Test 4 Answers:
Timed:

```
IT IS A MISTAKE TO THINK THAT MOVING FAST IS THE SAME AS
ACTUALLY GOING SOMEWHERE.
1)  IF WE HAD NO WINTER, THE SPRING WOULD NOT BE SO
    PLEASANT: IF WE DID NOT SOMETIMES TASTE OF ADVERSITY,
    PROSPERITY WOULD NOT BE SO WELCOME.
2)  NOTICE THAT THE STIFFEST TREE IS MOST EASILY CRACKED,
    WHILE THE BAMBOO OR WILLOW SURVIVES BY BENDING WITH THE
    WIND.
3)  I LOVE THE FEELING OF THE FRESH AIR ON MY FACE AND THE
    WIND BLOWING THROUGH MY HAIR.
4)  HEAT CANNOT BE SEPARATED FROM FIRE, OR BEAUTY FROM THE
    ETERNAL.
5)  ZYMLXZMFXIFVZFX
6)  a=9 b=9
```

To understand how to figure this out, we know

```
T(19)   =>  Y(24)
H(7)    =>  U(20)
E(4)    =>  T(19)
R(17)   =>  G(6)
E(4)    =>  T(19)
```

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 first two, write them as the formula and then solve for b initially: So we have:

$$a*19 + b \pmod{26} = 24$$
$$a*7 + b \pmod{26} = 20$$

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*17, and then second is a*4 we multiply the first by 4 and the second by 17

$$7*(a*19 + b \pmod{26}) = 7*24$$
$$19*(a*7 + b \pmod{26}) = 19*20$$

Simplify them to get:

$$133*a + 7*b \pmod{26} = 168$$
$$133*a + 19*b \pmod{26} = 380$$

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:

```
  133*a + 19*b (Mod 26) = 380
- 133*a + 7*b (Mod 26) = 168
 -------------------------
         12*b (Mod 26) = 212
```

Since the modulus is a one way transformation, we need to take the mod of the right hand side which is 4. So we know that:

```
         12*b (Mod 26) = 4 (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 `4/12=.25`. So we need to just keep adding 26 and dividing until we get a good answer.
Add `26` to get `30` and we observe that `30/12=2.5.`
Add another `26` to get `56` but `56/12=4.666`.
Add another `26` to get `82` but `82/12=6.833`.
Add another `26` to get `108` and we see that `108/12=9` which is an integer.

So we now know that b=9. Now we need to solve for a. All we have to do is substitute 9 in for b in either of the formulas and repeat the same process again. For convenience we use the second formula since it is easier to see if something is a power of 7 vs a power of 19

```
a*7 + 9 (Mod 26) = 20
a*7 + 9 -9 (Mod 26) = 20 - 9
a*7 (mod 26) = 11
```

Just like before we look for a modulus value which is a perfect multiple of `7`. We know that it isn't `2`, so we add `26` to `11` to get `37`. Since `37/7 = 5.285` we add another `26` to get `63` and see that `63/7=9` to tell us that a=9.

`7)  THEPARTYISTOMORROW`

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

D	B	U	L	C	H	D	G	M	S	D	A	E	A	H	H	A	K
											O		O			O	W

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:

```
O(14)   =>  A(0)
W(22)   =>  K(10)
```

To determine the values of a and b from the formula:
`Output =` $ax+b$ `(mod 26)`

Since we are given only two letters, write them as the formula and then solve for b initially: So we have:

```
a*14 + b (Mod 26) = 0
a*22 + b (Mod 26) = 10
```

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*17, and then second is a*4 we multiply the first by 4 and the second by 17

```
22*(a*14 + b (Mod 26)) = 0*22
14*(a*22 + b (Mod 26)) = 10*14
```

Simplify them to get:

```
308*a + 22*b (Mod 26) = 0
308*a + 14*b (Mod 26) = 140
```

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:

```
  308*a + 22*b (Mod 26) = 0
- 308*a + 14*b (Mod 26) = 140
 --------------------------
         8*b (Mod 26) = -140
```

Since the modulus is a one way transformation, we need to take the mod of the right hand side which is 14. (Trick on your calculator.. Divide -140/26 to get -5.384 and then add 6 to the value since it is negative. Then multiply back by 26 to get 16) . So we know that:

```
8*b (Mod 26) = 16 (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 can see that it is 2 right off the bat since b must be an integer and `16/8=2`.

