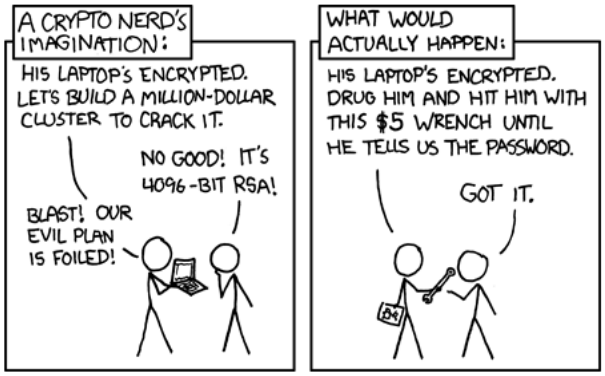
Anomaly's SSSS 2019 Codebusters Key



https://xkcd.com/538/

Competitors Names:

_____ _____ _____

Notes:

In this test packet, you'll find two tests. The first is a test of just regional level ciphers, as mentioned in the rules for the 2018-2019 season. There is also a supplement test, with one question of each type of state/national level cipher as outlined in those same rules.

Test 1

Question	Value	Incorrect letters	Deduction	Score
Timed	300			
1	200			
2	225			
3	120			
4	250			
5	100			
6	275			
7	400			
8	300			
9	500			
10	100			
11	115			
12	550			
13	150			
14	575			
15	300			
16	350			
17	200			
Bonus				
Final Score				

Test 2

Question	Value	Incorrect letters	Deduction	Score
1	215			
2	250			
3	175			
4	275			
5	215			
6	200			
7	100			
8	265			
9	305			
10	300			
11	120			
12	650			
Final Score				

Timed Question **[300 points]** Solve this quote from the 1994 movie *Forrest Gump*, which has since been slightly modified into a common saying. When you have solved it, raise your hand so that the time can be recorded and the solution checked.

UM UAUUL LCBLMH HLQS, "CQVJ BLH CQEJ L PAR AV
MY MOMMA ALWAYS SAID, "LIFE WAS LIKE A BOX OF

ITAIACLDJH. MAK YJXJW EYAB BTLD MAK'WJ OAYYL OJD."
CHOCOLATES. YOU NEVER KNOW WHAT YOU'RE GONNA GET."

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

1) **[200 points]** Solve this aristocrat, which is the famous last line from F. Scott Fitzgerald's *The Great Gatsby*

NW ER MRUG WK, MWUGN ULUPKNG GFR DZTTRKG, MWTKR MUDQ
SO WE BEAT ON, BOATS AGAINST THE CURRENT, BORNE BACK

DRUNRJRNNJI PKGW GFR AUNG.
CEASELESSLY INTO THE PAST.

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

2) **[225 points]** Solve this saying by Benjamin Franklin, published in his renowned *Poor Richard's Almanac*

TU MZO NKKNTEL PK MZTL SPEIY, DOU NEO LNROY, UPM HX
IN THE AFFAIRS OF THIS WORLD, MEN ARE SAVED, NOT BY

KNTMZ, HBM HX MZO INAG PK TM.
FAITH, BUT BY THE LACK OF IT.

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

3) **[120 points]** Encode this quote from *To Kill a Mockingbird* using a caesar shift of 18

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

C	A	N		H	I	T		'	E	M	,		B	U	T		R	E	M	E	M	B	E	R		I	T	'	S		A		S	I	N		T	O
U	**S**	**F**		**Z**	**A**	**L**		'	**W**	**E**	,		**T**	**M**	**L**		**J**	**W**	**E**	**W**	**E**	**T**	**W**	**J**		**A**	**L**	'	**K**		**S**		**K**	**A**	**F**		**L**	**G**

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

4) **[250 points]** Solve this famous quote from Shakespeare's *Romeo and Juliet*. It has been encoded with a K2 alphabet.

ANFO'L PU F UFTJ? ONFO ANPHN AJ HFSS F ZWLJ GC FUC
WHAT'S IN A NAME? THAT WHICH WE CALL A ROSE BY ANY

WONJZ UFTJ AWVSI LTJSS FL LAJJO.
OTHER NAME WOULD SMELL AS SWEET.

Replacement	**F**	**G**	**H**	**I**	**J**	**K**	**M**	**N**	**P**	**Q**	**R**	**S**	**T**	**U**	**W**	**X**	**Y**	**Z**	**L**	**O**	**V**	**E**	**A**	**B**	**C**	**D**
K2	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Frequency	5		2			9	1	2	1	8		5		5	5	2			5	3	4	1	3			2

5) **[100 points]** Decode this Atbash, which is a quote by chemist Dmitri Mendeleev

K	O	V	Z	H	F	I	V	H		U	O	R	G		Y	B		-		G	S	V	B		Z	I	V		L	M	O	B		U	L	I
P	**L**	**E**	**A**	**S**	**U**	**R**	**E**	**S**		**F**	**L**	**I**	**T**		**B**	**Y**		-		**T**	**H**	**E**	**Y**		**A**	**R**	**E**		**O**	**N**	**L**	**Y**		**F**	**O**	**R**

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

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

6) **[275 points]** Encode this vigenere, a quote by Carl Sagan, using a keyword of **creativity**

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

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

C
E
G

7) **[400 points]** Solve this patristocrat that is a quote from David Brinkley.

