Secret Codes

Henry Hale

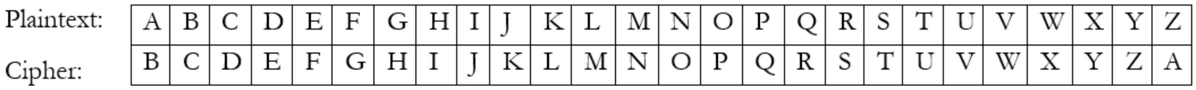
October, 2018

Ciphers have been used for thousands of years to keep information secret. There are many different types of ciphers, each with a unique and specific set of instructions for how to encode and decode the message. In the digital age, encryption methods are constantly in use in securing people's information. I am fascinated by the variety and complexity of ciphers, and I am interested in the challenge of mathematically describing various ciphers.

I will be examining 4 ciphers in this paper. For each cipher I will explain how to get the encrypted message from the original message, and how to get the original message from an encrypted message.

The Caesar Cipher

The first Cipher I will examine is the Caesar Cipher. This cipher works by shifting every letter in the alphabet by a specified amount[3].



Plaintext:	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
Cipher:	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

The table above displays a Caesar alphabet below a regular alphabet. The Caesar alphabet has been shifted by one letter. Using this cipher, the message "Hello World" becomes "IFMMPXPSME"

Let m = Original message

Let $m_i = i^{th}$ letter of original message

Let s = Value of shift. (s value of 1 shifts 'a' to 'b', s value of -2 shifts 'a' to 'y')

Let e = Encrypted message

Let $e_i = i^{th}$ letter of encrypted message

Using these variables we can represent any Caesar shift as the following:

$$e_i = m_i + s$$

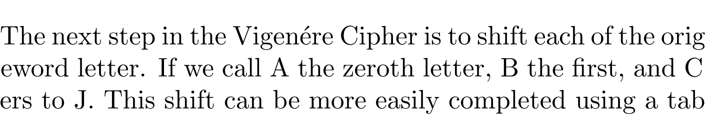
$$m_i = e_i - s$$

This shows that any encrypted letter can be found by adding the shift value to the original letter, and any original letter can be found by subtracting the shift value from the encrypted letter.

The Caesar cipher is more secure than leaving your information unencrypted, but just barely. With only 25 possible encryptions it would not take long to crack this code by hand. Modern computers could decrypt any Caesar shift in less than a second. I would not use the Caesar cipher to keep my sensitive information secure.

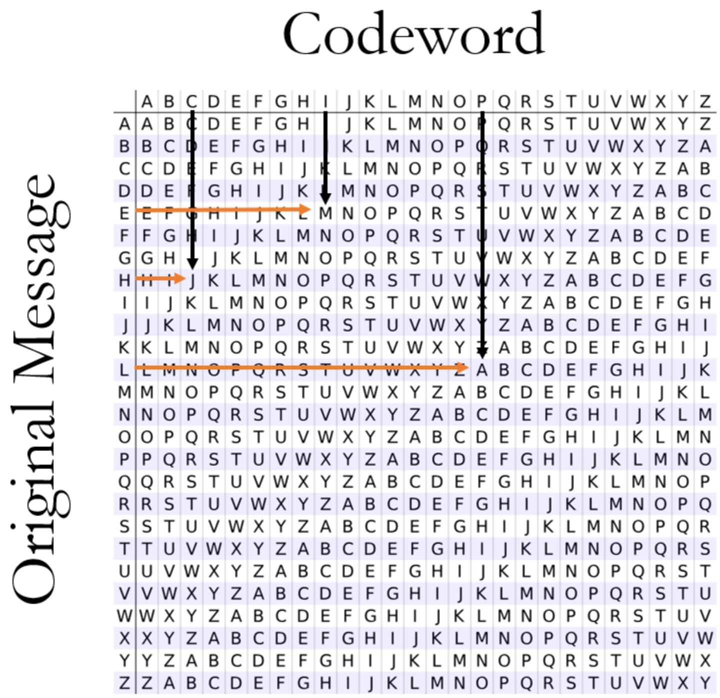
The Vigenére Cipher

The Vigenére Cipher operates on the same shifting principle as the Caesar, but now we will add use a codeword to specify the shift value[3]. The first step to encoding a message is to line up the original message below the repeated codeword. For this example the codeword is 'Cipher' and the original message is 'Hello World'.



