Science Olympiad — SSSS Codebusters - builderguy135

Timed Question **[400 points]** Decode this quote from Ta-Nehisi Coates's "Between the World and Me". When you have solved it, raise your hand so that the time can be recorded and the solution checked.

CTAYSNMCTSYIF TA P UTIC MR FYEEMETAS, PIC FQY FQEYPF
DISEMBODIMENT IS A KIND OF TERRORISM, AND THE THREAT

MR TF PGFYEA FQY MENTF MR PGG MWE GTKYA PIC, GTUY
OF IT ALTERS THE ORBIT OF ALL OUR LIVES AND, LIKE

FYEEMETAS, FQTA CTAFMEFTMI TA TIFYIFTMIPG.
TERRORISM, THIS DISTORTION IS INTENTIONAL.

	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	9		6		11	15	6		8		1		11	2		7	4	3	4	16	2		1		11	
Replacement	S	Z	D	Q	R	T	L	J	N	W	V	P	O	B	C	A	H	F	M	I	K	Y	U	G	E	X

1) **[125 points]** Decode this word, often used to describe rocks, which has been encoded with a Caesar cipher.

T	G	L	J	Q	G	V	A	S	D
B	**O**	**T**	**R**	**Y**	**O**	**D**	**I**	**A**	**L**

How to solve

At this point, we have to try a brute force method just going down the alphabet

Using the A row to decode the first few characters 'TGLJQGVASD', it comes out as 'TGLJQGVASD'

Using the B row to decode the first few characters 'TGLJQGVASD', it comes out as 'SFKIPFUZRC'

Using the C row to decode the first few characters 'TGLJQGVASD', it comes out as 'REJHOETYQB'

Using the D row to decode the first few characters 'TGLJQGVASD', it comes out as 'QDIGNDSXPA'

Using the E row to decode the first few characters 'TGLJQGVASD', it comes out as 'PCHFMCRWOZ'

Using the F row to decode the first few characters 'TGLJQGVASD', it comes out as 'OBGELBQVNY'

Using the G row to decode the first few characters 'TGLJQGVASD', it comes out as 'NAFDKAPUMX'

Using the H row to decode the first few characters 'TGLJQGVASD', it comes out as 'MZECJZOTLW'

Using the I row to decode the first few characters 'TGLJQGVASD', it comes out as 'LYDBIYNSKV'

Using the J row to decode the first few characters 'TGLJQGVASD', it comes out as 'KXCAHXMRJU'

Using the K row to decode the first few characters 'TGLJQGVASD', it comes out as 'JWBZGWLQIT'

Using the L row to decode the first few characters 'TGLJQGVASD', it comes out as 'IVAYFVKPHS'

Using the M row to decode the first few characters 'TGLJQGVASD', it comes out as 'HUZXEUJOGR'

Using the N row to decode the first few characters 'TGLJQGVASD', it comes out as 'GTYWDTINFQ'

Using the O row to decode the first few characters 'TGLJQGVASD', it comes out as 'FSXVCSHMEP'

Using the P row to decode the first few characters 'TGLJQGVASD', it comes out as 'ERWUBRGLDO'

Using the Q row to decode the first few characters 'TGLJQGVASD', it comes out as 'DQVTAQFKCN'

Using the R row to decode the first few characters 'TGLJQGVASD', it comes out as 'CPUSZPEJBM'

Using the S row to decode the first few characters 'TGLJQGVASD', it comes out as 'BOTRYODIAL'

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

2) **[125 points]** Encode "Encode this with a Caesar shit of ninety" with a Caesar shift of negative forty.

E	N	C	O	D	E		T	H	I	S		W	I	T	H		A		C	A	E	S	A	R		S	H	I	F	T		O	F
Q	**Z**	**O**	**A**	**P**	**Q**		**F**	**T**	**U**	**E**		**I**	**U**	**F**	**T**		**M**		**O**	**M**	**Q**	**E**	**M**	**D**		**E**	**T**	**U**	**R**	**F**		**A**	**R**

N	I	N	E	T	Y	.
Z	**U**	**Z**	**Q**	**F**	**K**	.

3) **[275 points]** Decode this aristocrat, which is the description of an amoebic parasite and the infection it can cause. The last word of the plaintext is the acronym PAM and the word "amoeba" is used once.

WRFLEFVUR ZJNEFVU UA R ZVFF-EUCUWL BUQVJAQJOUQ
NAEGLERIA FOWLERI IS A FREE-LIVING MICROSCOPIC

RBJFGR. UX QRW QRIAF R VRVF RWM ZRXRE UWZFQXUJW JZ
AMOEBA. IT CAN CAUSE A RARE AND FATAL INFECTION OF

XKF GVRUW QREEFM OVUBRVH RBFGUQ BFWUWLJFWQFOKREUXUA (
THE BRAIN CALLED PRIMARY AMEBIC MENINGOENCEPHALITIS (

ORB).
PAM).

	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	4	6	1		7	15	3	1	1	7	2	3	2	1	4		9	18			16	9	10	5		5
Replacement	S	M	V	J	L	E	B	Y	U	O	H	G	D	W	P	K	C	A	Z	Q	I	R	N	T	X	F

4) **[325 points]** Decode this text message which has been corrected of its grammar mistakes and encoded with a K1 aristocrat.

SYM SD ASTCBSJ, X'WC ZMYBXCB JSTC XU MFC IVZM MNS
OUT OF BOREDOM, I'VE STUDIED MORE IN THE LAST TWO

NCCHZ MFVU X FVWC XU MFC IVZM MNS PCVTZ.
WEEKS THAN I HAVE IN THE LAST TWO YEARS.

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	10	1		4		1	2	2			9	3		1			7	3	3	5	2	5	2	5
Replacement	B	D	E	F	G	H	J	K	L	M	P	Q	T	W	X	Y	Z	C	O	R	N	A	V	I	U	S

5) **[325 points]** Decode this aristocrat that discusses a concept in math.

M PREHQVAE HME KS MUUBAJVYMQSI KZ ROVEC M PVEVQS
A FUNCTION CAN BE APPROXIMATED BY USING A FINITE

ERYKSB AP QSBYO AP VQO QMZNAB OSBVSO.
NUMBER OF TERMS OF ITS TAYLOR SERIES.

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

6) **[375 points]** Decode this quote by Neil deGrasse Tyson which has been encoded as an Aristocrat.

K HSWRY-GKFFWQ, HSWRY-JKWW, GYOD GUOD HKRBM JQREQQO
A MULTI-PADDLE, MULTI-BALL, PING PONG MATCH BETWEEN

REU UBRUGSAQA EUSWF JQ KEQAUHQ RU EKRBM.
TWO OCTOPUSES WOULD BE AWESOME TO WATCH.

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

7) **[400 points]** Decode this meta-cipher encoded with a K2 alphabet.

KZVBJ NSCC XHQFKVDVCQUZ VDY YZXEYZ ZDXHQFKZY
TEAMS WILL CRYPTANALYZE AND DECODE ENCRYPTED

BZJJVRZJ LJSDR XHQFKVDVCQJSJ KZXIDSGLZJ AEH
MESSAGES USING CRYPTANALYSIS TECHNIQUES FOR

ISJKEHSXVC VDY BEYZHD VYMVDXZY XSFIZHJ.
HISTORICAL AND MODERN ADVANCED CIPHERS.

Replacement	V	W	X	Y	Z	A	R	I	S	T	O	C	B	D	E	F	G	H	J	K	L	M	N	P	Q	U
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	5	9	4	4	1	7	3	10	6	2	1	1			5	2	7		1	11		8	8	13

8) **[425 points]** Decode this text message which has been encoded as an Aristocrat. The plaintext includes texting language and is a run-on sentence.

V UWKKW TX GR MKQHVFJ JU NCE GR EMWPJMA PWK FMM UJMK
I WANNA DO MY ENGLISH HW BUT MY TEACHER CAN SEE WHEN

V TX VE WKT VEF EUX WG WKT V TXK'E UWKE JMA EX EJVKY
I DO IT AND ITS TWO AM AND I DON'T WANT HER TO THINK

V'G VKFWKM HGWX
I'M INSANE LMAO

	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		9	4	5	2		6	12		8	1		2	1	2		5	5	9	10	6	1	
Replacement	R	Q	U	F	T	S	M	L	V	H	N	Z	E	B	X	C	G	Y	J	D	W	I	A	O	K	P

9) **[550 points]** Decode this controversial quote by Randall Munroe which has been encoded as a K1 patristocrat.

RQEYL FLYLW HRTLN DEFGE HIJKL RGMWR FPXNI ZFIGQ
IHAVE NEVER LIKED CANTA LOUPE ITBRI NGSDO WNOTH

LWZRX LGEXG BOWJR GXEHE NXGQL WLRXE RNRG
ERWIS ETAST YFRUI TSALA DSTHE REISA IDIT

I have never liked cantaloupe. It brings down otherwise tasty fruit salads. There, I said it.

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

10) **[575 points]** Decode this statement by Edsger Dijkstra, a programmer and computer scientist, which is encoded as a Patristocrat using a K1 alphabet. The key is the country he was born in.

PNYDY PKFET MTWCE HPCDK TNMTJ DYDKF TWHJC TEGDO
IFWEW ISHTO COUNT LINES OFCOD EWESH OULDN OTREG

IGJEF DSIKH PCDKU GTJWM DJLWE IKHPC DKKUD CE
ARDTH EMASL INESP RODUC EDBUT ASLIN ESSPE NT

If we wish to count lines of code, we should not regard them as lines produced but as lines spent.

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			6	10	6	3	3	4	3	5	8	1	3	2	1	5			1	7	2		4		3	
Replacement	Y	Z	N	E	T	H	R	L	A	D	S	B	C	F	G	I	J	K	M	O	P	Q	U	V	W	X

11) **[650 points]** Decode this quote, encoded as a Patristocrat and taken from the trailer of the documentary "Float", which discusses F1D indoor free flight planes.

LTXYX ONIYL HDMHQ DKHIL SFBQN IYHQF ULTXY XVSLT
THERE SPART OFYOU FLOAT INGUP AROUN DTHER EWITH

SLIFU IGOHK QLXKM FHLTS FBSFL TXVHY KUJIF YXNKI
ITAND ABSOL UTELY NOTHI NGINT HEWOR LDCAN REPLA

JXLTI LDXXK SFB
CETHA TFEEL ING

There's part of you floating up around there with it... and absolutely nothing in the world can replace that feeling.

	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		3		8	1	7	8	2	6	11	2	3	2		4		6	6	3	2		10	6	
Replacement	J	G	X	F	V	N	B	O	A	C	L	T	Y	P	S	Z	U	K	I	H	D	W	Q	E	R	M

12) **[150 points]** Encode this phrase with the Affine cipher where a=15 and b=8.

