Character Ciphers and Block Ciphers

A **cipher** takes a message (the **plaintext**) and **encodes** it — puts it in a form (the **ciphertext**) where the information in the message is not obvious upon inspection. The recipient of the message takes the ciphertext and **decodes** it — performs an operation which recovers the plaintext from the ciphertext.

Example. (A **shift cipher**) This is also known as a **Caesar cipher**, since it was supposedly used by Julius Caesar.

The letters of the alphabet will be represented by the numbers $0, \ldots, 25$:

$$A = 0, B = 1, C = 2, \ldots, Z = 25.$$

If x is a letter, I'll encode it using

$$y = x + 11 \pmod{26}.$$

(I could use any nonzero number from 1 to 25 in place of 11.) The formula above replaces each letter with another letter; in effect, the alphabet gets "shifted" 11 places to the left.

The translation table for this cipher is:

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

(a) Use this cipher to encrypt the message

I WAS ASLEEP AT THE TIME

(b) Find the decoding transformation for this cipher.

"I" is replaced by "T", "W" by "H", and so on. I get the ciphertext

T HLD LWDPPA LE ESP ETXP

I'll group the letters into 5-letter words to hide the original word groupings:

THLDL DWPPA LEESP ETXPZ

I've thrown in an extra "Z" at the end to make the last group come out evenly. If you decode the message, you'd get

IWASA SLEEP ATTHE TIMEO

You can see that the 5-letters grouping and the extra "Z" did no harm, since it's evident what the plaintext was. □

(a) Solve the equation $y = x + 11 \pmod{26}$ x:

$$x = y + 15 \pmod{26}.$$

This equation is the decoding transformation; it's equivalent to reading the translation table backward. □

Example. Consider the shift cipher

$$y = x + 19 \pmod{26}.$$

Use it to encrypt the message "I MUST HAVE FOOD".

The encrypted message is "B FNLM ATOX YHHW".

I wrote a computer program to do this. There are only 26 possible shifts, so if you wanted to decode this by brute force, you could feed the ciphertext through 26 shift programs and see which one produced a sensible message. Shift ciphers are not of much use when it comes to protecting secrets! □

The next thing to try is an **affine transformation**:

$$y = ax + b \pmod{26}, \quad \text{where} \quad (a, 26) = 1.$$

I need the last condition in order to ensure that I can decode messages. This is equivalent to being able to invert the transformation. Now if $(a, 26) = 1$, then a is invertible mod 26, so

$$x = a^{-1}(y - b) \pmod{26}.$$

This equation can be used to decode messages.

Example. Consider the transformation $y = 5x + 14 \pmod{26}$.

(a) Encrypt the plaintext "WHEN WILL I BECOME A FISH".

(b) Find the decoding transformation.

(a) Here's the translation table:

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

The ciphertext is "UXIB UCRR C TIYGWI O NCAX". □

(b) Solve for x in terms of y:

$$\begin{aligned} y &= 5x + 14 \pmod{26} \\ y + 12 &= 5x \pmod{26} \\ 21(y + 12) &= 21 \cdot 5x \pmod{26} \\ 21y + 18 &= x \pmod{26} \end{aligned}$$

□

Example. Consider the following affine cipher:

$$y = 8x + 7 \pmod{26}.$$

Find two plaintexts (input letters) that produce the same ciphertext (output letter).

I can produce two inputs that give the same output by finding two inputs that make "$8x$" equal to 0 mod 26. One such value is 0; I can produce another by using 13, since $8 \cdot 13 = 104 = 0 \pmod{26}$.

$$8 \cdot 0 + 7 = 7 \pmod{26}, \quad 8 \cdot 13 + 7 = 7 \pmod{26}.$$

The inputs are $x = 0$ (which is "A") and $x = 13$ (which is "N"). □

This isn't a very good affine cipher, since you can't construct a decoding transformation.