XRTVV PRRIT MWXEC RJEPZ LJVXE MXKXI CGWIJ TEQXS
ASUCC ESSFU LMANI SONEW HOCAN LAYAF IRMFO UNDAT

CJEZC SLSLP HGCVD RJSLP GRLXN PSLGJ ZEXSL CW
IONWI THTHE BRICK SOTHE RSHAV ETHRO WNATH IM

A successful man is one who can lay a firm foundation with the bricks others have thrown at him

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

8) **[300 points]** Solve this baconian cipher, which is a quote by Michael Scott from *The Office*

!#%&(!@$#%&(!^*#)%&(!@#%$&^*(!#%)&(@!$#%&(^!#*%)&@(!#
AAAAAABBAAAAABBABAAAABAABABBAAAABAABABAAAABAABABABAAA
A N D I K N E W E X A

%&(!#$%^&(*!#)%@&$(^*!)#@%&(!$^*#%&(!)#%@&$(!^#%*)&@(
AAAAABABAABAABABABABBABABAAAABBBAAAAABAABABAABAABBABA
C T L Y W H A T T O

!#$^%*)&@(!#%$^&(*)@!#$%&^(!#%*)&(!#%&(!@#$^*%&)@(!#$
AABBABBABAAAABBAABBBAABAABAAAABBAAAAAAAABABBBAABBAAAB
D O B U T I N A M U C

%&(^*)!@#$^%*)&@$(!#%&(^!#*%&(!#%)&(!#%&(!@#$%^&(!*#%
AAABBBABABBABBABBAAAAAABAABAAAAAABAAAAAAAABABABAAABAA
H M O R E R E A L S

)&(!@$#%^&(!*#%)&(!@#%&(!$^*#%&(!#%&)@($^!#%*)&@($!#%
BAAABBAABAAABAABAAABAAAAABBBAAAAAAAABBABBAAABBABABAAA
E N S E I H A D N O I

&(!^*#%)&(!#%&(@!$#%&(^*)!#%&(@!#$%^&(*!#)@%$&(!^*#)@
AAABBAABAAAAAAABABAAAABBBAAAAABAABABAABAABBABAAABBABB
D E A W H A T T O D O

%$
AB

And I knew exactly what to do. But in a much more real sense, I had no idea what to do

The A letters are represented by '!#%&(' and the B letters by '@$^*)'

9) **[500 points]** Solve this patristocrat, a quote from the movie *Jaws.* It has the word "beach" in it.

KTKFF OLVFN MFCXT FGVXG UVIVF MFFMA WVYRJ TNMOW
ISITT RUETH ATMOS TPEOP LEGET ATTAC KEDBY SHARK

TKBFN OVVSV VFXSQ MFVOM RXLFF VBSVV FSOXC FNVRV MAN
SINTH REEFE ETOFW ATERA BOUTT ENFEE TFROM THEBE ACH

Is it true that most people get attacked by sharks in three feet of water about ten feet from the beach?

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

10) **[100 points]** Compute the decryption matrix for the keyword **bleb**

$$\begin{pmatrix} B & L \\ E & B \end{pmatrix} \equiv \begin{pmatrix} 1 & 11 \\ 4 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 19 \\ 14 & 3 \end{pmatrix}$$

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

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

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

$$(1 * 1 - 11 * 4) \mod 26 = -43 \mod 26 = 9$$

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:

$$(1 * 1 - 11 * 4)^{-1} \begin{pmatrix} 1 & -11 \\ -4 & 1 \end{pmatrix} \equiv 3 \begin{pmatrix} 1 & -11 \\ -4 & 1 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 3 * 1 & 3 * -11 \\ 3 * -4 & 3 * 1 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 3 & -33 \\ -12 & 3 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 3 \mod 26 & -33 \mod 26 \\ -12 \mod 26 & 3 \mod 26 \end{pmatrix} \equiv \begin{pmatrix} 3 & 19 \\ 14 & 3 \end{pmatrix}$$

11) **[115 points]** Decode this quote from *The Hunger Games* that has been encoded using a Caesar cipher.

G	T	B	T	B	Q	T	G	,	L	T	'	G	T	B	P	S	A	N	X	C	A	D	K	T	,	H	D	X	I	'	H
R	**E**	**M**	**E**	**M**	**B**	**E**	**R**	,	**W**	**E**	'	**R**	**E**	**M**	**A**	**D**	**L**	**Y**	**I**	**N**	**L**	**O**	**V**	**E**	,	**S**	**O**	**I**	**T**	'	**S**

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

A	X	Z	T		X	I	.
L	**I**	**K**	**E**		**I**	**T**	.

How to solve

Since there are no single letter words we look for the double letter words and find XC and HD and ID and BT.

We can use a simple trick to test them quickly which only requires looking up 8 characters: six letters mapping the beginning (A B I M O U) and two letters at the end (O E).The letters are for the beginning and for the end.

The starting letters match against As/At/An/Am, Be/By, In/It/Is/If, Me/My, Of/Or/On, and Up/Us. The ending letters match against dO/gO/nO/sO/tO and hE/wE.

