Grade 6 Math Circles

March 30, 2022

Cryptography - Problem Set

1. Agenṫ Alice and Agent Bob are sitting on a park bencḣ. Alicė puts down heṙ nėwspaper and leaves the park. Bob pi̇ckṡ up the ṅewspaper, reads the secret message, stands up, walks in the ȯpposiṫe direction, and finally tosses tḣe newspaper a recycli̇ṅġ bin on the way out.

   Evil Eve was watching this scene unfold from a distance. When the coast is clear, she rummages through the recycling bin and retrieves the paper. She flips through the pages but there is only yesterday's news; nothing else is written down on any of the pages. The only thing that Eve can find are tiny holes on the front page.

   Agent Alice and Agent Bob are using a cipher we have not yet discussed. Alice has poked a hole above different letters found in the frontpage article. Bob mentally noted the letters with holes above them in order, which then spell out the secret message that Alice was trying to convey.

   Determine the name of this cipher (Hint: The first paragraph of the Cryptography lesson hides the answer).

2. Recall the Atbash cipher:

$$\begin{array}{ccccccccccccc} A & B & C & D & E & F & G & H & I & J & K & L & M \\ \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow & \Updownarrow \\ Z & Y & X & W & V & U & T & S & R & Q & P & O & N \end{array}$$

   (a) Use the Atbash cipher to encrypt or decrypt the following:

      i. `YOU ARE A WIZARD`

      ii. `SZIIB KLGGVI`

      iii. `OVER AND UNDER`

   (b) Compare and contrast the Atbash cipher and the Caesar cipher.

3. Use the Caesar cipher to encrypt or decrypt the following messages using the shift number given in parentheses. You can complete the shift tables below if it helps.

   (a) `ONCE UPON A TIME` (2)

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

   (b) `GL Y EYJYVW DYP YUYW` (24)

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

4. Consider the Caesar cipher and the following ciphertext: `BWQS XCP`.

   (a) What would happen if we were to apply a shift number of 26 to the ciphertext?

   (b) What would happen if we were to apply a shift number of 30 to the ciphertext?

   (c) What would happen if we were to apply a shift number of -4 to the ciphertext?

   (d) **Challenge:** What would happen if we were to apply a shift number of 1000 to the ciphertext?

5. Consider frequency analysis as a means to break a substitution cipher.

   (a) One way to determine which letters are most commonly used is to parse a dictionary; we can count how many times each letter is used for every word in the language.

   What might this method assume? What limitations might this method have?

   (b) How might the length of a ciphertext affect its security? Is it easier to break a cipher when the length of the ciphertext is shorter or longer?

6. This question deals with the Vigenère cipher. The numbers correlating to letters given below.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

(a) Encrypt the plaintext given below using the Vigenère cipher and keyword `ADVIL`. Note, the final ciphertext will have spaces at the same locations as the plaintext.

`I HAVE A HEADACHE`

keyword	A	D	V	I	L	A	D	V	I	L	A	D	V	I
shift number														
plaintext	I	H	A	V	E	A	H	E	A	D	A	C	H	E
ciphertext														

(b) Another way of making an encrypted message really difficult to decipher is to apply an encryption multiple times.

Encrypt your ciphertext from part (a), this time with the keyword `PAIN`. Note, the final ciphertext will have spaces at the same locations as the plaintext.

keyword	P	A	I	N	P	A	I	N	P	A	I	N	P	A
shift number														
plaintext														
ciphertext														

7. We will know work on **decrypting** the following message using the Vigenère cipher.

`KONFQCPQFCGCQRILS`

(a) Complete the second row of shift numbers as you would have when encrypting a Vignière cipher.

keyword	Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O
shift number																	
plaintext																	
ciphertext	K	O	N	F	Q	C	P	Q	F	C	G	C	Q	R	I	L	S

If only there were online tools for creating Caesar Shift Tables quickly.

(b) Apply an appropriate reverse shift to each letter of the cipher.

(c) Determine the original plaintext by adding spaces in the right places.

(d) Were there any shortcuts or tricks that were helpful in the decryption process of part (c)?

8. Alana, Blaire, and Julio have entered a cryptography competition. In the first round, the contestants are asked to break a Vigenère cipher, given only a page ciphertext. They each come up with a different plan to succeed.

   - Alana's first step is to run a frequency analysis on the ciphertext. Her second step is to guess the keyword based on the most frequently appearing letters. Using a keyword determined from the previous step, she will then decrypt the message. If she observes a message that is gibberish, she only has to begin at the second step and guess another keyword.
   - Blaire's first step is to guess the length of the keyword. Her second step is to perform a frequency analysis on specific groups of letters. From there she will guess the possible keyword and then decrypt the message. If she observes a message that is gibberish, she will try different keywords and if she keeps getting gibberish, she can try a different keyword length.
   - Julio's first step is to write a Caesar cipher computer program that can brute force multiple inputted messages at a time. From here, he will input a keyword that he guesses. If he observes a message that is gibberish he will try a different keyword.

   Which contestant do you think has the best strategy?