Science Olympiad — Codebusters Test 2019

Timed Question **[200 points]** Decode this aristocrat. The message probably contains the phrase “United States”. When you have solved it, raise your hand so that the time can be recorded and the solution checked.

HVEQGUB INV XUGIVC HIMIVH SGPGIMEZ DASVH FGIN SMUZ
SERVING THE UNITED STATES MILITARY COMES WITH MANY

EVHJAUHGYGPGIGVH MH FVPP MH JEVHHXEV MUC
RESPONSIBILITIES AS WELL AS PRESSURE AND

MDDAXUIMYGPGIZ. NAFVQVE, INV SGPGIMEZ GHU’I OAE
ACCOUNTABILITY. HOWEVER, THE MILITARY ISN’T FOR

VQVEZAUV, YXI GI AOOVEH HA SXDN OAE INAHV FNA HVEQV.
EVERYONE, BUT IT OFFERS SO MUCH FOR THOSE WHO SERVE.

AUV INGUB INMI SXHI YV LUAFU MUC CVMPI FGIN GH INMI
ONE THING THAT MUST BE KNOWN AND DEALT WITH IS THAT

INGH DMEVVE DAXPC YV M PGOV INEVMIVUGUB AUV, MUC
THIS CAREER COULD BE A LIFE THREATENING ONE, AND

INVEV MEV SMUZ AYHIMDPVH AUV SXHI BA INEAXBN
THERE ARE MANY OBSTACLES ONE MUST GO THROUGH

YVOAEVNMUC.
BEFOREHAND.

	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	20	5	7	7	19	6	21	22	30	2		1	21	17	6	10	4		8		20	37		9	7	6
Replacement	O	G	D	C	R	W	I	S	T	P	Z	K	A	H	F	L	V	Q	M	X	N	E	J	U	B	Y

1) **[150 points]** Decode this Atbash cipher.

G	S	R	H		J	F	V	H	G	R	L	M		R	H		K	I	V	G	G	B		H	R	N	K	O	V		L	M	X	V		L	M	V		
T	**H**	**I**	**S**		**Q**	**U**	**E**	**S**	**T**	**I**	**O**	**N**		**I**	**S**		**P**	**R**	**E**	**T**	**T**	**Y**		**S**	**I**	**M**	**P**	**L**	**E**		**O**	**N**	**C**	**E**		**O**	**N**	**E**		

P	M	L	D	H		S	L	D		G	L		H	L	O	E	V		R	G	,		R	H	M	’	G		R	G ?
K	**N**	**O**	**W**	**S**		**H**	**O**	**W**		**T**	**O**		**S**	**O**	**L**	**V**	**E**		**I**	**T**	,		**I**	**S**	**N**	’	**T**		**I**	**T** ?

L	F	G	H	G	Z	M	W	R	M	T		D	L	I	P !
O	**U**	**T**	**S**	**T**	**A**	**N**	**D**	**I**	**N**	**G**		**W**	**O**	**R**	**K** !

2) **[250 points]** Encrypt the following plaintext using the Affine cipher where A is 23 and B is 7.

C	I	P	H	E	R	T	E	X	T		I	S		B	E	L	O	W		T	H	I	S		P	H	R	A	S	E	.
B	**J**	**O**	**M**	**V**	**I**	**C**	**V**	**Q**	**C**		**J**	**F**		**E**	**V**	**A**	**R**	**T**		**C**	**M**	**J**	**F**		**O**	**M**	**I**	**H**	**F**	**V**	.

How to solve

Using the given value of $\mathrm{a} = 23$ and $\mathrm{b} = 7$ we can calcuate using the formula $a * x + b \mod 26$

$$C(2) \rightarrow 2 * 23 + 7 \rightarrow 53 \mod 26 \rightarrow B(1)$$
$$I(8) \rightarrow 8 * 23 + 7 \rightarrow 191 \mod 26 \rightarrow J(9)$$
$$P(15) \rightarrow 15 * 23 + 7 \rightarrow 352 \mod 26 \rightarrow O(14)$$
$$H(7) \rightarrow 7 * 23 + 7 \rightarrow 168 \mod 26 \rightarrow M(12)$$
$$E(4) \rightarrow 4 * 23 + 7 \rightarrow 99 \mod 26 \rightarrow V(21)$$
$$R(17) \rightarrow 17 * 23 + 7 \rightarrow 398 \mod 26 \rightarrow I(8)$$
$$T(19) \rightarrow 19 * 23 + 7 \rightarrow 444 \mod 26 \rightarrow C(2)$$

