Science Olympiad — 2024 Brown Invitation Division C

Timed Question **[200 points]** Decode this Aristocrat, which contains a quote by Edward Chapin. When you have solved it, raise your hand so that the time can be recorded and the solution checked.

G EOZK AGV VKTKO IOKEH GRJZE MUH LSGQK UV EMK YJOSN,
A TRUE MAN NEVER FRETS ABOUT HIS PLACE IN THE WORLD,

RZE CZHE HSUNKH UVEJ UE RD EMK BOGTUEGEUJV JI MUH
BUT JUST SLIDES INTO IT BY THE GRAVITATION OF HIS

VGEZOK, GVN HYUVBH EMKOK GH KGHUSD GH G HEGO.
NATURE, AND SWINGS THERE AS EASILY AS A STAR.

	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	2	1	2	14		13	12	2	5	12	1	5	3	8		1	3	4	2	10	8			2	5
Replacement	M	G	J	Y	T	Z	A	S	F	O	E	P	H	D	R	X	C	B	L	V	I	N	K	Q	W	U

1) **[100 points]** Here is a quote encoded using the Porta cipher. Decrypt this quote, given that the key word is “Fame”.

F	A	M	E	F	A	M	E	F	A	M	E	F	A	M	E
T	I	X	C	J	J	T	N	N	V	M	P	S	B	I	C
E	**V**	**E**	**R**	**Y**	**W**	**A**	**L**	**L**	**I**	**S**	**A**	**D**	**O**	**O**	**R**

2) **[150 points]** Decrypt this quote by John Wooden that was encoded using an Aristocrat Cipher.

MJE’Z UWZ CRLZ OJB HLEEJZ MJ VEZWYTWYW CVZR OJB HLE
DON’T LET WHAT YOU CANNOT DO INTERFERE WITH YOU CAN

MJ
DO

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

3) **[200 points]** Decode this quote by Woody Allen that was encoded using a Nihilist Cipher. The Polybius Key is “up” and the key is “fame”.

45	44	58	47	68	67
E	**I**	**G**	**H**	**T**	**Y**

46	44	66	28	56	57	68
P	**E**	**R**	**C**	**E**	**N**	**T**

54	57
O	**F**

66	34	28	49	44	67	57
S	**U**	**C**	**C**	**E**	**S**	**S**

65	66
I	**S**

67	38	75	74	54	48	58
S	**H**	**O**	**W**	**I**	**N**	**G**

33	35
U	**P**

4) **[600 points]** Solve this K1 Aristocrat, which is an encrypted quote from Jane Austen’s *Pride and Prejudice.* Report the keyword of the K2 cipher to recieve credit for this question. Only your keyword will be graded. Writing out the entire decoded quote is not necessary and purely for personal convenience.

G NGBZ’T DOGEDFGUDPF DT WCSZ SGQDB; DU LVOQT JSPO

A LADY’S IMAGINATION IS VERY RAPID; IT JUMPS FROM

GBODSGUDPF UP NPWC, JSPO NPWC UP OGUSDOPFZ DF G

ADMIRATION TO LOVE, FROM LOVE TO MATRIMONY IN A

OPOCFU.

MOMENT.

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		3	4	10	1	6	9			2		1		3	9	10	2		6	3	7	1	3			3
Replacement	Z	D	E	I	G	N	A	B	C	F	H	J	K	L	M	O	P	Q	R	S	T	U	V	W	X	Y

5) **[250 points]** Decode this quote by Ralph Waldo Emerson that has been encoded using a Baconian cipher

✸✵❉✵✸☆✸✵❉☆✸✵❉✵✸☆✸✵✸✵❉✵❉☆✸☆✸☆✸✵✸✵✸✵✸✵❉✵❉✵✸☆✸☆✸✵❉✵✸✵❉✵✸
AABAABAABBAABAABAAAABABBABABAAAAAAAABABAABABAABAAABAA

E V E R Y W A L L I S

✵❉✵✸✵✸✵✸✵✸☆❉✵❉☆✸☆✸☆❉✵❉☆✸✵✸✵
ABAAAAAAAABBABBABABBABBAAAA

A D O O R

Every wall is a door

The A letters are represented by '<p><span style="background-color:rgb(211,214,219);color:rgb(0,0,0);">✸✵</span></p>' and the B letters by '<p><span style="background-color:rgb(211,214,219);color:rgb(0,0,0);">❉☆</span></p>'

6) **[300 points]** Decode this quote by Will Ferrell that an intern tried to encode using a K2 Aristocrat Cipher, but she forgot how to spell and ended up spelling some words wrong.

ADENQD XNT LZQX Z ODQRNM, XNT RGNTC EHQRS LZJ SGDL
BEFORE YOU MARY A PERSON, YOU SHOUD FIRST MAK THEM

TRD Z BNLOTSDQ VHSG RKNV HMSDQMDS SN RDZ VGN SGDX
USE A COMPUTER WITH SLOW INTERNET TO SEA WHO THEY

QDKKX ZQD.
RELLY ARE.

