The History of Substitution Ciphers

Kailey N. Cozart

School of Interdisciplinary Arts & Sciences

TMATH 420: History of Mathematics

Dr. Erik Tou

June 8, 2020

The History of Substitution Ciphers

For centuries, substitution ciphers have protected national and personal secrets alike, and they continue to be used today. Substitution ciphers encrypt text by replacing each letter with a different symbol based on some kind of key (Shimeall & Spring, 2014, p.160). The monoalphabetic Caesar cipher, polyalphabetic Vigenère cipher, and polygraphic Playfair cipher are three inventions crucial to the development of the substitution cipher.

One of the most well-known substitution ciphers is the monoalphabetic Caesar cipher, which was used in Julius Caesar's (100-44 BC) personal communications. Julius Caesar would utilize an encryption function such as $f(p) = (p + 3)\ mod\ 26$, which would shift each letter of the alphabet by three places (Manasrah & Al-Din, 2016, p. 1450). If one wanted to use the equation above to encrypt the word "ZIP," one would first note that A is the 0th letter in the alphabet and Z is the 25th letter in the alphabet. Therefore, Z = 25, I = 8, and P = 15. Then, the values for ZIP would be plugged into the encryption function as follows:

$f(25) = (25 + 3)\ mod\ 26 = 2 \rightarrow C$

$f(8) = (8 + 3)\ mod\ 26 = 11 \rightarrow L$

$f(15) = (15 + 3)\ mod\ 26 = 18 \rightarrow S$.

Thus, the encrypted value is "CLS." If someone wanted to decrypt the value, they would convert the known encryption function into a decryption function. Since the encryption function is $f(p) = (p + 3)\ mod\ 26$, it is easy to see that the decryption function is $p = f(p) - 3\ (mod\ 26)$. Plugging in C = 2, L = 11, and S = 18 into the decryption function yields the following:

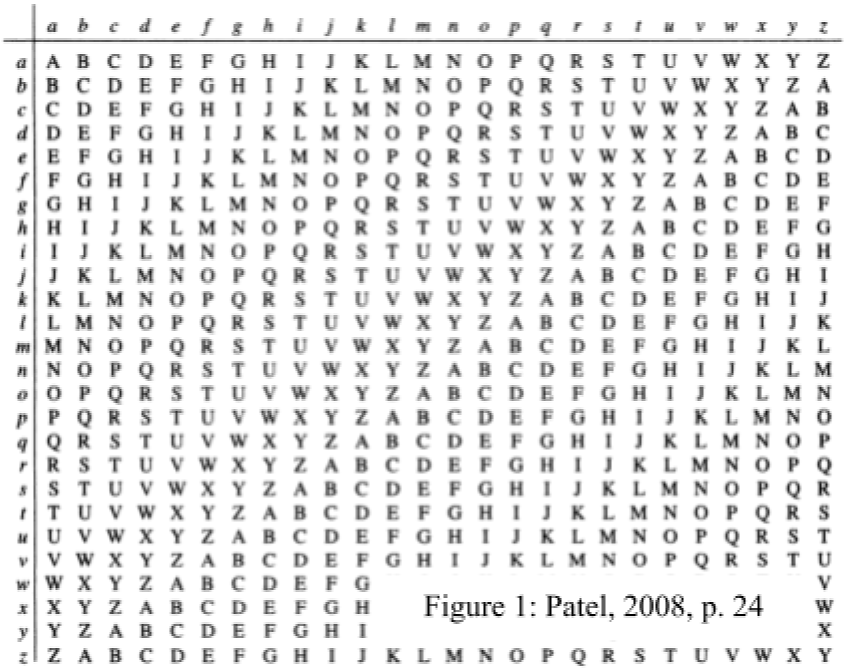
$p = 2 - 3\ (mod\ 26) =- 1(mod\ 26) = 25$

$p = 11 - 3\ (mod\ 26) = 8$

$p = 18 - 3\ (mod\ 26) = 15$.

Since Z = 25, I = 8, and P = 15, the expected decrypted value of “ZIP” is discovered. The simple Caesar cipher, as one might expect, has its downfalls. Without a key, monoalphabetic ciphers can be consistently broken by looking at how frequently letters appear (Shimeall & Spring, 2014, p.160). Additionally, one letter words, like “I” and “a,” as well as words with double letters, can be used to find the decrypted values of each letter (Churchhouse, 2001, p. 18). Therefore, while the standard Caesar cipher worked well in the first century BC, it lost its usefulness as mathematical code breaking techniques were developed. Regardless, the Caesar cipher was important to the development of substitution ciphers because it was one of the first monoalphabetic ciphers.

