Grade 6 Math Circles
November 14/15/16
Encryption Problem Set

1. Encode the following messages using a shift cipher

    (a) *My favourite type of pie is* (Use a shift of 4)

    (b) *three point one four one five nine* (Use a shift of 12)

2. Encode the following messages using a rail fence cipher

    (a) *My favourite type of pie is* (Use 3 rails)

    (b) *three point one four one five nine* (Use 5 rails)

3. Decode the following text that was encoded using a shift cipher

    DRO LSQ ZEBZVO NYQ GKC LSQQOB DRKX DRO YBKXQO NYQ

    Remember to use frequency analysis to help you figure our how much each letter was shifted by.

4. Sometimes, we are lucky enough to acquire both the encoded and decoded text. When this happens, we can easily figure out the cipher and use this to decode future messages.

    (a) Consider the following message

    My favourite cheese is cheddar

    and the message that was encoded using a shift cipher

    TF MHCVBYPAL JOLLZL PZ JOLKKHY

    What is the secret code that was used to encrypt the message?

    (b) Using the secret code that you found in (a), decode the following message

    ISBL JOLLZL PZ TF ZLJVUK MHCVBYPAL JOLLZL

5. If you want to make your messages even harder to decode, you can use multiple ciphers.

    (a) Encode the following message first using a shift cipher with a shift of 5, and then using a rail cipher with 4 rails.

    The square root of four is two

    (b) The following message was encoded first with a shift cipher with shift 2, and then with a rail cipher with 6 rails. Decode the message.

    YAATGVQQKKEJCWLPENQJCPIJGRVTGOVUGGC

6. Consider the message $m = 6$. Using prime numbers $p = 7$ and $q = 11$, encode the message using RSA encryption.

7. A common way to encode your sentences when speaking at school is to speak in *Pig Latin*. Pig Latin is a made up language that takes the first letter of a word, moves it to the end, and adds the sound "ay". For example, "Pig Latin" becomes "igpay atinlay", and "Math Circles" becomes "athmay irclescay".

    (a) Encode the following sentence into Pig Latin

    > *Hello what's your name?*

    (b) Write a small paragraph and encode it using Pig Latin.

    (c) Do you think Pig Latin is easier to decode then a shift cipher, or harder? Why?

8. Another simple cipher is called the **transposition cipher**. In a transposition cipher letters are swapped with each other. For example we can swap 'A' with 'N' and 'D' with 'T'. Then the word 'AND' becomes 'NAT'.

    In the below table, the top row represents the original letters, and the bottom row represents what the letters are switched with in our transposition cipher.

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

Using this cipher, 'baseball' gets encoded to 'ONVRONDD'.

    (a) Using the above transposition cipher, encode the following messages.

    > *two point seven one*
    > *the sky is blue*

    (b) Decode the following message using the above transposition cipher.

    > *RGAHSLIFYG*