We already computed for E and know that it is V

$$X(23) \rightarrow 23 * 23 + 7 \rightarrow 536 \mod 26 \rightarrow Q(16)$$

We already computed for T and know that it is C

We already computed for I and know that it is J

$$S(18) \rightarrow 18 * 23 + 7 \rightarrow 421 \mod 26 \rightarrow F(5)$$
$$B(1) \rightarrow 1 * 23 + 7 \rightarrow 30 \mod 26 \rightarrow E(4)$$

We already computed for E and know that it is V

$$L(11) \rightarrow 11 * 23 + 7 \rightarrow 260 \mod 26 \rightarrow A(0)$$
$$O(14) \rightarrow 14 * 23 + 7 \rightarrow 329 \mod 26 \rightarrow R(17)$$
$$W(22) \rightarrow 22 * 23 + 7 \rightarrow 513 \mod 26 \rightarrow T(19)$$

We already computed for T and know that it is C

We already computed for H and know that it is M

We already computed for I and know that it is J

We already computed for S and know that it is F

We already computed for P and know that it is O

We already computed for H and know that it is M

We already computed for R and know that it is I

$$A(0) \rightarrow 0 * 23 + 7 \rightarrow 7 \mod 26 \rightarrow H(7)$$

We already computed for S and know that it is F

We already computed for E and know that it is V

3) **[275 points]** Decrypt the Vigenère cipher below using "Bruce" as the key.

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

U C E	B R U C	E B R U C	-	E B R U	C E B R U	.
G C R	X Z N J	P B J Y T	-	P J B Y	H S D L M	.
M A N	**W I T H**	**L A S E R**	-	**L I K E**	**F O C U S**	.

4) **[250 points]** Solve this aristocrat. As a little hint, the second last word is "three".

ITGQ L SLM L WTFP, LMR PQ YLM QLZ WJE L RLV. CDZ
GIVE A MAN A FISH, AND HE CAN EAT FOR A DAY. BUT

ZQLYP L SLM PJN ZJ WTFP, LMR PQ'AA CQ RQLR JW
TEACH A MAN HOW TO FISH, AND HE'LL BE DEAD OF

SQEYDEV HJTFJMTMI TMFTRQ JW ZPEQQ VQLEF.
MERCURY POISONING INSIDE OF THREE YEARS.

	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	2	5	5	1	1	2	7		14	8	1		7	12	6	3	7		3	5		3	5
Replacement	L	Z	B	U	R	S	V	P	G	O	Q	A	N	W	X	H	E	D	M	I	K	Y	F	J	C	T

5) **[325 points]** Encrypt the message using the Hill cipher. The key is "Nerd".

$$\begin{pmatrix} N & E \\ R & D \end{pmatrix} \equiv \begin{pmatrix} 13 & 4 \\ 17 & 3 \end{pmatrix}$$

S	C	I	E	N	C	E	R	U	L	E	S
I	**A**	**Q**	**S**	**V**	**T**	**Q**	**P**	**S**	**J**	**U**	**S**

How to solve

$$\begin{pmatrix} N & E \\ R & D \end{pmatrix} * \begin{pmatrix} S \\ C \end{pmatrix} \equiv \begin{pmatrix} 13 & 4 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 18 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 13*18+4*2 \\ 17*18+3*2 \end{pmatrix} \equiv \begin{pmatrix} 242 \\ 312 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 0 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} I \\ A \end{pmatrix}$$

$$\begin{pmatrix} N & E \\ R & D \end{pmatrix} * \begin{pmatrix} I \\ E \end{pmatrix} \equiv \begin{pmatrix} 13 & 4 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 8 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 13*8+4*4 \\ 17*8+3*4 \end{pmatrix} \equiv \begin{pmatrix} 120 \\ 148 \end{pmatrix} \equiv \begin{pmatrix} 16 \\ 18 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} Q \\ S \end{pmatrix}$$