As monoalphabetic ciphers became easy to crack, polyalphabetic ciphers took their place. What is now known as the Vigenère cipher was named after Blaise de Vigenère (1523-1596). However, the Italian cryptographer Giovan Battista Bellaso (b.1505) was the first to describe it (Holden, 2017, p. 43). The Vigenère cipher took the monoalphabetic Caesar cipher and improved upon it by using multiple substitution alphabets instead of just one (Churchhouse, 2001, p. 30). In order to encrypt a message, the Vigenère cipher



	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															V
x	X	Y	Z	A	B	C	D	E	F	G	H															W
y	Y	Z	A	B	C	D	E	F	G	H	I															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

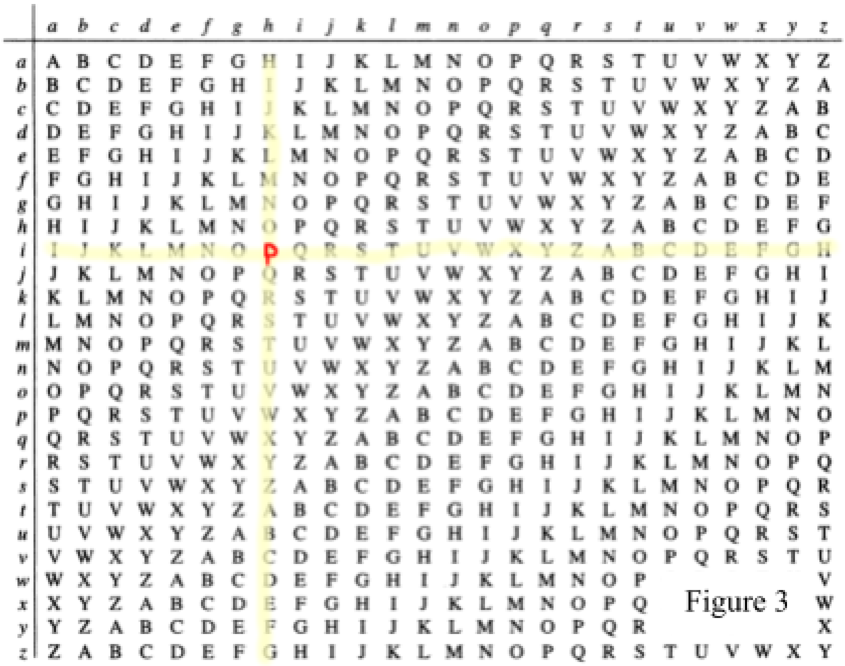
Figure 1: Patel, 2008, p. 24

uses a tabula recta like the one pictured in Figure 1 (Patel, 2008, p. 24). The current keystream letter is found across the top and the current letter of the decrypted value is found on the left side of the table (Holden, 2017, p. 41). For example, if the keyword was “hello” and the message was “I love math,” the table in Figure 2 could be created.

H	E	L	L	O	H	E	L	L
I	L	O	V	E	M	A	T	H
P	P	Z	G	S	T	E	E	S

Figure 2

The top row is the keystream, or the letter that will be selected on the top of the tabula recta. The second row is the unencrypted message, or the letter that will be selected on the left of the tabula recta. The last row contains the encrypted values. To encrypt the first letter, the letter ‘H’ is found at the top of the table and the letter ‘I’ is found on the left of the table. The intersection of the two lines is the letter ‘P’, so ‘P’ is the encrypted value. See Figure 3 for a visualization of the encryption process. This process is repeated for every letter that needs to be encoded.



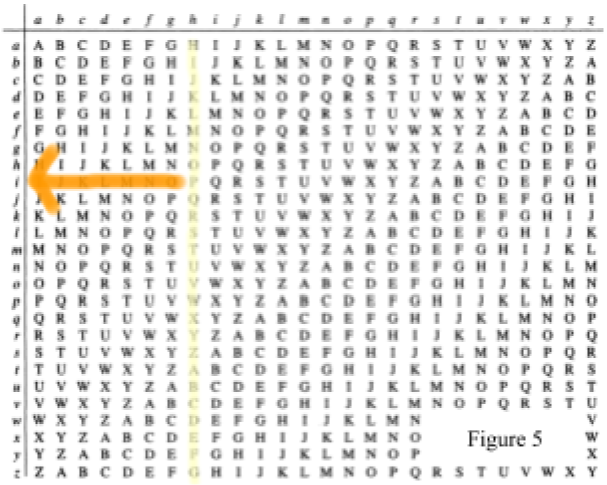
	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	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						V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q						W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R						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

Figure 3

H	E	L	L	O	H	E	L	L
P	P	Z	G	S	T	E	E	S
I	L	O	V	E	M	A	T	H

Figure 4

To decrypt the message, a similar process is utilized. A table like Figure 4 can be used. Once again, the top row is the keystream, or the letter that will be selected on the top of the tabula recta. This time, the encrypted letter is found in the column, and the row that it is in represents the unencrypted value. For example, taking the first ‘H’ in Figure 4 and highlighting the column that contains the letter H, one looks for the letter ‘P’ in the highlighted column. Once it is found, one sees what row the letter ‘P’ is in. In this example, the letter ‘P’ is in row ‘I,’ so the decrypted value is ‘I.’ See Figure 5 for a visualization of the decryption process. The Vigenère cipher, seen as unbreakable for centuries, was important to the development of substitution ciphers because it was one of the first widely used polyalphabetic ciphers.