So we now know that $b=2$. Now we need to solve for a. All we have to do is substitute 2 in for b in either of the formulas and repeat the same process again. For convenience we use the first formula since it is smaller.

```
a*14 + 2 (Mod 26) = 0
a*14 + 2 -2 (Mod 26) = 0 - 2
a*14 (mod 26) = 24
```

Just like before we look for a modulus value which is a perfect multiple of `14`. We keep adding 26 and trying to divide by 14 until we get to find that $a=11$.
`24/14=1.714`

50/14=3.571
76/14=5.428
102/14=7.285
128/14=9.142
154/14=11

Now that know a=11 and b=2, we can encode A by just looking the b value to see that A maps to C

D	B	U	L	C	H	D	G	M	S	D	A	E	A	H	H	A	K
				A							O		O			O	W

That doesn't give us enough to go on, so we calculate ETIN (we already had O given to us)

```
E(4)    =>  4*11+2   46   =>  U(20)
T(19)   =>  19*11+2  211  =>  D(3)
I(8)    =>  8*11+2   90   =>  M(12)
N(13)   =>  13*11+2  145  =>  P(15)
```

Filling in those we get:

D	B	U	L	C	H	D	G	M	S	D	A	E	A	H	H	A	K
T		E		A		T		I		T	O		O			O	W

It still isn't enough, so we take the next three letters

```
S(18)   =>  18*11+2  200  =>  S(18)
R(17)   =>  17*11+2  189  =>  H(7)
H(7)    =>  7*11+2   79   =>  B(1)
```

Filling in those we get:

D	B	U	L	C	H	D	G	M	S	D	A	E	A	H	H	A	K
T	H	E		A	R	T		I	S	T	O		O	R	R	O	W

Looking at it, it is pretty obvious that the E should be an M and we can calculate it to confirm.

```
M(11)   =>  11*11+2  134  =>  E(4)
```

Filling it in we get:

D	B	U	L	C	H	D	G	M	S	D	A	E	A	H	H	A	K
T	H	E		A	R	T		I	S	T	O	M	O	R	R	O	W

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 P and Y respectively.

```
P(15)   =>  15*11+2  167  =>  L(11)
Y(24)   =>  24*11+2  266  =>  G(6)
```

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

D	B	U	L	C	H	D	G	M	S	D	A	E	A	H	H	A	K
T	H	E	P	A	R	T	Y	I	S	T	O	M	O	R	R	O	W

8) LEARNING IS NOT DONE TO YOU IT IS SOMETHING YOU CHOOSE TO DO.

9) NO SE PUEDE SACAR AGUA DE UNA PIEDRE.
Translation: *You cannot get water from a stone*

10) PLEASE LOCK THE DOOR

11) WHEN THE FLOWER BLOSSOMS, THE BEE WILL COME.
12) NF FN HX MO SB

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

$$\begin{pmatrix} H & E \\ L & P \end{pmatrix}\begin{pmatrix} F \\ O \end{pmatrix} \equiv \begin{pmatrix} 7 & 4 \\ 11 & 15 \end{pmatrix}\begin{pmatrix} 5 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 7\times 5+4\times 14 \\ 11\times 5+15\times 14 \end{pmatrix} \equiv \begin{pmatrix} 91 \\ 265 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 15 \\ 5 \end{pmatrix} \equiv \begin{pmatrix} N \\ F \end{pmatrix}$$

$$\begin{pmatrix} H & E \\ L & P \end{pmatrix}\begin{pmatrix} R \\ E \end{pmatrix} \equiv \begin{pmatrix} 7 & 4 \\ 11 & 15 \end{pmatrix}\begin{pmatrix} 17 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 7\times 17+4\times 4 \\ 11\times 17+15\times 4 \end{pmatrix} \equiv \begin{pmatrix} 135 \\ 247 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 5 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} F \\ N \end{pmatrix}$$

$$\begin{pmatrix} H & E \\ L & P \end{pmatrix}\begin{pmatrix} N \\ S \end{pmatrix} \equiv \begin{pmatrix} 7 & 4 \\ 11 & 15 \end{pmatrix}\begin{pmatrix} 13 \\ 18 \end{pmatrix} \equiv \begin{pmatrix} 7\times 13+4\times 18 \\ 11\times 13+15\times 18 \end{pmatrix} \equiv \begin{pmatrix} 163 \\ 413 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 7 \\ 23 \end{pmatrix} \equiv \begin{pmatrix} H \\ C \end{pmatrix}$$

$$\begin{pmatrix} H & E \\ L & P \end{pmatrix}\begin{pmatrix} I \\ C \end{pmatrix} \equiv \begin{pmatrix} 7 & 4 \\ 11 & 15 \end{pmatrix}\begin{pmatrix} 8 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 7\times 8+4\times 2 \\ 11\times 8+15\times 2 \end{pmatrix} \equiv \begin{pmatrix} 64 \\ 118 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 12 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} M \\ O \end{pmatrix}$$

$$\begin{pmatrix} H & E \\ L & P \end{pmatrix}\begin{pmatrix} S \\ Z \end{pmatrix} \equiv \begin{pmatrix} 7 & 4 \\ 11 & 15 \end{pmatrix}\begin{pmatrix} 18 \\ 25 \end{pmatrix} \equiv \begin{pmatrix} 7\times 18+4\times 25 \\ 11\times 18+15\times 25 \end{pmatrix} \equiv \begin{pmatrix} 226 \\ 573 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 18 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} S \\ B \end{pmatrix}$$

