8.2 PROJECT

AFFINE SHIFT CIPHERS

In Section 8.2, you learned about modular arithmetic. In this project, you will use modular arithmetic to encode and decode messages.

One method of encoding messages is to simply convert the letters of the alphabet to numbers by identifying A with 0, B with 1, and so on.

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
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

A message encoded in this manner would be a string of numbers. We can make this encryption slightly more advanced by using a shift cipher, also called a Caesar cipher, which converts the message back to a string of letters. To use a shift cipher on the numerically encoded alphabet, add a fixed value (the "shift" value) to the number and then calculate the result modulo 26, then substitute the corresponding value into the encoded string.

For example, suppose we want to encode the letter T using a shift cipher with a shift of 9. First, we need to know that T corresponds to 19. Adding the shift value results in a value of 28, which is not a number modulo 26. We can calculate that 28 mod 26 = 2. The letter we'd use in the encoded message is C.

1. Encode the word NOTE using a shift cipher with a shift value of 11.

If the value of the shift is known, a shift cipher is easy for anyone to decode. In the example with a shift of 9, the encoded letter was C, which corresponds to a value of 2. To decode this letter, we subtract the shift value to get −7. Since this number is negative, we can add 26 to get a value between 0 and 25. In this case, we get 19, which corresponds to T.

2. Decode DLQP that was coded using a shift cipher with a shift of 11.

Since shift ciphers are relatively easy to decode, more advanced coding methods are used to keep information safe. One slightly more advanced method is an affine shift cipher. This method involves multiplying the letter value by a number relatively prime to 26, called the key, before adding the shift value. For example, suppose we want to encode the letter T using an affine shift cipher with a key of 7 and a shift of 9. We would compute $7(19)+9=142$. Next, we would calculate 142 mod 26 = 12. This means the encoded letter is M.

3. Encode the word CODE using an affine shift cipher with a key of 5 and a shift of 11.

To decode a message encoded with a shift cipher, the shift value is subtracted. To decode a message encoded with an affine shift cipher, the shift value is first subtracted and then division modulo 26 is performed. Division in modular arithmetic is a little tricky; it involves multiplying by the multiplicative inverse of the key modulo 26. For example, if the value of the key is k, we need to find a value d so that $kd \equiv 1 \pmod{26}$. This is the reason we want k to be relatively prime to 26: d is the multiplicative inverse of k modulo 26.

4. List out the numbers less than 26 that are relatively prime to 26.

5. Suppose you intercept a message and discover that it is encoded using an affine shift cipher with a key of 3 and a shift of 12. Determine the multiplicative inverse of the key modulo 26. (**Hint:** Use the list created in part 4 and determine the value of each product modulo 26.)

6. You intercept a message that you know has been encoded with an affine shift cipher that has a key of 3 and a shift of 12. Decode the following message.

   OCO MOOKORMZSY LYIUKLYV

7. You are told that the following responses to such messages are common.

   - SENDING
   - DECLINE
   - UNCLEAR

   Choose a response to the message and encode it using the same cypher.