Replacement	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
K2	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	1	1	12	2		5	3		1	3	4	3	9	2		8	6	8	5		3		5		6

7) **[350 points]** A quote by Klaus Hargreeves from *The Umbrella Academy* has been encoded using the Fractionated Morse Cipher for you to decode. You are told that the quote ends with `IDIOT`.

```
 I  Q  N  A  Y  O  J  G
−●−−×−−−×●●−××●−×●−●×●××
Y    O   U  / A  R   E/

 H  U  B  E  J  M  D  O  F  F  J  S  F  N  N  G
−●●×●×●−−●×●−●×●●×●●●−×●●×−●×−−●××●●●×−−−×−−×●××
D   E P    R   I  V    I  N  G  / S   O   M  E/

 D  O  E  H  T  M  C  K  U  W  O  P
●●●−×●●×●−●●×●−●●×●−×−−●×●××−−−×●●−●
V    I  L    L    A  G   E/ O   F

 Z  S  M  E  E  J  S  V  E  F  N  R
××−×●●●●×●×●●×●−●××●●×−●●×●●×−−−×−××
/ T H    E I  R  / I  D   I  O    T
```

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

How to solve

With the crib of Idiot mapped to the ciphertext S V E F N we now know the mapping of 5 characters. Since we are told the mapping of SVEFN ciphertext, we can build the following table:

It is known that `V` maps to ×−●

The mapping of the letters between `V` and `Z` are now known because the number of unknowns exactly matches the distance between the letters.

It is known that `S` maps to ×●●

The mapping of the letters between `S` and `V` are now known because the number of unknowns exactly matches the distance between the letters.

It is known that `N` maps to —×

Fill in possibilities between `N` and `S`.

It is known that `F` maps to ●×−

Fill in possibilities between `F` and `N`.

It is known that `E` maps to ●×●

The mapping of the letters between `E` and `F` are now known because the number of unknowns exactly matches the distance between the letters.

Replacement							E	F							N				S	T	U	V	W	X	Y	Z
Morse fraction	● ● ●	● ● −	● ● ×	● − ●	● − −	● − ×	● × ●	● × −	● × ×	− ● ●	− ● −	− ● ×	− − ●	− − −	− − ×	− × ●	− × −	− × ×	× ● ●	× ● −	× ● ×	× − ●	× − −	× − ×	× × ●	× × −

We can approximate the keyword length to be around 2. Based on what is known from the replacement table, the remaining possible mappings are:

Possibilities	A,B C,D G,H I,J K,L M,O P,Q R	A,B C,D G,H I,J K,L M,O P,Q R	A,B C,D G,H I,J K,L M,O P,Q R	A,B C,D G,H I,J K,L M,O P,Q R	A,B C,D G,H I,J K,L M,O P,Q R	A,B C,D G,H I,J K,L M,O P,Q R	**E**	**F**	G,H	H,I	I,J	J,K	K,L	L,M	**N**	O,P	P,Q	Q,R	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Morse fraction	● ● ●	● ● –	● ● ×	● – ●	● – –	● – ×	● × ●	● × –	● × ×	– ● ●	– ● –	– ● ×	– – ●	– – –	– – ×	– × ●	– × –	– × ×	× ● ●	× ● –	× ● ×	× – ●	× – –	× – ×	× × ●	× × –

Based on that information we can map the cipher text to:

```
 I Q N A Y O J G
?? ?  ––×●? ××●?  ?? ●
```

```
 H U B E J M D O F F J S F N N G
?  ×●×●? ●×●?? ?? ●? ?  ●×–●×–?? ×●●●×–––×––×●
   E              N    S  O M
```

```
 D O E H T M C K U W O P
●? ?  ●×●?  ×●–?? ●? ?? ×●××––?  ?
                 E /
```

```
 Z S M E E J S V E F N R
××–×●●?? ●×●●×●?? ×●●×–●●×●●×–––×?
/ T     I    I D  I O
```

At this point in time, 14 ciphertext characters still need to be mapped.

Look for an unknown mapping BEFORE a **2** morse digit fragment to eliminate invalid morse sequences and reduce the possible mappings for the letter. We find cipher text letter `Q` before a known morse fragment of —×. Valid morse character sequence that end with —× are: —, ●—, ——, ●——, –●—, ●●●—, ●●——, ●———, ————. Combining this list with what `Q` can possibly be... If `Q` maps to ●●●, it would yield a number in the plain-text, so we will elminate it for now. If `Q` maps to ●●–, it would yield a number in the plain-text, so we will elminate it for now. `Q` might be ●●×. If `Q` maps to ●—, it would yield a number in the plain-text, so we will elminate it for now. `Q` might be ●–×. `Q` might be –×–. `Q` might be –××.

