Timed question:

OPTIMISM IS THE FAITH THAT LEADS TO ACHIEVEMENT. NOTHING CAN BE DONE WITHOUT HOPE AND CONFIDENCE.

1)

X	C	S	P	Y	F	Z	Z	R	C	I	H	H	W	V	C	S	W	F	R	C	P
D	E	C	R	Y	P	T	T	H	E	A	F	F	I	N	E	C	I	P	H	E	R

Note that this one cannot be solved if we were given the clues of the last two letters. Here's how we would try to get to the answer in that case. Since we are given that

E (4) → C (2)

R (17) → P(15)

From this we know:

$$(a \times 4 + b)\ mod\ 26 = 2$$
$$(a \times 17 + b)\ mod\ 26 = 15$$

Looking at the formulas we see that it is easiest to subtract the first from the last.

$$(a \times 17 + b)\ mod\ 26 = 15$$
$$\underline{-(a \times 4 + b)\ mod\ 26 = 2\ }$$
$$(a \times 13)\ mod\ 26 = 13$$

This one presents us with a challenge given that a could be 1 and you will quickly notice that a could also be 3, 5, 7 or any odd number. (Although we can eliminate 13 since it is not coprime with 26) so we must look for another solution. Solving for b might be illuminating in this case.

$$(a \times 4 + b)\ mod\ 26 = 2$$
$$(a \times 17 + b)\ mod\ 26 = 15$$

Multiply them both by each other to see what you get.

$$(a \times 4 \times 17 + b \times 4)\ mod\ 26 = 15 \times 4$$
$$(a \times 4 \times 17 + b \times 17)\ mod\ 26 = 2 \times 17$$

We want to subtract the first from the second one to get.

$$(a \times 4 \times 17 + b \times 17)\ mod\ 26 = 2 \times 17$$
$$\underline{-(a \times 4 \times 17 + b \times 4)\ mod\ 26 = 15 \times 4}$$
$$(b \times 13)\ mod\ 26 = -26\ mod\ 26$$
$$(b \times 13)\ mod\ 26 = 0$$

Once again, we are stumped and only know that b is an even number. We could try all odd numbers for *a* and all even numbers for *b*, but that would be unreasonable to see on a test.

So given a proper clue instead of:

D (3) → X (23)

E (4) → C (2)

From this we know:

$$(a \times 3 + b)\ mod\ 26 = 23$$
$$(a \times 4 + b)\ mod\ 26 = 2$$

Looking at the formulas we see that it is easiest to subtract the first from the last.

$$(a \times 4 + b)\ mod\ 26 = 2$$
$$\underline{-(a \times 3 + b)\ mod\ 26 = 23\ }$$
$$a\ mod\ 26 = -21$$
$$a\ mod\ 26 = 5$$

Now that we know that $a = 5$

Popping that back into any of the formulas (we pick the first one because it is the lowest multiplier)

$$(5 \times 3 + b)\ mod\ 26 = 23$$
$$(15 + b)\ mod\ 26 = 23$$

We can then subtract 15 from both sides

$$(15 + b)\ mod\ 26 - 15 = (23 - 15)\ mod\ 26$$
$$b\ mod\ 26 = 8\ mod\ 26$$

And we see that $b = 8$. However, we only know a few of the letters in the cipher:

X	C	S	P	Y	F	Z	Z	R	C	I	H	H	W	V	C	S	W	F	R	C	P
D	E								E						E					E	

Our first step is to encode the common letters ETAOIN to see what they would map to. Note that we already know the mapping for E so we don't have to do that one.

E

E(4)	→	$4 \times 5 + 8$	28	→	C(2)
T(19)	→	$19 \times 5 + 8$	103	→	Z(25)
A(0)	→	$0 \times 5 + 8$	8	→	I(8)
O(14)	→	$14 \times 5 + 8$	78	→	A(0)
I(8)	→	$8 \times 5 + 8$	48	→	W(22)
N(13)	→	$13 \times 5 + 8$	73	→	V(21)

Filling in the letters we found (ZIAWV) we get a bit more of the answer.

X	C	S	P	Y	F	Z	Z	R	C	I	H	H	W	V	C	S	W	F	R	C	P
D	E					T	T		E	A			I	N	E		I			E	

This doesn't give us enough to solve it quickly do we just take the next 5 letters SRHLD.