	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								V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O								W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P								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

Figure 5

Despite its complexity, the Vigenère cipher was eventually cracked by Chales Babbage, and the method of solving the cipher was publicly published by Friedrich Kasiski in 1863 (Franksen, 1993, p. 356). However, by then, cryptographers had discovered that, if more than one letter was used in each encryption process, the encryption would be harder to break. Thus, polygraphic ciphers were born. The Playfair cipher, invented in 1854 by Charles Wheatstone, was the first polygraphic substitution cipher (Reynard, 1997, p. 31). The cipher, and variations of it, was used during WWI by German High Command (Churchhouse, 2001, p. 57). Later on, it was the primary cipher of the British Special Operations Executive from 1940 to 1942 (Reynard, 1997, p. 30). Additionally, the Japanese Merchant Navy also used this kind of polygraphic cipher during WWII (Churchhouse, 2001, p. 58). The Playfair cipher worked as follows. Suppose that the keyword is “keyword.” Because a 5x5 grid is used, one must remove a letter from the alphabet. Traditionally, the letter J is removed. Then, the 5x5 grid is filled with the keyword followed by the letters of the alphabet, excluding J, that are not in the keyword. This results in the following grid.

k	e	y	w	o
r	d	a	b	c
f	g	h	i	l
m	n	p	q	s
t	u	v	x	z

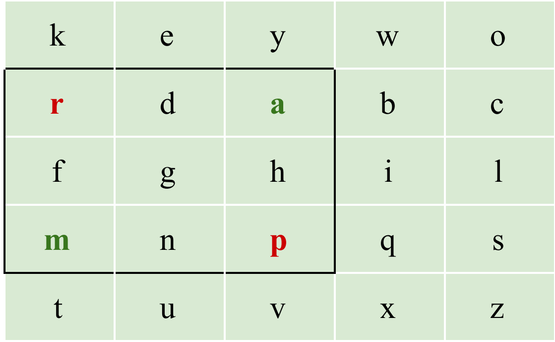
Figure 6

Now, the letters of the message are split into pairs, with duplicated letters separated by the letter X. Additionally, if there is an odd letter at the end of the message, the letter X is inserted into the missing space. If the message was “math history,” the letters would be prepared for encryption as follows:

MA TH HI ST OR YX.

Next, each pair of letters is inserted into its own table. There are three cases. If the pair of letters are in the same column, each letter is moved down. If the pair of letters are in the same row, each letter is moved to the right. If the pair of letters are not in the same column or row, they are swapped with the letters in the opposite corner of the square formed by the two letters. In this example, the first pair of letters is MA. M and A are not in the same column or row. Thus, a box is drawn around the two letters and the letters are swapped with the letters in the opposite corner.

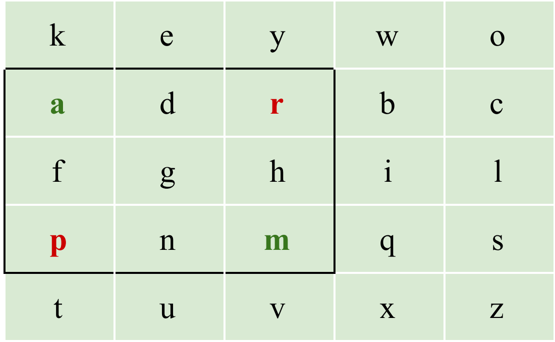
Make a square with M and A.



k	e	y	w	o
r	d	**a**	b	c
f	g	h	i	l
m	n	**p**	q	s
t	u	v	x	z

Figure 7

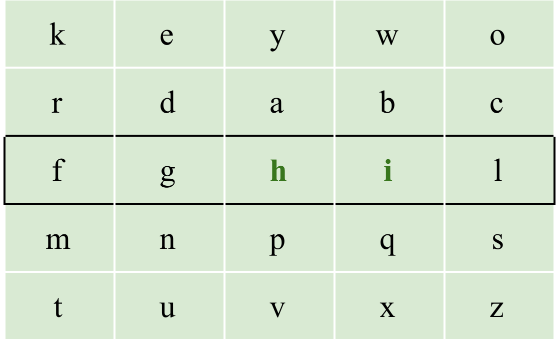
Swap each letter with the opposite corner.