Codeword:	C	I	P	H	E	R	C	I	P	H
Original message:	H	E	L	L	O	W	O	R	L	D

The next step in the Vigenére Cipher is to shift each of the original letters by the value of the corresponding codeword letter. If we call A the zeroth letter, B the first, and C the second, then we would shift H over two letters to J. This shift can be more easily completed using a table.


Codeword
Original Message

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

Here I have shown the shift of the first three letters of the original message: ‘H’, ‘E’, and ‘L’, by the first three letters of the codeword ‘C’, ‘I’, and ‘P’. The complete encrypted message is ‘JMASSNQZAK’.

Let m = Original message

Let $m_i = i^{th}$ letter of original message

Let c = Codeword

Let $c_i = i^{th}$ letter of codeword

Let e = Encrypted message

Let $e_i = i^{th}$ letter of encrypted message

Using these variables we can represent any Vigenére shift as:

$$e_i = m_i + c_i$$

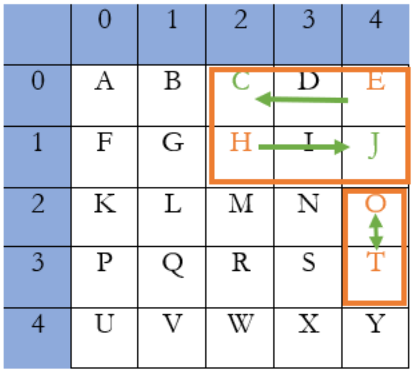
$$m_i = e_i - c_i$$

This shows that any encrypted letter can be found by adding the corresponding codeword value to the original letter. Any original letter can be found by subtracting the corresponding codeword value from the encrypted letter.

The Vigenére cipher is much stronger than the Caesar. Because the shift is dependent on the codeword, there are theoretically infinite ways to encrypt using this cipher. But realistically, this cipher is easily crackable from guessing words from the dictionary. It is also possible to crack this code by examining the letter frequency. I would not use the Vigenére cipher to keep my sensitive information secure.

The Playfair Cipher

The first step in the Playfair cipher is to draw a 5 x 5 grid with an alphabet letter in each space. You can arrange the letters in any way you like, so long as you communicate the arrangement with the intended recipient. For our example, the letters are arranged alphabetically. Because there are 26 letters, and only 25 spaces, we will have to omit a letter from the grid. We will omit the letter Z. This means that any letter Z in the original text will also be a letter Z in the cipher text. The next step is to separate the original message into pairs of letters. If “Hello There World” is our original message, we would separate it as follows: HE LL OT HE RE WO RL D. Then we find the first pair of letters on the grid.



	0	1	2	3	4
0	A	B	C	D	E
1	F	G	H	I	J
2	K	L	M	N	O
3	P	Q	R	S	T
4	U	V	W	X	Y

The letters from the original pair become the corners of a rectangle on the grid. H becomes one corner, and E becomes another. The encrypted letters can be found by moving horizontally from the original letters to the opposite corners of the rectangle[2]. So, for the original pair HE, the encrypted pair is JC.

The next pair of letters is LL, which presents a problem: What do we do when the pair of letters are the same letter? We will leave the original pair LL as LL in the ciphertext.

The next pair of letters is OT, which presents yet another dilemma: What do we do when the two letters are in the same column? We will still imagine a rectangle constructed from the two letters, but since we only have two corners to use, we will simply trade O and T. Thus, the original pair OT becomes the encrypted pair TO. We would do the same if the letters were in the same row. For example, the original pair KM would become the encoded pair MK.

Alas, our message has an odd number of letters. The last letter does not have a second letter to make a pair. We will add the letter X to the end of our message to create a final pair. So the last original pair DX becomes the encrypted pair XD.

The entire original message "Hello there world" would become: JCLLTOCJTCYMQMXD.