R	A	I	S	E	D
D	**I**	**Y**	**S**	**Q**	**B**

S	U	B	M	E	D	I	A	N	T
S	**W**	**X**	**G**	**Q**	**B**	**Y**	**I**	**V**	**H**

How to solve

Using the given value of $\mathrm{a} = 15$ and $\mathrm{b} = 8$ we can calcuate using the formula $a * x + b \mod 26$

$$R(17) \rightarrow 17 * 15 + 8 \rightarrow 263 \mod 26 \rightarrow D(3)$$
$$A(0) \rightarrow 0 * 15 + 8 \rightarrow 8 \mod 26 \rightarrow I(8)$$
$$I(8) \rightarrow 8 * 15 + 8 \rightarrow 128 \mod 26 \rightarrow Y(24)$$
$$S(18) \rightarrow 18 * 15 + 8 \rightarrow 278 \mod 26 \rightarrow S(18)$$
$$E(4) \rightarrow 4 * 15 + 8 \rightarrow 68 \mod 26 \rightarrow Q(16)$$
$$D(3) \rightarrow 3 * 15 + 8 \rightarrow 53 \mod 26 \rightarrow B(1)$$

We already computed for S and know that it is S

$$U(20) \rightarrow 20 * 15 + 8 \rightarrow 308 \mod 26 \rightarrow W(22)$$
$$B(1) \rightarrow 1 * 15 + 8 \rightarrow 23 \mod 26 \rightarrow X(23)$$
$$M(12) \rightarrow 12 * 15 + 8 \rightarrow 188 \mod 26 \rightarrow G(6)$$

We already computed for E and know that it is Q

We already computed for D and know that it is B

We already computed for I and know that it is Y

We already computed for A and know that it is I

$$N(13) \rightarrow 13 * 15 + 8 \rightarrow 203 \mod 26 \rightarrow V(21)$$
$$T(19) \rightarrow 19 * 15 + 8 \rightarrow 293 \mod 26 \rightarrow H(7)$$

13) **[200 points]** Decode the name of a part of the ear with the Affine cipher. The 1st letter is "b" and the last letter is "e".

P	K	W	Y	N	K	R
B	**A**	**S**	**I**	**L**	**A**	**R**

S	E	S	P	R	K	X	E
M	**E**	**M**	**B**	**R**	**A**	**N**	**E**

How to solve

Here is how we get the answer. Since we are given that:

$$B(1) \rightarrow P(15)$$
$$E(4) \rightarrow E(4)$$

From this we know:

$$(a * 4 + b) \mod 26 = 4$$
$$(a * 1 + b) \mod 26 = 15$$

Next, subtract the formulas:

$$\begin{aligned} (a * 4 + b) \mod 26 &= 4 \\ -(a * 1 + b) \mod 26 &= 15 \\ \hline a * 3 \mod 26 &= -11 \\ a * 3 \mod 26 &= 15 \end{aligned}$$

So we now know that $\mathrm{a} = 5$

To find b, substitute that back into the equation with the lowest multiplier.

$$\begin{aligned} (5 * 1 + b) \mod 26 &= 15 \\ (5 + b) \mod 26 &= 15 \end{aligned} \qquad \begin{aligned} (5 + b) \mod 26 - 5 &= (15 - 5) \mod 26 \\ b \mod 26 &= 10 \mod 26 \\ b \mod 26 &= 10 \mod 26 \end{aligned}$$

Subtract 5 from both sides:

And we see that $\mathrm{b} = 10$

However, we only know a few of the letters in the cipher.

P	**K**	**W**	**Y**	**N**	**K**	**R**	**S**	**E**	**S**	**P**	**R**	**K**	**X**	**E**
B								**E**		**B**				**E**

The first step is to encode the common letters **ETAOIN** to see what they would map to.

$$
\begin{array}{rcrcrcl}
E(4) & \rightarrow & 4*5+10 & \rightarrow & 30 \mod 26 & \rightarrow & E(4) \\
T(19) & \rightarrow & 19*5+10 & \rightarrow & 105 \mod 26 & \rightarrow & B(1) \\
A(0) & \rightarrow & 0*5+10 & \rightarrow & 10 \mod 26 & \rightarrow & K(10) \\
O(14) & \rightarrow & 14*5+10 & \rightarrow & 80 \mod 26 & \rightarrow & C(2) \\
I(8) & \rightarrow & 8*5+10 & \rightarrow & 50 \mod 26 & \rightarrow & Y(24) \\
N(13) & \rightarrow & 13*5+10 & \rightarrow & 75 \mod 26 & \rightarrow & X(23)
\end{array}
$$

Filling in the letter we found (EBKCYX), we get a bit more of the answer.

P	K	W	Y	N	K	R	S	E	S	P	R	K	X	E
B	A		I		A			E		B		A	N	E

Next, encode the next 5 common letters **SRHLD**.

$$
\begin{array}{rcrcrcl}
S(18) & \rightarrow & 18*5+10 & \rightarrow & 100 \mod 26 & \rightarrow & W(22) \\
R(17) & \rightarrow & 17*5+10 & \rightarrow & 95 \mod 26 & \rightarrow & R(17) \\
H(7) & \rightarrow & 7*5+10 & \rightarrow & 45 \mod 26 & \rightarrow & T(19) \\
L(11) & \rightarrow & 11*5+10 & \rightarrow & 65 \mod 26 & \rightarrow & N(13) \\
D(3) & \rightarrow & 3*5+10 & \rightarrow & 25 \mod 26 & \rightarrow & Z(25)
\end{array}
$$

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

P	K	W	Y	N	K	R	S	E	S	P	R	K	X	E
B	A	S	I	L	A	R		E		B	R	A	N	E

We will convert the next 5 most frequent letters **CUMFP**.

$$
\begin{array}{rcrcrcl}
C(2) & \rightarrow & 2*5+10 & \rightarrow & 20 \mod 26 & \rightarrow & U(20) \\
U(20) & \rightarrow & 20*5+10 & \rightarrow & 110 \mod 26 & \rightarrow & G(6) \\
M(12) & \rightarrow & 12*5+10 & \rightarrow & 70 \mod 26 & \rightarrow & S(18) \\
F(5) & \rightarrow & 5*5+10 & \rightarrow & 35 \mod 26 & \rightarrow & J(9) \\
P(15) & \rightarrow & 15*5+10 & \rightarrow & 85 \mod 26 & \rightarrow & H(7)
\end{array}
$$

The next 5 letters we know are (UGSJH), so we will fill those in.

P	K	W	Y	N	K	R	S	E	S	P	R	K	X	E
B	A	S	I	L	A	R	M	E	M	B	R	A	N	E

The solution is now complete!

14) **[175 points]** Decrypt this phrase using the Vigenere Cipher with a key of "wright". Do not decode the numbers.

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

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

15) **[200 points]** Encode the phrase "pentel orenz nero zero point three" with the Vigenere Cipher with key "pencil"

P	E	N	C	I	L	P	E	N	C	I	L	P	E	N	C	I	L	P	E	N	C	I	L	P	E	N	C	I
E	I	A	V	M	W	D	V	R	P	H	Y	T	V	B	B	M	C	D	T	B	K	V	E	I	L	E	G	M
P	**E**	**N**	**T**	**E**	**L**	**O**	**R**	**E**	**N**	**Z**	**N**	**E**	**R**	**O**	**Z**	**E**	**R**	**O**	**P**	**O**	**I**	**N**	**T**	**T**	**H**	**R**	**E**	**E**

16) **[200 points]** Decrypt this word, given that the block size is 3 and the last 3 letters are "phy"

E	E	G	E	E	G	E	E	G	E	E	G	E	E	G	E	E	G	E	E	G	E	E	G
I	P	K	G	X	X	S	I	T	G	I	V	L	E	R	S	X	U	K	V	G	T	L	E
E	**L**	**E**	**C**	**T**	**R**	**O**	**E**	**N**	**C**	**E**	**P**	**H**	**A**	**L**	**O**	**T**	**O**	**G**	**R**	**A**	**P**	**H**	**Y**

17) **[275 points]** Decode the name of this cryptographic algorithm which is a prime example of encoding with a Baconian Cipher.

42356728943572356789243576235782359472365782357293457235
BAAABAABBBAAAAAABABBABAAABAAAABAAABBAAABAABAAAAABABAAAA
S H A M I R S S E C R

57623857924357623894572356723578235794235768293574235 67
AABAABAABABAAABAABBBAAAAABAAAAABAAAABBAAAABBABAAABAAABA
E T S H A R I N G S C

23894576235879423657
AABBBAABAAABABBAABAA
H E M E

Shamir's secret sharing scheme

The A letters are represented by '2357' and the B letters by '4689'

18) **[300 points]** Decrypt this disease which has been encoded using a Baconian cipher.

APPLY AFTER FEWER BEADS ABOUT CAKES ALARM CAUSE AWAKE
ABBBA ABBAB BAAAB BAABA ABAAB AAAAA ABABA AAAAA AAAAA
P O S T K A L A A

DEPTH AWAKE BOOKS EGYPT GERMS BEAMS ADAPT ISAAC ALIBI
BABBB AAAAA BAAAA AAABB AABAA BAAAA ABABB AAAAA ABABA
Z A R D E R M A L

ALONE MOVIE IDEAS TIGER WALTZ GRUNT MESSY INDIA CROOK
ABABA AABAA ABAAA BAAAB AABBB ABABB AAAAA ABBAA ABAAA
L E I/J S H M A N I/J

SMOKE JOKER CRAIG TWIST
AAAAA BAAAB ABAAA BAAAB
A S I/J S

post kala azar dermal leishmaniasis

The letters are mapped as:

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
A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B

19) **[600 points]** Decode this quote by Joshua Marine which has been encoded as a Xenocrypt.

VEX JCXYOAEX XES VEX BKC ZYWCS BKC VY LAJY XCY
LOS DESAFIOS SON LOS QUE HACEN QUE LA VIDA SEA

ASUCNCXYSUC I XKÑCNYNVEX CX VE BKC ZYWC VY LAJY
INTERESANTE Y SUPERARLOS ES LO QUE HACE LA VIDA

XAFSAOAWYUALY
SIGNIFICATIVA

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

Translation: *Challenges are what make life interesting and overcoming them is what makes life meaningful.*

20) **[250 points]** Encode the phrase "larus argentatus(z)" with the Hill Cipher with a keyword of "bird".

