Grade 11/12 Math Circles

Cryptography, Part 1 - Problem Set

1. In this question, we will explore a couple pitfalls of using transposition ciphers.

   (a) Why is it a bad idea to use a transposition cipher to encrypt a very short message? Is a substitution cipher better in this situation?

   (b) The longer the plaintext becomes, the greater the chance of an error being introduced. In the transposition example, Example 1 of the lesson, where Nick sends

   EMTRMATIIYETDLRAEE

   to Shefaza, suppose he accidentally forgets one of the Ts, sending

   EMRMATIIYETDLRAEE

   instead. Using the same key, what would Shefaza get for a plaintext? Would the same type of problem happen with a substitution cipher?

   (c) Taking this idea further, suppose Nick encrypts a long message using a transposition cipher, and the second half of the message gets lost somehow (maybe it was on a different sheet of paper). Would Shefaza be able to recover any of the plaintext? What if a substitution cipher was used instead?

2. Using this encryption table,

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

   try encrypting the following plaintext:

   It was a bright day in April, and the clocks were striking thirteen.

   (This is the first line from George Orwell's famous novel, *1984*.)

3. Suppose you have intercepted the following ciphertext, which you know for sure has been encrypted using a shift cipher:

   ALKLQDLTEBOBQEBMXQEJXVIBXADLFKPQBXATEBOBQEBOBFPKLMXQEXKAIB XSBXQOXFI

   What is the corresponding plaintext?

4. (a) Using the monoalphabetic substitution cipher, how many keys are possible?
   (b) Suppose you wanted to try breaking the monoalphabetic substitution cipher by brute force, trying every key until you get a sensible message. Let's be generous and say you managed to convince a billion of the Earth's inhabitants to help you on your quest. If every one of you could try one key per minute, roughly how many years would it take to try all the keys? For simplicity, assume each year has 365 days. (Let's also assume people live forever and can spend all of their time checking keys.)
   (c) The current age of the universe is estimated to be 13.772 billion years. Roughly how many times the current age of the universe would it take those billion people to finish checking the keys?

5. We mentioned that the onetime pad is only secure if:
   (1) The key is generated completely randomly.
   (2) Every key is used only once.

   The goal of this question is to see what kinds of problems pop up if either rule is broken.
   (a) Rather than using a random key, suppose we form a key by repeating a short word over and over again, such as KINGKINGKINGKING..., looping this until we get to the end of the plaintext. This special case of the one-time pad cipher was mentioned way back in 1553 by Giovan Battista Bellaso, but carries the name *Vigenère cipher* due to a misattribution to a 19th century French man named Blaise de Vigenère.
      i. If you happen to know the length of the repeated word, how can you reduce the problem of breaking the cipher to the problem of cracking a small number of shift ciphers?
      ii. Even if you don't know how long the repeated word is, it is often still possible to find out. Suppose you got your hands on a ciphertext, and saw that "TPC" appears twice, 75 letters apart, and "APSA" also appears twice, 27 letters apart. Based on this, how long is the repeated word that forms the key likely to be?

(b) Suppose two teachers use the onetime pad to encrypt answers to true-false tests (just to keep them away from the prying eyes of their students). The plaintexts are just strings of T's and F's. So, for example, the answers to a ten-question test might be TFFFTTFTFF. Now suppose the teachers were negligent and used the same onetime pad key to encrypt the answers to two different tests with the same number of questions. If you can see both ciphertexts, how you can determine which questions on these tests have the same answer, and which don't? (If you've already written the first test, this will give you all the answers for the second one!)

6. One problem with the type of cryptography described in this lesson (*symmetric key cryptography*) is the huge number of keys required to make sure everyone can communicate. Suppose we lived in an alternate universe, where this is the only form of cryptography we have discovered. In this scenario, the Government of Canada maintains a secure database of keys, and any pair of Canadians wishing to communicate securely establishes a key by connecting to the government server and storing their shared key there.

   For simplicity, assume the population of Canada is 38 million people. How many keys would the government need to store to guarantee that any pair of Canadians could communicate securely? If a new Canadian comes along, how many new keys would the government have to store?