Look for an unknown mapping AFTER a **2** morse digit fragment to eliminate invalid morse sequences and reduce the possible mappings for the letter. We find cipher text letter `M` after a known morse fragment of ×●– . Valid morse character sequences that start with ×●– are: ●–, ●–●, ●—, ●–●●, ●—●, ●——, ●———. Combining this list with what `M` can possibly be... `M` might be ●●×. If `M` maps to ——, it would yield a number in the plain-text, so we will elminate it for now. That leaves one possibility for `M`, which is this ●●×.

The letter `M` is likely in the keyword

It is known that `L` maps to ——

Fill in possibilities between `L` and `N`.

The updated table containing possible mappings is:

Possibilities	A,B C,D O,P Q,R	A,B C,D O,P Q,R	**M**	A,B C,D O,P Q,R	A,B C,D O,P Q,R	A,B C,D O,P Q,R	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**N**	O,P	P,Q	Q,R	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Morse fraction	● ● ●	● ● –	● ● ×	● – ●	● – –	● – ×	● × ●	● × –	● × ×	– ● ●	– ● –	– ● ×	– – ●	– – –	– – ×	– × ●	– × –	– × ×	× ● ●	× ● –	× ● ×	× – ●	× – –	× – ×	× × ●	× × –

Based on that information we can map the cipher text as:

```
 I Q N A Y O J G
–●–?  ––×●? ××●?  –●×●××
```

```
                     E/

 H  U  B  E  J  M  D  O  F  F  J  S  F  N  N  G
–●●×●×●? ●×●–●×●●×●? ?  ●×–●×––●××●●●×–––×––×●××
D   E      R   I          N  G   / S   O   M   E/

 D  O  E  H  T  M  C  K  U  W  O  P
●? ?  ●×●–●●×●–●●×●? ––●×●××––?  ?
        L    L           E /

 Z  S  M  E  E  J  S  V  E  F  N  R
××–×●●●●×●×●●×●–●××●●×–●●×●●×–––×?
/ T H    E I  R   / I  D   I  O
```

At this point in time, 8 ciphertext characters still need to be mapped.

Look for an unknown mapping AFTER a **2** morse digit fragment to eliminate invalid morse sequences and reduce the possible mappings for the letter. We find cipher text letter `O` after a known morse fragment of ×— . Valid morse character sequences that start with ×— are: —, —●, ——, —●●, —●–, —●●●, ——●●, ———●, ————. Combining this list with what `O` can possibly be... If `O` maps to ●●●, it would yield a number in the plain-text, so we will elminate it for now. `O` might be ●–×. `O` might be –×●.

Try some of the possibilities... We know `O` can be one of ●–×, –×●.

Trying ●–× for `O`, we'd get:

```
 I  Q  N  A  Y  O  J  G
–●––  ––×●? ××●●–×–●×●××
              U   N  E/

 H  U  B  E  J  M  D  O  F  F  J  S  F  N  N  G
–●●×●×●? ●×●–●×●●×●? ●–×●×–●×––●××●●●×–––×––×●××
D   E      R   I        E N  G   / S   O   M   E/

 D  O  E  H  T  M  C  K  U  W  O  P
●? ●–×●×●–●●×●–●●×●? ––●×●××––●–×?
      E L    L           E / Q

. . .
```

That guess does not look too promising.

Trying –×● for `O`, we'd get:

```
 I  Q  N  A  Y  O  J  G
–●––  ––×●? ××●–×●–●×●××
              A  R   E/

 H  U  B  E  J  M  D  O  F  F  J  S  F  N  N  G
–●●×●×●? ●×●–●×●●×●? –×●●×–●×––●××●●●×–––×––×●××
D   E      R   I       I  N  G   / S   O   M   E/

 D  O  E  H  T  M  C  K  U  W  O  P
●? –×●●×●–●●×●–●●×●? ––●×●××–––×●?
     I  L    L           E / O

. . .
```

That makes sense. Update our table with the mapping of `O` to –×●.

It is known that `O` maps to –×●

Fill in possibilities between `O` and `S`.

It is known that `K` maps to —●

The mapping of the letters between `K` and `L` are now known because the number of unknowns exactly matches the distance between the letters.

It is known that `J` maps to −●×

The mapping of the letters between `J` and `K` are now known because the number of unknowns exactly matches the distance between the letters.

It is known that `I` maps to −●−

The mapping of the letters between `I` and `J` are now known because the number of unknowns exactly matches the distance between the letters.