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

L	A	R	U	S	A	R	G	E	N	T	A	T	U	S	
L	**F**	**V**	**L**	**S**	**U**	**N**	**V**	**E**	**D**	**T**	**L**	**X**	**T**	**K**	**R**

How to solve

$$\begin{pmatrix} B & I \\ R & D \end{pmatrix} * \begin{pmatrix} L \\ A \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 11 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 * 11 + 8 * 0 \\ 17 * 11 + 3 * 0 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 187 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 5 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} L \\ F \end{pmatrix}$$

$$\begin{pmatrix} B & I \\ R & D \end{pmatrix} * \begin{pmatrix} R \\ U \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 17 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} 1 * 17 + 8 * 20 \\ 17 * 17 + 3 * 20 \end{pmatrix} \equiv \begin{pmatrix} 177 \\ 349 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 11 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} V \\ L \end{pmatrix}$$

$$\begin{pmatrix} B & I \\ R & D \end{pmatrix} * \begin{pmatrix} S \\ A \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 18 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 * 18 + 8 * 0 \\ 17 * 18 + 3 * 0 \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 306 \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 20 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} S \\ U \end{pmatrix}$$

$$\begin{pmatrix} B & I \\ R & D \end{pmatrix} * \begin{pmatrix} R \\ G \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 17 \\ 6 \end{pmatrix} \equiv \begin{pmatrix} 1 * 17 + 8 * 6 \\ 17 * 17 + 3 * 6 \end{pmatrix} \equiv \begin{pmatrix} 65 \\ 307 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 21 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} N \\ V \end{pmatrix}$$

$$\begin{pmatrix} B & I \\ R & D \end{pmatrix} * \begin{pmatrix} E \\ N \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 4 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 1 * 4 + 8 * 13 \\ 17 * 4 + 3 * 13 \end{pmatrix} \equiv \begin{pmatrix} 108 \\ 107 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 3 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} E \\ D \end{pmatrix}$$

$$\begin{pmatrix} B & I \\ R & D \end{pmatrix} * \begin{pmatrix} T \\ A \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 19 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 * 19 + 8 * 0 \\ 17 * 19 + 3 * 0 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 323 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 11 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} T \\ L \end{pmatrix}$$

$$\begin{pmatrix} B & I \\ R & D \end{pmatrix} * \begin{pmatrix} T \\ U \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 19 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} 1 * 19 + 8 * 20 \\ 17 * 19 + 3 * 20 \end{pmatrix} \equiv \begin{pmatrix} 179 \\ 383 \end{pmatrix} \equiv \begin{pmatrix} 23 \\ 19 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} X \\ T \end{pmatrix}$$

$$\begin{pmatrix} B & I \\ R & D \end{pmatrix} * \begin{pmatrix} S \\ Z \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 \\ 17 & 3 \end{pmatrix} * \begin{pmatrix} 18 \\ 25 \end{pmatrix} \equiv \begin{pmatrix} 1 * 18 + 8 * 25 \\ 17 * 18 + 3 * 25 \end{pmatrix} \equiv \begin{pmatrix} 218 \\ 381 \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 17 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} K \\ R \end{pmatrix}$$

21) **[350 points]** Decode the name of this parasite given that the encryption keyword is "trematoda" using a 3x3 Hill Cipher.

$$\begin{pmatrix} T & R & E \\ M & A & T \\ O & D & A \end{pmatrix} \equiv \begin{pmatrix} 19 & 17 & 4 \\ 12 & 0 & 19 \\ 14 & 3 & 0 \end{pmatrix} \qquad Decode \begin{pmatrix} T & R & E \\ M & A & T \\ O & D & A \end{pmatrix}^{-1} \equiv \begin{pmatrix} 1 & 8 & 3 \\ 4 & 6 & 21 \\ 24 & 21 & 20 \end{pmatrix}$$

P	J	C	C	G	S	P	U	Y	U	I	W	Q	T	G	X	Q	D	T	W	N
P	**A**	**R**	**A**	**G**	**O**	**N**	**I**	**M**	**U**	**S**	**W**	**E**	**S**	**T**	**E**	**R**	**M**	**A**	**N**	**I**

How to solve

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

$$M^{-1} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}^{-1} = det(M)^{-1} \begin{pmatrix} A & B & C \\ D & E & F \\ G & H & I \end{pmatrix}^{T} = det(M)^{-1} \begin{pmatrix} A & D & G \\ B & E & H \\ C & F & I \end{pmatrix}$$

Where:

$$A = (ei - fh), D = -(bi - ch), G = (bf - ce),$$

$$B = -(di - fg), E = (ai - cg), H = -(af - cd),$$

$$C = (dh - eg), F = -(ah - bg), I = (ae - bd),$$

and,

$$det(M) = aA + bB + cC$$

In this case we will compute $det(M)^{-1}$ Using modular multiplicative inverse (https://en.wikipedia.org/wiki/Invertible_matrix) math.

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

$$det(M) = (19 * -57 + 17 * 266 + 4 * 36) \mod 26 = 3583 \mod 26 = 21$$

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

$$\begin{pmatrix} 19 & 17 & 4 \\ 12 & 0 & 19 \\ 14 & 3 & 0 \end{pmatrix}^{-1} \equiv 5 \begin{pmatrix} -57 & 266 & 36 \\ 12 & -56 & 181 \\ 323 & -313 & -204 \end{pmatrix}^{T} \mod 26 \equiv 5 \begin{pmatrix} -57 & 12 & 323 \\ 266 & -56 & -313 \\ 36 & 181 & -204 \end{pmatrix} \mod 26$$

Completing the calculation, we get:

$$\begin{pmatrix} 5*-57 & 5*12 & 5*323 \\ 5*17 & 5*-56 & 5*-313 \\ 5*36 & 5*181 & 5*-204 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} -285 & 60 & 1615 \\ 1330 & -280 & -1565 \\ 180 & 905 & -1020 \end{pmatrix} \mod 26 \equiv$$
$$\begin{pmatrix} -285 \mod 26 & 60 \mod 26 & 1615 \mod 26 \\ 1330 \mod 26 & -280 \mod 26 & -1565 \mod 26 \\ 180 \mod 26 & 905 \mod 26 & -1020 \mod 26 \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 & 3 \\ 4 & 6 & 21 \\ 24 & 21 & 20 \end{pmatrix}$$

With the inverse matrix we can now decode

$$\begin{pmatrix} B & I & D \\ E & G & V \\ Y & V & U \end{pmatrix} * \begin{pmatrix} P \\ J \\ C \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 & 3 \\ 4 & 6 & 21 \\ 24 & 21 & 20 \end{pmatrix} * \begin{pmatrix} 15 \\ 9 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 1*15+8*9+3*2 \\ 4*15+6*9+21*2 \\ 24*15+21*9+20*2 \end{pmatrix} \equiv \begin{pmatrix} 93 \\ 156 \\ 589 \end{pmatrix} \equiv$$
$$\begin{pmatrix} 15 \\ 0 \\ 17 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} P \\ A \\ R \end{pmatrix}$$
$$\begin{pmatrix} B & I & D \\ E & G & V \\ Y & V & U \end{pmatrix} * \begin{pmatrix} C \\ G \\ S \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 & 3 \\ 4 & 6 & 21 \\ 24 & 21 & 20 \end{pmatrix} * \begin{pmatrix} 2 \\ 6 \\ 18 \end{pmatrix} \equiv \begin{pmatrix} 1*2+8*6+3*18 \\ 4*2+6*6+21*18 \\ 24*2+21*6+20*18 \end{pmatrix} \equiv \begin{pmatrix} 104 \\ 422 \\ 534 \end{pmatrix} \equiv$$
$$\begin{pmatrix} 0 \\ 6 \\ 14 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} A \\ G \\ O \end{pmatrix}$$
$$\begin{pmatrix} B & I & D \\ E & G & V \\ Y & V & U \end{pmatrix} * \begin{pmatrix} P \\ U \\ Y \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 & 3 \\ 4 & 6 & 21 \\ 24 & 21 & 20 \end{pmatrix} * \begin{pmatrix} 15 \\ 20 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 1*15+8*20+3*24 \\ 4*15+6*20+21*24 \\ 24*15+21*20+20*24 \end{pmatrix} \equiv$$
$$\begin{pmatrix} 247 \\ 684 \\ 1260 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 8 \\ 12 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} N \\ I \\ M \end{pmatrix}$$
$$\begin{pmatrix} B & I & D \\ E & G & V \\ Y & V & U \end{pmatrix} * \begin{pmatrix} U \\ I \\ W \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 & 3 \\ 4 & 6 & 21 \\ 24 & 21 & 20 \end{pmatrix} * \begin{pmatrix} 20 \\ 8 \\ 22 \end{pmatrix} \equiv \begin{pmatrix} 1*20+8*8+3*22 \\ 4*20+6*8+21*22 \\ 24*20+21*8+20*22 \end{pmatrix} \equiv$$
$$\begin{pmatrix} 150 \\ 590 \\ 1088 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 18 \\ 22 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} U \\ S \\ W \end{pmatrix}$$
$$\begin{pmatrix} B & I & D \\ E & G & V \\ Y & V & U \end{pmatrix} * \begin{pmatrix} Q \\ T \\ G \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 & 3 \\ 4 & 6 & 21 \\ 24 & 21 & 20 \end{pmatrix} * \begin{pmatrix} 16 \\ 19 \\ 6 \end{pmatrix} \equiv \begin{pmatrix} 1*16+8*19+3*6 \\ 4*16+6*19+21*6 \\ 24*16+21*19+20*6 \end{pmatrix} \equiv \begin{pmatrix} 186 \\ 304 \\ 903 \end{pmatrix} \equiv$$
$$\begin{pmatrix} 4 \\ 18 \\ 19 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} E \\ S \\ T \end{pmatrix}$$

$$\begin{pmatrix} B & I & D \\ E & G & V \\ Y & V & U \end{pmatrix} * \begin{pmatrix} X \\ Q \\ D \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 & 3 \\ 4 & 6 & 21 \\ 24 & 21 & 20 \end{pmatrix} * \begin{pmatrix} 23 \\ 16 \\ 3 \end{pmatrix} \equiv \begin{pmatrix} 1*23+8*16+3*3 \\ 4*23+6*16+21*3 \\ 24*23+21*16+20*3 \end{pmatrix} \equiv \begin{pmatrix} 160 \\ 251 \\ 948 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 17 \\ 12 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} E \\ R \\ M \end{pmatrix}$$

$$\begin{pmatrix} B & I & D \\ E & G & V \\ Y & V & U \end{pmatrix} * \begin{pmatrix} T \\ W \\ N \end{pmatrix} \equiv \begin{pmatrix} 1 & 8 & 3 \\ 4 & 6 & 21 \\ 24 & 21 & 20 \end{pmatrix} * \begin{pmatrix} 19 \\ 22 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 1*19+8*22+3*13 \\ 4*19+6*22+21*13 \\ 24*19+21*22+20*13 \end{pmatrix} \equiv \begin{pmatrix} 234 \\ 481 \\ 1178 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 13 \\ 8 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} A \\ N \\ I \end{pmatrix}$$

22) **[250 points]** Decrypt this phrase which has been encoded using the Morbit Cipher. 1=x•, 2=--, 3=•-, 4=•x, 5=xx, 6=••

```
9 9 8 3 7 3 8 4 2 7 3 8 3 4 3 4 9 2 1 9 4 3 8 1 5 2 4
-●-●x-●--x●-x-●x---x●-x-●-●x●-●x-●--x●-●●x●-x-x●xx--●x
C    Y    A  N  O   A  C    R   Y    L    A  T E/ G

3 6 1 3 1 5 6 1 6 5 9 6 1 7 9 4 1 3 4 2 7 3 4 8 3 7
●-●●x●●-x●xx●●x●●●xx-●●●x●-x-●●xx●●-●x---x●-●xx-●--x
L    U   E/ I  S  / B    A  D   /F    O   R   /Y

2 7 6 7 3 4 1 9 4 6 7 9 8 9 1 6
---x●●-x●-●xx●-●●x●●-x-●x--●x●●●
O   U   R   /L    U   N  G   S
```

How to solve

Since we are told the mapping of 123456 ciphertext, we can build the following table:

1	2	3	4	5	6	7	8	9
×●	—	●–	●×	××	●●	–● –× ×–	–● –× ×–	–● –× ×–

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

```
9 9 8 3 7 3 8 4 2 7 3 8 3 4 3 4 9 2 1 9 4 3 8 1 5 2 4
      ●-  ●-  ●x--  ●-  ●-●x●-●x  --x●  ●x●-  x●xx--●x
                              R                E/ G

3 6 1 3 1 5 6 1 6 5 9 6 1 7 9 4 1 3 4 2 7 3 4 8 3 7
●-●●x●●-x●xx●●x●●●xx  ●●x●    ●xx●●-●x--  ●-●x  ●-
 L    U   E/ I  S  /           / F

2 7 6 7 3 4 1 9 4 6 7 9 8 9 1 6
--  ●●  ●-●xx●  ●x●●        x●●●
          /                 S
```

