1.0 Changing Placement

Suppose you had the letters B, E, E, H, I, K, L, S, S, T, U, and Y – could you figure out the original phrase that these letters came from? People who play Scrabble or Words with Friends could use their vocabulary knowledge to make different words from available letters, but what we want is to recreate the original phrase that these letters made.

What if instead of giving just the list of letters in alphabetical order you were given the same set of letters but written in this form: HTS EYK SI LBEU – does that help in figuring out the original phrase? Time to take a closer look!

1.0.0 Explore: ngMaki It Dciuflfti to daeR

Focus Question: How can you use patterns to rearrange the elements of a message?

1) On the front board of the classroom for anyone to see, Sandy wrote the following message to her best friend Terry who will have class in the same room next period right before lunch:

   LSTE OREDR A PAZZI FRO LHCNU

   Sandy and Terry came up with their private writing system a few weeks ago and feel confident that people who don't know the method will not be able to figure out what their messages say.

   a) Are you able to figure out what their message says? Explain how you went about trying to figure out what their message says.

   b) The next morning Terry wrote a message to Sandy about this weekend's party for Jill.

   NDEE YUO TO SNGI TEH BYAD CDRA

   What does the message say?

   c) Describe (not verbally but on paper) how the method used by Sandy and Terry works.

d) Terry and Sandy realized that they had to change their message system the day they walked into a class together and saw the following written on the front board:

WE FDOHTEM IRU GOYT UUODER

Terry and Sandy worked together and made a change to their system and at the end of the class wrote the following response message on the front board:

SEE IC FAA YND ORTI UEHS

Do you think their new system is more secure? Explain.

2) Now that someone has figured out their writing pattern, Sandy spent some time over the weekend brainstorming new patterns for writing a message. Below are examples of the same message written using five different methods:

- **HT8P MMEE TATT HELI BRAR YTON IG**
- **MLNE II EBG TRHAATT R8TYPHT MEO**
- **THGI MMP8 ATEE EHTT RBIL TYRA NO**
- **TEEM TA EHT YRARBIL THGINOT MP8**
- **HIM RTN HTB MYA IE8 RET TGL PAE OT**

a) Rank the different methods from the easiest to the most difficult to "figure out" and write a brief explanation for how you decided your ranking of the methods. Your explanation should reference specific features of each method.

b) Which methods are similar and what makes them similar? Which method seem to be unlike the others? What makes this method seem different?

c) Compare/discuss your answers to the questions. Then come to a consensus as a group of how the methods should be ranked from easiest to most difficult to "figure out" and post your ranking on the board.

1.0.1 Investigate: Counting the Ways

Focus Question: How do you count the total number of different ways of mixing up the order of the letters in a message?

Suppose you intercept a message from Sandy to Terry but you don't know the pattern that Sandy used to hide the message. One guaranteed method for discovering the original message is to try *every possible* rearrangement of the letters. But how long would doing that take? How do you count the number of possible rearrangements?

1) How many *different* ways can the letters from the word "EAT" be arranged in a row from left to right? How many of those arrangements form words? How many of those arrangements form non-words?

2) How many *different* ways can the letters from the word "LIME" be arranged in a row from left to right? How many of those arrangements form words? How many of those arrangements form non-words?

3) How many *different* ways can the letters from the message "time for lunch" be arranged in a row while keeping the letters from each individual word grouped together and keeping the word groups in the same order? For example, "eimt rof huncl" would be one way and "eimt orf huncl" would be another way.

4) How many *different* ways are there for concealing the message "time for lunch" by rearranging the order of the letters without having to keep the letters of the individual words grouped together? For example, "tfor ime lunch" would count as one way and "lime tor funch" would count as another way.

5) Suppose someone intercepted the concealed message "time for lunch" and was planning on uncovering the message by writing out every possible rearrangement of the characters. Assuming it would take 1 second to write out one of the possible rearrangements, how long would it take to write the entire list of possibilities?

6) How many *different* ways can the letters from the word "MEET" be arranged in a row from left to right?

1.0.2 Notes: Vocabulary

Instead of having to repeatedly come up with different ways of saying "the original message" and "the message written with its letters rearranged" let's make it easier by introducing some terms that are standard use in the study of cryptography.

- ***plaintext*** will refer to the message in its original, easy to read, non-rearranged form
- ***ciphertext*** will refer to the message in its concealed, more difficult to read, rearranged form
- ***character*** will refer to a single symbol that appears in the plaintext
- Should the spaces between words count as symbols? The answer for most in cryptography is that spaces ***do not*** count as symbols because the number of spaces in a message reveals the number of words in the message.

