Cipher Series Workbook

In my upcoming novel, *The Cause of These Disturbances,* the protagonist faces a complex cipher hidden in graffiti around his university's campus. In his honour I have created twelve different messages encrypted in historical ciphers for you to solve. Each one reveals a passage from Chapter One of the novel.

Every month a new secret message will be posted on my website. This exclusive workbook gives you a sneak peek into the ciphers that will be used, as well as instructions and space to record your answer.

If you email the correct solution to margaret@mebondbooks.com before the last Wednesday of each month, you'll be entered into a draw for a chance to win the grand prize at the end of the series (August 2016).

Look for the solutions in the email newsletter at the end of each month.

Thank you for joining me. Happy deciphering!

www.mebondbooks.com

WHERE SECRETS OF
THE *past* MEET STORIES
OF THE *present*

September 2015 – The Atbash Cipher

This is one of the earliest substitution ciphers, first used on the Hebrew alphabet. The cipher is solved by simply reversing the alphabet, so A=Z, B=Y, C=X, etc.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

October 2015 – The Rail Fence Cipher

This is a simple transposition cipher, in which the letters are written in a certain pattern. The only thing you need to know to decipher the message is the key number. With a key of 3 the phrase "watch your back" would be enciphered thus:

W				H				R				K
	A		C		Y		U		B		C	
		T				O				A		

WHRKACYUBCTOA

Of course a different key number could be used, resulting in a "fence" with a different number of "rails."

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

November 2015 – The Polybius Square

A Polybius square is a five-by-five grid used to encipher messages. To make it more secure a key word is used to begin the square before the rest of the alphabet is filled in. Each letter of the plain text is enciphered with two digits, the one to the left of the corresponding row and then the one at the top of the corresponding column. Using this square the word "November" becomes 42-15-53-12-41-24-12-21.

	1	2	3	4	5
1	K	E	Y	W	O
2	R	D	A	B	C
3	F	G	H	I/J	L
4	M	N	P	Q	S
5	T	U	V	X	Z

Before you can solve this month's cipher you have to figure out the keyword. (Hint: It's on this page.)

_____

_____

_____

_____

_____

_____

_____

_____

_____

December 2015 – The Caesar Shift

 This is one of the earliest and simplest ciphers, used by Julius Caesar to send messages to Rome while he was campaigning in other parts of Europe. The message is encrypted by shifting each letter a certain number of places down the alphabet. For example, here is a shift of three:

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
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

"Hello" becomes EBIIL.

How many letters do you have to shift to solve this month's cipher?

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

January 2016 – The Vigenère Square

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

To solve this type of cipher you need to know the keyword, which you repeat (creating a "key stream") alongside the cipher text. For example:

key stream	W	I	N	T	E	R	W	I	N	T	E	R	W	I	N	T	E	R	W	I	N	T	E	R	W	I
cipher text	D	B	F	B	W	Z	W	V	J	W	E	F	H	X	J	F	Z	Y	P	E	L	L	P	K	S	R
plain text	T	H	I	S	I	S	A	N	E	X	A	M	P	L	E	O	F	T	H	E	C	I	P	H	E	R

To decipher the cipher text, you find the first letter of the key stream in the row at the top of the Vigenère table, follow the column down until you find the first letter of the cipher text, then follow the row to the leftmost column and you have the first letter of the plain text. Repeat until finished!
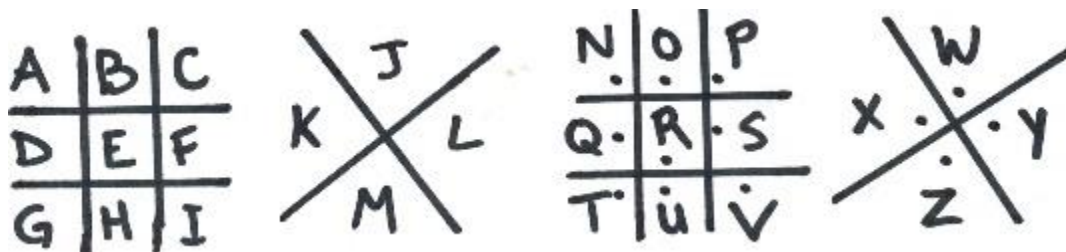(Hint: The keyword is related to "winter.")