S(18)	→	$18 \times 5 + 8$	98	→	U(20)
R(17)	→	$17 \times 5 + 8$	93	→	P(15)
H(7)	→	$7 \times 5 + 8$	43	→	R(17)
L(11)	→	$11 \times 5 + 8$	63	→	L(11)
D(3)	→	$3 \times 5 + 8$	23	→	X(23)

We know the reverse mapping of 5 more letters (UPRLX) which we can fill in.

X	C	S	P	Y	F	Z	Z	R	C	I	H	H	W	V	C	S	W	F	R	C	P
D	E		R			T	T	H	E	A			I	N	E		I		H	E	R

While we could take some guesses (THE clearly shows up in the text) we can attack 5 more letters CUMFP from the frequency table that we were given with the test.

C(2)	→	$2 \times 5 + 8$	18	→	S(18)
U(20)	→	$20 \times 5 + 8$	108	→	E(4)
M(12)	→	$12 \times 5 + 8$	68	→	Q(16)
F(5)	→	$5 \times 5 + 8$	33	→	H(7)
P(15)	→	$15 \times 5 + 8$	83	→	F(5)

This gives us the reverse mapping of 5 more letters (SEQHF) which we can fill in.

X	C	S	P	Y	F	Z	Z	R	C	I	H	H	W	V	C	S	W	F	R	C	P
D	E	C	R		P	T	T	H	E	A	F	F	I	N	E	C	I	P	H	E	R

This leaves us with only one letter that we don’t know (although it is obvious). At this point you have three options

a) Leave it blank since you can have two wrong and still get the full points for the question
b) Guess that it is the letter Y and fill it in
c) Confirm that it is the letter by doing the math $(24 \times 5 + 8 = 128\, mod\ 26\ \ \equiv 24)$

2)

H	I	S	T	O	R	I	C	A	L	A	C	C	U	R	A	C	Y
B	M	S	D	A	H	M	Y	C	T	C	Y	Y	O	H	C	Y	G

3) $a = 15, b = 15$

Here’s how we figured that out. We are given:
F(5) → M(12)
U(20) → D(3)
N(13) → C(2)
Y(24) → L(11)

From this we know:

$$(a \times 5 + b)\ mod\ 26 = 12$$
$$(a \times 20 + b)\ mod\ 26 = 3$$
$$(a \times 13 + b)\ mod\ 26 = 2$$
$$(a \times 24 + b)\ mod\ 26 = 11$$

Looking at the formulas we want to solve for a and we only need two formulas. For simplicity we can take the second and the last.

$$(a \times 24 + b)\ mod\ 26 = 11$$
$$(a \times 20 + b)\ mod\ 26 = 3$$

To solve for a we can just subtract them

$$(a \times 24 + b)\ mod\ 26 = 11$$
$$\underline{-(a \times 20 + b)\ mod\ 26 = 3\ }$$
$$(a \times 4)\ mod\ 26 = 8$$

An obvious solution here says that $a = 2$ BUT we know that a cannot be 2 because 2 is not coprime with 26 [The only possible values for a are 1, 3, 5, 7, 9, 11 ,15, 17, 19, 21, 23 and 25] so we must look for another solution

So we try the next mod 26 value $8 + 26 = 34$ but $34 \div 4 = 8.5$ which is not divisible by 4 so we go onto the next one… $34 + 26 = 60$ and we see $60 \div 4 = 15$ which is indeed coprime with 26 so we know that $a = 15$

Popping that back into any of the formulas (we pick the first one because it is the lowest multiplier)

$$(15 \times 5 + b)\ mod\ 26 = 12$$
$$(75 + b)\ mod\ 26 = 12$$

We can then subtract 75 from both sides

$$(75 + b)\ mod\ 26 - 75 = (12 - 75)\ mod\ 26$$
$$b\ mod\ 26 = -63\ mod\ 26$$

Taking the -63 we can quickly add 26 until we get in the 0-25 range (-37, -11, 15)

$$b \; mod \; 26 = 15$$

And we see that $b = 15$

4)

VNG JOQ DM GHWLJVODC OU VNG BCDEFGHIG,

THE AIM OF EDUCATION IS THE KNOWLEDGE,

CDV DM MJLVU, KWV DM XJFWGU

NOT OF FACTS, BUT OF VALUES.