Teacher Guide for Lesson 1.0: Changing Placement

Lesson Objective:	• Introduce different methods for making a message difficult to read through moving the individual characters of a message • Develop methods/strategies for counting • Recognize the need for keys that make it possible to undo a rearrangement method
Standards for Mathematical Practice:	• SMP.1: Make sense of problems and persevere in solving them. • SMP.3: Construct viable arguments and critique the reasoning of others. • SMP.4: Model with mathematics • SMP.6: Attend to precision. • SMP.7: Look for and make use of structure.
Length of Activity:	3 - 4 hours
Materials:	Student handout: Changing up the Order
Lesson Overview:	This lesson introduces students to fundamental ideas used to create and evaluate cipher systems such as the need for an algorithmic method, the need for counting the number of options that a method can generate, and the need for reversibility of the method. The strength/security of a system is connected to the time it would take to try all possibilities. Calculating the time required to try all possibilities requires knowing how many possibilities exist. This leads to a need for developing counting methods. The rearrangement method used by the sender must be able to be "undone" by the intended receiver of the message. This leads to the idea of keys as information used to for "undoing" the rearrangement.
Closure:	After each task, teacher can have students briefly reflect on the focus questions posed at the beginning of each task. At the end of the lesson, have students respond to the following question: How you could use some of the methods for hiding a message that were presented to create methods that are similar yet not exactly the same?
Homework:	All problems in the problem set. Teachers can break up the set to be done over several class periods.

1.0 Changing Placement

Suppose you had the letters B, E, E, H, I, K, L, S, S, T, U, and Y – could you figure out the original phrase that these letters came from? People who play Scrabble or Words with Friends could use their vocabulary knowledge to make different words from available letters, but what we want is to recreate the original phrase that these letters made.

What if instead of giving just the list of letters in alphabetical order you were given the same set of letters but written in this form: HTS EYK SI LBEU – does that help in figuring out the original phrase? Time to take a closer look!

1.0.0 Explore: ngMaki It Dciuflfti to daeR

Focus Question: How can you use patterns to rearrange the elements of a message?

Teacher Notes: *The goal for of this investigation is to get students working with and thinking about transposition (rearranging) cipher systems (a method for acting on the individual characters of a message rather than on the words). Along the way, students will likely want to start suggesting their own ideas/methods for rearranging the letters in a message – if time permits, allow for that but inform students that there will be plenty of time/opportunity at the end of the unit for them to work on creating their own methods.*

1) On the front board of the classroom for anyone to see, Sandy wrote the following message to her best friend Terry who will have class in the same room next period right before lunch:

LSTE OREDR A PAZZI FRO LHCNU

Sandy and Terry came up with their private writing system a few weeks ago and feel confident that people who don't know the method will not be able to figure out what their messages say.

a) Are you able to figure out what their message says? Explain how you went about trying to figure out what their message says.

Solution: "LETS ORDER A PIZZA FOR LUNCH"

Answers will vary, but it is likely students will notice the word LETS and then search for a second word. The presence of two of the letter Z should also help narrow word possibilities.

b) The next morning Terry wrote a message to Sandy about this weekend's party for Jill.

NDEE YUO TO SNGI TEH BYAD CDRA

What does the message say?

Solution: "NEED YOU TO SIGN THE BDAY CARD"

Students should notice the word LETS and then follow the pattern established from the previous question. The abbreviation of BIRTHDAY as BDAY might spark discussion about how vocabulary knowledge as well as slang is a resource for attempting to figure out a message.

c) Describe (not verbally but on paper) how the method used by Sandy and Terry works.

For each word in the message, write the first letter of the word but then take the remaining letters of the word and write them in reverse order.

d) Terry and Sandy realized that they had to change their message system the day they walked into a class together and saw the following written on the front board:

WE FDOHTEM IRU GOYT UUODER

Terry and Sandy worked together and made a change to their system and at the end of the class wrote the following response message on the front board:

SEE IC FAA YND ORTI UEHS

Do you think their new system is more secure? Explain.

It is possible that it will take groups a long time to figure out what the message says (SEE IF YOU CAN READ THIS). There should be consensus that their new system is more secure because the new system is different from the original system – specifically, the difference is that the letters of each word have not been kept within their original word group; instead, the letters have been distributed to different word groups.

2) Now that someone has figured out their writing pattern, Sandy spent some time over the weekend brainstorming new patterns for writing a message. Below are examples of the same message written using five different methods:

- **HT8P MMEE TATT HELI BRAR YTON IG**
- **MLNE II EBG TRHAATT R8TYPHT MEO**
- **THGI MMP8 ATEE EHTT RBIL TYRA NO**
- **TEEM TA EHT YRARBIL THGINOT MP8**
- **HIM RTN HTB MYA IE8 RET TGL PAE OT**

a) Rank the different methods from the easiest to the most difficult to "figure out" and write a brief explanation for how you decided your ranking of the methods. Your explanation should reference specific features of each method.