$$\begin{pmatrix} N & E \\ R & D \end{pmatrix} * \begin{pmatrix} N \\ C \end{pmatrix} \equiv \begin{pmatrix} 13 & 4 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 13 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 13*13+4*2 \\ 17*13+3*2 \end{pmatrix} \equiv \begin{pmatrix} 177 \\ 227 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 19 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} V \\ T \end{pmatrix}$$

$$\begin{pmatrix} N & E \\ R & D \end{pmatrix} * \begin{pmatrix} E \\ R \end{pmatrix} \equiv \begin{pmatrix} 13 & 4 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 4 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 13*4+4*17 \\ 17*4+3*17 \end{pmatrix} \equiv \begin{pmatrix} 120 \\ 119 \end{pmatrix} \equiv \begin{pmatrix} 16 \\ 15 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} Q \\ P \end{pmatrix}$$

$$\begin{pmatrix} N & E \\ R & D \end{pmatrix} * \begin{pmatrix} U \\ L \end{pmatrix} \equiv \begin{pmatrix} 13 & 4 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 20 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 13*20+4*11 \\ 17*20+3*11 \end{pmatrix} \equiv \begin{pmatrix} 304 \\ 373 \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 9 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} S \\ J \end{pmatrix}$$

$$\begin{pmatrix} N & E \\ R & D \end{pmatrix} * \begin{pmatrix} E \\ S \end{pmatrix} \equiv \begin{pmatrix} 13 & 4 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 4 \\ 18 \end{pmatrix} \equiv \begin{pmatrix} 13*4+4*18 \\ 17*4+3*18 \end{pmatrix} \equiv \begin{pmatrix} 124 \\ 122 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 18 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} U \\ S \end{pmatrix}$$

6) **[350 points]** Decrypt the following Baconian cipher to see a famous quote from Albert Einstein.

```
*-******--*****-**--**-***--***--*--***-*---***-*****
ABAAAAABBBAAAAABAABBAABAAABBAAABBABBAAABABBBAAABAAAAA
  I    H    A    V    E    N    O    S    P    E    C

-**-*********-*-*-**-*******-*-***-***--**-**-**-****
BAABAAAAAAAAABABABAABAAAAAAABABAAABAAABBAABAABAABAAAA
    I    A    L    T    A    L    E    N    T    I

*****-*--*--*-*--***-*-*-*--**---******-***-***-*-**
AAAAABABBABBABABBAAABABABABBAABBBAAAAAABAAABBAAABABAA
 A    M    O    N    L    Y    P    A    S    S    I

**--*-*--*******-**-***-***-*-*-*--****-*-**--*****-
AABBABABBAAAAAAABAABAAABAAABABABABBAAAABABAABBBAAAAAB
   O    N    A    T    E    L    Y    C    U    R

****--*--**---***-
AAAABBABBAABBBAAAB
I    O    U    S
```

I have no special talent. I am only passionately curious.

The A letters are represented by '*' and the B letters by '-'

7) **[300 points]** Solve this aristocrat to read an interesting message.

LWSYS RJ DILWRDN QIYS DILZVUS RD JIEYZLSJ LWZD LWZL
THERE IS NOTHING MORE NOTABLE IN SOCRATES THAN THAT

WS BIHDF LRQS, XWSD WS XZJ ZD IUF QZD, LI USZYD
HE FOUND TIME, WHEN HE WAS AN OLD MAN, TO LEARN

QHJRE ZDF FZDERDN, ZDF LWIHNWL RL LRQS XSUU JMSDL.
MUSIC AND DANCING, AND THOUGHT IT TIME WELL SPENT.

	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		15	3	5		3	8	6		14	1	3			5	8	13		5	1	9	3	4	11
Replacement	K	F	Z	N	C	D	V	U	O	S	Y	T	P	G	J	Q	M	I	E	X	L	B	H	W	R	A

8) **[300 points]** Encode the phrase with the Vigenère cipher using "Truth" as the key. Some good advice I suppose...