The updated table containing possible mappings is:

Possibilities	A,B C,D P,Q R	A,B C,D P,Q R	**M**	A,B C,D P,Q R	A,B C,D P,Q R	A,B C,D P,Q R	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**N**	**O**	P,Q	Q,R	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Morse fraction	● ● ●	● ● −	● ● ×	● − ●	● − −	● − ×	● × ●	● × −	● × ×	− ● ●	− ● −	− ● ×	− − ●	− − −	− − ×	− × ●	− × −	− × ×	× ● ●	× ● −	× ● ×	× − ●	× − −	× − ×	× × ●	× × −

Based on that information we can map the cipher text as:

```
 I  Q  N  A  Y  O  J  G
−●−?  −−×●? ××●−×●−●×●××
              A  R   E/
```

```
 H  U  B  E  J  M  D  O  F  F  J  S  F  N  N  G
−●●×●×●? ●×●−●×●●×●? −×●●×−●×−−●××●●●×−−−×−−×●××
D   E      R   I       I  N  G   / S   O   M  E/
```

```
 D  O  E  H  T  M  C  K  U  W  O  P
●? −×●●×●−●●×●−●●×●? −−●×●××−−−×●?
     I  L    L           E / O
```

```
 Z  S  M  E  E  J  S  V  E  F  N  R
××−×●●●●×●×●●×●−●××●●×−●●×●●×−−−×?
/ T H    E I  R   / I  D   I  O
```

At this point in time, 7 ciphertext characters still need to be mapped.
Try some of the possibilities... We know `Q` can be one of ●●×, ●−×, −×−, −××.

Trying ●●× for `Q`, we'd get:

```
 I  Q  N  A  Y  O  J  G
−●−●●×−−×●? ××●−×●−●×●××
/ M       A  R   E/
```

...

That guess does not look too promising.

Trying ●−× for `Q`, we'd get:

```
 I  Q  N  A  Y  O  J  G
−●−●−×−−×●? ××●−×●−●×●××
/ M       A  R   E/
```

...

That guess does not look too promising.

Trying −×− for `Q`, we'd get:

```
 I  Q  N  A  Y  O  J  G
−●−−×−−−×●? ××●−×●−●×●××
Y    O        A  R   E/
```

. . .

That makes sense. Update our table with the mapping of `Q` to −×−.

It is known that `R` maps to −××

The mapping of the letters between `R` and `S` are now known because the number of unknowns exactly matches the distance between the letters.

It is known that `Q` maps to −×−

The mapping of the letters between `Q` and `R` are now known because the number of unknowns exactly matches the distance between the letters.

The updated table containing possible mappings is:

Possibilities	A,B C,D P	A,B C,D P	M	A,B C,D P	A,B C,D P	A,B C,D P	E	F	G	H	I	J	K	L	N	O	Q	R	S	T	U	V	W	X	Y	Z
Morse fraction	● ● ●	● ● −	● ● ×	● − ●	● − −	● − ×	● × ●	● × −	● × ×	− ● ●	− ● −	− ● ×	− − ●	− − −	− − ×	− × ●	− × −	− × ×	× ● ●	× ● −	× ● ×	× − ●	× − −	× − ×	× × ●	× × −

Based on that information we can map the cipher text as:

```
 I  Q  N  A  Y  O  J  G
−●−−×−−−×●? ××●−×●−●×●××
Y    O        A  R   E/

 H  U  B  E  J  M  D  O  F  F  J  S  F  N  N  G
−●●×●×●? ●×●−●×●●×●? −×●●×−●×−−●××●●●×−−−×−−×●××
D   E      R   I       I  N  G   / S   O   M  E/

 D  O  E  H  T  M  C  K  U  W  O  P
●? −×●●×●−●●×●−●●×●? −−●×●××−−−×●●?
     I  L    L           E / O

 Z  S  M  E  E  J  S  V  E  F  N  R
××−×●●●●×●×●●×●−●××●●×−●●×●●×−−−×−××
/ T H    E I  R   / I  D   I  O   T/
```

At this point in time, 5 ciphertext characters still need to be mapped. There are no more automated solving techniques, so you need to do some trial and error with the remaining unknowns. Please feel free to submit an issue with the example so we can improve this.

8) **[450 points]** Decrypt this K1 patristocrat, which is a quote by Oscar Wilde

```
TPNFD BVTFI BQQJO FTTXI FSFWF SUIFZ HPPUI FSTXI
SOMEC AUSEH APPIN ESSWH EREVE RTHEY GOOTH ERSWH

FOFWF SUIFZ HP
ENEVE RTHEY GO
```

Some cause happiness wherever they go; others whenever they go

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		2		1		12		2	6	1				1	2	4	2		4	5	3	1	2	2		2
Replacement	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

9) **[250 points]** Decode this quote by Gina Linetti from *Brooklyn Nine* which has been encoded using a Fractionated Morse Cipher. You are told that the word “tweet” appears somewhere in the quote.

```
 B  A  I  B  V  G  G  Z  S  P  L  L  W  V  O
●●×●●–●××●●××–●●×●●×●××–×●●–×●–●×–●××––×–●––×
I  F  / I / D  I  E/ T U  R  N / M Y  /

 X  E  U  H  S  I  B  L  Q  O  T  Z  C  W  Q  O  K
×–×●––×●×●×–×●●●××●●×–●×–×–––××●–××–●●●×–––×–––×–●–
 T W  E E T S / I  N  T O / A / B  O  O  K
```

