

Test 5 Answers:

Timed:

IS THAT EVERYTHING? IT SEEMED LIKE HE SAID QUITE A BIT MORE THAN THAT.

- 1) AND WHEN IT RAINS ON YOUR PARADE, LOOK UP RATHER THAN DOWN. WITHOUT THE RAIN, THERE WOULD BE NO RAINBOW.
- 2) YESTERDAY IS NOT OURS TO RECOVER, BUT TOMORROW IS OURS TO WIN OR LOSE.
- 3) THE FIRST PRINCIPLE IS THAT YOU MUST NOT FOOL YOURSELF AND YOU ARE THE EASIEST PERSON TO FOOL.
- 4) DON'T FOOL YOURSELF THAT IMPORTANT THINGS CAN BE PUT OFF TILL TOMORROW; THEY CAN BE PUT OFF FOREVER, OR NOT AT ALL.
- 5) DZBYEZMAZMVXYXXOL
- 6) a=3 b=8

To understand how to figure this out, we know

F(5) => X(23)
R(17) => H(7)
I(8) => G(6)
E(4) => U(20)
N(13) => V(21)
D(3) => R(17)

To determine the values of a and b from the formula:

Output = $ax+b \pmod{26}$

You only need to have two letters mapped. For convenience, we just pick the third and the last one, write them as the formula and then solve for b initially: So we have:

$$\begin{aligned} a*8 + b \pmod{26} &= 6 \\ a*3 + b \pmod{26} &= 17 \end{aligned}$$

You can cancel out the a in both of them by multiplying each by the other a value. I.e. since the first is $a*8$, and then second is $a*3$ we multiply the first by 3 and the second by 8

$$\begin{aligned} 3*(a*8 + b \pmod{26}) &= 3*6 \\ 8*(a*3 + b \pmod{26}) &= 8*17 \end{aligned}$$

Simplify them to get:

$$\begin{aligned} 24*a + 3*b \pmod{26} &= 18 \\ 24*a + 8*b \pmod{26} &= 136 \end{aligned}$$

Don't worry about the mod 26 portion for now, we will handle it in a bit. Next we need to subtract to cancel out the a. For convenience, subtract the smaller from the larger:

$$\begin{array}{r} 24*a + 8*b \pmod{26} = 136 \\ - 24*a + 3*b \pmod{26} = 18 \\ \hline 5*b \pmod{26} = 118 \end{array}$$

Since the modulus is a one way transformation, we need to take the mod of the right hand side which is 14. So we know that:

$$5*b \pmod{26} = 14 \text{ (or some other mod 26 value)}$$

To discover which value of b there is, simply compute the other modulus values and see which is a perfect multiple. We know it can't be 1 since b must be an integer and $14/5=2.8$. So we need to just keep adding 26 and dividing until we get a good answer. Add 26 to get 40 and we observe that $40/5=8$ which is an integer.

So we now know that $b=8$. Now we need to solve for a. All we have to do is substitute 8 in for b in either of the formulas and repeat the same process again. For convenience we use the second formula but you could choose to use any.

$$\begin{aligned} a*3 + 8 \pmod{26} &= 17 \\ a*3 + 8 - 8 \pmod{26} &= 17 - 8 \\ a*3 \pmod{26} &= 9 \end{aligned}$$

Just like before we look for a modulus value which is a perfect multiple of 3. In this case it is easy because we learned a long time ago that $9/3=3$ which tells us that $a=3$.

7) DONTFORGETTHEPIZZA

To solve this, you first fill in the letters we know.

Z	Y	R	H	N	Y	T	U	G	H	H	B	G	F	I	X	X	E
															Z	Z	A

You could attempt to solve this as a standard cryptogram at this point, or since you know it is an Affine cipher calculate the values of a and b.

