First Name:**_____ **ID:**_____

Q1		8
Q2		6
Q3		6
Q4		12
Total		32

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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