K1	**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**
Frequency		1	3	6	1	2	6	2	1	4	1	2	4	2	3		1				3	6	3	1		
Replacement	Z	K	N	O	W	L	E	D	G	A	B	C	F	H	I	J	M	P	Q	R	S	T	U	V	X	Y

5) XC BV IE GU QE NN NV

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

$$\begin{pmatrix} B & F \\ O & X \end{pmatrix}\begin{pmatrix} F \\ O \end{pmatrix} \equiv \begin{pmatrix} 1 & 5 \\ 14 & 23 \end{pmatrix}\begin{pmatrix} 5 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 1 \times 5 + 5 \times 14 \\ 14 \times 5 + 23 \times 14 \end{pmatrix} \equiv \begin{pmatrix} 75 \\ 392 \end{pmatrix} mod \; 26 \equiv \begin{pmatrix} 23 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} X \\ C \end{pmatrix}$$

$$\begin{pmatrix} B & F \\ O & X \end{pmatrix}\begin{pmatrix} U \\ R \end{pmatrix} \equiv \begin{pmatrix} 1 & 5 \\ 14 & 23 \end{pmatrix}\begin{pmatrix} 20 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 1 \times 20 + 5 \times 17 \\ 14 \times 20 + 23 \times 17 \end{pmatrix} \equiv \begin{pmatrix} 105 \\ 671 \end{pmatrix} mod \; 26 \equiv \begin{pmatrix} 1 \\ 21 \end{pmatrix} \equiv \begin{pmatrix} B \\ V \end{pmatrix}$$

$$\begin{pmatrix} B & F \\ O & X \end{pmatrix}\begin{pmatrix} M \\ U \end{pmatrix} \equiv \begin{pmatrix} 1 & 5 \\ 14 & 23 \end{pmatrix}\begin{pmatrix} 12 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} 1 \times 12 + 5 \times 20 \\ 14 \times 12 + 23 \times 20 \end{pmatrix} \equiv \begin{pmatrix} 112 \\ 628 \end{pmatrix} mod \; 26 \equiv \begin{pmatrix} 8 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} I \\ E \end{pmatrix}$$

$$\begin{pmatrix} B & F \\ O & X \end{pmatrix}\begin{pmatrix} S \\ I \end{pmatrix} \equiv \begin{pmatrix} 1 & 5 \\ 14 & 23 \end{pmatrix}\begin{pmatrix} 18 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 1 \times 18 + 5 \times 8 \\ 14 \times 18 + 23 \times 8 \end{pmatrix} \equiv \begin{pmatrix} 58 \\ 436 \end{pmatrix} mod \; 26 \equiv \begin{pmatrix} 6 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} G \\ U \end{pmatrix}$$

$$\begin{pmatrix} B & F \\ O & X \end{pmatrix}\begin{pmatrix} C \\ I \end{pmatrix} \equiv \begin{pmatrix} 1 & 5 \\ 14 & 23 \end{pmatrix}\begin{pmatrix} 2 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 1 \times 2 + 5 \times 8 \\ 14 \times 2 + 23 \times 8 \end{pmatrix} \equiv \begin{pmatrix} 42 \\ 212 \end{pmatrix} mod \; 26 \equiv \begin{pmatrix} 16 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} Q \\ E \end{pmatrix}$$

$$\begin{pmatrix} B & F \\ O & X \end{pmatrix}\begin{pmatrix} A \\ N \end{pmatrix} \equiv \begin{pmatrix} 1 & 5 \\ 14 & 23 \end{pmatrix}\begin{pmatrix} 0 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 1 \times 0 + 5 \times 13 \\ 14 \times 0 + 23 \times 13 \end{pmatrix} \equiv \begin{pmatrix} 65 \\ 299 \end{pmatrix} mod \; 26 \equiv \begin{pmatrix} 13 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} N \\ N \end{pmatrix}$$

$$\begin{pmatrix} B & F \\ O & X \end{pmatrix}\begin{pmatrix} S \\ Z \end{pmatrix} \equiv \begin{pmatrix} 1 & 5 \\ 14 & 23 \end{pmatrix}\begin{pmatrix} 18 \\ 25 \end{pmatrix} \equiv \begin{pmatrix} 1 \times 18 + 5 \times 25 \\ 14 \times 18 + 23 \times 25 \end{pmatrix} \equiv \begin{pmatrix} 143 \\ 827 \end{pmatrix} mod \; 26 \equiv \begin{pmatrix} 13 \\ 21 \end{pmatrix} \equiv \begin{pmatrix} N \\ V \end{pmatrix}$$