At this point in time, 3 ciphertext characters still need to be mapped. Looking for unknowns next to ×× which would result in three in a row, we find the sequence 59 where we know that 5 is ×× which means that 9 cannot start with ×, so we can eliminate those possibilities

1	2	3	4	5	6	7	8	9
×●	—	●–	●×	××	●●	–● –× ×–	–● –× ×–	–● –×

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

```
9 9 8 3 7 3 8 4 2 7 3 8 3 4 3 4 9 2 1 9 4 3 8 1 5 2 4
```

```
- -   ●-  ●-  ●×--  ●-  ●-●×●-●×- --×●- ●×●-  ×●××--●×
                          R                  E/ G

3 6 1 3 1 5 6 1 6 5 9 6 1 7 9 4 1 3 4 2 7 3 4 8 3 7
●-●●×●●-×●××●●×●●●××- ●●×●  - ●××●●-●×--  ●-●×  ●-
 L    U   E/ I  S  /           / F

2 7 6 7 3 4 1 9 4 6 7 9 8 9 1 6
--  ●●  ●-●××●- ●×●●  -   - ×●●●
          /                S
```

At this point in time, 3 ciphertext characters still need to be mapped. Trying our remaining candidates on the ciphertext, Attempting to substutite –● for 8 doesn't work because we end up with the sequence 7384 as –●—●●× which is not a legal morse code character, so we can eliminate it as a possibility. Also, Attempting to substutite –× for 8 doesn't work because we end up with the sequence 998 as –●–●–× which is not a legal morse code character, so we can eliminate it as a possibility. Which means we know that 8 must map to ×–

1	2	3	4	5	6	7	8	9
×●	—	●–	●×	××	●●	–● –×	×–	–● –×

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

```
9 9 8 3 7 3 8 4 2 7 3 8 3 4 3 4 9 2 1 9 4 3 8 1 5 2 4
- - ×-●-- ●-×-●×--- ●-×-●-●×●-●×- --×●- ●×●-×-×●××--●×
             N        C    R           A  T E/ G

3 6 1 3 1 5 6 1 6 5 9 6 1 7 9 4 1 3 4 2 7 3 4 8 3 7
●-●●×●●-×●××●●×●●●××- ●●×●- - ●××●●-●×--- ●-●××-●--
 L    U   E/ I  S  /           / F          /

2 7 6 7 3 4 1 9 4 6 7 9 8 9 1 6
---  ●●-  ●-●××●- ●×●●- - ×-- ×●●●
          /                S
```

At this point in time, 2 ciphertext characters still need to be mapped. Since 7 has several options we simply try them and look at the first word or two to see if it makes sense. Trying –● for 7 gives us a chunk: CRTMAEATEGLUEISTI. Trying –× for 7 gives us a chunk: CYANOACRYLATEGLUEISBADFORYOURLUNGS. Which means we know that 7 must map to –× Eliminating –× as an option for 9 means that 9 must be –●.

1	2	3	4	5	6	7	8	9
×●	—	●–	●×	××	●●	–×	×–	–●

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

```
9 9 8 3 7 3 8 4 2 7 3 8 3 4 3 4 9 2 1 9 4 3 8 1 5 2 4
-●-●×-●--×●-×-●×---×●-×-●-●×●-●×-●--×●-●●×●-×-×●××--●×
C    Y    A  N  O   A  C    R   Y    L    A  T E/ G

3 6 1 3 1 5 6 1 6 5 9 6 1 7 9 4 1 3 4 2 7 3 4 8 3 7
```

```
●–●●×●●–×●××●●×●●●××–●●●×●–×–●●××●●–●×–––×●–●××–●––×
 L    U   E/ I  S  / B    A  D  / F    O   R  / Y

2 7 6 7 3 4 1 9 4 6 7 9 8 9 1 6
–––×●●–×●–●××●–●●×●●–×–●×––●×●●●
 O   U   R  / L    U   N  G   S
```

Now that we have mapped all the ciphertext characters, the decoded morse code is the answer:

CYANOACRYLATE GLUE IS BAD FOR YOUR LUNGS

23) **[350 points]** Decode the nickname of this fictional character which has been encoded in a Morbit Cipher. Only 5 mappings are given.

```
4 9 5 7 5 9 8 4 9 5 1 2 5 3 2 4 9 3 4 8 8 9 8
-●●●x---x-●●●x-●●●x-●--xx-x●-x-●●●x●-●●x●x●●●x
B    O   B    B    Y    /T A  B    L    E S
```

How to solve

Since we are told the mapping of 67123 ciphertext, we can build the following table:

1	2	3	4	5	6	7	8	9
●–	–×	×●	●● ●× –● ×–	●● ●× –● ×–	××	—	●● ●× –● ×–	●● ●× –● ×–

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

```
4 9 5 7 5 9 8 4 9 5 1 2 5 3 2 4 9 3 4 8 8 9 8
      --              ●--x  x●-x    x●
                            A
```

At this point in time, 4 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.

24) **[375 points]** Decode this phrase which has been encoded with the Morbit Cipher. The numbers 7267232 decrypt to "ITIS".

```
4 6 4 2 3 8 7 5 3 8 5 1 2 9 6 7 2 6 7 2 3 2 7 6 8 1
●−−×●−●×●●×−×●××●●×−××−●●×−−−××●●×−××●●×●●●××●−××−−●
W   R   I  T E/ I  T/ D   O   /I  T /I  S   /A  /G

7 6 4 2 1 3 7 6 9 2 2 7 7 3 6 2 1 8 5 1 1 7 3 2 4
×●−×●−●×−●●●×●−×−−●×●××●×●●●−×●×−●×−××−●−●×●●●●×●−
 A  R   B    A  G   E /E V    E N  T/ C    H    A

8 2 9 2 2 8 6 1 9 5 9 7 2 1 8 3
×−●×−−●×●××−−×−●−−××−−×●●×−●×−●●
 N  G   E /M  Y   / M  I  N  D
```

How to solve

With the crib of ITIS mapped to the ciphertext 6726723 we now know the mapping of 4 characters. Since we are told the mapping of 6723 ciphertext, we can build the following table:

1	2	3	4	5	6	7	8	9
●− −● — ×− ××	●×	●●	●− −● — ×− ××	●− −● — ×− ××	−×	×●	●− −● — ×− ××	●− −● — ×− ××

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

```
4 6 4 2 3 8 7 5 3 8 5 1 2 9 6 7 2 6 7 2 3 2 7 6 8 1
  −×  ●×●●  ×●  ●●      ●×  −××●●×−××●●×●●●××●−×
                          / I  T/ I  S  / A

7 6 4 2 1 3 7 6 9 2 2 7 7 3 6 2 1 8 5 1 1 7 3 2 4
×●−×  ●×  ●●×●−×  ●×●××●×●●●−×●×          ×●●●●×
  A          A      E/ E V    E            H

8 2 9 2 2 8 6 1 9 5 9 7 2 1 8 3
  ●×  ●×●×  −×        ×●●×    ●●
      E               I
```

At this point in time, 5 ciphertext characters still need to be mapped. With ×× unknown, looking at unknowns which are next to × which would result in three in a row, we find the sequence 64 where we know that 6 ends with × which means that 4 cannot be ××, so we can eliminate that possibility. Also,we find the sequence 87 where we know that 7 starts with × which means that 8 cannot be ××, so we can eliminate that possibility. Also,we find the sequence 29 where we know that 2 ends with × which means that 9 cannot be ××, so we can eliminate that possibility. Also,we find the sequence 17 where we know that 7 starts with × which means that 1 cannot be ××, so we can eliminate that possibility.

1	2	3	4	5	6	7	8	9
●– –● — ×–	●×	●●	●– –● — ×–	●– –● — ×– ××	–×	×●	●– –● — ×–	●– –● — ×–

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

```
4 6 4 2 3 8 7 5 3 8 5 1 2 9 6 7 2 6 7 2 3 2 7 6 8 1
 ?–x ?●x●● ?x●  ●● ?   ?●x ?–xx●●x–xx●●x●●●xx●–x ? ?
                              / I  T/ I  S  / A

7 6 4 2 1 3 7 6 9 2 2 7 7 3 6 2 1 8 5 1 1 7 3 2 4
x●–x ?●x ?●●x●–x ?●x●xx●x●●●–x●x ? ?   ? ?x●●●●x ?
  A           A      E/ E V    E            H

8 2 9 2 2 8 6 1 9 5 9 7 2 1 8 3
 ?●x ?●x●x ?–x ? ?   ?x●●x ? ?●●
       E              I
```

At this point in time, 5 ciphertext characters still need to be mapped. Looking for unique mappings, 5 is the only cipher text character that can map to ×× so we mark it as such.

1	2	3	4	5	6	7	8	9
●– –● — ×–	●×	●●	●– –● — ×–	××	–×	×●	●– –● — ×–	●– –● — ×–

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

```
4 6 4 2 3 8 7 5 3 8 5 1 2 9 6 7 2 6 7 2 3 2 7 6 8 1
 ?–x ?●x●● ?x●xx●● ?xx ?●x ?–xx●●x–xx●●x●●●xx●–x ? ?
             E/     /        / I  T/ I  S  / A

7 6 4 2 1 3 7 6 9 2 2 7 7 3 6 2 1 8 5 1 1 7 3 2 4
x●–x ?●x ?●●x●–x ?●x●xx●x●●●–x●x ? ?xx ? ?x●●●●x ?
  A           A      E/ E V    E     /      H

8 2 9 2 2 8 6 1 9 5 9 7 2 1 8 3
 ?●x ?●x●x ?–x ? ?xx ?x●●x ? ?●●
       E         /    I
```

At this point in time, 4 ciphertext characters still need to be mapped. Looking for unknowns next to ×× which would result in three in a row, we find the sequence 51 where we know that 5 is ×× which means that 1 cannot start with ×, so we can eliminate those possibilities Also,we find the sequence 51 where we know that 5 is ×× which means that 1 cannot start with ×, so we can eliminate those possibilities Also,we find the sequence 59 where we know that 5 is ×× which means that 9 cannot start with ×, so we can eliminate those possibilities

1	2	3	4	5	6	7	8	9
●– –● —	●×	●●	●– –● — ×–	××	–×	×●	●– –● — ×–	●– –● —

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

```
4 6 4 2 3 8 7 5 3 8 5 1 2 9 6 7 2 6 7 2 3 2 7 6 8 1
 ?–x ?●x●● ?x●xx●● ?xx??●x??–xx●●x–xx●●x●●●xx●–x ???
             E/     /        / I  T/ I  S  / A

7 6 4 2 1 3 7 6 9 2 2 7 7 3 6 2 1 8 5 1 1 7 3 2 4
x●–x ?●x??●●x●–x??●x●xx●x●●●–x●x?? ?xx????x●●●●x ?
  A           A      E/ E V    E     /      H

8 2 9 2 2 8 6 1 9 5 9 7 2 1 8 3
 ?●x??●x●x ?–x????xx??x●●x?? ?●●
        E         /    I
```

At this point in time, 4 ciphertext characters still need to be mapped. Trying our remaining candidates on the ciphertext, Attempting to substutite — for 8 doesn't work because we end up with the sequence 2387 as ●●—×● which is not a legal morse code character, so we can eliminate it as a possibility.Since 9 has several options we simply try them and look at the first word or two to see if it makes sense. Trying ●– for 9 gives us a chunk: AREEVE . Trying –● for 9 gives us a chunk: ADEEVE . Trying — for 9 gives us a chunk: AGEEVE . Which means we know that 9 must map to —

