Cryptographic Word Search

Tom Edgar and Andrew Lloyd

Everyone loves a word search puzzle, but they are typically completed without much thought. And, by necessity, many of the letters in the puzzle go unused. Based on these two ideas, we have created a cryptographic word search within a word search. Once the first puzzle has been completed, the unused letters represent an encrypted ciphertext. Decrypt this message, arrange the resulting string in a 10×10 grid, and obtain a new word search.

The goal of any encryption scheme is to encode a message, known as the plaintext, to produce the ciphertext. Of course, there are many methods of encryption. We focus on an interesting, but elementary, method that uses modular arithmetic. The 26 letters in the English alphabet have a natural correspondence to numbers 0,1,...,25, as shown in table 1; thus, we will work modulo 26.

Two integers, a and b, are equivalent modulo (or mod) 26 if $b-a$ is a multiple of 26. For instance, 61 and 9 are equivalent mod 26 because $61-9=52=2\cdot26$. Every integer is equivalent (mod 26) to a unique integer in the set $Z_{26}=\{0,1,2,...,25\}$, given precisely by the remainder when dividing. We can perform addition, subtraction, and multiplication of elements in Z_{26} by performing the operation using integers and taking the remainder when divided by 26. For instance, $20+12=32=1\cdot26+6$, so $20+12=6 \mod 26$, and $7\cdot15=105=4\cdot26+1$, so $7\cdot15=1 \mod 26$.

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

Table 1. Correspondence between letters of the alphabet and the numbers 0,1,...,25.

To "divide" by an element a, we must find another element a^{-1} in Z_{26}, such that $a^{-1}\cdot a=1 \mod 26$. Such a multiplicative inverse exists if, and only if, the greatest common divisor of a and 26 is 1. The 12 elements of Z_{26} satisfying this condition are

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}.$$

We know that both 1 and 25 (which is equivalent to -1) are self-inverses, and earlier we saw that 7 and 15 are inverses. We could use the Euclidean algorithm to find the other four pairs of inverse elements, but because the set is small, a brute force approach may be easiest. We leave that as an exercise.

One way to encrypt messages is to use an invertible function from Z_{26} to Z_{26}. To get from the ciphertext back to the plaintext, we decode the message using the inverse function. One such type of function is an affine linear function, which has the form $f(x)=ax+b \mod 26$, where a and b are in Z_{26}. If the domain were the set of real numbers, then f would be invertible provided $a\neq0$, but the domain is Z_{26}, and so f is invertible only when a is invertible.

Ciphers of this form are known as affine ciphers. Let's see how the process works. Suppose we want to encrypt the plaintext message WORD SEARCH using the affine cipher with $a=3$ and $b=20$, that is, using the function $f(x)=3x+20 \mod 26$. We replace each letter by its corresponding number in Z_{26}, apply f to each number, and replace each resulting number by its corresponding letter in the alphabet. The newly obtained string is the ciphertext. For example, the first letter, W, corresponds to the number 22, and $f(22)=3\cdot22+20=8 \mod 26$. Thus, we replace W with I. Similarly, O corresponds to 14, and $f(14)=10 \mod 26$, which corresponds to K. Continuing in this manner we obtain the full ciphertext: IKTD WGUTAP.

As long as we know the key, in this case a and b, we can decrypt the ciphertext to recover the plaintext using the function

$f^{-1}(x) = a^{-1} \cdot (x + (26 - b)) = a^{-1} \cdot x + a^{-1} \cdot (26 - b) \mod 26$.

This function undoes the encryption function because a^{-1} is the multiplicative inverse of a in Z_{26} and $26 - b$ is the additive inverse of b in Z_{26}; consequently, when composing the two functions, we see $(f^{-1} \circ f)(x) = 1 \cdot x + 0 \mod 26$ is the identity function.

The following 10 strings are ciphertexts that have been encrypted using the previous affine cipher, $f(x) = 3x + 20 \mod 26$. Observe that 9 is the multiplicative inverse of 3 $(3 \cdot 9 = 1 \mod 26)$, $26 - 20 = 6$, and $9 \cdot 6 = 2 \mod 26$. So, the decryption function is $f^{-1}(x) = 9x + 2 \mod 26$. As a warm-up exercise, decrypt the following ciphertexts.

IKTD	PSDDGH
WGUTAP	GHATONZ
EKDCBUT	AKDG
SHFGTZ	ASNPGT
SHZGMGT	UBMGXTU

Without further ado, we leave you the following word search within a word search puzzle. As with any word search, we have provided the list of words you must find—the words highlighted blue in this article. The second word search comes from the 100 unused characters; they must be decrypted and then arranged in a 10×10 grid, written left-to-right and top-to-bottom. Of course, in the spirit of cryptography and the secrecy desired, we have neglected to tell you the key for decrypting the letters. To find the numbers a and b used to encrypt the smaller word search, you must play the role of code breaker. You could check the $312 = 12 \cdot 26$ affine ciphers over Z_{26} (there are 12 choices for a and 26 choices for b) one at a time. But, as a hint, when we used a and b to encrypt HORIZONS, we obtained FCXMBCVE. You must find 10 words in the second word search: the ones we asked you to decrypt in the warm-up exercise. Good luck! (The values of a and b, the solutions to the two puzzles, and Sage code that performs this cryptographic technique on the alphabet can be found at *maa.org/mathhorizons/supplemental.htm.*) ■

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

Tom Edgar is an assistant professor at Pacific Lutheran University, where he has been working since 2009. His research interests lie in the areas of algebra and combinatorics—especially where the two overlap. He enjoys making Easter eggs.
Email: edgartj@plu.edu

Andrew Lloyd has lived in Washington state since he joined the U.S. Air Force in 2006. He graduated from Pacific Lutheran University in May 2014 with a bachelor of science in mathematics and a computer science minor.
Email: lloydam@plu.edu

http://dx.doi.org/10.4169/mathhorizons.22.2.26