Replacement	C	A	B	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Morse fraction	● ● ●	● ● –	● ● ×	● – ●	● – –	● – ×	● × ●	● × –	● × ×	– ● ●	– ● –	– ● ×	– – ●	– – –	– – ×	– × ●	– × –	– × ×	× ● ●	× ● –	× ● ×	× – ●	× – –	× – ×	× × ●	× × –

How to solve

With the crib of tweet mapped to the ciphertext X E U H we now know the mapping of 4 characters. Since we are told the mapping of XEUH ciphertext, we can build the following table:

At least 5 Hint Digits are needed to automatically generate a solution

10) **[500 points]** Decrypt this K1 xenocrypt, which is a quote from the movie *Coco* about the future

```
ÑBEJF JCB B SFHBMBSNF NJ GVUVSP. NF DPSSFTQPÑEJB B
NADIE IBA A REGALARME MI FUTURO. ME CORRESPONDIA A

NJ FTGPSABSNF QPS NJ TVFOP, BHBSSBSMP DPÑ GVFSAB Z
MI ESFORZARME POR MI SUEÑO, AGARRARLO CON FUERZA Y

DPÑWFSUJSMP FÑ SFBMJEBE
CONVERTIRLO EN REALIDAD
```

K1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	2	14	1	3	4	12	3	2		8			4	6	5	1	10	2		15	3	2	4	1			1
Replacement	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

11) **[200 points]** Decode this Baconian Cipher that contains a quote by Benjamin Franklin.

♢♦♠♥♦♥♦♢♥♦♥♠♦♢♥♦♠♥♢♦♥♦♥♠♢♦♠♢♥♠♦♢♠♥♦♥♦♢♥♦♥♠♦♥♦♢♥♦♥♠♦♥♦
BABAAAABAAABABAABABAAAABBABBABABBAAAABAAABAAABAAABAAA

W E L L D O N E I S B

♥♢♦♥♠♦♥♢♦♥♠♦♢♥♦♠♥♦♥♢♦♥♠♦♥♦♥♢♦♥♠♦♥♦♢♠♢♥♦♥♦♥♦♠♢♥♦♠♥♢♦♥♦
ABAABAABAABABAABAAABAABAAAABAABAAABBBAAAAAABBAABABAAA

E T T E R T H A N W

♥♠♦♥♦♢♥♠♦♥♢♦♠♥♢♦♥♦♠♥♦♥♦♥♦♢♥♦♥♦♥♦♠♢
ABAAABABAABABABAAABAAAAAABAAAAAABB

E L L S A I D

Well done is better than well said.

The A letters are represented by '<p><span style="background-color:rgb(211,214,219);color:rgb(0,0,0);">♦♥</span></p>' and the B letters by '<p><span style="background-color:rgb(211,214,219);color:rgb(0,0,0);">♢♠</span></p>'

12) **[200 points]** Decode this quote by Vincent Van Gogh, which has a crib word of "passion"

WAISH OXOTE SARXU HOINE XIRDA TBMDR PNFOX LEFOO

DX

Answer: _**I WOULD RATHER DIE OF PASSION THAN OF BOREDOM.**_

13) **[250 points]** The following cryptarithm provides the key to decoding the values `8238244184`. What do they decode to?

Values to decode for solution

8	2	3	8	2	4	4	1	8	4
R	E	P	R	E	S	S	O	R	S

Cryptarithm formula

```
     Y E A R S
     5 2 0 8 4
  P E R S O N
+ 3 2 8 4 1 6
  P E R S O N
+ 3 2 8 4 1 6
-------------
  C A R B O N
  7 0 8 9 1 6  YEARS+PERSON+PERSON=CARBON
```

	0	1	2	3	4	5	6	7	8	9
A										
B										
C										
E										
N										
O										
P										
R										
S										
Y										

14) **[250 points]** Decrypt this quote from the 2023 Barbie movie about motherhood encrypted using a K2 alphabet.

VDLNS GDQRR SZMCR SHKKR NNTQC ZTFGS DQRBZ MKNNJ
WEMOT HERSS TANDS TILLS OOURD AUGHT ERSCA NLOOK

AZBJS NRDDG NVEZQ SGDXG ZUDBN LD
BACKT OSEEH OWFAR THEYH AVECO ME

We mothers stand still so our daughters can look back to see how far they have come.

Replacement	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
K2	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	2	8	1	1	5	1		2	3	2	2	8			4	6	6	2	1	2		1		6

15) **[200 points]** Decrypt this quote from *The X-Files* that has been encoded using the Complete Columnar cipher.