Using the same logic from question 6, we know:

$$\begin{aligned} A(0) &=> E(4) \\ Z(25) &=> X(23) \end{aligned}$$

To determine the values of a and b from the formula:

$$\text{Output} = ax+b \pmod{26}$$

We get pretty lucky here since having A as one of the letters makes the formula trivial

$$a \cdot 0 + b \pmod{26} = 4$$

Which tells us that $b=4$. Now we need to solve for a . All we have to do is substitute 2 in for b in the other formula and repeat the same process again.

$$a \cdot 25 + 4 \pmod{26} = 23$$

$$a \cdot 25 + 4 - 4 \pmod{26} = 23 - 4$$

$$a \cdot 25 \pmod{26} = 19$$

Just like before we look for a modulus value which is a perfect multiple of 25. We keep adding 26 and trying to divide by 25 until we get to find that $a=7$.

$$19/25 = .76$$

$$45/25 = 1.8$$

$$71/25 = 2.84$$

$$97/25 = 3.88$$

$$123/25 = 4.92$$

$$149/25 = 5.96$$

$$175/25 = 7$$

Now that we know $a=7$ and $b=4$, we can encode ETOIN

$$E(4) \Rightarrow 4 \cdot 7 + 4 = 32 \Rightarrow G(6)$$

$$T(19) \Rightarrow 19 \cdot 7 + 4 = 137 \Rightarrow H(7)$$

$$O(14) \Rightarrow 14 \cdot 7 + 4 = 102 \Rightarrow Y(24)$$

$$I(8) \Rightarrow 8 \cdot 7 + 4 = 60 \Rightarrow I(8)$$

$$N(13) \Rightarrow 13 \cdot 7 + 4 = 95 \Rightarrow R(17)$$

Filling in those we get:

Z	Y	R	H	N	Y	T	U	G	H	H	B	G	F	I	X	X	E
	O	N	T		O			E	T	T		E		I	Z	Z	A

Looking at it, three letters stand out. Z is probably D (to make DONT), B is probably H (to make THE) and F most certainly must be a P (for PIZZA), so we test that out

$$D(3) \Rightarrow 3 \cdot 7 + 4 = 25 \Rightarrow Z(25)$$

$$H(1) \Rightarrow 1 \cdot 7 + 4 = 11 \Rightarrow B(1)$$

$$P(15) \Rightarrow 15 \cdot 7 + 4 = 109 \Rightarrow F(5)$$

Filling in those we get:

Z	Y	R	H	N	Y	T	U	G	H	H	B	G	F	I	X	X	E
D	O	N	T		O			E	T	T	H	E	P	I	Z	Z	A

Since we aren't sure what the other letters are, we can just go to the next three letters in the frequency table (S, R, H) but we already did H so we just do two of them.

$$S(18) \Rightarrow 18 \cdot 11 + 2 = 130 \Rightarrow A(0)$$

$$R(17) \Rightarrow 17 \cdot 11 + 2 = 123 \Rightarrow T(19)$$

Filling it in we get:

Z	Y	R	H	N	Y	T	U	G	H	H	B	G	F	I	X	X	E
D	O	N	T		O	R		E	T	T	H	E	P	I	Z	Z	A

Since we have all but two letters which is enough to count for a correct answer, we could go on to another problem, or we can guess that the last two letters are F and G respectively.

$$F(5) \Rightarrow 5 \cdot 11 + 2 = 39 \Rightarrow N(13)$$

$$G(6) \Rightarrow 6 \cdot 11 + 2 = 46 \Rightarrow U(20)$$

Which of course confirms our guess and we get a final answer of:

Z	Y	R	H	N	Y	T	U	G	H	H	B	G	F	I	X	X	E
D	O	N	T	F	O	R	G	E	T	T	H	E	P	I	Z	Z	A

8) THE RIGHT TO BE HEARD DOES NOT INCLUDE THE RIGHT TO BE TAKEN SERIOUSLY.