Using the beginning letter A gives AF with a key of X and AW with a key of H and AV with a key of I a common word and AS with a key of B

Using the beginning letter B gives BG with a key of W and BX with a key of G and BW with a key of H and BT with a key of A

Using the beginning letter I gives a common word IN with a key of P and IE with a key of Z a common word and ID with a key of A and IA with a key of T

Using the beginning letter M gives MR with a key of L and MI with a key of V and MH with a key of W a common word and ME with a key of P

Using the beginning letter O gives OT with a key of J a common word and OK with a key of T and OJ with a key of U and OG with a key of N

Using the beginning letter U gives UZ with a key of D and UQ with a key of N a common word and UP with a key of O a common word and UM with a key of H

Using the ending letter O gives 'JO' with a key of O a common word and 'SO' with a key of P a common word and 'TO' with a key of P and 'WO' with a key of F

Using the ending letter E gives 'ZE' with a key of Y and 'IE' with a key of Z and 'JE' with a key of Z a common word and 'ME' with a key of P

Since we have several possible choices, we have to try them out on the first long word 'GTBTBQTG'

Using the B row to decode the first long word 'GTBTBQTG', it comes out as 'FSASAPSF'

Using the P row to decode the first long word 'GTBTBQTG', it comes out as 'REMEMBER'

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

---

12) **[550 points]** Solve this xenocrypt quote by Richard Nixon, which has been translated into Spanish and encoded with a K1 Alphabet with an English keyword

EF HT ID JCCFDENJE, HT EVMCFCJE GDCCTIJE. BDCT EF HT
SI NO TE ARRIESGAS, NO SUFRIRAS DERROTAS. PERO SI NO

ID JCCFDENJE, HT NJHJE WFLITCFJE.
TE ARRIESGAS, NO GANAS VICTORIAS.

K1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency		1	10	6	11	7	1	5	4	9		1	1	3							7		1	1			
Replacement	Z	P	R	E	S	I	D	N	T	A	B	C	F	G	H	J	K	L	M	Ñ	O	Q	U	V	W	X	Y

Translation: *If you take no risks, you will suffer no defeats. But if you take no risks, you win no victories.*

13) **[150 points]** Encode this quote from Louisa May Alcott's *Little Women* using the values a=9 and b=18

I		A	M		N	O	T		A	F	R	A	I	D		O	F		S	T	O	R	M	S	,		F	O	R		I		A	M
M		**S**	**W**		**F**	**O**	**H**		**S**	**L**	**P**	**S**	**M**	**T**		**O**	**L**		**Y**	**H**	**O**	**P**	**W**	**Y**	,		**L**	**O**	**P**		**M**		**S**	**W**

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

How to solve

Using the given value of $\mathrm{a} = 9$ and $\mathrm{b} = 18$ we can calcuate using the formula $a * x + b \mod 26$

$$I(8) \rightarrow 8 * 9 + 18 \rightarrow 90 \mod 26 \rightarrow M(12)$$
$$A(0) \rightarrow 0 * 9 + 18 \rightarrow 18 \mod 26 \rightarrow S(18)$$
$$M(12) \rightarrow 12 * 9 + 18 \rightarrow 126 \mod 26 \rightarrow W(22)$$
$$N(13) \rightarrow 13 * 9 + 18 \rightarrow 135 \mod 26 \rightarrow F(5)$$
$$O(14) \rightarrow 14 * 9 + 18 \rightarrow 144 \mod 26 \rightarrow O(14)$$
$$T(19) \rightarrow 19 * 9 + 18 \rightarrow 189 \mod 26 \rightarrow H(7)$$

We already computed for A and know that it is S

$$F(5) \rightarrow 5 * 9 + 18 \rightarrow 63 \mod 26 \rightarrow L(11)$$
$$R(17) \rightarrow 17 * 9 + 18 \rightarrow 171 \mod 26 \rightarrow P(15)$$

We already computed for A and know that it is S

We already computed for I and know that it is M

$$D(3) \rightarrow 3 * 9 + 18 \rightarrow 45 \mod 26 \rightarrow T(19)$$

We already computed for O and know that it is O

We already computed for F and know that it is L

$$S(18) \rightarrow 18 * 9 + 18 \rightarrow 180 \mod 26 \rightarrow Y(24)$$

We already computed for T and know that it is H

We already computed for O and know that it is O

We already computed for R and know that it is P

We already computed for M and know that it is W

We already computed for S and know that it is Y

We already computed for F and know that it is L

We already computed for O and know that it is O

We already computed for R and know that it is P

We already computed for I and know that it is M

We already computed for A and know that it is S

We already computed for M and know that it is W

$$L(11) \quad \rightarrow \quad 11 * 9 + 18 \quad \rightarrow \quad 117 \mod 26 \quad \rightarrow \quad N(13)$$
$$E(4) \quad \rightarrow \quad 4 * 9 + 18 \quad \rightarrow \quad 54 \mod 26 \quad \rightarrow \quad C(2)$$

We already computed for A and know that it is S

We already computed for R and know that it is P

We already computed for N and know that it is F

We already computed for I and know that it is M

We already computed for N and know that it is F

$$G(6) \quad \rightarrow \quad 6 * 9 + 18 \quad \rightarrow \quad 72 \mod 26 \quad \rightarrow \quad U(20)$$
$$H(7) \quad \rightarrow \quad 7 * 9 + 18 \quad \rightarrow \quad 81 \mod 26 \quad \rightarrow \quad D(3)$$

We already computed for O and know that it is O

$$W(22) \quad \rightarrow \quad 22 * 9 + 18 \quad \rightarrow \quad 216 \mod 26 \quad \rightarrow \quad I(8)$$

We already computed for T and know that it is H

We already computed for O and know that it is O

We already computed for S and know that it is Y

We already computed for A and know that it is S

We already computed for I and know that it is M

We already computed for L and know that it is N

We already computed for M and know that it is W

$$Y(24) \quad \rightarrow \quad 24 * 9 + 18 \quad \rightarrow \quad 234 \mod 26 \quad \rightarrow \quad A(0)$$

We already computed for S and know that it is Y

We already computed for H and know that it is D

We already computed for I and know that it is M

$$P(15) \quad \rightarrow \quad 15 * 9 + 18 \quad \rightarrow \quad 153 \mod 26 \quad \rightarrow \quad X(23)$$

14) **[575 points]** Solve this patristocrat quote from one of the *Mortal Instruments* books. It has the word "love" in it three times.

