cmput 210 W2016 **study guide** **chapter 1 part A**

1. What were Singh's two motivations for writing *The Code Book* ?

2. Explain the difference between steganography and cryptography.

3. Explain substitution. Give an example of a substitution cipher.

4. Explain transposition. Give an example of a transposition cipher.

5. Describe the cryptographic scheme mentioned in Caesar's *Gallic Wars*.

6. Describe the Caesar cipher mentioned by Suetonius (which Caesar used for his diary).

7. Compare and contrast the Caesar shift cipher, atbash, and the *mlecchita-vikalpa* cipher from the Kama Sutra. Which of these is the hardest to break? Why? The easiest? Why? Roughly how old are the records that describe these ciphers?

8. Where can you find a copy of the text by Valerius Probus on Caesar's ciphers?

9. Describe Al-Kindi's method of cryptanalysis. Explain why the method cannot be blindly followed. Explain how the method can be strengthened, and use the strengthened method to break the following substitution cipher. Explain the numbers below.

   ```
   uko vqbo uj cyrejwoq roeqour yr coolma ygbqtygoc yg kvntg gtuvqo;

   owog uko motru evqyjvr nygc yr qjvroc ha uko lqjnyro jd rktqygb

   igjxmocbo xyukkomc dqjn jukoqr.  sjkg ektcxyei
   ```

a	b	c	d	e	g	h	i	j	k	l	m	n	o	q	r	s	t	u	v	w	x	y
2	4	8	2	5	10	1	2	10	10	2	4	4	20	11	11	1	6	9	6	2	3	12

10. Explain the relationship between the novel *La Disparition* by George Perec (and its English translation by Gilbert Adair) and Al Kindi's method for cryptanalyzing a monoalphabetic substitution cipher.

11. Roughly how big is 26! (26 factorial) ? And what does this number have to do with substitution ciphers?

12. Roughly how big is 50! ? And what does this number have to do with breaking a 50-character plaintext that has been encrypted with a transposition cipher?

13. Historically, why do you think transposition ciphers were not more popular?

14. What did it matter whether Elizabeth could read the intercepted letters of Mary Queen of Scots? When was the trial of Mary Queen of Scots? When was she executed?