cmput210 **asn1** **due in class 930am Jan 24** **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. `baabtjcdbkjogtxfqifkfttjmsifqftsfcsgbmsgfijqoqfcfdftitpqtjmdpmrivfts, oqfeifqqjmhsphqpxbmpqhbimjyfcbmicbeekvfimstpdjfsz.`

   This ciphertext was created by starting with a plaintext that does not use all 26 letters of the alphabet, removing spaces, inserting nulls (only one of the unused characters is used for nulls), and encrypting the resulting garbled plaintext with a substitution cipher.

   a) explain briefly why the cryptogram solver quipquip does not solve this cipher.

   b) find the garbled plaintext

   c) find the original plaintext

   d) read Singh's description of how to cryptanalyze a ciphertext from chapter I: then write a similar but shorter (at most 200 words) report that describes how you found the answer to c).

u	v	t	x	f	k	b	s	p	w	q	z	l	n	c	e	i	d	h	j	a	o	y	r	m	g	total
1457	1115	1031	917	830	783	768	754	733	553	525	353	334	297	285	266	241	236	219	200	122	105	15	14	7	5	12165

	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
a	0	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	6	85	0	0	13	0	0
b	29	0	30	0	25	232	1	4	23	6	0	0	0	28	5	26	39	0	73	12	22	110	60	17	2	0
c	0	12	6	3	0	1	0	0	0	0	44	4	0	0	0	20	0	0	2	13	27	0	9	26	0	0
d	0	3	0	0	1	8	0	3	0	0	0	0	0	1	0	3	1	0	15	4	12	9	8	25	0	0
e	0	11	0	2	4	0	0	0	0	0	80	17	0	0	12	5	0	0	0	27	40	12	11	45	0	0
f	0	23	132	18	27	3	0	0	4	0	1	4	0	1	6	0	149	1	23	7	63	70	18	62	0	0
g	0	1	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
h	0	5	0	9	0	0	0	0	0	0	0	29	0	0	0	21	0	0	3	11	78	3	26	32	0	0
i	0	9	0	0	0	0	0	0	10	0	0	11	0	0	0	20	0	0	0	11	15	12	5	38	0	0
j	0	12	0	0	0	0	0	0	0	15	8	7	0	0	0	22	0	0	5	18	46	5	17	14	0	0
k	0	108	0	7	0	1	0	14	0	0	0	4	0	2	0	7	0	0	0	134	363	31	0	61	0	0
l	0	7	22	0	9	39	1	4	0	23	0	0	0	11	0	37	3	0	43	8	4	72	36	0	1	0
m	0	0	0	0	0	0	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	0	0	0	0	0
n	0	23	0	8	0	0	0	4	1	6	0	8	0	2	0	35	0	0	4	82	52	0	0	12	0	0
o	0	11	0	3	0	18	0	0	0	0	0	0	0	0	0	0	0	0	8	1	27	0	1	0	0	0
p	2	78	1	12	11	21	0	1	4	14	1	9	0	6	4	10	22	0	58	56	152	34	15	55	0	0
q	2	29	1	6	0	7	0	0	2	0	0	4	0	0	0	14	4	1	7	15	55	0	2	41	0	0
r	0	0	0	0	0	0	0	0	0	0	0	8	0	0	0	0	0	0	0	2	0	0	0	3	0	0
s	0	33	0	9	10	5	0	1	0	18	59	21	0	3	10	0	0	0	15	31	82	84	8	49	0	3
t	30	39	4	32	52	176	1	29	10	11	0	7	0	13	17	103	58	0	113	0	0	148	59	0	0	8
u	26	15	5	15	19	122	0	0	9	14	3	0	0	14	4	211	101	1	88	73	63	55	87	7	12	33
v	0	53	0	13	4	0	0	0	2	0	323	16	0	2	0	22	0	0	25	33	85	61	16	108	0	6
w	2	38	0	52	0	1	0	0	7	2	0	12	0	2	5	0	41	0	4	63	74	7	92	33	0	7
x	22	16	1	12	6	120	0	4	87	17	1	128	0	57	16	93	22	0	18	6	6	36	23	43	0	52
y	0	3	0	0	1	0	0	0	0	5	0	0	0	0	0	0	0	0	0	3	0	3	0	0	0	0
z	0	41	0	0	0	14	0	0	0	0	62	0	0	0	0	1	0	0	7	75	59	0	0	36	0	0

3. Above are letter and letter-pair frequencies for English monoalphabetic substitution ciphertext.

   a) which ciphertext character corresponds to plaintext character `q` ? justify briefly

   b) which ciphertext character corresponds to plaintext character `u` ? justify briefly

   c) assume as in TCB that the 3 most common ciphertext characters (here `u v t`) correspond to some permutation of the 3 most common English characters: arguing as in TCB, give the most likely match between ciphertext `u v t` and plaintext `e t a`.

4. Give the number of transpositions of `thecatinthehat` . Show your work.

   Give the number of transpositions of `the_cat_in_the_hat` (include the 4 underlines as characters). Show your work.

5. Give the number of keys for the Caesar shift cipher.

   Give the number of keys for a general monoalphabetic substitition cipher.

   State Kerchoff's principle.

   Explain why having a large number of keys is necessary for a cryptosystem to be secure.

   Explain why having a large number of keys is not sufficient for a cryptosystem to be secure.

6. During the reign of Elizabeth I, many Catholics believed that Mary Queen of Scots — not Elizabeth — was the rightful heir to the English throne. Explain their argument briefly (at most 30 words).

7. i) Encrypt `lysanderofspartausedascytale` using a 4-sided scytale. Show your work.

   ii) Encrypt `transpositionsscramble` using a depth-4 down-only railfence cipher. Show your work.

   iii) Take the ciphertext from i) and further encrypt it using the cipher from ii). Show the resulting text. Explain briefly.

8. Unexplained phenomena are often attributed either to magic or to the work of some mythical being. Give such an example from the story of the arrival of cryptanalysis in Europe.

9. The postscript to Mary's letter to Babington was a forgery. Perhaps the rest of the letter was also a forgery? Give evidence for or against this claim.

10. This is the contents of file `ptxt`: `there was a public outcry at the horror of their execution`
    Show the contents of file `ctxt` after executing this linux command:

    ```
    tr 'a-z' 'thequickbrownfxjmpsvlazydg' < ptxt > ctxt
    ```

    Give a similar command that decrypts `ctxt`.

11. Explain briefly why applying Al Kindi's rule unconditionally does not usually crack ciphertext.

    Explain briefly how Al Kindi's rule together with a dictionary can be used to break monoalphabetic substitution ciphers.