T	R	U		T	H	T	R		U	T	H	T	R		U	T	H	T		R	U	T	H		T	R	U	T		-		H	T	R
Y	O	U		H	A	V	E		P	O	W	E	R		O	V	E	R		Y	O	U	R		M	I	N	D		-		N	O	T
R	**F**	**O**		**A**	**H**	**O**	**V**		**J**	**H**	**D**	**X**	**I**		**I**	**O**	**L**	**K**		**P**	**I**	**N**	**Y**		**F**	**Z**	**H**	**W**		-		**U**	**H**	**K**

U	T	H	T	R	U	T		H	T	R	U	T	H	.		T	R	U	T	H	T	R		U	T	H	T		R	U	T		H	T	R
O	U	T	S	I	D	E		E	V	E	N	T	S	.		R	E	A	L	I	Z	E		T	H	I	S		A	N	D		Y	O	U
I	**N**	**A**	**L**	**Z**	**X**	**X**		**L**	**O**	**V**	**H**	**M**	**Z**	.		**K**	**V**	**U**	**E**	**P**	**S**	**V**		**N**	**A**	**P**	**L**		**R**	**H**	**W**		**F**	**H**	**L**

U	T	H	T		R	U	T	H		T	R	U	T	H	T	R	U	.
W	I	L	L		F	I	N	D		S	T	R	E	N	G	T	H	.
Q	**B**	**S**	**E**		**W**	**C**	**G**	**K**		**L**	**K**	**L**	**X**	**U**	**Z**	**K**	**B**	.

9) **[450 points]** Solve this patristocrat.

HSDPL CIQHM OIXLD WIYHX TLUDP UXTPD PFEQT ELCTL
UPONT HESUB JECTO FEDUC ATION ICANO NLYSA YTHAT

UGUIR ULTQL CIBDQ LUBSD NLTPL QHMOI XLRCU XCRIT
IVIEW ITAST HEMOS TIMPO RTANT SUBJE CTWHI CHWEA

QSIDS FIXTP MIIPV TVIYU P
SPEOP LECAN BEENG AGEDI N

Upon the subject of education ... I can only say that I view it as the most important subject which we as people can be engaged in.

	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	5	7	2	2	1	4	12			11	3	1	2	8	6	3	4	9	8	2	1	6	2	
Replacement	Z	M	H	O	Y	L	V	U	E	K	Q	T	B	R	J	N	S	W	P	A	I	G	F	C	D	X

10) **[400 points]** Decrypt the goofy message below using the Hill cipher where the encryption keyword is "Bruh".

$$\begin{pmatrix} B & R \\ U & H \end{pmatrix} \equiv \begin{pmatrix} 1 & 17 \\ 20 & 7 \end{pmatrix}$$

L	V	R	P	V	S	A	M	K	V	H	F
W	**H**	**E**	**N**	**P**	**I**	**G**	**S**	**F**	**L**	**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

$$\begin{pmatrix} 1 & 17 \\ 20 & 7 \end{pmatrix}^{-1} = (1 * 7 - 17 * 20)^{-1} \begin{pmatrix} 7 & -17 \\ -20 & 1 \end{pmatrix}$$

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

$$(1 * 7 - 17 * 20) \mod 26 = -333 \mod 26 = 5$$

Looking up 5 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 21 which we substitute into the formula to compute the matrix:

$$(1 * 7 - 17 * 20)^{-1} \begin{pmatrix} 7 & -17 \\ -20 & 1 \end{pmatrix} \equiv 21 \begin{pmatrix} 7 & -17 \\ -20 & 1 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 21 * 7 & 21 * -17 \\ 21 * -20 & 21 * 1 \end{pmatrix}$$

$$\mod 26 \equiv \begin{pmatrix} 147 & -357 \\ -420 & 21 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 147 \mod 26 & -357 \mod 26 \\ -420 \mod 26 & 21 \mod 26 \end{pmatrix} \equiv \begin{pmatrix} 17 & 7 \\ 22 & 21 \end{pmatrix}$$