6) INB HLG QYG DLB MCR

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

$$\begin{pmatrix} D & O & W \\ E & B & L \\ I & N & K \end{pmatrix}\begin{pmatrix} S \\ T \\ A \end{pmatrix} \equiv \begin{pmatrix} 3 & 14 & 22 \\ 4 & 1 & 11 \\ 8 & 13 & 10 \end{pmatrix}\begin{pmatrix} 18 \\ 19 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 3 \times 18 + 14 \times 19 + 22 \times 0 \\ 4 \times 18 + 1 \times 19 + 11 \times 0 \\ 8 \times 18 + 13 \times 19 + 10 \times 0 \end{pmatrix} \equiv \begin{pmatrix} 320 \\ 91 \\ 391 \end{pmatrix} mod \; 26 \equiv \begin{pmatrix} 8 \\ 13 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} I \\ N \\ B \end{pmatrix}$$

$$\begin{pmatrix} D & O & W \\ E & B & L \\ I & N & K \end{pmatrix}\begin{pmatrix} G \\ C \\ O \end{pmatrix} \equiv \begin{pmatrix} 3 & 14 & 22 \\ 4 & 1 & 11 \\ 8 & 13 & 10 \end{pmatrix}\begin{pmatrix} 17 \\ 8 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 3 \times 17 + 14 \times 8 + 22 \times 13 \\ 4 \times 17 + 1 \times 8 + 11 \times 13 \\ 8 \times 17 + 13 \times 8 + 10 \times 13 \end{pmatrix} \equiv \begin{pmatrix} 449 \\ 219 \\ 370 \end{pmatrix} mod \; 26 \equiv \begin{pmatrix} 7 \\ 11 \\ 6 \end{pmatrix} \equiv \begin{pmatrix} H \\ L \\ G \end{pmatrix}$$

$$\begin{pmatrix} D & O & W \\ E & B & L \\ I & N & K \end{pmatrix}\begin{pmatrix} N \\ T \\ E \end{pmatrix} \equiv \begin{pmatrix} 3 & 14 & 22 \\ 4 & 1 & 11 \\ 8 & 13 & 10 \end{pmatrix}\begin{pmatrix} 6 \\ 2 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 3 \times 6 + 14 \times 2 + 22 \times 14 \\ 4 \times 6 + 1 \times 2 + 11 \times 14 \\ 8 \times 6 + 13 \times 2 + 10 \times 14 \end{pmatrix} \equiv \begin{pmatrix} 354 \\ 180 \\ 214 \end{pmatrix} mod\ 26 \equiv \begin{pmatrix} 16 \\ 24 \\ 6 \end{pmatrix} \equiv \begin{pmatrix} Q \\ Y \\ G \end{pmatrix}$$

$$\begin{pmatrix} D & O & W \\ E & B & L \\ I & N & K \end{pmatrix}\begin{pmatrix} R \\ I \\ N \end{pmatrix} \equiv \begin{pmatrix} 3 & 14 & 22 \\ 4 & 1 & 11 \\ 8 & 13 & 10 \end{pmatrix}\begin{pmatrix} 13 \\ 19 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 3 \times 13 + 14 \times 19 + 22 \times 4 \\ 4 \times 13 + 1 \times 19 + 11 \times 4 \\ 8 \times 13 + 13 \times 19 + 10 \times 4 \end{pmatrix} \equiv \begin{pmatrix} 393 \\ 115 \\ 391 \end{pmatrix} mod\ 26 \equiv \begin{pmatrix} 3 \\ 11 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} D \\ L \\ B \end{pmatrix}$$

$$\begin{pmatrix} D & O & W \\ E & B & L \\ I & N & K \end{pmatrix}\begin{pmatrix} S \\ T \\ Z \end{pmatrix} \equiv \begin{pmatrix} 3 & 14 & 22 \\ 4 & 1 & 11 \\ 8 & 13 & 10 \end{pmatrix}\begin{pmatrix} 18 \\ 19 \\ 25 \end{pmatrix} \equiv \begin{pmatrix} 3 \times 18 + 14 \times 19 + 22 \times 25 \\ 4 \times 18 + 1 \times 19 + 11 \times 25 \\ 8 \times 18 + 13 \times 19 + 10 \times 25 \end{pmatrix} \equiv \begin{pmatrix} 870 \\ 366 \\ 641 \end{pmatrix} mod\ 26 \equiv \begin{pmatrix} 12 \\ 2 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} M \\ C \\ R \end{pmatrix}$$