1	2	3	4	5	6	7	8	9
●– –●	●×	●●	●– –● ×–	××	–×	×●	●– –● ×–	—

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

```
4 6 4 2 3 8 7 5 3 8 5 1 2 9 6 7 2 6 7 2 3 2 7 6 8 1
 ?–x ?●x●● ?x●xx●● ?xx??●x–––xx●●x–xx●●x●●●xx●–x ???
             E/     /     O  / I  T/ I  S  / A

7 6 4 2 1 3 7 6 9 2 2 7 7 3 6 2 1 8 5 1 1 7 3 2 4
x●–x ?●x??●●x●–x––●x●xx●x●●●–x●x?? ?xx????x●●●●x ?
  A           A  G   E/ E V    E     /      H

8 2 9 2 2 8 6 1 9 5 9 7 2 1 8 3
 ?●x––●x●x ?–x??––xx––x●●x?? ?●●
    G   E         / M  I
```

At this point in time, 3 ciphertext characters still need to be mapped. Since 1 has several options we simply try them and look at the first word or two to see if it makes sense. Trying ●– for 1 gives us a chunk: ROITISA. Trying –● for 1 gives us a chunk: DOITISA. Which means we know that 1 must map to –●

1	2	3	4	5	6	7	8	9
–●	●×	●●	●– ×–	××	–×	×●	●– ×–	——

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

```
4 6 4 2 3 8 7 5 3 8 5 1 2 9 6 7 2 6 7 2 3 2 7 6 8 1
 ––× –●×●● –×●××●● –××–●●×–––××●●×–××●●×●●●××●–× ––●
            E/     / D   O  / I  T/ I  S  / A

7 6 4 2 1 3 7 6 9 2 2 7 7 3 6 2 1 8 5 1 1 7 3 2 4
×●–× –●×–●●●×●–×––●×●××●×●●●–×●×–● –××–●–●×●●●●× –
  A      B    A  G   E/ E V    E     / C    H

8 2 9 2 2 8 6 1 9 5 9 7 2 1 8 3
 –●×––●×●× ––×–●––××––×●●×–● –●●
    G   E     Y   / M  I
```

At this point in time, 2 ciphertext characters still need to be mapped. Since 4 has several options we simply try them and look at the first word or two to see if it makes sense. Trying ●– for 4 gives us a chunk: WRITEITDOITISAGARBAGEEVENTCHANGEMYMIND. Trying ×– for 4 gives us a chunk: MNVEVDOITISAPANBAGEEVEXCHCGEWYMI. Which means we know that 4 must map to ●– Eliminating ●– as an option for 8 means that 8 must be ×–.

1	2	3	4	5	6	7	8	9
–●	●×	●●	●–	××	–×	×●	×–	——

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

```
4 6 4 2 3 8 7 5 3 8 5 1 2 9 6 7 2 6 7 2 3 2 7 6 8 1
●––×●–●×●●×–×●××●●×–××–●●×–––××●●×–××●●×●●●××●–××––●
W   R   I  T E/ I  T/ D   O  / I  T/ I  S  / A / G

7 6 4 2 1 3 7 6 9 2 2 7 7 3 6 2 1 8 5 1 1 7 3 2 4
×●–×●–●×–●●●×●–×––●×●××●×●●●–×●×–●×–××–●–●×●●●●×●–
  A  R   B    A  G   E/ E V    E N  T/ C    H    A

8 2 9 2 2 8 6 1 9 5 9 7 2 1 8 3
×–●×––●×●××––×–●––××––×●●×–●×–●●
  N  G   E/ M  Y   / M  I  N  D
```

Now that we have mapped all the ciphertext characters, the decoded morse code is the answer:

WRITE IT DO IT IS A GARBAGE EVENT CHANGE MY MIND

25) **[225 points]** Decode the name of this class of indoor free flight planes. The letters 2, 3, 4, 6, 7, and 8 all decode to -.

```
52150159229519291925190522101021925925220952219521591 2
●–●●×●●×––×●●×–×●×–●●××●––●×●×–●×–●×–●––××●––●×●–●●×●–
L    I  M  I  T E D    P    E N  N  Y     P    L    A

92105
×–●×●
 N  E
```

How to solve

Since we are told the mapping of 234678 ciphertext, we can build the following table:

0	1	2	3	4	5	6	7	8	9
●–×	●–×	–	–	–	●–×	–	–	–	●–×

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

```
52150159229519291925190522101021925925220952219521591 2
 –       ––     –    –      ––     –  –  – ––    ––    –     –

92105
 –
```

At this point in time, 4 ciphertext characters still need to be mapped. The first morse code character can never be an ×,

0	1	2	3	4	5	6	7	8	9
●–×	●–×	–	–	–	●–	–	–	–	●–×

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

```
52150159229519291925190522101021925925220952219521591 2
?– ?  ? –– ?  –   –?   ?––    –  –? –?––  ?––  ?– ?  –

92105
 –  ?
```

At this point in time, 4 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.

26) **[250 points]** Decode this definition from urban dictionary which has been encoded using a Pollux Cipher. 0,5=x, 1,3=•, 2,4=-

```
4809024030088032041009202300390280880248038908012032 31
--x●x--x●xx--x●-x-●xx●-x-●xx●●x--x--x---x●-●x-x●-x●-●●
M  E M  E  M  A  N   A  N   I  M  M  O   R   T A  L

0021310301302102890091910300910139003033801092108922
xx-●●●x●x●●x-●x--●xx●●●●x●xx●●x●●●xx●x●●●-x●x●-●x-●--
  B    E I  N  G    H    E  I  S    E V    E R   Y

0382031910301230100231103180400180381903310228008908 82
x●--x●●●●x●x●-●x●xx-●●●x●●-x-xx●-x●-●●x●●●x---xx-●x---
 W   H    E R   E  B    U   T  A  L    S   O    N  O

0982031910301810 3
x●--x●●●●x●x●-●x●
 W   H    E R   E
```

How to solve

Since we are told the mapping of 012345 ciphertext, we can build the following table:

0	1	2	3	4	5	6	7	8	9
×	●	–	●	–	×	●–×	●–×	●–×	●–×

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

```
4809024030088032041009202300390280880248038908012032 31
- x x--x●xx  x●-x-●xx -x-●xx● x- x  x-- x●  x x●-x●-●●
    M  E/    A  N /    N /                    A  L

0021310301302102890091910300910139003033801092108922
xx-●●●x●x●●x-●x-  xx ● ●x●xx ●x●● xx●x●●● x●x -●x  --
/ B    E I  N    /      E/       / E     E

0382031910301230100231103180400180381903310228008908 82
x● -x●● ●x●x●-●x●xx-●●●x●● x-xx● x● ● x●●●x-- xx  x  -
         E R   E/ B       T/         S     /

0982031910301810 3
x  -x●● ●x●x● ●x●
         E     E
```

At this point in time, 2 ciphertext characters still need to be mapped. Looking at the ciphertext, we see the sequence 008 which would result in three ×s in a row if 8 were an ×. Also, we see the sequence 009 which would result in three ×s in a row if 9 were an ×.

0	1	2	3	4	5	6	7	8	9

0	1	2	3	4	5	6	7	8	9
×	●	–	●	–	×	●–×	●–×	●–	●–

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

```
480902403008803204100920230039028088024803890801203231
–?×?×––×●××??×●–×–●××?–×–●××●?×–?×??×––?×●??×?×●–×●–●●
     M  E/    A  N /    N /                    A  L

002131030130210289009191030091013900303338010921089 22
××–●●●×●×●●×–●×–??××?●?●×●××?●×●●?××●×●●●?×●×?–●×??––
/ B    E I  N     /      E/       / E     E

038203191030123010023110318040018038190331022800890882
×●?–×●●?●×●×●–●×●××–●●●×●●?×–××●?×●?●?×●●●×––?××??×??–
          E R   E/ B        T/         S      /

0982031910301810 3
×??–×●●?●×●×●?●×●
          E     E
```

At this point in time, 2 ciphertext characters still need to be mapped. Since 8 can still map to ●– we simply try them and look at the first word or two to see if it makes sense. Trying ● for 8 gives us a chunk: ERE BST I. Trying – for 8 gives us a chunk: ERE BUT A. Which means we know that 8 must map to –

0	1	2	3	4	5	6	7	8	9
×	●	–	●	–	×	●–×	●–×	–	●–

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

```
480902403008803204100920230039028088024803890801203231
––×?×––×●××––×●–×–●××?–×–●××●?×––×––×–––×●–?×–×●–×●–●●
M    M  E/ M  A  N /    N /    M  M  O       T A  L

002131030130210289009191030091013900303338010921089 22
××–●●●×●×●●×–●×––?××?●?●×●××?●×●●?××●×●●●–×●×?–●×–?––
/ B    E I  N     /      E/       / E V    E

038203191030123010023110318040018038190331022800890882
×●––×●●?●×●×●–●×●××–●●●×●●–×–××●–×●–●?×●●●×–––××–?×–––
 W        E R   E/ B    U   T/ A       S   O  /    O

0982031910301810 3
×?––×●●?●×●×●–●×●
          E R   E
```

At this point in time, 1 ciphertext characters still need to be mapped. Based on the sequence 8922 with 9 possibly being one of '●–, only ● results in a legal morse code character, so we can mark 9 as being ●.

0	1	2	3	4	5	6	7	8	9

0	1	2	3	4	5	6	7	8	9
×	●	–	●	–	×	●–×	●–×	–	●

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

```
4809024030088032041009202300390280880248038908012032 31
--×●×--×●××--×●-×-●××●-×-●××●●×--×--×---×●-●×-×●-×●-●●
M  E M  E/ M  A  N / A  N / I  M  M  O   R   T A  L

00213103013021028900919103009101390030333801092108922
××-●●●×●×●●×-●×--●××●●●●×●××●●×●●●××●×●●●-×●×●-●×-●--
/ B    E I  N  G  / H    E/ I  S  / E V    E R   Y

03820319103012301002311031804001803819033102280089088 2
×●--×●●●●×●×●-●×●××-●●●×●●-×-××●-×●-●●×●●●×---××-●×---
 W   H    E R   E/ B    U   T/ A  L    S   O  / N  O

0982031910301810 3
×●--×●●●●×●×●-●×●
 W   H    E R   E
```

Now that we have mapped all the ciphertext characters, the decoded morse code is the answer:

MEME MAN AN IMMORTAL BEING HE IS EVERYWHERE BUT ALSO NOWHERE

27) **[350 points]** Decode this phrase which has been encoded with a Pollux Cipher. The numbers "32363121913" encode to the letters "TERE".

```
5045342596149345901436619537416630890488121313241901801 6
-●--x---x●●-xx--x●●-x●●●x-xx-●●●x●xx●-xx●-●x●x--●x●●x●●●
Y    O   U    M  U   S   T  B    E  A   R   E G   I  S

3236312191351637243082282110768620372557209947666096981646
x-x●x●-●x●x-●●xx--x●x--x-●●●x●x●-●xx---x-●xx-x●●●●x●xx●●-●
 T E R   E D    M  E M  B    E R    O   N   T H    E  F

3252804030053523757422930726131094870556912855690311 1
x---x●-●x●●-x--xx-x---xx●x-●●x●●x-xx●--●x●-x--●x●x●●●
 O   R   U   M   T O    E D   I  T  P   A  G   E S
```