ZGXNU SXTPF RZJZG GGXNU SXTTF WZGZR ZUPFR ZQWIU
ILOVE YOUAN DIWIL LLOVE YOUUN TILID IEAND IFTHE

EUZYG ZQUPQ WUEWI PWZGG GXNUS XTWIU F
REISL IFEAF TERTH ATILL LOVEY OUTHE N

I love you, and I will love you until I die, and if there is life after that, I'll love you then

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

15) **[300 points]** Solve this quote by William Jennings Bryan, which has been encoded using the Baconian cipher.

A GIRL GAVE A VISIT TO ONE WHOSE STRAW PILLS ARISE
AAABB AABAA BAAAB BAABA ABAAA ABBAA BABBA ABAAA
D E S T I/J N Y I/J

TO OUR ATTIC IN HER LIMBS WE SEE A HAND AS YOU BE ITS
BAAAB ABBAA ABBAB BAABA AAAAA ABABB AAAAA BAABA
S N O T A M A T

DYING CURSE DOES A SPLIT MORON GUIDE WORLD AS YOU
BAABA AABAA BAAAA ABBAB AABAB AAABA AABBB AAAAA
T E R O F C H A

ANNOY EMILY AS NOW A HOME BUMPS GREEK BACON COMES
ABBAA AAABA AABAA ABAAA BAABA ABAAA BAAAB AAAAA
N C E I/J T I/J S A

SPILL AS YOU TASTE FISHY CYRUS BOOKS STRIP SOBER
ABABB AAAAA BAABA BAABA AABAA BAAAA ABBAB AABAB
M A T T E R O F

SWORE EARTH OTHER SPICY COINS CUTIE
AAABA AABBB ABBAB ABAAA AAABA AABAA
C H O I/J C E

Destiny is not a matter of chance; it is a matter of choice.

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

16) **[350 points]** Solve this aristocrat, a quote said by socialist Eugene V. Debs.

C IUQM AP SPGAXVL XP ECFIX EPV; RL SPGAXVL CB XIM
I HAVE NO COUNTRY TO FIGHT FOR; MY COUNTRY IS THE

MUVXI, UAO C UR U SCXCYMA PE XIM TPVJO.
EARTH, AND I AM A CITIZEN OF THE WORLD.

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

17) **[200 points]** Decode this vigenere, a quote by Dr. Wyatt from the TV show, *Grey's Anatomy,* that was encoded using the keyword **happiness.**

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

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

E	S	S	H	A	P	P	I	N	E	S	S	H	A	P
K	K	L	O	A	I	H	B	U	I	H	G	P	N	I
G	**S**	**T**	**H**	**A**	**T**	**S**	**T**	**H**	**E**	**P**	**O**	**I**	**N**	**T**

1) **[215 points]** Decode this quote from the old show *I Love Lucy*. The first two letters map out to ID.

E	'	F		X	Q	H	Z	K	X		X	K	U	X	K	H		H	Z	K		H	Z	E	D	U	C		E	'	R	K		F	I	D	K
I	'	**D**		**R**	**A**	**T**	**H**	**E**	**R**		**R**	**E**	**G**	**R**	**E**	**T**		**T**	**H**	**E**		**T**	**H**	**I**	**N**	**G**	**S**		**I**	'	**V**	**E**		**D**	**O**	**N**	**E**

H	Z	Q	D		X	K	U	X	K	H		H	Z	K		H	Z	E	D	U	C		E		Z	Q	R	K	D	'	H		F	I	D	K	.
T	**H**	**A**	**N**		**R**	**E**	**G**	**R**	**E**	**T**		**T**	**H**	**E**		**T**	**H**	**I**	**N**	**G**	**S**		**I**		**H**	**A**	**V**	**E**	**N**	'	**T**		**D**	**O**	**N**	**E**	.

How to solve

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

$$I(8) \rightarrow E(4)$$
$$D(3) \rightarrow F(5)$$

From this we know:

$$(a * 8 + b) \mod 26 = 4$$
$$(a * 3 + b) \mod 26 = 5$$

Next, subtract the formulas:

$$\begin{aligned} (a * 8 + b) \mod 26 &= 4 \\ -(a * 3 + b) \mod 26 &= 5 \\ \hline a * 5 \mod 26 &= -1 \\ a * 5 \mod 26 &= 25 \end{aligned}$$

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

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

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

$$\begin{aligned} (15 + b) \mod 26 - 15 &= (5 - 15) \mod 26 \\ b \mod 26 &= -10 \mod 26 \\ b \mod 26 &= 16 \mod 26 \end{aligned}$$

Subtract 15 from both sides:

And we see that $\mathrm{b} = 16$

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

E	**F**	**X**	**Q**	**H**	**Z**	**K**	**X**	**X**	**K**	**U**	**X**	**K**	**H**	**H**	**Z**	**K**	**H**	**Z**	**E**	**D**	**U**	**C**	**E**	**R**	**K**	**F**	**I**	**D**	**K**	**H**	**Z**	**Q**	**D**	**X**	**K**	**U**	**X**	**K**	**H**	**H**	**Z**	**K**	**H**	**Z**
I	**D**																		**I**				**I**			**D**																				

