# Chapter 1 Project

# Just Between You and Me

**An activity to demonstrate the use of whole number arithmetic in real life.**

Cryptography deals with turning a message from plaintext into a code known as ciphertext. Ciphertext appears to the general public as nonsense but can be decoded by the intended recipient. Over the past few hundred years, the field of cryptography has advanced greatly. Around 2000 years ago, all that was usually needed to encode (or encrypt) a message was whole number arithmetic.

To work with this classic form of encryption, often called a shift cipher, there is just one additional thing we need to know. Shift ciphers work similar to how a 12-hour clock shows the same time every 12 hours, even though it's a different time, or even a different day. Extending this concept to the alphabet, Table 1 assigns each letter a number, starting with 0, and repeats the cycle after the letter Z.

| 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 | A | B | C | … |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | … |

Using subtraction, we can find that the numbers representing the two As are 26 apart. Similarly, the two Bs are 26 apart. Just like the digits on a clock begin to repeat after 12 hours, the letters will begin to repeat after 26 letters.

1. Notice C is represented by 28.
   a. Determine the remainder when 28 is divided by 26.
   b. Compare the value of the remainder found in part a. to the values in Table 1. What do you notice about this value and 28?

The idea behind a *shift* cipher is to shift the letters in the plaintext by a given number of letters to form the ciphertext. This encryption can be done with a right-shift or a left-shift.

A *right-shift* is obtained by adding the same value to each of the numbers associated with the letters. Since each letter in Table 1 is associated with a whole number, we will add the value of the right-shift, and then divide by 26, using the letter associated with the *remainder*.

For example, we will apply a right-shift by 14 to encrypt the plaintext HELLO:

**Step 1:** H, E, L, L, O is turned into 7, 4, 11, 11, 14.

**Step 2:** Adding 14 to each of these results in 21, 18, 25, 25, 28.

**Step 3:** When dividing by the 26, the remainders are 21, 18, 25, 25, 2, so the ciphertext is VSZZC.

2. Encrypt the word ZYGOTE using a right-shift by 3.

A *left-shift* is obtained by subtracting the same value from each of the numbers associated with the letters. We will first add 26 to the number associated with the letter, subtract the value of the left-shift, and then divide by 26, using the letter associated with the *remainder*.

For example, to decrypt the ciphertext VSZZC (which was encrypted using a right-shift by 14), we will apply a left-shift by 14:

**Step 1:** VSZZC becomes 21, 18, 25, 25, 2. Adding 26 to each of these results in 47, 44, 51, 51, 28.

**Step 2:** Subtracting 14 from each of these results in 33, 30, 37, 37, 14.

**Step 3:** When dividing by 26, the remainders are 7, 4, 11, 11, 14, so the plaintext is HELLO.

Notice that we added 26 to each number during Step 1. This is a necessary step when applying a left-shift to avoid negative numbers.

3. When the message has more than one word, all letters are capitalized and there are no spaces nor punctuation. This adds to the look of the text being nonsense, but for someone that knows how the plaintext was encoded, part of decoding will be properly separating things out. Suppose a colleague sends the following encrypted message, and you know the colleague used a right-shift by 8.

   QABPMUMMBQVOIBVWWV

   **a.** Convert the letters in the ciphertext to numbers using Table 1.

   **b.** What would it take to undo a right-shift by 8? State this and state what numbers are obtained.

   **c.** Convert these back to letters using Table 1.

   **d.** Separate out the plain text into individual words to completely recover your colleague's original message.

Suppose you are not the intended recipient of the following ciphertext, but you have intercepted the message. You know that a right-shift by a certain amount has been used, but you do not know by how much.

EWWLEWSLLZWUGXXWWKZGHSLFAFW

For very short messages, a "brute force" approach could be used to check every possible right-shift and undo that shift. But that would mean trying 25 different possibilities. This would be too time-consuming for messages moderately long to very long.

4. Why would there 25 possibilities to check?

5. Instead of checking every possible right-shift, messages can often be decoded using the fact that E is the most commonly used letter in the English language.

   **a.** Count how many times each letter occurs in the intercepted ciphertext.

   **b.** Assume that the letter that shows up most frequently in the ciphertext was the letter E in the plaintext. What was the amount of the right-shift?

   **c.** Based on your answer from part b., decrypt the message. Separate out the plain text into individual words to completely recover the plaintext of the original message you intercepted.