HHTTT TTSEE IHROR UUE

Answer: _**THE TRUTH IS OUT THERE.**_

16) **[250 points]** Decrypt this hill cipher, which is the name of a song from a famous musical, using the given key word of “TEST”.

$$\begin{pmatrix} T & E \\ S & T \end{pmatrix} \equiv \begin{pmatrix} 19 & 4 \\ 18 & 19 \end{pmatrix}$$

U	K	S	V	W	R	T	U	F	C	K	X
S	**E**	**I**	**Z**	**E**	**T**	**H**	**E**	**D**	**A**	**Y**	**Z**

How to solve

The inverse of the matrix can be computed using the formula:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

In this case we have to compute $(ad - bc)^{-1}$ Using modular multiplicative inverse (https://en.wikipedia.org/wiki/Modular_multiplicative_inverse) math

$$\begin{pmatrix} 19 & 4 \\ 18 & 19 \end{pmatrix}^{-1} = (19 * 19 - 4 * 18)^{-1} \begin{pmatrix} 19 & -4 \\ -18 & 19 \end{pmatrix}$$

We start by finding the modulo 26 value of the determinent:

$$(19 * 19 - 4 * 18) \mod 26 = 289 \mod 26 = 3$$

Looking up 3 in the table supplied with the test (or by computing it with the Extended Euclidean algorithm (https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm)) we find that it is 9 which we substitute into the formula to compute the matrix:

$$(19 * 19 - 4 * 18)^{-1} \begin{pmatrix} 19 & -4 \\ -18 & 19 \end{pmatrix} \equiv 9 \begin{pmatrix} 19 & -4 \\ -18 & 19 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 9 * 19 & 9 * -4 \\ 9 * -18 & 9 * 19 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 171 & -36 \\ -162 & 171 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 171 \mod 26 & -36 \mod 26 \\ -162 \mod 26 & 171 \mod 26 \end{pmatrix} \equiv \begin{pmatrix} 15 & 16 \\ 20 & 15 \end{pmatrix}$$

With the inverse matrix we can now decode

$$\begin{pmatrix} P & Q \\ U & P \end{pmatrix} * \begin{pmatrix} U \\ K \end{pmatrix} \equiv \begin{pmatrix} 15 & 16 \\ 20 & 15 \end{pmatrix} * \begin{pmatrix} 20 \\ 10 \end{pmatrix} \equiv \begin{pmatrix} 15 * 20 + 16 * 10 \\ 20 * 20 + 15 * 10 \end{pmatrix} \equiv \begin{pmatrix} 460 \\ 550 \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 4 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} S \\ E \end{pmatrix}$$

$$\begin{pmatrix} P & Q \\ U & P \end{pmatrix} * \begin{pmatrix} S \\ V \end{pmatrix} \equiv \begin{pmatrix} 15 & 16 \\ 20 & 15 \end{pmatrix} * \begin{pmatrix} 18 \\ 21 \end{pmatrix} \equiv \begin{pmatrix} 15 * 18 + 16 * 21 \\ 20 * 18 + 15 * 21 \end{pmatrix} \equiv \begin{pmatrix} 606 \\ 675 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 25 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} I \\ Z \end{pmatrix}$$

$$\begin{pmatrix} P & Q \\ U & P \end{pmatrix} * \begin{pmatrix} W \\ R \end{pmatrix} \equiv \begin{pmatrix} 15 & 16 \\ 20 & 15 \end{pmatrix} * \begin{pmatrix} 22 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 15 * 22 + 16 * 17 \\ 20 * 22 + 15 * 17 \end{pmatrix} \equiv \begin{pmatrix} 602 \\ 695 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 19 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} E \\ T \end{pmatrix}$$

$$\begin{pmatrix} P & Q \\ U & P \end{pmatrix} * \begin{pmatrix} T \\ U \end{pmatrix} \equiv \begin{pmatrix} 15 & 16 \\ 20 & 15 \end{pmatrix} * \begin{pmatrix} 19 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} 15 * 19 + 16 * 20 \\ 20 * 19 + 15 * 20 \end{pmatrix} \equiv \begin{pmatrix} 605 \\ 680 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 4 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} H \\ E \end{pmatrix}$$

$$\begin{pmatrix} P & Q \\ U & P \end{pmatrix} * \begin{pmatrix} F \\ C \end{pmatrix} \equiv \begin{pmatrix} 15 & 16 \\ 20 & 15 \end{pmatrix} * \begin{pmatrix} 5 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 15 * 5 + 16 * 2 \\ 20 * 5 + 15 * 2 \end{pmatrix} \equiv \begin{pmatrix} 107 \\ 130 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 0 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} D \\ A \end{pmatrix}$$

$$\begin{pmatrix} P & Q \\ U & P \end{pmatrix} * \begin{pmatrix} K \\ X \end{pmatrix} \equiv \begin{pmatrix} 15 & 16 \\ 20 & 15 \end{pmatrix} * \begin{pmatrix} 10 \\ 23 \end{pmatrix} \equiv \begin{pmatrix} 15 * 10 + 16 * 23 \\ 20 * 10 + 15 * 23 \end{pmatrix} \equiv \begin{pmatrix} 518 \\ 545 \end{pmatrix} \equiv \begin{pmatrix} 24 \\ 25 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} Y \\ Z \end{pmatrix}$$