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

$$\begin{array}{lllll} E(4) & \rightarrow & 4 * 5 + 16 & \rightarrow & 36 \mod 26 \rightarrow K(10) \\ T(19) & \rightarrow & 19 * 5 + 16 & \rightarrow & 111 \mod 26 \rightarrow H(7) \\ A(0) & \rightarrow & 0 * 5 + 16 & \rightarrow & 16 \mod 26 \rightarrow Q(16) \\ O(14) & \rightarrow & 14 * 5 + 16 & \rightarrow & 86 \mod 26 \rightarrow I(8) \\ I(8) & \rightarrow & 8 * 5 + 16 & \rightarrow & 56 \mod 26 \rightarrow E(4) \\ N(13) & \rightarrow & 13 * 5 + 16 & \rightarrow & 81 \mod 26 \rightarrow D(3) \end{array}$$

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

E	**F**	**X**	**Q**	**H**	**Z**	**K**	**X**	**X**	**K**	**U**	**X**	**K**	**H**	**H**	**Z**	**K**	**H**	**Z**	**E**	**D**	**U**	**C**	**E**	**R**	**K**	**F**	**I**	**D**	**K**	**H**	**Z**	**Q**	**D**	**X**	**K**	**U**	**X**	**K**	**H**	**H**	**Z**	**K**	**H**	**Z**
I	**D**		**A**	**T**		**E**			**E**			**E**	**T**	**T**		**E**	**T**		**I**	**N**			**I**		**E**	**D**	**O**	**N**	**E**	**T**		**A**	**N**		**E**			**E**	**T**	**T**		**E**	**T**	

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

$$
\begin{array}{lcrcrcl}
S(18) & \rightarrow & 18*5+16 & \rightarrow & 106 & \mod 26 & \rightarrow & C(2) \\
R(17) & \rightarrow & 17*5+16 & \rightarrow & 101 & \mod 26 & \rightarrow & X(23) \\
H(7) & \rightarrow & 7*5+16 & \rightarrow & 51 & \mod 26 & \rightarrow & Z(25) \\
L(11) & \rightarrow & 11*5+16 & \rightarrow & 71 & \mod 26 & \rightarrow & T(19) \\
D(3) & \rightarrow & 3*5+16 & \rightarrow & 31 & \mod 26 & \rightarrow & F(5)
\end{array}
$$

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

E	F	X	Q	H	Z	K	X	X	K	U	X	K	H	H	Z	K	H	Z	E	D	U	C	E	R	K	F	I	D	K	H	Z	Q	D	X	K	U	X	K	H	H	Z	K	H	Z
I	D	R	A	T	H	E	R	R	E		R	E	T	T	H	E	T	H	I	N		S	I		E	D	O	N	E	T	H	A	N	R	E		R	E	T	T	H	E	T	H

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

$$
\begin{array}{lcrcrcl}
C(2) & \rightarrow & 2*5+16 & \rightarrow & 26 & \mod 26 & \rightarrow & A(0) \\
U(20) & \rightarrow & 20*5+16 & \rightarrow & 116 & \mod 26 & \rightarrow & M(12) \\
M(12) & \rightarrow & 12*5+16 & \rightarrow & 76 & \mod 26 & \rightarrow & Y(24) \\
F(5) & \rightarrow & 5*5+16 & \rightarrow & 41 & \mod 26 & \rightarrow & P(15) \\
P(15) & \rightarrow & 15*5+16 & \rightarrow & 91 & \mod 26 & \rightarrow & N(13)
\end{array}
$$

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

E	F	X	Q	H	Z	K	X	X	K	U	X	K	H	H	Z	K	H	Z	E	D	U	C	E	R	K	F	I	D	K	H	Z	Q	D	X	K	U	X	K	H	H	Z	K	H	Z
I	D	R	A	T	H	E	R	R	E		R	E	T	T	H	E	T	H	I	N		S	I		E	D	O	N	E	T	H	A	N	R	E		R	E	T	T	H	E	T	H

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

$$
\begin{array}{lcrcrcl}
G(6) & \rightarrow & 6*5+16 & \rightarrow & 46 & \mod 26 & \rightarrow & U(20) \\
W(22) & \rightarrow & 22*5+16 & \rightarrow & 126 & \mod 26 & \rightarrow & W(22) \\
Y(24) & \rightarrow & 24*5+16 & \rightarrow & 136 & \mod 26 & \rightarrow & G(6) \\
B(1) & \rightarrow & 1*5+16 & \rightarrow & 21 & \mod 26 & \rightarrow & V(21) \\
V(21) & \rightarrow & 21*5+16 & \rightarrow & 121 & \mod 26 & \rightarrow & R(17)
\end{array}
$$

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

E	F	X	Q	H	Z	K	X	X	K	U	X	K	H	H	Z	K	H	Z	E	D	U	C	E	R	K	F	I	D	K	H	Z	Q	D	X	K	U	X	K	H	H	Z	K	H	Z
I	D	R	A	T	H	E	R	R	E	G	R	E	T	T	H	E	T	H	I	N	G	S	I	V	E	D	O	N	E	T	H	A	N	R	E	G	R	E	T	T	H	E	T	H

The solution is now complete!

