Grade 6 Math Circles

March 30, 2022

Cryptography - Solutions

Exercise Solutions

Exercise 1

Encrypt and decrypt the respective plaintext and ciphertext using the Atbash cipher.

(a) `SLICE OF PI`

(b) `HRTNZ HFNNZGRLM`

Exercise 1 Solution

(a) `SLICE OF PI` = `HORXV LU KR`

(b) `HRTNZ HFNNZGRLM` = `SIGMA SUMMATION`

Exercise 2

Encrypt or decrypt the following messages using the shift number given in parentheses.

(a) `MY SALAD NEEDS DRESSING` (8)

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
ciphertext	I												

plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext													

(b) `GUR YRGGHPR UNF R PBYV` (13)

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
ciphertext	N												

plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext													

Exercise 2 Solution

(a) `MY SALAD NEEDS DRESSING` (8)

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

Encrypting the plaintext gives `UG AITIL VMMLA LZMAAQVO`.

(b) `GUR YRGGHPR UNF R PBYV` (13)

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

The decrypted ciphertext gives `THE LETTUCE HAS E COLI`.

Exercise 3

Consider the ciphertext

`RXHX GX WF UWUYK`

What is the most common letter in the ciphertext? Assuming that the plaintext is in English, what letter in the ciphertext likely corresponds to the plaintext letter `E`?

Note that you do not have to decode this cipher.

Exercise 3 Solution

If we assume that the most frequent letter in the plaintext is `E`, then the most frequent letter in the ciphertext, `X`, is probably `E`. This is not certain, as messages can contain letters that have lower frequencies of the letter `E`.

Exercise 4

Complete the Vigenère encryption from Example 5. Note, the final ciphertext will have spaces at the same locations as the plaintext:

TIME FOR COOKIE

keyword	C	O	D	E	C	O	D	E	C	O	D	E	C
shift number	2	14	3	4	2	14	3	4	2	14	3	4	2
plaintext	T	I	M	E	F	O	R	C	O	O	K	I	E
ciphertext	V	W											

Exercise 4 Solution

TIME FOR COOKIE

keyword	C	O	D	E	C	O	D	E	C	O	D	E	C
shift number	2	14	3	4	2	14	3	4	2	14	3	4	2
plaintext	T	I	M	E	F	O	R	C	O	O	K	I	E
ciphertext	V	W	P	H	H	C	U	F	Q	C	N	L	G

The ciphertext that we get is

VWPH HCU FQCNLG

Problem Set Solutions

1. Agent Alice and Agent Bob are sitting on a park bench. Alice puts down her newspaper and leaves the park. Bob picks up the newspaper, reads the secret message, stands up, walks in the opposite direction, and finally tosses the newspaper a recycling 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).

Solution: In the lesson, these letters have dots above them.
Cryṗtography is the study of hi̇ddeṅ writing, or reading and writing secret messages or codes. The word cryptograph**ẏ** cȯmes from the Greek word *kryptos* ($\kappa\rho\upsilon\tau\varsigma$), meaning "hidden", and *graphein* ($\gamma\rho\alpha\phi\omega$), meaning "writing". There are some key words that wi̇ll come up frequently in today's lėsson.
This is known as a **pinhole cipher**. Besides poking the paper with a pin, you could also place dots above the letters in pen for example.

2. Recall the Atbash cipher:

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

   (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.

Solution:

(a) i. `YOU ARE A WIZARD` = `BLF ZIV Z DRAZIW`. Notice how `DRAZIW` is `WIZARD` spelled backwards.

ii. `SZIIB KLGGVI` = `HARRY POTTER`

iii. `OVER AND UNDER` = `LEVI ZMW FMWVI`

(b) Answers may vary.

For similarities, they are both substitution ciphers, so by definition they replace letters of the alphabet with other letters of the alphabet. If we wanted to discuss security, both the Atbash and Caesar ciphers can be decrypted by brute force with

the right computer program or very determined codebreaker.

For differences, mainly the Atbash cipher is always the same, whereas you have up to 26 unique shift numbers for 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													

Solution:

(a) If you know the alphabet really well you could go two letters forwards in the alphabet.

`ONCE UPON A TIME` (2)

plaintext	A	B	C	D	E	F	G	H	I	J	K	L	M
ciphertext	C	D	E	F	G	H	I	J	K	L	M	N	O

plaintext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
ciphertext	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

The final ciphertext will be `QPEG WRQP C VKOG`.

(b) If you know the alphabet really well you could go two letters backwards in the alphabet.

`GL Y EYJYVW DYP YUYW` (24)

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

The initial plaintext was `IN A GALAXY FAR AWAY`.

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?

Solution:

(a) With a shift of 26, the ciphertext does not change (still `BWQS XCP`). Shifting 26 letters by 26 spaces does not affect it.

(b) The first 26 shifts do not change the ciphertext. But the remaining $30 - 26 = 4$ shifts will change `BWQS XCP` into `FAUW BGT`.