With the inverse matrix we can now decode

$$\begin{pmatrix} R & H \\ W & V \end{pmatrix} * \begin{pmatrix} L \\ V \end{pmatrix} \equiv \begin{pmatrix} 17 & 7 \\ 22 & 21 \end{pmatrix} * \begin{pmatrix} 11 \\ 21 \end{pmatrix} \equiv \begin{pmatrix} 17 * 11 + 7 * 21 \\ 22 * 11 + 21 * 21 \end{pmatrix} \equiv \begin{pmatrix} 334 \\ 683 \end{pmatrix} \equiv \begin{pmatrix} 22 \\ 7 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} W \\ H \end{pmatrix}$$

$$\begin{pmatrix} R & H \\ W & V \end{pmatrix} * \begin{pmatrix} R \\ P \end{pmatrix} \equiv \begin{pmatrix} 17 & 7 \\ 22 & 21 \end{pmatrix} * \begin{pmatrix} 17 \\ 15 \end{pmatrix} \equiv \begin{pmatrix} 17 * 17 + 7 * 15 \\ 22 * 17 + 21 * 15 \end{pmatrix} \equiv \begin{pmatrix} 394 \\ 689 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 13 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} E \\ N \end{pmatrix}$$

$$\begin{pmatrix} R & H \\ W & V \end{pmatrix} * \begin{pmatrix} V \\ S \end{pmatrix} \equiv \begin{pmatrix} 17 & 7 \\ 22 & 21 \end{pmatrix} * \begin{pmatrix} 21 \\ 18 \end{pmatrix} \equiv \begin{pmatrix} 17 * 21 + 7 * 18 \\ 22 * 21 + 21 * 18 \end{pmatrix} \equiv \begin{pmatrix} 483 \\ 840 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 8 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} P \\ I \end{pmatrix}$$

$$\begin{pmatrix} R & H \\ W & V \end{pmatrix} * \begin{pmatrix} A \\ M \end{pmatrix} \equiv \begin{pmatrix} 17 & 7 \\ 22 & 21 \end{pmatrix} * \begin{pmatrix} 0 \\ 12 \end{pmatrix} \equiv \begin{pmatrix} 17 * 0 + 7 * 12 \\ 22 * 0 + 21 * 12 \end{pmatrix} \equiv \begin{pmatrix} 84 \\ 252 \end{pmatrix} \equiv \begin{pmatrix} 6 \\ 18 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} G \\ S \end{pmatrix}$$

$$\begin{pmatrix} R & H \\ W & V \end{pmatrix} * \begin{pmatrix} K \\ V \end{pmatrix} \equiv \begin{pmatrix} 17 & 7 \\ 22 & 21 \end{pmatrix} * \begin{pmatrix} 10 \\ 21 \end{pmatrix} \equiv \begin{pmatrix} 17 * 10 + 7 * 21 \\ 22 * 10 + 21 * 21 \end{pmatrix} \equiv \begin{pmatrix} 317 \\ 661 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 11 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} F \\ L \end{pmatrix}$$

$$\begin{pmatrix} R & H \\ W & V \end{pmatrix} * \begin{pmatrix} H \\ F \end{pmatrix} \equiv \begin{pmatrix} 17 & 7 \\ 22 & 21 \end{pmatrix} * \begin{pmatrix} 7 \\ 5 \end{pmatrix} \equiv \begin{pmatrix} 17 * 7 + 7 * 5 \\ 22 * 7 + 21 * 5 \end{pmatrix} \equiv \begin{pmatrix} 154 \\ 259 \end{pmatrix} \equiv \begin{pmatrix} 24 \\ 25 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} Y \\ Z \end{pmatrix}$$

11) **[300 points]** Decode this Affine cipher to show a terrible joke where A = 19 and B = 6

```
U E K D E R L G U   C   K G I   G   Q W U   K F C H H   G H H   J C K
Y E S T E R D A Y   I   S A W   A   G U Y   S P I L L   A L L   H I S

K S R G Z Z H E   H E D D E R K   M T   D J E   R M G L .   C   G K O E L
S C R A B B L E   L E T T E R S   O N   T H E   R O A D .   I   A S K E D

J C A ,   " I J G D ' K   D J E   I M R L   M T   D J E   K D R E E D ? "
H I M ,   " W H A T ' S   T H E   W O R D   O N   T H E   S T R E E T ? "
```

Click on any two columns to choose the decode problem

How to solve

Indeterminate Solution! Please choose other letters.