2) **[250 points]** Encode the word **playground** using the keyword **OSTRACIZE**.

$$\begin{pmatrix} O & S & T \\ R & A & C \\ I & Z & E \end{pmatrix} \equiv \begin{pmatrix} 14 & 18 & 19 \\ 17 & 0 & 2 \\ 8 & 25 & 4 \end{pmatrix}$$

P	L	A	Y	G	R	O	U	N	D		
S	**V**	**F**	**N**	**A**	**U**	**X**	**E**	**O**	**F**	**X**	**V**

How to solve

$$\begin{pmatrix} O & S & T \\ R & A & C \\ I & Z & E \end{pmatrix} * \begin{pmatrix} P \\ L \\ A \end{pmatrix} \equiv \begin{pmatrix} 14 & 18 & 19 \\ 17 & 0 & 2 \\ 8 & 25 & 4 \end{pmatrix} * \begin{pmatrix} 15 \\ 11 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 14*15+18*11+19*0 \\ 17*15+0*11+2*0 \\ 8*15+25*11+4*0 \end{pmatrix} \equiv \begin{pmatrix} 408 \\ 255 \\ 395 \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 21 \\ 5 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} S \\ V \\ F \end{pmatrix}$$

$$\begin{pmatrix} O & S & T \\ R & A & C \\ I & Z & E \end{pmatrix} * \begin{pmatrix} Y \\ G \\ R \end{pmatrix} \equiv \begin{pmatrix} 14 & 18 & 19 \\ 17 & 0 & 2 \\ 8 & 25 & 4 \end{pmatrix} * \begin{pmatrix} 24 \\ 6 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 14*24+18*6+19*17 \\ 17*24+0*6+2*17 \\ 8*24+25*6+4*17 \end{pmatrix} \equiv \begin{pmatrix} 767 \\ 442 \\ 410 \end{pmatrix} \equiv \begin{pmatrix} 13 \\ 0 \\ 20 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} N \\ A \\ U \end{pmatrix}$$

$$\begin{pmatrix} O & S & T \\ R & A & C \\ I & Z & E \end{pmatrix} * \begin{pmatrix} O \\ U \\ N \end{pmatrix} \equiv \begin{pmatrix} 14 & 18 & 19 \\ 17 & 0 & 2 \\ 8 & 25 & 4 \end{pmatrix} * \begin{pmatrix} 14 \\ 20 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 14*14+18*20+19*13 \\ 17*14+0*20+2*13 \\ 8*14+25*20+4*13 \end{pmatrix} \equiv \begin{pmatrix} 803 \\ 264 \\ 664 \end{pmatrix} \equiv \begin{pmatrix} 23 \\ 4 \\ 14 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} X \\ E \\ O \end{pmatrix}$$

$$\begin{pmatrix} O & S & T \\ R & A & C \\ I & Z & E \end{pmatrix} * \begin{pmatrix} D \\ Z \\ Z \end{pmatrix} \equiv \begin{pmatrix} 14 & 18 & 19 \\ 17 & 0 & 2 \\ 8 & 25 & 4 \end{pmatrix} * \begin{pmatrix} 3 \\ 25 \\ 25 \end{pmatrix} \equiv \begin{pmatrix} 14*3+18*25+19*25 \\ 17*3+0*25+2*25 \\ 8*3+25*25+4*25 \end{pmatrix} \equiv \begin{pmatrix} 967 \\ 101 \\ 749 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 23 \\ 21 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} F \\ X \\ V \end{pmatrix}$$

3) **[175 points]** Decode the text below using the keyword **JEEP**.

$$\begin{pmatrix} J & E \\ E & P \end{pmatrix} \equiv \begin{pmatrix} 9 & 4 \\ 4 & 15 \end{pmatrix}$$

R	S	A	L	U	Q	N	O	H	J	C	K	C	F
H	**I**	**E**	**R**	**O**	**G**	**L**	**Y**	**P**	**H**	**I**	**C**	**S**	**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

$$\begin{pmatrix} 9 & 4 \\ 4 & 15 \end{pmatrix}^{-1} = (9 * 15 - 4 * 4)^{-1} \begin{pmatrix} 15 & -4 \\ -4 & 9 \end{pmatrix}$$

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

$$(9 * 15 - 4 * 4) \mod 26 = 119 \mod 26 = 15$$

Looking up 15 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 7 which we substitute into the formula to compute the matrix:

$$(9 * 15 - 4 * 4)^{-1} \begin{pmatrix} 15 & -4 \\ -4 & 9 \end{pmatrix} \equiv 7 \begin{pmatrix} 15 & -4 \\ -4 & 9 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 7 * 15 & 7 * -4 \\ 7 * -4 & 7 * 9 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 105 & -28 \\ -28 & 63 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 105 \mod 26 & -28 \mod 26 \\ -28 \mod 26 & 63 \mod 26 \end{pmatrix} \equiv \begin{pmatrix} 1 & 24 \\ 24 & 11 \end{pmatrix}$$