Let m = Original message

Let $m_i = i^{th}$ letter of original message

Let m_{ix} = The x value of the i^{th} letter of the original message

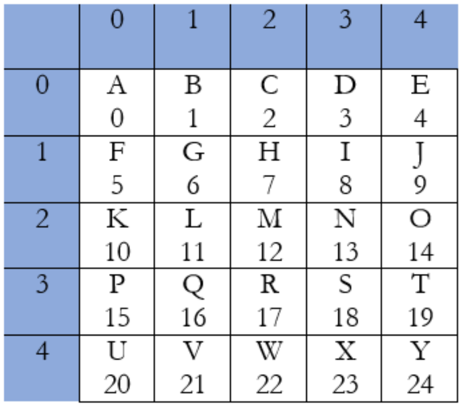
Let m_{iy} = The y value of the i^{th} letter of the original message

Let e = Encrypted message

Let $e_i = i^{th}$ letter of encrypted message

Let e_{ix} = The x value of the i^{th} letter of encrypted message

Let e_{iy} = The y value of the i^{th} letter of encrypted message



	0	1	2	3	4
0	A 0	B 1	C 2	D 3	E 4
1	F 5	G 6	H 7	I 8	J 9
2	K 10	L 11	M 12	N 13	O 14
3	P 15	Q 16	R 17	S 18	T 19
4	U 20	V 21	W 22	X 23	Y 24

In order to determine any encrypted letter from the original letter, we will need to assign each letter a number value. A = 0, B = 1, C = 2... Each letter will also need to receive coordinates based on the location on the grid. The axes are labeled with numbers as shown above. A = (0,0), B = (1,0), F = (0,1) ... Determining any encrypted letter from the original letter will involve 3 steps:

1. First we need to get from the original letter's assigned value to its assigned coordinate:
$$m_i \rightarrow (m_{ix}, m_{iy})$$
2. Then we need to get from the original letter's coordinates to the encrypted letter's coordinates:
$$(m_{ix}, m_{iy}) \rightarrow (e_{ix}, e_{iy})$$
3. Lastly, we need to get from the encrypted letter's coordinates, to its number value:
$$(e_{ix}, e_{iy}) \rightarrow e_i$$

Step one: Getting a number value from coordinates is simple. The number value is equal to five times the y value plus the x value. This is true because moving vertically in the grid will change the number value by five, and moving horizontally changes the number value by one. But we need to find the coordinate given the number value, so we need to perform the inverse of that operation. The Y value is equal to the number of the row the letter is in, or the number of 5s that can be fit into the number value. For example the y value of letter 17 would be 3, because you can fit 3 5s in 17 before you run out of room. We can represent this function mathematically by using the floor ($\lfloor x \rfloor$) function. The floor function finds the next lowest whole number of a decimal. The floor of 3.5 is 3, the floor of 63.279 is 63.

$m_{iy} = \lfloor \frac{m_i}{5} \rfloor$ The y value for any point is equal to the floor of the number value divided by 5. If we tried to find the y value for number 14, we would find that $\lfloor \frac{14}{5} \rfloor = \lfloor 2.8 \rfloor = 2$. If we look on the grid, we will find that the y value for number 14 is in fact 2.

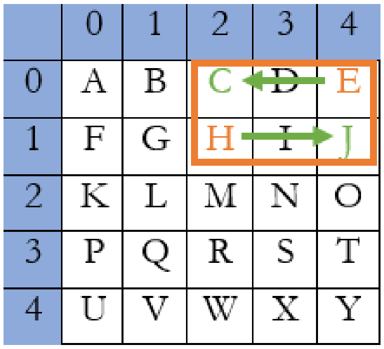
Now we need to determine the x value. Earlier we concluded that $m_i = m_{ix} + 5m_{iy}$, therefore, $m_{ix} = m_i - 5m_{iy}$. Using substitution we can conclude that $m_{ix} = m_i - 5\lfloor \frac{m_i}{5} \rfloor$

Step two: We now need to mathematically describe the shift that happens when we trade letters on the grid.

$m =$ HE LL OT HE RE WO RL DX

$m_0 = H$

$m_1 = E$



	0	1	2	3	4
0	A	B	C	D	E
1	F	G	H	I	J
2	K	L	M	N	O
3	P	Q	R	S	T
4	U	V	W	X	Y

Looking at the transformation on the grid, we can see that the encrypted letter H (J), has the same y value as the original H, but the x value of the original letter E. Similarly, the encrypted letter E (C), has the same y value as the original E, but the x value of the original letter H. Encrypted letters keep the y value of the original letter, but trade x values with the other letter in their pair.