Suggested Lesson Activity: *Have students work individually to answer this question. Expect that students will have different opinions and ways of viewing these five methods and that is perfectly ok as long as they provide reasonable explanation/rationale. Emphasize that their explanations should point to specific, describable characteristics like "there doesn't seem to be a pattern in the letter arrangement" or "the letters are written in reverse-order"*

Solution: Note that the goal of this activity is not to go into the details of how each method works – the goal is to promote discussion of how not all rearrangement methods have the same level of difficulty when it comes to trying to discover the pattern that was used. All of the ciphertexts were generated from the plaintext MEET AT THE LIBRARY TONIGHT 8PM

In terms of the ranking of difficulty, answers will vary, but most likely the last method will be ranked as the most difficult as the majority of students will not "see" the pattern.

The method used to create each ciphertext has been shown using the entire English alphabet to help clarify the patterns:

- **VWXY ZABC DEFG HIJK LMNO PQRS TU**
  ABCD EFGH IJKL MNOP QRST UVWX YZ
- **AVQL GB WRM HCXDNID YTOJEZU PKF**
  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
- **WVUT AZYX EDCB IHGF MLKJ QPON SR**
  TUVW XYZA BCDE FGHI JKLM NOPQ RS
- **DCBA FE IHG PONMLKJ WVUTSRQ ZYX**
  ABCD EF GHI JKLMNOP QRSTUVW XYZ
- **VKZ ODS HWL APE TIX MBQ FUJ YNC RG**
  --- --- --- 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

b) Which methods are similar and what makes them similar? Which method seem to be unlike the others? What makes this method seem different?

Suggested Lesson Activity: *Have students work individually to answer this question. While some students might have different observations, there should be many areas of agreement among students. Emphasize that their explanations should point to specific, describable characteristics like "both methods use backwards writing"*

Solution: Answers will vary, but some ideas that should surface include whether or not word groupings are preserved and whether or not individual characters are moved.

c) Compare/discuss your answers to the questions. Then come to a consensus as a group of how the methods should be ranked from easiest to most difficult to "figure out" and post your ranking on the board.

Suggested Lesson Activity: *Arrange students in small groups and allow time for them to complete part (c). Once the rankings are posted from all groups, allow for a class discussion about the rankings, especially highlighting areas of agreement and areas of disagreement.*

Solution: Answers will vary, but most likely the last method will be ranked as the most difficult as the majority of students will not "see" a pattern.

Pocket Questions

- How successful do you think you would be trying to figure out the pattern for a message that was written in a language you didn't read or speak? Explain.
- What advantage does grouping the letters of a message into equal sizes provide?

1.0.1 Investigate: Counting the Ways

Focus Question: How do you count the total number of different ways of mixing up the order of the letters in a message?

Teacher Notes: *The goal for of these investigation is to get students to develop strategies for counting. While some students may have experience with some formulas for counting (permutations and combinations), the hope is that students will begin to realize that structure can be used as a means to help with counting by providing insights for generalizing.*

Suppose you intercept a message from Sandy to Terry but you don't know the pattern that Sandy used to hide the message. One guaranteed method for discovering the original message is to try *every possible* rearrangement of the letters. But how long would doing that take? How do you count the number of possible rearrangements?

1) How many different ways can the letters from the word "EAT" be arranged in a row from left to right? How many of those arrangements form words? How many of those arrangements form non-words?

Suggested Lesson Activity: *Initially have students work individually on the first two questions. Ideally teachers should refrain from direct instruction and instead monitor student work. Some students may recognize these questions as similar to some questions that were asked in the Graph Theory Unit. When most students have shown reasonable attempts at answering both questions, have students move into their groups to discuss/check/compare their strategies for counting.*

Solution: There are 6 different ways to arrange the letters in the word "EAT" in a row from left to right and 4 of the arrangements form words (EAT, TEA, ATE, ETA) while 2 of the arrangements (AET, TAE) form non-words, assuming we are limiting discussion to the English language.

There are different ways to arrive at the count of 6 with listing all possibilities as a most typical method. To ensure that listing all possibilities is done in a way that doesn't duplicate or omit possibilities, the listing method should involve a systematic process (i.e. start with placing "e" as the first letter and then considering the two different ways of arranging the letters "a" and "t", then place "a" as the first letter, …) or using a tree diagram from the Graph Theory unit.