How to solve

With the crib of TERE mapped to the ciphertext 163236312191 we now know the mapping of 5 characters. Since we are told the mapping of 16329 ciphertext, we can build the following table:

0	1	2	3	4	5	6	7	8	9
●–×	●	–	×	●–×	●–×	●	●–×	●–×	×

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

```
5045342596149345901436619537416630890488121313241901801 6
    x - x●● xx  x ● x●●●x x  ●●●x  x    ●-●x●x- ●x ●  ●●
          /       S                    E

3236312191351637243082282110768620372557209947666096981646
x-x●x●-●x●x ●●x - x  -- -●●  ● ●- x -   - xx  ●●● x●x ●● ●
 T E R   E                              /       E

3252804030053523757422930726131094870556912855690311 1
x- -    x   x -x    --xx  -●●x● x      ●x●-   ●x x●●●
                     /                       S
```

At this point in time, 5 ciphertext characters still need to be mapped. The first morse code character can never be an ×,

0	1	2	3	4	5	6	7	8	9
●–×	●	–	×	●–×	●–	●	●–×	●–×	×

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

```
5045342596149345901436619537416630890488121313241901801 6
?  ?x -?x●● xx ?x ● x●●●x?x  ●●●x  x    ●-●x●x- ●x ●  ●●
          /       S                    E

3236312191351637243082282110768620372557209947666096981646
```

```
x–x●x●–●x●x?●●x – x  –– –●●  ● ●– x –?? – ××  ●●● x●x ●● ●
 T E R   E                                    /       E

3252804030053523757422930726131094870556912855690311 1
x–?–    x  ?x?–x ?  ––×× –●●×● x    ??●x●– ??●x x●●●
                    /                          S
```

At this point in time, 5 ciphertext characters still need to be mapped. Looking at the ciphertext, we see the sequence 493 which would result in three ×s in a row if 4 were an ×. Also, we see the sequence 099 which would result in three ×s in a row if 0 were an ×.

0	1	2	3	4	5	6	7	8	9
●–	●	–	×	●–	●–	●	●–×	●–×	×

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

```
5045342596149345901436619537416630890488121313241901801 6
????x?–?x●●?××??x?●?x●●●x?x ?●●●x? x??  ●–●x●x–?●x?● ?●●
          /       S                    E

3236312191351637243082282110768620372557209947666096981646
x–x●x●–●x●x?●●x –?x? –– –●●? ● ●–?x –?? –?××? ●●●?x●x ●●?●
 T E R   E                                /       E

3252804030053523757422930726131094870556912855690311 1
x–?– ???x???x?–x ? ?––××? –●●x●?x?  ???●x●– ??●x?x●●●
                    /                          S
```

At this point in time, 5 ciphertext characters still need to be mapped. Since 5 can still map to ●– we simply try them and look at the first word or two to see if it makes sense. Trying ● for 5 gives us a chunk: TERES. Trying – for 5 gives us a chunk: TERED. Which means we know that 5 must map to –

0	1	2	3	4	5	6	7	8	9
●–	●	–	×	●–	–	●	●–×	●–×	×

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

```
5045342596149345901436619537416630890488121313241901801 6
–??–x?––x●●?××?–x?●?x●●●x–x ?●●●x? x??  ●–●x●x–?●x?● ?●●
          /       S   T                E

3236312191351637243082282110768620372557209947666096981646
x–x●x●–●x●x–●●x –?x? –– –●●? ● ●–?x ––– –?××? ●●●?x●x ●●?●
 T E R   E D                              /       E

3252804030053523757422930726131094870556912855690311 1
x––– ???x??–x––x – ?––××? –●●x●?x?  ?––●x●– ––●x?x●●●
          M         /                          S
```

At this point in time, 4 ciphertext characters still need to be mapped. Based on the sequence 128556 with 8 possibly being one of '●–×, only × results in a legal morse code character, so we can mark 8 as being ×.

0	1	2	3	4	5	6	7	8	9
●–	●	–	×	●–	–	●	●–×	×	×

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

```
5045342596149345901436619537416630890488121313241901801 6
-??-x?--x●●?××?-x?●?x●●●x-x ?●●●x?××??××●-●x●x-?●x?●x?●●
             /        S   T        /   / R   E

3236312191351637243082282110768620372557209947666096981646
x-x●x●-●x●x-●●x -?x?x--x-●●? ●x●-?x --- -?××? ●●●?x●××●●?●
 T E R   E D         M                    /        E/

3252804030053523757422930726131094870556912855690311 1
x---x???x??-x--x - ?--××? -●●x●?x?x ?--●x●-x--●x?x●●●
 O           M        /                  A  G     S
```

At this point in time, 3 ciphertext characters still need to be mapped. Since 0 can still map to ●– we simply try them and look at the first word or two to see if it makes sense. Trying ● for 0 gives us a chunk: ISTERED. Trying – for 0 gives us a chunk: NDTERED. Which means we know that 0 must map to ●

0	1	2	3	4	5	6	7	8	9
●	●	–	×	●–	–	●	●–×	×	×

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

```
5045342596149345901436619537416630890488121313241901801 6
-●?-x?--x●●?××?-x●●?x●●●x-x ?●●●x●××●?××●-●x●x-?●x●●x●●●
             /        S   T       E/   / R   E     I  S

3236312191351637243082282110768620372557209947666096981646
x-x●x●-●x●x-●●x -?x●x--x-●●● ●x●-●x --- -●××? ●●●●x●××●●?●
 T E R   E D       E M         R          /        E/

3252804030053523757422930726131094870556912855690311 1
x---x●?●x●●-x--x - ?--××● -●●x●●x?x ●--●x●-x--●x●x●●●
 O       U   M        /       I          A  G   E S
```

At this point in time, 2 ciphertext characters still need to be mapped. Based on the sequence 211076 with 7 possibly being one of '●–×, only × results in a legal morse code character, so we can mark 7 as being ×.

0	1	2	3	4	5	6	7	8	9
●	●	–	×	●–	–	●	×	×	×

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

```
5045342596149345901436619537416630890488121313241901801 6
-●?-x?--x●●?××?-x●●?x●●●x-xx?●●●x●××●?××●-●x●x-?●x●●x●●●
```

```
          /       S   T/     E/   / R   E     I   S

3236312191351637243082282110768620372557209947666096981646
x–x●x●–●x●x–●●xx–?x●x––x–●●●x●x●–●xx–––x–●xx?x●●●●x●xx●●?●
 T E R   E D  /    E M  B    E R  / O   N /   H    E/

3252804030053523757422930726131094870556912855690311 1
x–––x●?●x●●–x––xx–x?––xx●x–●●x●●x?xx●––●x●–x––●x●x●●●
 O       U   M / T    / E D   I   / P    A  G   E S
```

At this point in time, 1 ciphertext characters still need to be mapped. Since 4 can still map to ●– we simply try them and look at the first word or two to see if it makes sense. Trying ● for 4 gives us a chunk: XWS ASST HE I REDISTERED NEMBER ON EHE HOSUM TW EDIE PAGE. Trying – for 4 gives us a chunk: YOU MUST BE A REGISTERED MEMBER ON THE FORUM TO EDIT PAGE. Which means we know that 4 must map to –

0	1	2	3	4	5	6	7	8	9
●	●	–	×	–	–	●	×	×	×

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

```
5045342596149345901436619537416630890488121313241901801 6
–●––x–––x●●–xx––x●●–x●●●x–xx–●●●x●xx●–xx●–●x●x––●x●●x●●●
Y    O   U  / M  U   S   T/ B    E/ A / R   E G   I  S

3236312191351637243082282110768620372557209947666096981646
x–x●x●–●x●x–●●xx––x●x––x–●●●x●x●–●xx–––x–●xx–x●●●●x●xx●●–●
 T E R   E D  / M  E M  B    E R  / O   N / T H    E/ F

3252804030053523757422930726131094870556912855690311 1
x–––x●–●x●●–x––xx–x–––xx●x–●●x●●x–xx●––●x●–x––●x●x●●●
 O   R   U   M / T O  / E D   I  T/ P    A  G   E S
```

Now that we have mapped all the ciphertext characters, the decoded morse code is the answer:

YOU MUST BE A REGISTERED MEMBER ON THE FORUM TO EDIT PAGES

28) **[175 points]** Andrew and Brooklin want to communicate with each other using RSA for encryption. Andrew generates RSA keys obtaining the following values:

n = 20016863 q = 2039

p = 9817 d = 18819931

Φ = 20005008 e = 7516195

Likewise, Brooklin also generates RSA keys resulting in the values

d = 21336781 p = 5923

n = 30675217 Φ = 30664116

q = 5179 e = 18266425

They ask each other for the public keys in order to communicate.What information do they each need to transmit in response?

You must also determine what formula Andrew needs to calculate in order to transmit the value 2205 to Brooklin

Enter the minimum values that Brooklin needs to transmit to Andrew:

30675217	**18266425**	

These two numbers can be in either order.

Enter the minimum values that Andrew needs to transmit to Brooklin:

20016863	**7516195**	

These two numbers can be in either order.

Write the formula Andrew needs to calculate in order to transmit the value 2205 to Brooklin

2205 ^ 18266425 mod 30675217

How to solve

Brooklin needs to send only their public key (*e*=18266425, *n*=30675217) to Andrew
Andrew needs to send only their public key (*e*=7516195, *n*=20016863) to Brooklin
Andrew needs to use Brooklin's public key (n = 30675217, e = 18266425) in order to encrypt the value 2205.

Hence the formula is: `value ^ e mod n`

29) **[525 points]** Jake, has faithfully followed the steps of the RSA key-generation algorithm. Here are the results:

p = 347

q = 337

n = 116939

Φ = 116256

e = 110077

Unfortunately, Jake doesn't know how to compute the value of *d* and needs you to do that final step for them.

Enter the computed value of *d*, NOT the formula.

75541

How to solve

To compute d, you need to use the extended Euclidean Algorithm (https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm) to compute the greatest common divisor of integers $e = 110077$ and $\Phi = 116256$ and the integer coefficients of Bézout's identity. (https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity)
In each iteration, the quotient q_i is calculated by:
$q_i = \lfloor r_{i-1} \div r_i \rfloor$
The remainder and two coefficients are calculated with the formulas:

$r_{i+1} = r_{i-1} - q_i r_i$	$s_{i+1} = s_{i-1} - q_i s_i$	$t_{i+1} = t_{i-1} - q_i t_i$

Therefore, using the initial conditions as specified for the extended Euclidean Algorithm (https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm):

$r_0 = 116256$	$s_0 = 1$	$t_0 = 0$
$r_1 = 110077$	$s_1 = 0$	$t_1 = 1$

Calculate r_i, s_i, t_i until $r_i = 1$; at which time, $t_i = d$ which is the modular multiplicative inverse of $e \mod \Phi$
(Note: When $r_i = 1$, s_i will be the modular multiplicative inverse of $\Phi \mod e$)

Iteration 1 ...