17) **[300 points]** Solve this Baconian Cipher that contains a quote by Jim Hopper from *Stranger Things.*

£¥฿₴¥£₴¥฿₴¥£฿£฿£₴¥฿£฿₴£฿£฿¥₴£฿£฿¥₴£¥฿£฿₴£฿£฿£¥฿£฿£฿£₴
ABABBABBABBAAAAABBAAABAAAABBAAAABBABAAABAAAAABAAAAAAB

M O R N I N G S A R E

฿£฿£¥฿₴£¥₴฿¥₴£฿£฿£฿£¥฿£₴¥฿₴£฿¥£₴฿£¥฿₴£฿¥£฿£฿₴£฿£฿£฿£฿
AAAABABABBABBAAAAAAABAABBABAABABAABABAABAAAABAAAAAAAA

F O R C O F F E E A

¥₴£฿£฿£¥₴฿£฿¥£฿₴¥£₴฿¥₴£฿¥£฿₴£฿£¥฿£฿₴£¥₴฿¥₴¥£฿₴£¥฿£฿£฿
BBAAAAABBAAABAABBABABBAABAABAAABAAABABBABBBAABABAAAAA

N D C O N T E M P L A

£₴฿£¥฿£₴฿£฿£¥₴฿¥£₴¥฿£
ABAABAABAAAABBABABBAA

T I O N

Mornings are for coffee and contemplation.

The A letters are represented by '<p><span style="background-color:rgb(211,214,219);color:rgb(0,0,0);">£฿</span></p>' and the B letters by '<p><span style="background-color:rgb(211,214,219);color:rgb(0,0,0);">¥₴</span></p>'

18) **[250 points]** Decode the following quote which was encoded as a 2x2 Hill Cipher using a keyword of **BIRD**.

$$\begin{pmatrix} B & I \\ R & D \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 \\ 17 & 3 \end{pmatrix}$$

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

How to solve

The inverse of the matrix can be computed using the formula:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

In this case we have to compute $(ad - bc)^{-1}$ Using modular multiplicative inverse (https://en.wikipedia.org/wiki/Modular_multiplicative_inverse) math

$$\begin{pmatrix} 1 & 8 \\ 17 & 3 \end{pmatrix}^{-1} = (1 * 3 - 8 * 17)^{-1} \begin{pmatrix} 3 & -8 \\ -17 & 1 \end{pmatrix}$$

We start by finding the modulo 26 value of the determinent:

$$(1 * 3 - 8 * 17) \mod 26 = -133 \mod 26 = 23$$

Looking up 23 in the table supplied with the test (or by computing it with the Extended Euclidean algorithm (https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm)) we find that it is 17 which we substitute into the formula to compute the matrix:

$$(1 * 3 - 8 * 17)^{-1} \begin{pmatrix} 3 & -8 \\ -17 & 1 \end{pmatrix} \equiv 17 \begin{pmatrix} 3 & -8 \\ -17 & 1 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 17 * 3 & 17 * -8 \\ 17 * -17 & 17 * 1 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 51 & -136 \\ -289 & 17 \end{pmatrix}$$
$$\mod 26 \equiv \begin{pmatrix} 51 \mod 26 & -136 \mod 26 \\ -289 \mod 26 & 17 \mod 26 \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix}$$