We can describe the encryption of the letter H as $(H_x, H_y) \rightarrow ((H+1)_x, H_y)$. Notice that the $H+1$ refers not to the next letter in the **alphabet** after H, but the next letter in the **message**.

We can describe the encryption of the letter E as $(E_x, E_y) \rightarrow ((E-1)_x, E_y)$. Again, the E-1 refers to the previous letter in the message, not the alphabet. The x value for an encrypted letter is equal to the x value of the original letter's pair. Letter H's pair was 1 step ahead in the message, while letter E's pair was 1 step behind in the message. This is why the encryption process for letter E is slightly different than the encryption process for letter H. Because of this, we will need to split our encryption formula between odd and even letters. Letters 0, 2, and 4 will have one formula, and letters 1, 3, and 5 will have another.

If $i \in$ even, $e_{ix} = m_{(i+1)x}$ $e_{iy} = m_{iy}$

If $i \in$ odd, $e_{ix} = m_{(i-1)x}$ $e_{iy} = m_{iy}$

Step 3: Finally, we need to get from the coordinate of our encrypted point, to its number value. This is the inverse of step 1. The encrypted letter's number value is equal to five times its y value plus its x value.

$$e_i = e_{ix} + 5e_{iy}$$

Now using substitution, we can combine these 3 steps into one rule.

If $i \in$ even,

$$e_i = 5\lfloor \frac{m_i}{5} \rfloor + m_{(i+1)} - 5\lfloor \frac{m_{(i+1)}}{5} \rfloor$$

If $i \in$ odd,

$$e_i = 5\lfloor \frac{m_i}{5} \rfloor + m_{(i-1)} - 5\lfloor \frac{m_{(i-1)}}{5} \rfloor$$

The Playfair Cipher is definitely the strongest cipher of the ciphers we have examined so far. Because we can arrange the alphabet in any way we want we have about 10^{26} possible encryptions. This is significantly more than either the Caesar or the Vigénere, but it is still susceptible to a brute force attack from modern computers. I would not use the Playfair Cipher to keep my sensitive information secure.

RSA Encryption

The previous ciphers we have examined have all used the same key to encrypt and decrypt the message. Because of this, those ciphers can be called symmetric. But RSA on the other hand, uses two separate keys for encryption and decryption. The sender encrypts the message using e, while the receiver decrypts the message using d. So RSA is asymmetric.

The first step in RSA encryption is to generate 3 numbers e, d, and N, such that $ed \equiv 1 \pmod{N}$. e is kept secret so that only the receiver knows it's value, while d and N are made public.

Next, the message sender will encrypt their message by raising it to e. If we represent the ciphertext with variable C, and the original message with variable M then we can say that $C = M^e$. The sender now sends the encrypted message, C, to the receiver. The receiver can decrypt the ciphertext by following the formula $C^d \equiv M \pmod{N}$[1].

This math holds true because of Fermat's Little Theorem, equation 1.

$$a^p \equiv a \pmod{p} \tag{1}$$

During my research I learned about modular arithmetic. I learned how to read mod notation as well as understand how Fermat's Little Theorem allows for RSA encryption to work.

The need for private, secure information has existed for centuries, but in the information age, it is more important than ever. As financial institutions move their information onto the web, encryption is the only thing stopping hackers from having access to your money. In addition, hackers could track your location from your phone if not for modern encryption technology. For this reason it is important to understand what makes a strong cipher. It makes much more sense to secure information using RSA encryption than the easily crackable Caesar Cipher.

References

[1] Margaret Cozzens and Steven J. Miller. *The Mathematics of Encryption: An Elementary Introduction.* American Mathematical Soc., 2013. ISBN: 0821883216, 9780821883211.

[2] Helen Fouché Gaines. *Cryptanalysis: a study of ciphers and their solutions.* Dover, 1956 (1939). ISBN: 9780486800592.

[3] Simon Singh. *The Code Book.* Doubleday, 1999. ISBN: 9788388087455.