Shift ciphers and affine transformation ciphers are called **substitution** or **character ciphers** because each letter is replaced by another letter. They're simple to use, but relatively easy to crack. For example,

with any reasonably large message you can count the letters in the ciphertext and guess the substitution using frequency tables for letters in the English language.

As a partial remedy to frequency analysis, you might think of enciphering blocks of k letters at a time. To do this, encode letters as number from 0 to 25 in the usual way. Consider a block of k letters $a_1 a_2 \dots a_k$. As the cipher key, choose a $k \times k$ matrix M which is invertible mod 26. (M will be invertible mod 26 if $\det M$ is relatively prime to 26.) Then the cipher transformation is $\vec{c} = M\vec{a} \pmod{26}$, i.e.

$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{bmatrix} = M \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{bmatrix} \pmod{26}.$$

You can decipher messages using $\vec{a} = M^{-1}\vec{c} \pmod{26}$.

Example. (a **digraphic cipher**) Consider the cipher

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 5 & 3 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \pmod{26}.$$

(a) Encode the message "SPICY MEATBALLS".

(b) Find the decoding transformation.

(a) Break the message up into two-letter groups and convert them to 2-dimensional vectors:

SP	IC	YM	EA	TB	AL	LS
$(18, 15)$	$(8, 2)$	$(24, 12)$	$(4, 0)$	$(19, 1)$	$(0, 11)$	$(11, 18)$

Finally, use M to encode each vector. For example,

$$\begin{bmatrix} 5 & 3 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 18 \\ 15 \end{bmatrix} = \begin{bmatrix} 5 \\ 3 \end{bmatrix} \pmod{26}.$$

$(5, 3) =$ FD, so the first two letters of the ciphertext are "FD".
Continuing in this way, you obtain the ciphertext

FD UW AG UI UP HH FY □

(b) Let

$$M = \begin{bmatrix} 5 & 3 \\ 2 & 3 \end{bmatrix}.$$

Since $\det M = 9$ and $(9, 26) = 1$, M is invertible mod 26. In fact,

$$M^{-1} = 9^{-1} \begin{bmatrix} 3 & -3 \\ -2 & 5 \end{bmatrix} = 3 \cdot \begin{bmatrix} 3 & 23 \\ 24 & 5 \end{bmatrix} = \begin{bmatrix} 9 & 17 \\ 20 & 15 \end{bmatrix}.$$

(Note that $\dfrac{1}{9} = 9^{-1} = 3$, because $3 \cdot 9 = 1 \pmod{26}$.)
The decoding transformation is

$$\begin{bmatrix} p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} 9 & 17 \\ 20 & 15 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \pmod{26}. \quad \square$$

Example. Consider the following block cipher:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 5 & 7 \\ 3 & 5 \end{bmatrix} \begin{bmatrix} u \\ v \end{bmatrix} \pmod{26}.$$

Find two different inputs (u_1, v_1) and (u_2, v_2) which produce the same output.

I'll find two different inputs which produce the same output $(0, 0)$. One such input is $(0, 0)$.
To find another, do the matrix multiplication and write out the two equations:

$$5u + 7v = 0$$
$$3u + 5v = 0$$

I can get a (nonzero) solution to the first equation by "switching and negating":

$$5 \cdot 7 + 7 \cdot (-5) = 0 \pmod{26}, \quad \text{or} \quad 5 \cdot 7 + 7 \cdot 21 = 0 \pmod{26}.$$

I try $(7, 21)$ in the second equation:

$$3 \cdot 7 + 5 \cdot 21 = 126 = 22 \pmod{26}.$$

I didn't get 0, but since 22 has a factor of 2, I can get 0 by multiplying everything by 13:

$$13 \cdot (7, 21) = (91, 273) = (13, 13) \pmod{26}.$$

This still satisfies $5u + 7v = 0 \pmod{26}$.
Thus, $(0, 0)$ and $(13, 13)$ are two inputs which give the same output. This shows that this block cipher is a poor cipher, since you won't be able to construct a decoding transformation. □