13) AJL GQU NZM SRU OGZ

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

$$\begin{pmatrix} H & E & L \\ P & F & O \\ R & U & S \end{pmatrix}\begin{pmatrix} D \\ Y \\ N \end{pmatrix} \equiv \begin{pmatrix} 17 & 4 & 11 \\ 15 & 5 & 14 \\ 17 & 20 & 18 \end{pmatrix}\begin{pmatrix} 3 \\ 24 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 17\times 3+4\times 24+11\times 13 \\ 15\times 3+5\times 24+14\times 13 \\ 17\times 3+20\times 24+18\times 13 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 347 \\ 765 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 0 \\ 9 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} A \\ J \\ L \end{pmatrix}$$

$$\begin{pmatrix} H & E & L \\ P & F & O \\ R & U & S \end{pmatrix}\begin{pmatrix} A \\ M \\ I \end{pmatrix} \equiv \begin{pmatrix} 17 & 4 & 11 \\ 15 & 5 & 14 \\ 17 & 20 & 18 \end{pmatrix}\begin{pmatrix} 0 \\ 12 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 17\times 0+4\times 12+11\times 8 \\ 15\times 0+5\times 12+14\times 8 \\ 17\times 0+20\times 12+18\times 8 \end{pmatrix} \equiv \begin{pmatrix} 136 \\ 172 \\ 384 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 6 \\ 16 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} G \\ Q \\ U \end{pmatrix}$$

$$\begin{pmatrix} H & E & L \\ P & F & O \\ R & U & S \end{pmatrix}\begin{pmatrix} C \\ P \\ L \end{pmatrix} \equiv \begin{pmatrix} 17 & 4 & 11 \\ 15 & 5 & 14 \\ 17 & 20 & 18 \end{pmatrix}\begin{pmatrix} 2 \\ 15 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 17\times 2+4\times 15+11\times 11 \\ 15\times 2+5\times 15+14\times 11 \\ 17\times 2+20\times 15+18\times 11 \end{pmatrix} \equiv \begin{pmatrix} 195 \\ 259 \\ 532 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 13 \\ 25 \\ 12 \end{pmatrix} \equiv \begin{pmatrix} N \\ Z \\ M \end{pmatrix}$$

$$\begin{pmatrix} H & E & L \\ P & F & O \\ R & U & S \end{pmatrix}\begin{pmatrix} A \\ N \\ E \end{pmatrix} \equiv \begin{pmatrix} 17 & 4 & 11 \\ 15 & 5 & 14 \\ 17 & 20 & 18 \end{pmatrix}\begin{pmatrix} 0 \\ 13 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 17\times 0+4\times 13+11\times 4 \\ 15\times 0+5\times 13+14\times 4 \\ 17\times 0+20\times 13+18\times 4 \end{pmatrix} \equiv \begin{pmatrix} 96 \\ 121 \\ 332 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 18 \\ 17 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} S \\ R \\ U \end{pmatrix}$$

$$\begin{pmatrix} H & E & L \\ P & F & O \\ R & U & S \end{pmatrix}\begin{pmatrix} T \\ Z \\ Z \end{pmatrix} \equiv \begin{pmatrix} 17 & 4 & 11 \\ 15 & 5 & 14 \\ 17 & 20 & 18 \end{pmatrix}\begin{pmatrix} 19 \\ 25 \\ 25 \end{pmatrix} \equiv \begin{pmatrix} 17\times 19+4\times 25+11\times 25 \\ 15\times 19+5\times 25+14\times 25 \\ 17\times 19+20\times 25+18\times 25 \end{pmatrix} \equiv \begin{pmatrix} 508 \\ 760 \\ 1273 \end{pmatrix} \bmod 26 \equiv \begin{pmatrix} 14 \\ 6 \\ 25 \end{pmatrix} \equiv \begin{pmatrix} O \\ G \\ Z \end{pmatrix}$$

14) MUIR UJ YIRP YBBHEMN GUYY VRVLL FBFR NM BHP IYFGGSUGVMS

The easiest way to approach this is to write the letters FUNNY 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.

F	U	N	N		Y	F		U	N	N	Y		F	U	N	N	Y	F	U		N	N	Y	F
H	A	V	E		W	E		E	V	E	R		T	H	O	U	G	H	T		T	H	A	T
M	U	I	R		U	J		Y	I	R	P		Y	B	B	H	E	M	N		G	U	Y	Y

U	N	N	Y	F		U	N	N	Y		F	U		N	N	Y		F	U	N	N	Y	F	U	N	N	Y	F
B	E	I	N	G		L	O	S	T		I	S		O	U	R		D	E	S	T	I	N	A	T	I	O	N
V	R	V	L	L		F	B	F	R		N	M		B	H	P		I	Y	F	G	G	S	U	G	V	M	S

15) THERE ARE SOME THINGS YOUR MIND HAS BEEN HIDING FROM YOU. (the key word is THINK)
16) THERE IS NOTHING BETTER THAN A FRIEND, UNLESS IT IS A FRIEND WITH CHOCOLATE.
17) YOU CAN CUT ALL THE FLOWERS BUT YOU CANNOT KEEP SPRING FROM COMING
18) EWE CAN FOOL AWL THE PEOPLE SUM OF THE THYME, AND SUM OF THE PEOPLE AWL THE THYME, BUT EWE CANNOT FOOL AWL THE PEOPLE AWL THE THYME.