With the inverse matrix we can now decode

$$\begin{pmatrix} B & Y \\ Y & L \end{pmatrix} * \begin{pmatrix} R \\ S \end{pmatrix} \equiv \begin{pmatrix} 1 & 24 \\ 24 & 11 \end{pmatrix} * \begin{pmatrix} 17 \\ 18 \end{pmatrix} \equiv \begin{pmatrix} 1 * 17 + 24 * 18 \\ 24 * 17 + 11 * 18 \end{pmatrix} \equiv \begin{pmatrix} 449 \\ 606 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 8 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} H \\ I \end{pmatrix}$$

$$\begin{pmatrix} B & Y \\ Y & L \end{pmatrix} * \begin{pmatrix} A \\ L \end{pmatrix} \equiv \begin{pmatrix} 1 & 24 \\ 24 & 11 \end{pmatrix} * \begin{pmatrix} 0 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 1 * 0 + 24 * 11 \\ 24 * 0 + 11 * 11 \end{pmatrix} \equiv \begin{pmatrix} 264 \\ 121 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 17 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} E \\ R \end{pmatrix}$$

$$\begin{pmatrix} B & Y \\ Y & L \end{pmatrix} * \begin{pmatrix} U \\ Q \end{pmatrix} \equiv \begin{pmatrix} 1 & 24 \\ 24 & 11 \end{pmatrix} * \begin{pmatrix} 20 \\ 16 \end{pmatrix} \equiv \begin{pmatrix} 1 * 20 + 24 * 16 \\ 24 * 20 + 11 * 16 \end{pmatrix} \equiv \begin{pmatrix} 404 \\ 656 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 6 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} O \\ G \end{pmatrix}$$

$$\begin{pmatrix} B & Y \\ Y & L \end{pmatrix} * \begin{pmatrix} N \\ O \end{pmatrix} \equiv \begin{pmatrix} 1 & 24 \\ 24 & 11 \end{pmatrix} * \begin{pmatrix} 13 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 1 * 13 + 24 * 14 \\ 24 * 13 + 11 * 14 \end{pmatrix} \equiv \begin{pmatrix} 349 \\ 466 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 24 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} L \\ Y \end{pmatrix}$$

$$\begin{pmatrix} B & Y \\ Y & L \end{pmatrix} * \begin{pmatrix} H \\ J \end{pmatrix} \equiv \begin{pmatrix} 1 & 24 \\ 24 & 11 \end{pmatrix} * \begin{pmatrix} 7 \\ 9 \end{pmatrix} \equiv \begin{pmatrix} 1 * 7 + 24 * 9 \\ 24 * 7 + 11 * 9 \end{pmatrix} \equiv \begin{pmatrix} 223 \\ 267 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 7 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} P \\ H \end{pmatrix}$$

$$\begin{pmatrix} B & Y \\ Y & L \end{pmatrix} * \begin{pmatrix} C \\ K \end{pmatrix} \equiv \begin{pmatrix} 1 & 24 \\ 24 & 11 \end{pmatrix} * \begin{pmatrix} 2 \\ 10 \end{pmatrix} \equiv \begin{pmatrix} 1 * 2 + 24 * 10 \\ 24 * 2 + 11 * 10 \end{pmatrix} \equiv \begin{pmatrix} 242 \\ 158 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 2 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} I \\ C \end{pmatrix}$$

$$\begin{pmatrix} B & Y \\ Y & L \end{pmatrix} * \begin{pmatrix} C \\ F \end{pmatrix} \equiv \begin{pmatrix} 1 & 24 \\ 24 & 11 \end{pmatrix} * \begin{pmatrix} 2 \\ 5 \end{pmatrix} \equiv \begin{pmatrix} 1 * 2 + 24 * 5 \\ 24 * 2 + 11 * 5 \end{pmatrix} \equiv \begin{pmatrix} 122 \\ 103 \end{pmatrix} \equiv \begin{pmatrix} 18 \\ 25 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} S \\ Z \end{pmatrix}$$

4) **[275 points]** Decode this quote from Georg C. Lichtenberg that has been encoded using a 9 letter keyword. The 28th through 36th letters (XUWJGOMFF) map out to **INARYMENMA**

P	H	Y	S	I	C	I
X	A	G	K	A	V	Z
I	**T**	**I**	**S**	**S**	**T**	**R**

S	T	P	H	Y	S	I
S	G	V	L	R	Z	I
A	**N**	**G**	**E**	**T**	**H**	**A**

C	I	S	T	P	H	Y
V	W	F	E	N	L	V
T	**O**	**N**	**L**	**Y**	**E**	**X**

S	I	C	I	S	T	P
L	Z	C	W	J	W	X
T	**R**	**A**	**O**	**R**	**D**	**I**

H	Y	S	I	C	I	S
U	Y	J	G	O	M	F
N	**A**	**R**	**Y**	**M**	**E**	**N**

T	P	H	Y	S	I	C
F	P	R	C	L	P	G
M	**A**	**K**	**E**	**T**	**H**	**E**

I	S	T	P	H	Y	S
L	A	L	R	V	T	W
D	**I**	**S**	**C**	**O**	**V**	**E**

I	C	I	S	T	P	H
Z	K	M	K	P	W	P
R	**I**	**E**	**S**	**W**	**H**	**I**

Y	S	I	C	I	S	T
A	Z	T	C	B	W	K
C	**H**	**L**	**A**	**T**	**E**	**R**

P	H	Y	S	I	C	I
P	W	N	W	I	T	A
A	**P**	**P**	**E**	**A**	**R**	**S**

S	T	P	H	Y	S	I
G	X	P	Z	W	S	V
O	**E**	**A**	**S**	**Y**	**A**	**N**

C	I	S	T	P	H	Y
F	A	A	F	E	S	C
D	**S**	**I**	**M**	**P**	**L**	**E**

5) **[215 points]** Encode this quote from the musical *Hamilton* using Karl Marx's *Communist Manifesto* as the key.

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

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

U	G	G		L	E	S		F	R	E		E
T	H	E		M	A	F		R	A	I		D
N	**N**	**K**		**X**	**E**	**X**		**W**	**R**	**M**		**H**

6) **[200 points]** The following quote from *Harry Potter and the Sorcerer's Stone* has been encoded using a famous document. What does it say?