(c) A shift of -4 can be interpreted as a backwards shift of 4 or equivalently as a shift of $26 - 4 = 22$. The ciphertext would then become `XSMO TYL`

(d) A shift of 1000 is equivalent to a shift of 12 because of math! With a shift of 12 the ciphertext becomes `NICE JOB`!

Solutions to getting this may vary!

If you are familiar with Modular Arithmetic (or a modulus function in Computer Science), then you might have found that $1000 \equiv 12 \pmod{26}$, and therefore a shift of 1000 is equivalent to a shift of 12.

If you are unfamiliar with the above method, then imagine that everytime we shift 26 letters, nothing about the cipher changes. If we divide 1000 by 26 we get $1000 \div 26 = 38$ with remainder 12. This remainder of 12 is what actually shifts the numbers.

If you didn't use division you can subtract each and every shift of 26 from 1000 to ignore them. Our calculations will end up as follows:

$$1000 - 26 = 974,\ 974 - 26 = 948,\ \cdots,\ 38 - 26 = 12$$

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?

Solution: Answers may vary.

(a) This method of parsing a dictionary assumes that every word in the English language is equally likely to be used in a phrase/sentence/message. This is a limitation because the assumption is simply not true; we have to consider which words are frequently used in each language.

For example, consider the words "there" and "wagon". How many times in your daily life do you use the word "there" compared to "wagon"? It is unfair to say that the letters T, H, and R are equally as common as the letters W, G, and N?

(b) In general a longer ciphertext provides more information than a shorter ciphertext. A longer ciphertext provides more data to perform an accurate frequency analysis on, and so *generally* a longer ciphertext is more easily broken (even if it takes much more time).

For example, compare the word "STOP" to the entirety of the novel *The Hitchhiker's Guide to the Galaxy* by Douglas Adams. Which message/text is more likely to have the letter "E" appear most frequently?

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														

Solution:

(a) The plaintext is `I HAVE A HEADACHE` with keyword `ADVIL`.

keyword	A	D	V	I	L	A	D	V	I	L	A	D	V	I
shift number	0	3	21	8	11	0	3	21	8	11	0	3	21	8
plaintext	I	H	A	V	E	A	H	E	A	D	A	C	H	E
ciphertext	I	K	V	D	P	A	K	Z	I	O	A	F	C	M

The ciphertext with spaces is then `I KVDP A KZIOAFCM`.

(b) The plaintext is now `I KVDP A KZIOAFCM` with the keyword `PAIN`.

keyword	P	A	I	N	P	A	I	N	P	A	I	N	P	A
shift number	15	0	8	13	15	0	8	13	15	0	8	13	15	0
plaintext	I	K	V	D	P	A	K	Z	I	O	A	F	C	M
ciphertext	X	K	D	Q	E	A	S	M	X	O	I	S	R	M

The final ciphertext with spaces is then `X KDQE A SMXOISRM`.

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)?

Solution:

(a) It won't fit on the page but you should get the following second row.

	Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O
	24	14	20	24	14	20	24	14	20	24	14	20	24	14	20	24	14
	K	O	N	F	Q	C	P	Q	F	C	G	C	Q	R	I	L	S

(b) There are multiple ways correct that you could do a reverse shift, but you should get the following in the end.

	Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O	U	Y	O
	24	14	20	24	14	20	24	14	20	24	14	20	24	14	20	24	14
	M	A	T	H	C	I	R	C	L	E	S	I	S	D	O	N	E
	K	O	N	F	Q	C	P	Q	F	C	G	C	Q	R	I	L	S

(c) The intended plaintext is `MATH CIRCLES IS OVER`.

(d) Answers may vary. For example, if you have already decoded `MATHCIR`, you might have guessed that the next 4 letters are `CLES` based on context clues.

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?

Solution: Answers will vary!

- **Blaire**'s strategy is actually how one might break a Vigenère cipher. We first determine a possible length for the keyword (there is a mathematical formula for this but it is complicated); guessing is an option.

  For example, we can guess length 5. You would then have to do 5 separate frequency analyses. One on the 1st, 6th, 11th, 16th, ... letters, another of the 2nd, 7th, 12th, 17th, ..., letters, and so on. This is because the 1st, 6th, 11th, 16th, ... letters will have a common shift number, the 2nd, 7th, 12th, 17th, ..., letters will have a common shift number, etc.

  Then you do have to just try different shift numbers given by different keywords until something works. This is still not an easy thing to do without any technology, and even then, computer programs made to decode Vigenère ciphers might still have some sort of manual input to them.

- Julio might be able to solve it the fastest if he gets extremely lucky with his guess. Luck, coincidence, and context clues are all less mathematical but more practical components of cryptography. If he gets unlucky, then he will have a great computer program but no actual strategy beyond it.

- Alana is trying her best! She seems to know about the different components of breaking ciphers but misses the mark in the order that she uses them. Frequency analysis on the first step is not particularly helpful. As we saw in the lesson's Vigenère cipher, duplicate letters in the plaintext might have different ciphertext counterparts (e.g. the two `O`'s in `COOKIE` can become two different letters). While this strategy is not proven to be good, Alana might still win with a lucky guess like Julio.