9) LA FAMILIA ES COMO LA MÚSICA, ALGUNAS NOTAS ALTAS, OTRAS BAJAS, PERO SIEMPRE ES UNA HERMOSA CANCIÓN.

Translation: *The family is like music, some high notes, others low, but it is always a beautiful song*

10) PUSH TO OPEN THE DOOR

11) THIS SENTENCE CONTRADICTS ITSELF - NO ACTUALLY IT DOESN'T.

12) FM SW CM DT IX

here's how you get the answer (remember to add the Z at the end to make it an even group of two letters):

$$\begin{pmatrix} F & I \\ N & D \end{pmatrix} \begin{pmatrix} F \\ R \end{pmatrix} \equiv \begin{pmatrix} 5 & 8 \\ 13 & 3 \end{pmatrix} \begin{pmatrix} 5 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 5 \times 5 + 8 \times 17 \\ 13 \times 5 + 3 \times 17 \end{pmatrix} \equiv \begin{pmatrix} 161 \\ 116 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 5 \\ 12 \end{pmatrix} \equiv \begin{pmatrix} F \\ M \end{pmatrix}$$

$$\begin{pmatrix} F & I \\ N & D \end{pmatrix} \begin{pmatrix} E \\ Q \end{pmatrix} \equiv \begin{pmatrix} 5 & 8 \\ 13 & 3 \end{pmatrix} \begin{pmatrix} 4 \\ 6 \end{pmatrix} \equiv \begin{pmatrix} 5 \times 4 + 8 \times 6 \\ 13 \times 4 + 3 \times 6 \end{pmatrix} \equiv \begin{pmatrix} 148 \\ 100 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 18 \\ 22 \end{pmatrix} \equiv \begin{pmatrix} S \\ W \end{pmatrix}$$

$$\begin{pmatrix} F & I \\ N & D \end{pmatrix} \begin{pmatrix} U \\ E \end{pmatrix} \equiv \begin{pmatrix} 5 & 8 \\ 13 & 3 \end{pmatrix} \begin{pmatrix} 20 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 5 \times 20 + 8 \times 4 \\ 13 \times 20 + 3 \times 4 \end{pmatrix} \equiv \begin{pmatrix} 132 \\ 272 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 2 \\ 12 \end{pmatrix} \equiv \begin{pmatrix} C \\ M \end{pmatrix}$$

$$\begin{pmatrix} F & I \\ N & D \end{pmatrix} \begin{pmatrix} N \\ C \end{pmatrix} \equiv \begin{pmatrix} 5 & 8 \\ 13 & 3 \end{pmatrix} \begin{pmatrix} 13 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 5 \times 13 + 8 \times 2 \\ 13 \times 13 + 3 \times 2 \end{pmatrix} \equiv \begin{pmatrix} 81 \\ 175 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 3 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} D \\ T \end{pmatrix}$$

$$\begin{pmatrix} F & I \\ N & D \end{pmatrix} \begin{pmatrix} Y \\ Z \end{pmatrix} \equiv \begin{pmatrix} 5 & 8 \\ 13 & 3 \end{pmatrix} \begin{pmatrix} 24 \\ 25 \end{pmatrix} \equiv \begin{pmatrix} 5 \times 24 + 8 \times 25 \\ 13 \times 24 + 3 \times 25 \end{pmatrix} \equiv \begin{pmatrix} 320 \\ 387 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 8 \\ 23 \end{pmatrix} \equiv \begin{pmatrix} I \\ X \end{pmatrix}$$

13) QRF ZPL ZCI IBD ZXB

Here's how you get the answer (remember you add two Zs at the end to make it a group of three letters).

