

Code Busters Answer Key

2018 – 2019

Division C

1. Fast is fine, but accuracy is everything.
2. WCHM IF DBQZT, FNCGVCR TM NWNT.
3. Science is organized knowledge.
4. Science literacy is the artery through which the solutions of tomorrow's problems flow.
5. My life is my message.
6. You live in intimate association with bacteria, and you couldn't survive without them.
7. OGMAAPG MKZFWMWY H
8. Statistics is the grammar of science.
9. Persistence is half the battle.
10. 751
11. Feeling tired should almost never be an excuse, because your body has huge reserves of energy.
12.
$$\begin{bmatrix} 24 & 23 & 13 \\ 9 & 16 & 18 \\ 4 & 17 & 0 \end{bmatrix} = \begin{bmatrix} Y & X & N \\ J & Q & S \\ E & R & A \end{bmatrix}.$$
13. But no, I dont genrely half trubble with spelng misteaks.
14. Nada hay más surreal que la realidad.
Note: Full credit should still be given if the a in más does not have the accent.
15. Nobody remembers who finished second but the guy who finished second.
16. The greater the obstacle, the more glory in overcoming it.
Note: Do not deduct any points if there is an additional z at the end of the quote.

Solutions

1. We can first identify the word **IQITENYVHJ** to be the word **EVERYTHING**. After this, we can figure out that **VP** corresponds to the word **IS**, and that **SWN** corresponds to the word **BUT**. From there, it is not difficult to deduce the rest of the quote:

Fast is fine, but accuracy is everything.

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

2. Converting the quote to numbers, we have our plaintext written as numbers:

11, 8, 5, 4/8, 18/18, 7, 14, 17, 19/18, 2, 8, 4, 13, 2, 4/8, 18/11, 14, 13, 6.

After adding our key **LUCIAN** = 11, 20, 2, 8, 0, 13, we have our ciphertext written as numbers:

22, 2, 7, 12/8, 5/3, 1, 16, 25, 19/5, 13, 2, 6, 21, 2, 17/, 19, 12/13, 22, 13, 19.

Converting this into ciphertext letters, it becomes

WCHM IF DBQZT, FNCGVCR TM NWNT.

3. Converting the quote to numbers, we have our ciphertext written as numbers:

23, 16, 2, 21, 5, 4, 18/25, 22/14, 4, 9, 18, 17, 3, 3, 17, 1/14, 13, 5, 14, 11, 10, 17, 20, 24.

After subtracting our running key **FOUR SCORE AND SEVEN YEARS AGO OU** =

5, 14, 20, 17, 18, 2, 14/17, 4/0, 13, 3, 18, 3, 21, 4, 13, 24/4, 0, 17, 18, 0, 6, 14, 14, 20,

we have our plaintext written as numbers:

18, 2, 1, 4, 13, 2, 4/8, 18/14, 17, 6, 0, 13, 8, 25, 4, 3/10, 13, 14, 22, 11, 4, 3, 6, 4.

Converting this into plaintext letters, it becomes

Science is organized knowledge.

4. We see that the ciphertext **A** in **BWUWZZWE'A** must be the plaintext letter **S**. Since we know it is a Caesar cipher, we can easily find the rest of the key to decrypt the ciphertext. This yields the quote Science literacy is the artery through which the solutions of tomorrow's problems flow.

5. Note: we are using a' and b' to denote constants to convert from ciphertext to plaintext. Normally, we use a and b to denote constants to convert from plaintext to ciphertext, but solving for them first is generally slower for decryption.

Using the information of the first two letters, we have the following two congruences (mod 26):

$$3a' + b' \equiv 12$$

$$21a' + b' \equiv 24$$

Solving for these equations, gives us that $a' = 5$ and $b' = 23 \equiv -3$. Note that a' cannot be 18 as it must be relatively prime to 26.

If we were asked to calculate a and b (which we are not), we would get that $a = 21$ and $b = 11$.

Using this, we can then use this key to decrypt the ciphertext (left side) into plaintext (right side).

$$\begin{aligned}
 I = 8 &\rightarrow 8 \times 5 - 3 = 37 \equiv 11 = L \\
 X = 23 &\rightarrow 23 \times 5 - 3 = 112 \equiv 8 = I \\
 M = 12 &\rightarrow 12 \times 5 - 3 = 57 \equiv 5 = F \\
 R = 17 &\rightarrow 17 \times 5 - 3 = 82 \equiv 4 = E \\
 Z = 25 &\equiv -1 \rightarrow -1 \times 5 - 3 = -8 \equiv 18 = S \\
 L = 11 &\rightarrow 11 \times 5 - 3 = 52 \equiv 0 = A \\
 H = 7 &\rightarrow 7 \times 5 - 3 = 32 \equiv 6 = G
 \end{aligned}$$

Using these to decrypt, our plaintext is

My life is my message.