12) **[250 points]** Decode this aristocrat.

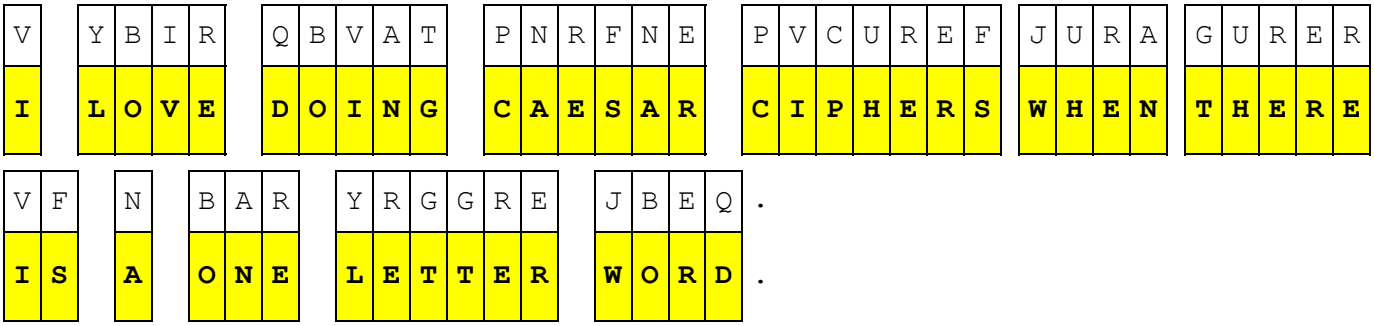
JOMMAYCS, ALAWSNRKYQ TZJ IAZONKEOC. NRA TZS JRA
SUDDENLY, EVERYTHING WAS BEAUTIFUL. THE WAY SHE

LKATAM NRA TUWCM TZJ YUNRKYQ BUWA ION Z WAECAGNKUY
VIEWED THE WORLD WAS NOTHING MORE BUT A REFLECTION

UE RAWJACE.
OF HERSELF.

	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	14	1	5		4		1		2	5	5	2	4	7	4		2	6	3	5	5		5		5	5
Replacement	E	M	L	J	F	Q	C	P	B	S	I	V	D	T	U	X	G	H	Y	W	O	Z	R	K	N	A

13) **[100 points]** Solve this Caesar cipher.



How to solve

We start out by looking for short words to decode and then see if that encoding makes sense. Since we have a single letter word, we try out V=A and V=I.

With V=A we look in the decoding table for a V in the A column and see that it is the V row

Using the V row to decode the first long word 'PNRFNE', it comes out as 'USWKSJ'

With V=I we look in the decoding table for a V in the I column and see that it is the N row

Using the N row to decode the first long word 'PNRFNE', it comes out as 'CAESAR'

Based on this, we believe that the key row is N which we can use to decode the remaining letters

14) **[300 points]** Find the decryption matrix for a hill cipher encryption matrix where the keyword is "Help".

$$\begin{pmatrix} H & E \\ L & P \end{pmatrix} \equiv \begin{pmatrix} 7 & 4 \\ 11 & 15 \end{pmatrix}$$

$$\begin{pmatrix} 19 & 14 \\ 19 & 21 \end{pmatrix}$$

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

$$\begin{pmatrix} 7 & 4 \\ 11 & 15 \end{pmatrix}^{-1} = (7*15 - 4*11)^{-1} \begin{pmatrix} 15 & -4 \\ -11 & 7 \end{pmatrix}$$

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

$$(7*15 - 4*11) \mod 26 = 61 \mod 26 = 9$$

Looking up 9 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 3 which we substitute into the formula to compute the matrix:

$$(7*15 - 4*11)^{-1} \begin{pmatrix} 15 & -4 \\ -11 & 7 \end{pmatrix} \equiv 3 \begin{pmatrix} 15 & -4 \\ -11 & 7 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 3*15 & 3*-4 \\ 3*-11 & 3*7 \end{pmatrix}$$

$$\mod 26 \equiv \begin{pmatrix} 45 & -12 \\ -33 & 21 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 45 \mod 26 & -12 \mod 26 \\ -33 \mod 26 & 21 \mod 26 \end{pmatrix} \equiv \begin{pmatrix} 19 & 14 \\ 19 & 21 \end{pmatrix}$$

15) **[450 points]** Solve this patristocrat. Good luck!