Start with first set of values for the remainder and coefficients: $r_0 = 116256, s_0 = 1, t_0 = 0$
... and the second set of values for them: $r_1 = 110077, s_1 = 0, t_1 = 1$
The quotient for this step is computed from $q_i = \lfloor 116256 \div 110077 \rfloor = 1$

$r_2 = r_0 - (q_1 * r_1)$ $r_2 = 116256 - (1 * 110077)$ $r_2 = 116256 - 110077$ $r_2 = 6179$	$s_2 = s_0 - (q_1 * s_1)$ $s_2 = 1 - (1 * 0)$ $s_2 = 1 - 0$ $s_2 = 1$	$t_2 = t_0 - (q_1 * t_1)$ $t_2 = 0 - (1 * 1)$ $t_2 = 0 - 1$ $t_2 = -1$

Iteration 2 ...

Start with first set of values for the remainder and coefficients: $r_1 = 110077, s_1 = 0, t_1 = 1$
... and the second set of values for them: $r_2 = 6179, s_2 = 1, t_2 = -1$
The quotient for this step is computed from $q_i = \lfloor 110077 \div 6179 \rfloor = 17$

$r_3 = r_1 - (q_2 * r_2)$ $r_3 = 110077 - (17 * 6179)$ $r_3 = 110077 - 105043$ $r_3 = 5034$	$s_3 = s_1 - (q_2 * s_2)$ $s_3 = 0 - (17 * 1)$ $s_3 = 0 - 17$ $s_3 = -17$	$t_3 = t_1 - (q_2 * t_2)$ $t_3 = 1 - (17 * -1)$ $t_3 = 1 - (-17)$ $t_3 = 18$

Iteration 3 ...

Start with first set of values for the remainder and coefficients: $r_2 = 6179, s_2 = 1, t_2 = -1$
... and the second set of values for them: $r_3 = 5034, s_3 = -17, t_3 = 18$
The quotient for this step is computed from $q_i = \lfloor 6179 \div 5034 \rfloor = 1$

$r_4 = r_2 - (q_3 * r_3)$ $r_4 = 6179 - (1 * 5034)$ $r_4 = 6179 - 5034$ $r_4 = 1145$	$s_4 = s_2 - (q_3 * s_3)$ $s_4 = 1 - (1 * -17)$ $s_4 = 1 - (-17)$ $s_4 = 18$	$t_4 = t_2 - (q_3 * t_3)$ $t_4 = -1 - (1 * 18)$ $t_4 = -1 - 18$ $t_4 = -19$

Iteration 4 ...

Start with first set of values for the remainder and coefficients: $r_3 = 5034, s_3 = -17, t_3 = 18$
... and the second set of values for them: $r_4 = 1145, s_4 = 18, t_4 = -19$
The quotient for this step is computed from $q_i = \lfloor 5034 \div 1145 \rfloor = 4$

$r_5 = r_3 - (q_4 * r_4)$ $r_5 = 5034 - (4 * 1145)$ $r_5 = 5034 - 4580$ $r_5 = 454$	$s_5 = s_3 - (q_4 * s_4)$ $s_5 = -17 - (4 * 18)$ $s_5 = -17 - 72$ $s_5 = -89$	$t_5 = t_3 - (q_4 * t_4)$ $t_5 = 18 - (4 * -19)$ $t_5 = 18 - (-76)$ $t_5 = 94$

Iteration 5 ...

Start with first set of values for the remainder and coefficients: $r_4 = 1145, s_4 = 18, t_4 = -19$
... and the second set of values for them: $r_5 = 454, s_5 = -89, t_5 = 94$
The quotient for this step is computed from $q_i = \lfloor 1145 \div 454 \rfloor = 2$

$r_6 = r_4 - (q_5 * r_5)$ $r_6 = 1145 - (2 * 454)$ $r_6 = 1145 - 908$ $r_6 = 237$	$s_6 = s_4 - (q_5 * s_5)$ $s_6 = 18 - (2 * -89)$ $s_6 = 18 - (-178)$ $s_6 = 196$	$t_6 = t_4 - (q_5 * t_5)$ $t_6 = -19 - (2 * 94)$ $t_6 = -19 - 188$ $t_6 = -207$

Iteration 6 ...

Start with first set of values for the remainder and coefficients: $r_5 = 454, s_5 = -89, t_5 = 94$
... and the second set of values for them: $r_6 = 237, s_6 = 196, t_6 = -207$
The quotient for this step is computed from $q_i = \lfloor 454 \div 237 \rfloor = 1$

$r_7 = r_5 - (q_6 * r_6)$ $r_7 = 454 - (1 * 237)$ $r_7 = 454 - 237$ $r_7 = 217$	$s_7 = s_5 - (q_6 * s_6)$ $s_7 = -89 - (1 * 196)$ $s_7 = -89 - 196$ $s_7 = -285$	$t_7 = t_5 - (q_6 * t_6)$ $t_7 = 94 - (1 * -207)$ $t_7 = 94 - (-207)$ $t_7 = 301$

Iteration 7 ...

Start with first set of values for the remainder and coefficients: $r_6 = 237, s_6 = 196, t_6 = -207$
... and the second set of values for them: $r_7 = 217, s_7 = -285, t_7 = 301$

The quotient for this step is computed from $q_i = \lfloor 237 \div 217 \rfloor = 1$

$r_8 = r_6 - (q_7 * r_7)$ $r_8 = 237 - (1 * 217)$ $r_8 = 237 - 217$ $r_8 = 20$	$s_8 = s_6 - (q_7 * s_7)$ $s_8 = 196 - (1 * -285)$ $s_8 = 196 - (-285)$ $s_8 = 481$	$t_8 = t_6 - (q_7 * t_7)$ $t_8 = -207 - (1 * 301)$ $t_8 = -207 - 301$ $t_8 = -508$

Iteration 8 ...

Start with first set of values for the remainder and coefficients: $r_7 = 217, s_7 = -285, t_7 = 301$
... and the second set of values for them: $r_8 = 20, s_8 = 481, t_8 = -508$
The quotient for this step is computed from $q_i = \lfloor 217 \div 20 \rfloor = 10$

$r_9 = r_7 - (q_8 * r_8)$ $r_9 = 217 - (10 * 20)$ $r_9 = 217 - 200$ $r_9 = 17$	$s_9 = s_7 - (q_8 * s_8)$ $s_9 = -285 - (10 * 481)$ $s_9 = -285 - 4810$ $s_9 = -5095$	$t_9 = t_7 - (q_8 * t_8)$ $t_9 = 301 - (10 * -508)$ $t_9 = 301 - (-5080)$ $t_9 = 5381$

Iteration 9 ...

Start with first set of values for the remainder and coefficients: $r_8 = 20, s_8 = 481, t_8 = -508$
... and the second set of values for them: $r_9 = 17, s_9 = -5095, t_9 = 5381$
The quotient for this step is computed from $q_i = \lfloor 20 \div 17 \rfloor = 1$

$r_{10} = r_8 - (q_9 * r_9)$ $r_{10} = 20 - (1 * 17)$ $r_{10} = 20 - 17$ $r_{10} = 3$	$s_{10} = s_8 - (q_9 * s_9)$ $s_{10} = 481 - (1 * -5095)$ $s_{10} = 481 - (-5095)$ $s_{10} = 5576$	$t_{10} = t_8 - (q_9 * t_9)$ $t_{10} = -508 - (1 * 5381)$ $t_{10} = -508 - 5381$ $t_{10} = -5889$

Iteration 10 ...

Start with first set of values for the remainder and coefficients: $r_9 = 17, s_9 = -5095, t_9 = 5381$
... and the second set of values for them: $r_{10} = 3, s_{10} = 5576, t_{10} = -5889$
The quotient for this step is computed from $q_i = \lfloor 17 \div 3 \rfloor = 5$

$r_{11} = r_9 - (q_{10} * r_{10})$ $r_{11} = 17 - (5 * 3)$ $r_{11} = 17 - 15$ $r_{11} = 2$	$s_{11} = s_9 - (q_{10} * s_{10})$ $s_{11} = -5095 - (5 * 5576)$ $s_{11} = -5095 - 27880$ $s_{11} = -32975$	$t_{11} = t_9 - (q_{10} * t_{10})$ $t_{11} = 5381 - (5 * -5889)$ $t_{11} = 5381 - (-29445)$ $t_{11} = 34826$

Iteration 11 ...

Start with first set of values for the remainder and coefficients: $r_{10} = 3, s_{10} = 5576, t_{10} = -5889$
... and the second set of values for them: $r_{11} = 2, s_{11} = -32975, t_{11} = 34826$
The quotient for this step is computed from $q_i = \lfloor 3 \div 2 \rfloor = 1$

$r_{12} = r_{10} - (q_{11} * r_{11})$ $r_{12} = 3 - (1 * 2)$ $r_{12} = 3 - 2$ $r_{12} = 1$	$s_{12} = s_{10} - (q_{11} * s_{11})$ $s_{12} = 5576 - (1 * -32975)$ $s_{12} = 5576 - (-32975)$ $s_{12} = 38551$	$t_{12} = t_{10} - (q_{11} * t_{11})$ $t_{12} = -5889 - (1 * 34826)$ $t_{12} = -5889 - 34826$ $t_{12} = -40715$

Success!

Since the value for *d* is negative, add the modulus 116256

$-40715 + 116256 = 75541$

$d = 75541$

Therefore, let's check that $d \cdot e = 1 \mod \Phi$

$75541 \cdot 110077 = 1 \mod 116256$

$8315326657 = 1 \mod 116256$

$1 + 8315326656 = 1 \mod 116256$

$1 + (71526 \cdot 116256) = 1 \mod 116256$

Hence 75541 and 116256 are inverses of each other

30) **[600 points]** Jesse has the following RSA public key:

`n = 38609821  e = 6315131`

Unfortunately for them, A quantum computer has successfully factored their *n*

```
38609821 = 8923 * 4327
```

Compute the value of their private key:

Enter the computed private key:

21408179

How to solve

To find the private key, First we need to find Φ using the formula:
$\Phi = (p-1) * (q-1)$
$\Phi = (8923-1) * (4327-1) = 8922 * 4326 = 38596572$
We now know that we know that $\Phi = 38596572$

Second, we use the extended Euclidean Algorithm (https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm) using 6315131 and 38596572

In each iteration, the quotient q_i is calculated by:
$q_i = \lfloor r_{i-1} \div r_i \rfloor$
The remainder and two coefficients are calculated with the formulas:

$r_{i+1} = r_{i-1} - q_i r_i$	$s_{i+1} = s_{i-1} - q_i s_i$	$t_{i+1} = t_{i-1} - q_i t_i$

Therefore, using the initial conditions as specified for the extended Euclidean Algorithm (https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm):

$r_0 = 38596572$	$s_0 = 1$	$t_0 = 0$
$r_1 = 6315131$	$s_1 = 0$	$t_1 = 1$

Calculate r_i, s_i, t_i until $r_i = 1$; at which time, $t_i = d$ which is the modular multiplicative inverse of $e \mod \Phi$
(Note: When $r_i = 1$, s_i will be the modular multiplicative inverse of $\Phi \mod e$)

Iteration 1 ...