6. We can likely assume that the last six ciphertext letters of the word **WDFNUS'G** correspond to the plaintext letters **OULDN'T**. After this, we can then identify several plaintext words such as **WITHOUT**, **AND**, and **YOU**. From there, it is not difficult to deduce the rest of the quote:

You live in intimate association with bacteria, and you couldn't survive without them.

Ciphertext Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency	3		6	6		5	9	3			3	2	
Plaintext Letter	H		A	O		U	T	S			V	W	
Ciphertext Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	2		1	5	10	5		2	2	3	2	2	
Plaintext Letter	L		B	E	I	N		D	Y	C	M	R	

7. Converting the quote to numbers, we have our plaintext written as numbers:

18, 2, 8, 4, 13, 2, 4/14, 11, 24, 12, 15, 8, 0, 3/2.

The following math gives our ciphertext as numbers:

$$\begin{array}{c}
 \begin{bmatrix} 8 & 13 \\ 19 & 14 \end{bmatrix} \begin{bmatrix} 18 \\ 2 \end{bmatrix} \equiv \begin{bmatrix} 14 \\ 6 \end{bmatrix} = \begin{bmatrix} O \\ G \end{bmatrix} \\
 \begin{bmatrix} 8 & 13 \\ 19 & 14 \end{bmatrix} \begin{bmatrix} 8 \\ 4 \end{bmatrix} \equiv \begin{bmatrix} 12 \\ 0 \end{bmatrix} = \begin{bmatrix} M \\ A \end{bmatrix} \\
 \begin{bmatrix} 8 & 13 \\ 19 & 14 \end{bmatrix} \begin{bmatrix} 13 \\ 2 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 15 \end{bmatrix} = \begin{bmatrix} A \\ P \end{bmatrix} \\
 \begin{bmatrix} 8 & 13 \\ 19 & 14 \end{bmatrix} \begin{bmatrix} 4 \\ 14 \end{bmatrix} \equiv \begin{bmatrix} 6 \\ 12 \end{bmatrix} = \begin{bmatrix} G \\ M \end{bmatrix} \\
 \begin{bmatrix} 8 & 13 \\ 19 & 14 \end{bmatrix} \begin{bmatrix} 11 \\ 24 \end{bmatrix} \equiv \begin{bmatrix} 10 \\ 25 \end{bmatrix} = \begin{bmatrix} K \\ Z \end{bmatrix} \\
 \begin{bmatrix} 8 & 13 \\ 19 & 14 \end{bmatrix} \begin{bmatrix} 12 \\ 15 \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 22 \end{bmatrix} = \begin{bmatrix} F \\ W \end{bmatrix} \\
 \begin{bmatrix} 8 & 13 \\ 19 & 14 \end{bmatrix} \begin{bmatrix} 8 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 12 \\ 22 \end{bmatrix} = \begin{bmatrix} M \\ W \end{bmatrix} \\
 \begin{bmatrix} 8 & 13 \\ 19 & 14 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} \equiv \begin{bmatrix} 24 \\ 7 \end{bmatrix} = \begin{bmatrix} Y \\ H \end{bmatrix}
 \end{array}$$

Converting these numbers to ciphertext letters gives us

OGMAAPG MKZFWMWY H

8. We decrypt this using the variation of the Baconian cipher such that I and J share the same ciphertext, and U and V share the same ciphertext. Our plaintext turns out to be the following:

Statistics is the grammar of science.

9. Using the given information, we can determine that the first three letters of our key are **NIN**. First, we assume a three letter key, which yields plaintext doesn't make sense. Next, we assume a four letter key. We can guess that our plaintext letters **PER?IST?NCE** corresponds to the word **PERSISTENCE**, which means our key would be the word **NINE**. Using this key, gives us the following plaintext:

Persistence is half the battle.

10. To decrypt RSA, we take our ciphertext to the power of our private key with the mod in the public key. Here, our answer is $1195^{29} \bmod 2279$. We do the following to calculate this value:

$$1195^2 \equiv 1195^2 \equiv 1371$$

$$1195^4 \equiv 1371^2 \equiv 1745$$

$$1195^8 \equiv 1745^2 \equiv 281$$

$$1195^{16} \equiv 281^2 \equiv 1475$$

Multiplying out $1475 \cdot 281 \cdot 1745 \cdot 1195$ gives us the plaintext of 751.