$$\begin{pmatrix} T & H & E \\ W & O & R \\ D & S & Z \end{pmatrix} \begin{pmatrix} S \\ Y \\ N \end{pmatrix} \equiv \begin{pmatrix} 19 & 7 & 4 \\ 22 & 14 & 17 \\ 3 & 18 & 25 \end{pmatrix} \begin{pmatrix} 18 \\ 24 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 19 \times 18 + 7 \times 24 + 4 \times 13 \\ 22 \times 18 + 14 \times 24 + 17 \times 13 \\ 3 \times 18 + 18 \times 24 + 25 \times 13 \end{pmatrix} \equiv \begin{pmatrix} 562 \\ 953 \\ 811 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 16 \\ 17 \\ 51 \end{pmatrix} \equiv \begin{pmatrix} Q \\ R \\ F \end{pmatrix}$$

$$\begin{pmatrix} T & H & E \\ W & O & R \\ D & S & Z \end{pmatrix} \begin{pmatrix} C \\ H \\ R \end{pmatrix} \equiv \begin{pmatrix} 19 & 7 & 4 \\ 22 & 14 & 17 \\ 3 & 18 & 25 \end{pmatrix} \begin{pmatrix} 2 \\ 7 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 19 \times 2 + 7 \times 7 + 4 \times 17 \\ 22 \times 2 + 14 \times 7 + 17 \times 17 \\ 3 \times 2 + 18 \times 7 + 25 \times 17 \end{pmatrix} \equiv \begin{pmatrix} 155 \\ 431 \\ 557 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 25 \\ 15 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} Z \\ P \\ L \end{pmatrix}$$

$$\begin{pmatrix} T & H & E \\ W & O & R \\ D & S & Z \end{pmatrix} \begin{pmatrix} O \\ N \\ I \end{pmatrix} \equiv \begin{pmatrix} 19 & 7 & 4 \\ 22 & 14 & 17 \\ 3 & 18 & 25 \end{pmatrix} \begin{pmatrix} 14 \\ 13 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 19 \times 14 + 7 \times 13 + 4 \times 8 \\ 22 \times 14 + 14 \times 13 + 17 \times 8 \\ 3 \times 14 + 18 \times 13 + 25 \times 8 \end{pmatrix} \equiv \begin{pmatrix} 389 \\ 626 \\ 476 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 25 \\ 2 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} Z \\ C \\ I \end{pmatrix}$$

$$\begin{pmatrix} T & H & E \\ W & O & R \\ D & S & Z \end{pmatrix} \begin{pmatrix} S \\ I \\ N \end{pmatrix} \equiv \begin{pmatrix} 19 & 7 & 4 \\ 22 & 14 & 17 \\ 3 & 18 & 25 \end{pmatrix} \begin{pmatrix} 18 \\ 8 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 19 \times 18 + 7 \times 8 + 4 \times 13 \\ 22 \times 18 + 14 \times 8 + 17 \times 13 \\ 3 \times 18 + 18 \times 8 + 25 \times 13 \end{pmatrix} \equiv \begin{pmatrix} 450 \\ 729 \\ 523 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 8 \\ 1 \\ 3 \end{pmatrix} \equiv \begin{pmatrix} I \\ B \\ D \end{pmatrix}$$

$$\begin{pmatrix} T & H & E \\ W & O & R \\ D & S & Z \end{pmatrix} \begin{pmatrix} G \\ Z \\ Z \end{pmatrix} \equiv \begin{pmatrix} 19 & 7 & 4 \\ 22 & 14 & 17 \\ 3 & 18 & 25 \end{pmatrix} \begin{pmatrix} 6 \\ 25 \\ 25 \end{pmatrix} \equiv \begin{pmatrix} 19 \times 6 + 7 \times 25 + 4 \times 25 \\ 22 \times 6 + 14 \times 25 + 17 \times 25 \\ 3 \times 6 + 18 \times 25 + 25 \times 25 \end{pmatrix} \equiv \begin{pmatrix} 389 \\ 907 \\ 1093 \end{pmatrix} \pmod{26} \equiv \begin{pmatrix} 25 \\ 23 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} Z \\ X \\ B \end{pmatrix}$$

14) EQRI BA ELHZF EGL ES BA YSGMK

The easiest way to approach this is to write the letters TIME over and over above each of the letters in the phrase to decode and then look up the pair in the Vigenère table at the start of the test.