RTJJZ IFBBY MFBIM EYFJF IYMIA RTERT JJFIB MNEBZ
HAPPI NESSD OESNO TDEPE NDONW HATHA PPENS OUTSI

YFMHU MNKNE MIART ERTJJ FIBZI BZYFM HUMN
DEOFY OUBUT ONWHA THAPP ENSIN SIDEO FYOU

Happiness does not depend on what happens outside of you but on what happens inside of you.

	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	7			5	8		2	8	7	1		9	4				5		5	2				5	4
Replacement	W	S	G	J	T	E	Q	F	N	P	B	K	O	U	Z	R	M	H	X	A	Y	C	V	L	D	I

16) **[275 points]** Using the Affine cipher, encrypt the following plaintext where A is 5 and B is 11.

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

W	A	I	T	I	N	G	T	O	B	E	K	N	O	W	N	.
R	**L**	**Z**	**C**	**Z**	**Y**	**P**	**C**	**D**	**Q**	**F**	**J**	**Y**	**D**	**R**	**Y**	.

How to solve

Using the given value of a $=5$ and b $=11$ we can calcuate using the formula $a * x + b \mod 26$

$$S(18) \rightarrow 18 * 5 + 11 \rightarrow 101 \mod 26 \rightarrow X(23)$$
$$O(14) \rightarrow 14 * 5 + 11 \rightarrow 81 \mod 26 \rightarrow D(3)$$
$$M(12) \rightarrow 12 * 5 + 11 \rightarrow 71 \mod 26 \rightarrow T(19)$$
$$E(4) \rightarrow 4 * 5 + 11 \rightarrow 31 \mod 26 \rightarrow F(5)$$
$$W(22) \rightarrow 22 * 5 + 11 \rightarrow 121 \mod 26 \rightarrow R(17)$$
$$H(7) \rightarrow 7 * 5 + 11 \rightarrow 46 \mod 26 \rightarrow U(20)$$

We already computed for E and know that it is F

$$R(17) \rightarrow 17 * 5 + 11 \rightarrow 96 \mod 26 \rightarrow S(18)$$

We already computed for E and know that it is F

We already computed for S and know that it is X

We already computed for O and know that it is D

We already computed for M and know that it is T

We already computed for E and know that it is F

$$T(19) \rightarrow 19 * 5 + 11 \rightarrow 106 \mod 26 \rightarrow C(2)$$

We already computed for H and know that it is U

$$I(8) \rightarrow 8 * 5 + 11 \rightarrow 51 \mod 26 \rightarrow Z(25)$$
$$N(13) \rightarrow 13 * 5 + 11 \rightarrow 76 \mod 26 \rightarrow Y(24)$$
$$G(6) \rightarrow 6 * 5 + 11 \rightarrow 41 \mod 26 \rightarrow P(15)$$

We already computed for I and know that it is Z

We already computed for N and know that it is Y

$$C(2) \rightarrow 2 * 5 + 11 \rightarrow 21 \mod 26 \rightarrow V(21)$$

We already computed for R and know that it is S

We already computed for E and know that it is F

$$D(3) \quad \rightarrow \quad 3 * 5 + 11 \quad \rightarrow \quad 26 \mod 26 \quad \rightarrow \quad A(0)$$

We already computed for I and know that it is Z

$$B(1) \quad \rightarrow \quad 1 * 5 + 11 \quad \rightarrow \quad 16 \mod 26 \quad \rightarrow \quad Q(16)$$

$$L(11) \quad \rightarrow \quad 11 * 5 + 11 \quad \rightarrow \quad 66 \mod 26 \quad \rightarrow \quad O(14)$$