k	e	y	w	o
a	d	**r**	b	c
f	g	h	i	l
p	n	**m**	q	s
t	u	v	x	z

Figure 8

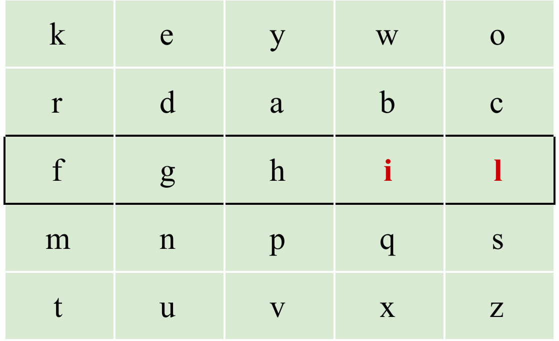
Find the similar row (or column).



k	e	y	w	o
r	d	a	b	c
f	g	**h**	**i**	l
m	n	p	q	s
t	u	v	x	z

Figure 9

Shift to the right (or down).



k	e	y	w	o
r	d	a	b	c
f	g	h	**i**	**l**
m	n	p	q	s
t	u	v	x	z

Figure 10

Therefore, MA is encoded as PR. In the same way, TH is encoded to VF, ST is encoded to MZ, OR is encoded to KC, and YX is encoded to WV. The letters HI are in the same row, so they are shifted to the right and encoded as IL. Therefore, the encoded message “math history” is now “prvfilmzkcwv.” To decrypt, one simply does the opposite of what was done to encrypt the message. The encrypted message is split up as follows:

PR VF IL MZ KC WV.

If the recipient of the message knows that the keyword is “keyword,” it is easy for the decrypter to generate the same grid as the encrypter. To decode, if the pair of letters are in the same column, each letter is moved up. If the pair of letters are in the same row, each letter is moved to the left. If the pair of letters are not in the same column or row, they are swapped with the letters in the opposite corner. Using these rules, the decrypter gets the original message: “mathhistoryx.” They would understand that the random X’s were part of the encryption process and remove them (Churchhouse, 2001, p. 30). While the Playfield cipher eventually lost its value when it was cracked by codebreakers, it was important to the development of the substitution cipher because it was the first polygraphic cipher.

In conclusion, the simple, monoalphabetic Caesar cipher from ancient Rome was used as an inspiration for the more complicated polyalphabetic Vigenère cipher of the 1500's and the polygraphic Playfair cipher in the 1800’s. Since then, substitution ciphers have continued to increase in complexity. For example, the Enigma machine, a mechanical polyalphabetic cipher, would take components from previous ciphers to create well-encrypted messages during World War II (Churchhouse, 2001, p. 112). Furthermore, block ciphers, which are similar to polygraphic ciphers, protect modern online data from prying eyes (Shimeall & Spring, 2014, p. 168). The Caesar, Vigenère, and Playfair ciphers may only be an odd curiosity today, but their existence has been crucial to the development of monoalphabetic, polyalphabetic, and polygraphic substitution ciphers.

Bibliography

Churchhouse, R. (2001). *Codes and ciphers: Julius Caesar, the Enigma, and the internet.* Cambridge University Press. Retrieved from https://ebookcentral-proquest-com.offcampus.lib.washington.edu/lib/washington/detail.action?docID=202096

Franksen, O. (1993). Babbage and cryptography. *Mathematics and Computers in Simulation, 35*(4), 327-367. Retrieved from https://www.sciencedirect.com/science/article/pii/037847549390063Z

Holden, J. (2017). *The mathematics of secrets: cryptography from Caesar ciphers to digital encryption.* Princeton University Press. Retrieved from https://ebookcentral-proquest-com.offcampus.lib.washington.edu/lib/washington/reader.action?docID=4797326&query=

Manasrah, A., & Al-Din, B. (2016). Mapping private keys into one public key using binary matrices and masonic cipher: Caesar cipher as a case study. *Security and communication networks, 9*(11), 1450-1461. Retrieved from https://onlinelibrary-wiley-com.offcampus.lib.washington.edu/doi/full/10.1002/sec.1431

Patel, D. (2008). *Information security theory and practice.* PHI Learning. Retrieved from https://www.google.com/books/edition/INFORMATION_SECURITY/FFPzGN8Uk9cC?hl=en&gbpv=0

Reynard, R. (1997). *Secret code breaker II: A cryptanalyst's handbook.* Smith & Daniel.

Retrieved from https://www.google.com/books/edition/Secret_Code_Breaker_II/3nTmBW0ONEEC?hl=en&gbpv=0

Shimeall, T., & Spring, J. (2014). *Introduction to information security: A strategic-based approach.* Elsevier. Retrieved from www.sciencedirect.com/book/9781597499699/introduction-to-information-security