T	I	M	E	T	I	M	E	T	I	M	E	T	I
L	I	F	E	I	S	S	H	O	R	T	A	N	D
E	Q	R	I	B	A	E	L	H	Z	F	E	G	L

M	E	T	I	M	E	T	I	M
S	O	I	S	M	O	N	E	Y
E	S	B	A	Y	S	G	M	K

15) DEAR MATH, PLEASE GROW UP AND SOLVE YOUR OWN PROBLEMS, I'M TIRED OF SOLVING THEM FOR YOU. (the key word is CLASS)

You solve it by putting in what you know and decoding it to determine the key word.

You see that it is CLASS.

C	L	A	S	S	C	L	A																	
F	P	A	J	E	C	E	H	H	D	G	L	S	W	Y	T	Z	W	M	H	C	Y	D	K	G

D	E	A	R	M
---	---	---	---	---

A	T	H		
---	---	---	--	--

--	--	--	--	--

--	--	--	--	--

--	--	--	--	--

Now that we know the keyword, simply repeat it across the remainder of the table and decode each letter. The groups of 5 in this case make it easy. We also have it really easy because a key letter of A means that it maps to the same letter so you can quickly fill in the table from the middle ones.

C	L	A	S	S
F	P	A	J	E
D	E	A	R	M

C	L	A	S	S
C	E	H	H	D
A	T	H		

C	L	A	S	S
G	L	S	W	Y
		S		

C	L	A	S	S
T	Z	W	M	H
		W		

C	L	A	S	S
C	Y	D	K	G
		D		

C	L	A	S	S
N	G	E	Q	G
		E		

C	L	A	S	S
W	C	O	O	F
		O		

C	L	A	S	S
R	C	O	T	D
		O		

C	L	A	S	S
G	X	S	A	E
		S		

C	L	A	S	S
V	T	R	W	V
		R		

C	L	A	S	S
Q	Q	S	G	D
		S		

C	L	A	S	S
X	T	N	Y	L
		N		

C	L	A	S	S
J	P	M	X	G
		M		

C	L	A	S
T	J	O	M
		O	

After filling in those, do the C and L and then you can do the two S columns quickly.

C	L	A	S	S
F	P	A	J	E
D	E	A	R	M

C	L	A	S	S
C	E	H	H	D
A	T	H	P	L

C	L	A	S	S
G	L	S	W	Y
E	A	S	E	G

C	L	A	S	S
T	Z	W	M	H
R	O	W	U	P

C	L	A	S	S
C	Y	D	K	G
A	N	D	S	O

C	L	A	S	S
N	G	E	Q	G
L	V	E	Y	O

C	L	A	S	S
W	C	O	O	F
U	R	O	W	N

C	L	A	S	S
R	C	O	T	D
P	R	O	B	L

C	L	A	S	S
G	X	S	A	E
E	M	S	I	M

C	L	A	S	S
V	T	R	W	V
T	I	R	E	D

C	L	A	S	S
Q	Q	S	G	D
O	F	S	O	L

C	L	A	S	S
X	T	N	Y	L
V	I	N	G	T

C	L	A	S	S
J	P	M	X	G
H	E	M	F	O

C	L	A	S
T	J	O	M
R	Y	O	U

- 16) WE CANNOT SOLVE OUR PROBLEMS WITH THE SAME THINKING WE USED WHEN WE CREATED THEM.
- 17) LIFE IS LIKE RIDING A BICYCLE. TO KEEP YOUR BALANCE, YOU MUST KEEP MOVING.
- 18) EWE LAUGH AT ME BECAUSE EYE AM DIFFERENT. EYE LAUGH AT EWE BECAUSE EWE ARE AWL THE SAME.

You laugh at me because I'm different, I laugh at you because you're all the same.