We already computed for E and know that it is F

We already computed for I and know that it is Z

We already computed for S and know that it is X

We already computed for W and know that it is R

$$A(0) \quad \rightarrow \quad 0 * 5 + 11 \quad \rightarrow \quad 11 \mod 26 \quad \rightarrow \quad L(11)$$

We already computed for I and know that it is Z

We already computed for T and know that it is C

We already computed for I and know that it is Z

We already computed for N and know that it is Y

We already computed for G and know that it is P

We already computed for T and know that it is C

We already computed for O and know that it is D

We already computed for B and know that it is Q

We already computed for E and know that it is F

$$K(10) \quad \rightarrow \quad 10 * 5 + 11 \quad \rightarrow \quad 61 \mod 26 \quad \rightarrow \quad J(9)$$

We already computed for N and know that it is Y

We already computed for O and know that it is D

We already computed for W and know that it is R

We already computed for N and know that it is Y

17) **[550 points]** Solve this Baconian cipher

++===++=+++++++=+++++++++++++=+==+==++===++=+=++=+++=
AABBBAABAAAAAAABAAAAAAAAAAAAABABBABBAABBBAABABAABAAAB
H E A R A B O U T T H

==++=+++==++++=++=+=++=++++++=++=+++==++=+++++++=++===
BBAABAAABBAAAABAABABAABAAAAAAABAABAAABBAABAAAAAAABAABBB
E N E W R E S T A U

+++++++++++==++=++=++++=+++++++=+=++=+=+++=++++++==+=++
AAAAAAAAAAABBAABAABAAAABAAAAAAABABAABABAAABAAAAAABBABAA
R A N T C A L L E D K

=+++++=+++++=+==+++++=++=+++===++=++=++++++=++=+++=+=
BAAAAABAAAAABABBAAAAABAABAAABBBAABAABAAAAAAABAABAAABAB
A R M A T H E R E S

=+++==+=+=+==++=+++==++=++===+==++==+==++==++==+++=++
BAAABBABABABBAABAAABBAABAABBBABBAABBABBAABBAABBAAABAA
N O M E N U Y O U G E

=++=+=+=++++===+++++=++=+=+==++==+==++==+++==++=++=++
BAABABABAAAABBBAAAAABAABABABBAABBABBAABBAAABBAABAABAA
T W H A T Y O U D E S

+=++=++=++++=++==++=++
ABAABAABAAAABAABBAABAA
E R V E

Hear about the new restaurant called Karma? There's no menu: You get what you deserve.

The A letters are represented by '+' and the B letters by '='

18) **[650 points]** Solve this xenocrypt.

MJQP JMLPFP MJQPLGJ GVEPFBIPFOG MA QPAAMV DSM
ESTA SEMANA ESTAMOS ORGANIZANDO EL TALLER QUE

JBMLHVM DSBJBJQM. SFG DSM MJ SFBÑG HMVG PSF LSR
SIEMPRE QUISISTE. UNO QUE ES UNICO PERO AUN MUY

HVPÑQBÑG R XSFÑBGFPA. MFQGFÑMJ, RP JMP DSM MJQM
PRACTICO Y FUNCIONAL. ENTONCES, YA SEA QUE ESTE

ÑVMPFOG SF QPAAMV OMJOM ÑMVG G JBLHAMLMFQM KSJÑPFOG
CREANDO UN TALLER DESDE CERO O SIMPLEMENTE BUSCANDO

BOMPJ HPVP LMWGVPV MA DSM QBMFM, DSMVVP DSMOPVJM
IDEAS PARA MEJORAR EL QUE TIENE, QUERRA QUEDARSE

HPVP CMV ÑGLG QGOG JM SFM.
PARA VER COMO TODO SE UNE.

	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	8	10	1	7	1	16	18	6	1	17	1	8	38		9	8	23	11	3	15			16	1	1		
Replacement	L	I	V	Q	G	N	O	P	Z	S	B	M	E	W	C	D	A	T	Y	U	K	X	R	J	F	Ñ	H

Translation: *This week we're putting together the workshop you always wanted. One that's unique but still very practical and functional. So whether you're creating a workshop from scratch or just looking for ideas to improve the one you have, you'll want to stick around to see it all come together.*