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

February 2016 – Bacon's Bilateral Alphabet

A = aaaaa	G = aabba	N = abbaa	T = baaba
B = aaaab	H = aabbb	O = abbab	U/V = baabb
C = aaaba	I/J = abaaa	P = abbba	W = babaa
D = aaabb	K = abaab	Q = abbbb	X = babab
E = aabaa	L = ababa	R = baaaa	Y = babba
F = aabab	M = ababb	S = baaab	Z = babbb

Invented by Francis Bacon, this cipher is based on a binary five-bit alphabet. The real message is hidden in a fake message, with the a's and b's represented by two different typefaces, or lowercase and uppercase letters. For example "whAT Do yOu neEd Now DEAr" can be converted to aabbb aabaa ababa abbba, which spells "Help."

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

March 2016 – The Pigpen Cipher

Also known as the Masonic cipher, this cipher has been around since the eighteenth century. It's relatively easy to use, memorize, and adapt. Each letter in the plain text is simply replaced by the part of the image housing the letter.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

April 2016 – The Templar Cipher

This variation of the Masonic cipher is based on the Maltese cross.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

May 2016 – Semaphore

Semaphore is a system for conveying messages at a distance using two flags.
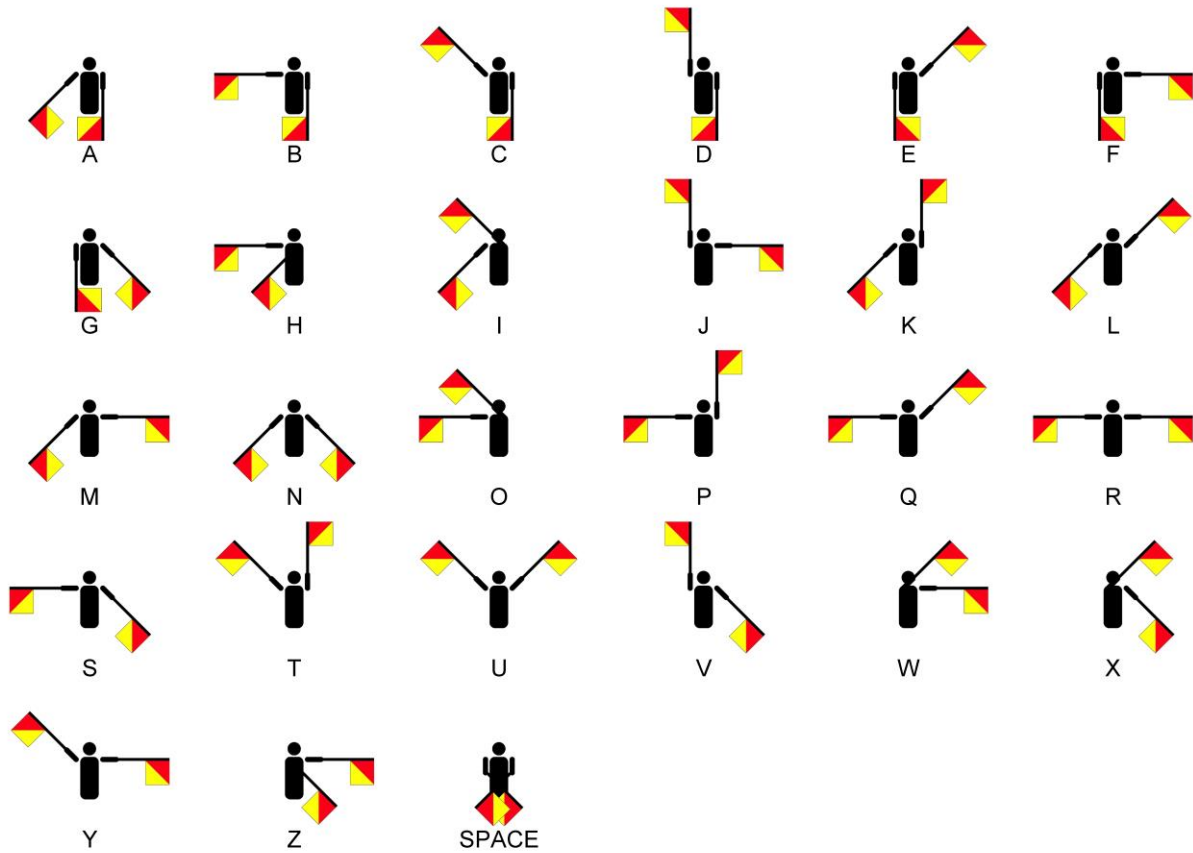
By Denelson83 [CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons

_____

_____

_____

_____

_____

_____

_____

_____

June 2016 – Morse Code

Designed for telegraph, Morse Code can be used by other systems like flashlamps and foghorns. (Of course, here it is simply written out.)

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

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

July 2016 – Columnar Transposition Cipher

In this type of cipher the message is encrypted by writing the letters across a grid and then reading down each column to scramble them. However, the cipher is complicated by using a keyword and then reading the corresponding columns in alphabetical order. When you know that the key word is "month" you can decrypt EEACIXISRUHSOMEEOULUBSOOV MCSLT to come up with the plain text, "I love summer because school is out."

M	O	N	T	H
I	L	O	V	E
S	U	M	M	E
R	B	E	C	A
U	S	E	S	C
H	O	O	L	I
S	O	U	T	X

H	M	N	O	T
E	I	O	L	V
E	S	M	U	M
A	R	E	B	C
C	U	E	S	S
I	H	O	O	L
X	S	U	O	T

Hint: This month's cipher is solved with four columns.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

August 2016 – The Bifid Cipher

There are three steps to encrypting a message with the bifid cipher. First you find each letter in the square and write down the corresponding numbers.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

	S	A	D	L	Y	T	H	I	S	I	S	T	H	E	L	A	S	T	C	I	P	H	E	R
row	4	1	1	3	5	4	2	2	4	2	4	4	2	1	3	1	4	4	1	2	3	2	1	4
column	3	1	4	1	4	4	3	4	3	4	3	4	3	5	1	1	3	4	3	4	5	3	5	2

The numbers are then divided into segments of a certain size (the period). Using a period of five you come up with:

41135   42242   44213   14412   3214

31414   43434   34351   13434   5352

Next you arrange the groups like this, each section in the top row followed by the section below it:

4113431414   4224243434   4421334351   1441213434   32145352

Then you re-encipher the numbers using the original key square to get the final cipher text: QCSDDRIIOOTFNSVDQGO OMDXW.

To decipher a bifid cipher text you must repeat each step in reverse order. As long as you know the period, the keyword, and the key square, you shouldn't have any trouble!

Hint: I've used the same key square and period as above, but you'll have to figure out the keyword!

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Suggested Reading

Crypto Corner http://crypto.interactive-maths.com/

Practical Cryptography http://practicalcryptography.com/

Wonders & Marvels Cryptography Series
http://www.wondersandmarvels.com/category/cryptography-vanderbilt

Secret Language: Codes, Tricks, Spies, Thieves, and Symbols by Barry J. Blake (Oxford University Press, 2010)

The Book of Codes: Understanding the World of Hidden Messages edited by Paul Lunde (University of California Press, 2009)

Codebreaker: The History of Codes and Ciphers, From the Ancient Pharaohs to Quantum Cryptography by Stephen Pincock (Walker Publishing Company, 2006)