With the inverse matrix we can now decode

$$\begin{pmatrix} Z & U \\ X & R \end{pmatrix} * \begin{pmatrix} H \\ Q \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix} * \begin{pmatrix} 7 \\ 16 \end{pmatrix} \equiv \begin{pmatrix} 25 * 7 + 20 * 16 \\ 23 * 7 + 17 * 16 \end{pmatrix} \equiv \begin{pmatrix} 495 \\ 433 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 17 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} B \\ R \end{pmatrix}$$
$$\begin{pmatrix} Z & U \\ X & R \end{pmatrix} * \begin{pmatrix} Q \\ I \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix} * \begin{pmatrix} 16 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 25 * 16 + 20 * 8 \\ 23 * 16 + 17 * 8 \end{pmatrix} \equiv \begin{pmatrix} 560 \\ 504 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 10 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} O \\ K \end{pmatrix}$$
$$\begin{pmatrix} Z & U \\ X & R \end{pmatrix} * \begin{pmatrix} E \\ D \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix} * \begin{pmatrix} 4 \\ 3 \end{pmatrix} \equiv \begin{pmatrix} 25 * 4 + 20 * 3 \\ 23 * 4 + 17 * 3 \end{pmatrix} \equiv \begin{pmatrix} 160 \\ 143 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 13 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} E \\ N \end{pmatrix}$$
$$\begin{pmatrix} Z & U \\ X & R \end{pmatrix} * \begin{pmatrix} I \\ H \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix} * \begin{pmatrix} 8 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 25 * 8 + 20 * 7 \\ 23 * 8 + 17 * 7 \end{pmatrix} \equiv \begin{pmatrix} 340 \\ 303 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 17 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} C \\ R \end{pmatrix}$$
$$\begin{pmatrix} Z & U \\ X & R \end{pmatrix} * \begin{pmatrix} K \\ U \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix} * \begin{pmatrix} 10 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} 25 * 10 + 20 * 20 \\ 23 * 10 + 17 * 20 \end{pmatrix} \equiv \begin{pmatrix} 650 \\ 570 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 24 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} A \\ Y \end{pmatrix}$$
$$\begin{pmatrix} Z & U \\ X & R \end{pmatrix} * \begin{pmatrix} O \\ R \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix} * \begin{pmatrix} 14 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 25 * 14 + 20 * 17 \\ 23 * 14 + 17 * 17 \end{pmatrix} \equiv \begin{pmatrix} 690 \\ 611 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 13 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} O \\ N \end{pmatrix}$$
$$\begin{pmatrix} Z & U \\ X & R \end{pmatrix} * \begin{pmatrix} G \\ W \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix} * \begin{pmatrix} 6 \\ 22 \end{pmatrix} \equiv \begin{pmatrix} 25 * 6 + 20 * 22 \\ 23 * 6 + 17 * 22 \end{pmatrix} \equiv \begin{pmatrix} 590 \\ 512 \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 18 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} S \\ S \end{pmatrix}$$
$$\begin{pmatrix} Z & U \\ X & R \end{pmatrix} * \begin{pmatrix} F \\ J \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix} * \begin{pmatrix} 5 \\ 9 \end{pmatrix} \equiv \begin{pmatrix} 25 * 5 + 20 * 9 \\ 23 * 5 + 17 * 9 \end{pmatrix} \equiv \begin{pmatrix} 305 \\ 268 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 8 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} T \\ I \end{pmatrix}$$
$$\begin{pmatrix} Z & U \\ X & R \end{pmatrix} * \begin{pmatrix} V \\ M \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix} * \begin{pmatrix} 21 \\ 12 \end{pmatrix} \equiv \begin{pmatrix} 25 * 21 + 20 * 12 \\ 23 * 21 + 17 * 12 \end{pmatrix} \equiv \begin{pmatrix} 765 \\ 687 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 11 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} L \\ L \end{pmatrix}$$
$$\begin{pmatrix} Z & U \\ X & R \end{pmatrix} * \begin{pmatrix} K \\ Y \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix} * \begin{pmatrix} 10 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 25 * 10 + 20 * 24 \\ 23 * 10 + 17 * 24 \end{pmatrix} \equiv \begin{pmatrix} 730 \\ 638 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 14 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} C \\ O \end{pmatrix}$$

$$\begin{pmatrix} Z & U \\ X & R \end{pmatrix} * \begin{pmatrix} T \\ V \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix} * \begin{pmatrix} 19 \\ 21 \end{pmatrix} \equiv \begin{pmatrix} 25 * 19 + 20 * 21 \\ 23 * 19 + 17 * 21 \end{pmatrix} \equiv \begin{pmatrix} 895 \\ 794 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 14 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} L \\ O \end{pmatrix}$$

$$\begin{pmatrix} Z & U \\ X & R \end{pmatrix} * \begin{pmatrix} J \\ A \end{pmatrix} \equiv \begin{pmatrix} 25 & 20 \\ 23 & 17 \end{pmatrix} * \begin{pmatrix} 9 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 25 * 9 + 20 * 0 \\ 23 * 9 + 17 * 0 \end{pmatrix} \equiv \begin{pmatrix} 225 \\ 207 \end{pmatrix} \equiv \begin{pmatrix} 17 \\ 25 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} R \\ Z \end{pmatrix}$$

19) **[400 points]** Decode this Aristocrat that contains a quote by Christopher Morley that has been encoded using a K2 alphabet.

PRIMI ZMI PRMII YGAMILYIGPO YG PRI AHHL EYNI:
THERE ARE THREE INGREDIENTS IN THE GOOD LIFE:

EIZMGYGA, IZMGYGA ZGL WIZMGYGA.
LEARNING, EARNING AND YEARNING.

Replacement	Z	C	U	L	I	N	A	R	Y	B	D	E	F	G	H	J	K	M	O	P	Q	S	T	V	W	X
K2	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	5				2		10	2	12			3	7	1	1	4		3					1		7	5