While there are more formal mathematical equations that can be used to count this, it is not suggested to introduce formal counting equations at this point as those will be further developed later in the course.

2) How many *different* ways can the letters from the word "LIME" be arranged in a row from left to right? How many of those arrangements form words? How many of those arrangements form non-words?

Solution: There are 24 different ways to arrange the letters in the word "LIME" in a row from left to right and 2 of the arrangements form words (LIME, MILE) while 22 of the arrangements form non-words.

There are many ways to arrive at the count of 24 different ways. In addition to the previous methods, there is another method that can draw from the previous question: take the first three letters (L, I, M) and we know that there are 6 different ways to arrange those in a row from left to right. Using that list of 6 arrangements, there are four options for "inserting" the

fourth letter (E), namely at the beginning, between the first and second letters, between the second and third letters, or at the end.

3) How many *different* ways can the letters from the message "time for lunch" be arranged in a row while keeping the letters from each individual words grouped together and keeping the word groups in the same order? For example, "eimt rof huncl" would be one way and "eimt orf huncl" would be another way.

Suggested Lesson Activity: *Allow students to work with their groups to get into the third question. Ideally teachers should refrain from direct instruction and instead monitor each group's work. When most groups have shown reasonable work towards answering the question, ask each group to post on the board their approach for counting. Allow time for students to read through/process other groups methods. At this point, there should be enough material to open a class discussion on techniques for counting.*

Solution: There are 17,280 different ways to do this. There are 4*3*2*1 = 24 ways to arrange the letters in the word "time", 3*2*1 = 6 ways to arrange the letters in the word "for", and 5*4*3*2*1 = 120 ways to arrange the letters in the word "lunch". Now thinking of the words themselves as the objects, there are 24*6*120 = 17,280 ways to arrange the words "time" "for" "lunch"

4) How many *different* ways are there for concealing the message "time for lunch" by rearranging the order of the letters without having to keep the letters of the individual words grouped together? For example, "tfor ime lunch" would count as one way and "lime tor funch" would count as another way.

Suggested Lesson Activity: *Allow students to work with their groups on the fourth question. Ideally teachers should refrain from direct instruction and instead monitor each group's work. When most groups have arrived at an answer to the question, ask each group to post on the board their answer. At this point, there should be enough material to open a class discussion on techniques for counting.*

Solution: There are 479,001,600 different ways to do this. Because there are 12 *distinct* letters, there are 12*11*10*9*8*7*6*5*4*3*2*1 ways to arrange the letters in a row without having to worry about maintain letters in their original word grouping.

5) Suppose someone intercepted the concealed message "time for lunch" and was planning on uncovering the message by writing out every possible rearrangement of the characters. Assuming it would take 1 second to write out one of the possible rearrangements, how long would it take to write the entire list of possibilities?

Suggested Lesson Activity: *Allow students to work with their groups on this question. This question allows for a discussion of unit conversions as well as introducing the idea of using technology for brute force methods that check all possibilities. While it would take a computer less than a second to check a possibility – but how many would the computer need to check each second to get through all the possibilities in a reasonable amount of time?*

Solution: It would take 479,001,600 seconds which is 7,983,360 minutes which is 133,056 hours which is 5,544 days which is a bit over 15 years.

There are 479,001,600 different ways to do this. Because there are 12 *distinct* letters, there are 12! ways to arrange the letters in a row without having to worry about maintain letters in their original word grouping.

6) How many *different* ways can the letters from the word "MEET" be arranged in a row from left to right?

Suggested Lesson Activity: *Initially have students work individually on the first two questions. Ideally teachers should refrain from direct instruction and instead monitor student work. When most students have shown reasonable attempts at answering both questions, have students move into their groups to discuss/check/compare their strategies for counting.*

Solution: There are 12 different ways to arrange the letters in the word "MEET" in a row from left to right (EEMT, EETM, MEET, TEEM, MTEE, TMEE, METE, EMET, ETEM, TEME, EMTE, ETME). One strategy for counting these involves thinking of the repeated letter E as an object with three cases: the two E's have no letters between them, the two E's have one letter between them, and the two E's have two letters between them.

1.0.2 Notes: Vocabulary

Instead of having to repeatedly come up with different ways of saying "the original message" and "the message written with its letters rearranged" let's make it easier by introducing some terms that are standard use in the study of cryptography.

plaintext will refer to the message in its original, easy to read, non-rearranged form

ciphertext will refer to the message in its concealed, more difficult to read, rearranged form

character will refer to a single symbol that appears in the plaintext

Should the spaces between words count as symbols? The answer for most in cryptography is that spaces ***do not*** count as symbols because the number of spaces in a message reveals the number of words in the message.