Start with first set of values for the remainder and coefficients: $r_0 = 38596572, s_0 = 1, t_0 = 0$
... and the second set of values for them: $r_1 = 6315131, s_1 = 0, t_1 = 1$
The quotient for this step is computed from $q_i = \lfloor 38596572 \div 6315131 \rfloor = 6$

$r_2 = r_0 - (q_1 * r_1)$	$s_2 = s_0 - (q_1 * s_1)$	$t_2 = t_0 - (q_1 * t_1)$
$r_2 = 38596572 - (6 * 6315131)$	$s_2 = 1 - (6 * 0)$	$t_2 = 0 - (6 * 1)$
$r_2 = 38596572 - 37890786$	$s_2 = 1 - 0$	$t_2 = 0 - 6$
$r_2 = 705786$	$s_2 = 1$	$t_2 = -6$

Iteration 2 ...

Start with first set of values for the remainder and coefficients: $r_1 = 6315131, s_1 = 0, t_1 = 1$
... and the second set of values for them: $r_2 = 705786, s_2 = 1, t_2 = -6$

The quotient for this step is computed from $q_i = \lfloor 6315131 \div 705786 \rfloor = 8$

$r_3 = r_1 - (q_2 * r_2)$ $r_3 = 6315131 - (8 * 705786)$ $r_3 = 6315131 - 5646288$ $r_3 = 668843$	$s_3 = s_1 - (q_2 * s_2)$ $s_3 = 0 - (8 * 1)$ $s_3 = 0 - 8$ $s_3 = -8$	$t_3 = t_1 - (q_2 * t_2)$ $t_3 = 1 - (8 * -6)$ $t_3 = 1 - (-48)$ $t_3 = 49$

Iteration 3 ...

Start with first set of values for the remainder and coefficients: $r_2 = 705786, s_2 = 1, t_2 = -6$
... and the second set of values for them: $r_3 = 668843, s_3 = -8, t_3 = 49$
The quotient for this step is computed from $q_i = \lfloor 705786 \div 668843 \rfloor = 1$

$r_4 = r_2 - (q_3 * r_3)$ $r_4 = 705786 - (1 * 668843)$ $r_4 = 705786 - 668843$ $r_4 = 36943$	$s_4 = s_2 - (q_3 * s_3)$ $s_4 = 1 - (1 * -8)$ $s_4 = 1 - (-8)$ $s_4 = 9$	$t_4 = t_2 - (q_3 * t_3)$ $t_4 = -6 - (1 * 49)$ $t_4 = -6 - 49$ $t_4 = -55$

Iteration 4 ...

Start with first set of values for the remainder and coefficients: $r_3 = 668843, s_3 = -8, t_3 = 49$
... and the second set of values for them: $r_4 = 36943, s_4 = 9, t_4 = -55$
The quotient for this step is computed from $q_i = \lfloor 668843 \div 36943 \rfloor = 18$

$r_5 = r_3 - (q_4 * r_4)$ $r_5 = 668843 - (18 * 36943)$ $r_5 = 668843 - 664974$ $r_5 = 3869$	$s_5 = s_3 - (q_4 * s_4)$ $s_5 = -8 - (18 * 9)$ $s_5 = -8 - 162$ $s_5 = -170$	$t_5 = t_3 - (q_4 * t_4)$ $t_5 = 49 - (18 * -55)$ $t_5 = 49 - (-990)$ $t_5 = 1039$

Iteration 5 ...

Start with first set of values for the remainder and coefficients: $r_4 = 36943, s_4 = 9, t_4 = -55$
... and the second set of values for them: $r_5 = 3869, s_5 = -170, t_5 = 1039$
The quotient for this step is computed from $q_i = \lfloor 36943 \div 3869 \rfloor = 9$

$r_6 = r_4 - (q_5 * r_5)$ $r_6 = 36943 - (9 * 3869)$ $r_6 = 36943 - 34821$ $r_6 = 2122$	$s_6 = s_4 - (q_5 * s_5)$ $s_6 = 9 - (9 * -170)$ $s_6 = 9 - (-1530)$ $s_6 = 1539$	$t_6 = t_4 - (q_5 * t_5)$ $t_6 = -55 - (9 * 1039)$ $t_6 = -55 - 9351$ $t_6 = -9406$

Iteration 6 ...

Start with first set of values for the remainder and coefficients: $r_5 = 3869, s_5 = -170, t_5 = 1039$
... and the second set of values for them: $r_6 = 2122, s_6 = 1539, t_6 = -9406$
The quotient for this step is computed from $q_i = \lfloor 3869 \div 2122 \rfloor = 1$

$r_7 = r_5 - (q_6 * r_6)$ $r_7 = 3869 - (1 * 2122)$ $r_7 = 3869 - 2122$ $r_7 = 1747$	$s_7 = s_5 - (q_6 * s_6)$ $s_7 = -170 - (1 * 1539)$ $s_7 = -170 - 1539$ $s_7 = -1709$	$t_7 = t_5 - (q_6 * t_6)$ $t_7 = 1039 - (1 * -9406)$ $t_7 = 1039 - (-9406)$ $t_7 = 10445$

Iteration 7 ...

Start with first set of values for the remainder and coefficients: $r_6 = 2122, s_6 = 1539, t_6 = -9406$

... and the second set of values for them: $r_7 = 1747, s_7 = -1709, t_7 = 10445$
The quotient for this step is computed from $q_i = \lfloor 2122 \div 1747 \rfloor = 1$

$r_8 = r_6 - (q_7 * r_7)$ $r_8 = 2122 - (1 * 1747)$ $r_8 = 2122 - 1747$ $r_8 = 375$	$s_8 = s_6 - (q_7 * s_7)$ $s_8 = 1539 - (1 * -1709)$ $s_8 = 1539 - (-1709)$ $s_8 = 3248$	$t_8 = t_6 - (q_7 * t_7)$ $t_8 = -9406 - (1 * 10445)$ $t_8 = -9406 - 10445$ $t_8 = -19851$

Iteration 8 ...

Start with first set of values for the remainder and coefficients: $r_7 = 1747, s_7 = -1709, t_7 = 10445$
... and the second set of values for them: $r_8 = 375, s_8 = 3248, t_8 = -19851$
The quotient for this step is computed from $q_i = \lfloor 1747 \div 375 \rfloor = 4$

$r_9 = r_7 - (q_8 * r_8)$ $r_9 = 1747 - (4 * 375)$ $r_9 = 1747 - 1500$ $r_9 = 247$	$s_9 = s_7 - (q_8 * s_8)$ $s_9 = -1709 - (4 * 3248)$ $s_9 = -1709 - 12992$ $s_9 = -14701$	$t_9 = t_7 - (q_8 * t_8)$ $t_9 = 10445 - (4 * -19851)$ $t_9 = 10445 - (-79404)$ $t_9 = 89849$

Iteration 9 ...

Start with first set of values for the remainder and coefficients: $r_8 = 375, s_8 = 3248, t_8 = -19851$
... and the second set of values for them: $r_9 = 247, s_9 = -14701, t_9 = 89849$
The quotient for this step is computed from $q_i = \lfloor 375 \div 247 \rfloor = 1$

$r_{10} = r_8 - (q_9 * r_9)$ $r_{10} = 375 - (1 * 247)$ $r_{10} = 375 - 247$ $r_{10} = 128$	$s_{10} = s_8 - (q_9 * s_9)$ $s_{10} = 3248 - (1 * -14701)$ $s_{10} = 3248 - (-14701)$ $s_{10} = 17949$	$t_{10} = t_8 - (q_9 * t_9)$ $t_{10} = -19851 - (1 * 89849)$ $t_{10} = -19851 - 89849$ $t_{10} = -109700$

Iteration 10 ...

Start with first set of values for the remainder and coefficients: $r_9 = 247, s_9 = -14701, t_9 = 89849$
... and the second set of values for them: $r_{10} = 128, s_{10} = 17949, t_{10} = -109700$
The quotient for this step is computed from $q_i = \lfloor 247 \div 128 \rfloor = 1$

$r_{11} = r_9 - (q_{10} * r_{10})$ $r_{11} = 247 - (1 * 128)$ $r_{11} = 247 - 128$ $r_{11} = 119$	$s_{11} = s_9 - (q_{10} * s_{10})$ $s_{11} = -14701 - (1 * 17949)$ $s_{11} = -14701 - 17949$ $s_{11} = -32650$	$t_{11} = t_9 - (q_{10} * t_{10})$ $t_{11} = 89849 - (1 * -109700)$ $t_{11} = 89849 - (-109700)$ $t_{11} = 199549$

Iteration 11 ...

Start with first set of values for the remainder and coefficients: $r_{10} = 128, s_{10} = 17949, t_{10} = -109700$
... and the second set of values for them: $r_{11} = 119, s_{11} = -32650, t_{11} = 199549$
The quotient for this step is computed from $q_i = \lfloor 128 \div 119 \rfloor = 1$

$r_{12} = r_{10} - (q_{11} * r_{11})$ $r_{12} = 128 - (1 * 119)$ $r_{12} = 128 - 119$ $r_{12} = 9$	$s_{12} = s_{10} - (q_{11} * s_{11})$ $s_{12} = 17949 - (1 * -32650)$ $s_{12} = 17949 - (-32650)$ $s_{12} = 50599$	$t_{12} = t_{10} - (q_{11} * t_{11})$ $t_{12} = -109700 - (1 * 199549)$ $t_{12} = -109700 - 199549$ $t_{12} = -309249$

Iteration 12 ...

Start with first set of values for the remainder and coefficients: $r_{11} = 119, s_{11} = -32650, t_{11} = 199549$
... and the second set of values for them: $r_{12} = 9, s_{12} = 50599, t_{12} = -309249$
The quotient for this step is computed from $q_i = \lfloor 119 \div 9 \rfloor = 13$

$r_{13} = r_{11} - (q_{12} * r_{12})$ $r_{13} = 119 - (13 * 9)$ $r_{13} = 119 - 117$ $r_{13} = 2$	$s_{13} = s_{11} - (q_{12} * s_{12})$ $s_{13} = -32650 - (13 * 50599)$ $s_{13} = -32650 - 657787$ $s_{13} = -690437$	$t_{13} = t_{11} - (q_{12} * t_{12})$ $t_{13} = 199549 - (13 * -309249)$ $t_{13} = 199549 - (-4020237)$ $t_{13} = 4219786$

Iteration 13 ...

Start with first set of values for the remainder and coefficients: $r_{12} = 9, s_{12} = 50599, t_{12} = -309249$
... and the second set of values for them: $r_{13} = 2, s_{13} = -690437, t_{13} = 4219786$
The quotient for this step is computed from $q_i = \lfloor 9 \div 2 \rfloor = 4$

$r_{14} = r_{12} - (q_{13} * r_{13})$ $r_{14} = 9 - (4 * 2)$ $r_{14} = 9 - 8$ $r_{14} = 1$	$s_{14} = s_{12} - (q_{13} * s_{13})$ $s_{14} = 50599 - (4 * -690437)$ $s_{14} = 50599 - (-2761748)$ $s_{14} = 2812347$	$t_{14} = t_{12} - (q_{13} * t_{13})$ $t_{14} = -309249 - (4 * 4219786)$ $t_{14} = -309249 - 16879144$ $t_{14} = -17188393$

Success!

Since the value for *d* is negative, add the modulus 38596572
$-17188393 + 38596572 = 21408179$
$d = 21408179$
Therefore, let's check that $d \cdot e = 1 \mod \Phi$
$21408179 \cdot 6315131 = 1 \mod 38596572$
$135195454856449 = 1 \mod 38596572$
$1 + 135195454856448 = 1 \mod 38596572$
$1 + (3502784 \cdot 38596572) = 1 \mod 38596572$

Hence 21408179 and 38596572 are inverses of each other