11. First, we can deduce that the ciphertext **J** is likely to be a plaintext **E**, and then that the ciphertext **D** is likely to be a plaintext **R**. From here, we can deduce the last three plaintext words to be **RESERVES OF ENERGY**. After this, we should have enough to deduce the first three plaintext words to be **FEELING TIRED SHOULD**. From there, it is not difficult to deduce the rest of the quote: Feeling tired should almost never be an excuse, because your body has huge reserves of energy.

Ciphertext Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency			3	6	2	3	2	4	4	16		1	3
Plaintext Letter			G	R	V	B	C	A	N	E		M	H
Ciphertext Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	2	3			3	3	2		2	1	5	7	5
Plaintext Letter	I	L			D	Y	F		T	X	O	S	U

12. First, we calculate the determinant, which is

$$(14)(0)(23) + (13)(19)(17) + (4)(12)(8) - (4)(0)(17) - (13)(12)(23) - (14)(19)(8) \equiv 11.$$

The inverse of this determinant, 11^{-1} , is 19. Next, we calculate our cofactor matrix to be

$$\begin{bmatrix} +4 & -5 & +18 \\ -7 & +20 & -21 \\ +13 & -10 & +0 \end{bmatrix} \text{ and then our adjugate matrix to be } \begin{bmatrix} +4 & -7 & +13 \\ -5 & +20 & -10 \\ +18 & -21 & +0 \end{bmatrix}.$$

We then multiply by the inverse of our determinant, 19, and then calculate it mod 26. This yields

$$\begin{bmatrix} 24 & 23 & 13 \\ 9 & 16 & 18 \\ 4 & 17 & 0 \end{bmatrix} = \begin{bmatrix} Y & X & N \\ J & Q & S \\ E & R & A \end{bmatrix}.$$

13. We can guess that ciphertext **C** corresponds to plaintext **I**. After some trial and error, we can deduce the ciphertext **MY** as plaintext **NO**, ciphertext **KYMO** as plaintext **DONT**, and ciphertext **LCQU** as plaintext **WITH**. At this point, it is likely that the ciphertext **P** corresponds to **E**. From here, it is possible to deduce the quote with a bit more trial and error. The end result is the quote But no, I dont genrely half trubble with speling mistakes.

Ciphertext Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency	3		4	3	2	1	1			2	1	1	4
Plaintext Letter	B		I	S	G	Y	M			A	D	W	N

Ciphertext Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	4		5	5	2	1	1	2	2		1	2	
Plaintext Letter	L		E	T	U	K	P	H	R		F	O	

14. Since we know that the ciphertext **X** is likely to be a plaintext **A** and that Dali was a surrealist artist, we can deduce that the ciphertext **DJQQBXO** is likely to be the plaintext **SURREAL**. From there, it is not difficult to deduce the rest of the quote:

Nada hay más surreal que la realidad.

Ciphertext Letter	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Frequency		3	3	2		1				2	1			1
Plaintext Letter		E	D	S		Q				U	N			Y

Ciphertext Letter	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency		3	1	3	1				1		8		
Plaintext Letter		L	I	R	M				H		A		

15. Based on the letter frequency, we can assume ciphertext **H** is plaintext **E**. After some trial and error, we can discover that ciphertext **DZH** corresponds to plaintext **THE** especially due to the duplicate ciphertext **EZGUTQQTOZHJOHYGQ**. We can then deduce plaintext words such as **BUT** and **REMEMBERS**. In addition, we can then assume ciphertext **G** is plaintext **O**. After some trial and error, we eventually arrive at the plaintext:

Nobody remembers who finished second but the guy who finished second.

Ciphertext Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency	2		2	2	2	1	6	8		5	2		
Plaintext Letter	Y		M	T	W	G	O	E		D	U		

Ciphertext Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	3	5	2	5			4	2				2	5
Plaintext Letter	B	S	R	N			I	F				C	H

16. If we look at the frequency distribution, it seems relatively standard, hinting that it may be a transposition cipher. In fact, it is a transposition cipher that is also a Hill cipher with a key of $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Essentially, we are looking at every pair of letters and switching them around. This is true for both the encryption and the decryption, which will yield the plaintext as

The greater the obstacle, the more glory in overcoming it.