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

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

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

7) **[100 points]** Agent Bobert has faithfully followed the steps of the RSA key-generation algorithm. But has forgotten the last step—how to encrypt a message. First, Here are the results from the other steps:

p = 1217 e = 5054497

q = 9337 Φ = 11352576

d = 4617697 n = 11363129

As it comes to pass, Agent Jennifer is on vacation in Hawaii, and Agent Bobert needs a document that is stored in the company safe. They are communicating via email, and both know it is very unwise to trust the security of computers in a hotel lobby. Agent Bobert needs to tell Agent Jennifer his public key, knowing well that it can be read by untrustworthy parties. List the minimum set of numbers that Agent Bobert needs to email to Agent Jennifer in order for Agent Jennifer to be able to decode the message.

Additionally, Agent Jennifer wants to transmit the combination to the safe (which is 89771) in the response email, but encrypted with RSA. What should formula should Agent Jennifer compute in order to know the ciphertext to transmit?

Enter the minimum values to transmit:

11363129	**5054497**	

These two numbers can be in either order.

Enter the formula (using correct numbers) to transmit:

89771 ^ 5054497 mod 11363129

How to solve

In order for Jennifer to be able to read Taylor's RSA encrypted message, Taylor has to transmit their public key (*n*,*e*) and nothing else. In this case it is `n = 11363129, e = 5054497`

To encode the safe combination of 89771, Jennifer will have to raise it to the power of *e* and take the modulus *n*. Hence the formula `v ^ e mod n`

8) **[265 points]** Special Agent, Joshua, has the following RSA public key:

`n = 197801  e = 186805`

Unfortunately for him, a quantum computer has successfully factored him *n*

```
197801 = 887 * 223
```

Compute the value of his private key:

Enter the computed private key:

143953

How to solve

To find the private key, First we need to find Φ using the formula:

$\Phi = (p-1) * (q-1)$

$\Phi = (887-1) * (223-1) = 886 * 222 = 196692$

We now know that we know that $\Phi = 196692$

Second, we use the extended Euclidean Algorithm (https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm) using 186805 and 196692

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):

$r_0 = 196692$	$s_0 = 1$	$t_0 = 0$
$r_1 = 186805$	$s_1 = 0$	$t_1 = 1$

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: $r_0 = 196692, s_0 = 1, t_0 = 0$

... and the second set of values for them: $r_1 = 186805, s_1 = 0, t_1 = 1$

The quotient for this step is computed from $q_i = \lfloor 196692 \div 186805 \rfloor = 1$

$r_2 = r_0 - (q_1 * r_1)$ $r_2 = 196692 - (1 * 186805)$ $r_2 = 196692 - 186805$ $r_2 = 9887$	$s_2 = s_0 - (q_1 * s_1)$ $s_2 = 1 - (1 * 0)$ $s_2 = 1 - 0$ $s_2 = 1$	$t_2 = t_0 - (q_1 * t_1)$ $t_2 = 0 - (1 * 1)$ $t_2 = 0 - 1$ $t_2 = -1$

Iteration 2 ...

Start with first set of values for the remainder and coefficients: $r_1 = 186805, s_1 = 0, t_1 = 1$

... and the second set of values for them: $r_2 = 9887, s_2 = 1, t_2 = -1$

The quotient for this step is computed from $q_i = \lfloor 186805 \div 9887 \rfloor = 18$

$r_3 = r_1 - (q_2 * r_2)$ $r_3 = 186805 - (18 * 9887)$ $r_3 = 186805 - 177966$ $r_3 = 8839$	$s_3 = s_1 - (q_2 * s_2)$ $s_3 = 0 - (18 * 1)$ $s_3 = 0 - 18$ $s_3 = -18$	$t_3 = t_1 - (q_2 * t_2)$ $t_3 = 1 - (18 * -1)$ $t_3 = 1 - (-18)$ $t_3 = 19$

Iteration 3 ...

Start with first set of values for the remainder and coefficients: $r_2 = 9887, s_2 = 1, t_2 = -1$

... and the second set of values for them: $r_3 = 8839, s_3 = -18, t_3 = 19$

The quotient for this step is computed from $q_i = \lfloor 9887 \div 8839 \rfloor = 1$

$r_4 = r_2 - (q_3 * r_3)$ $r_4 = 9887 - (1 * 8839)$ $r_4 = 9887 - 8839$ $r_4 = 1048$	$s_4 = s_2 - (q_3 * s_3)$ $s_4 = 1 - (1 * -18)$ $s_4 = 1 - (-18)$ $s_4 = 19$	$t_4 = t_2 - (q_3 * t_3)$ $t_4 = -1 - (1 * 19)$ $t_4 = -1 - 19$ $t_4 = -20$

Iteration 4 ...

Start with first set of values for the remainder and coefficients: $r_3 = 8839, s_3 = -18, t_3 = 19$
... and the second set of values for them: $r_4 = 1048, s_4 = 19, t_4 = -20$
The quotient for this step is computed from $q_i = \lfloor 8839 \div 1048 \rfloor = 8$

$r_5 = r_3 - (q_4 * r_4)$	$s_5 = s_3 - (q_4 * s_4)$	$t_5 = t_3 - (q_4 * t_4)$
$r_5 = 8839 - (8 * 1048)$	$s_5 = -18 - (8 * 19)$	$t_5 = 19 - (8 * -20)$
$r_5 = 8839 - 8384$	$s_5 = -18 - 152$	$t_5 = 19 - (-160)$
$r_5 = 455$	$s_5 = -170$	$t_5 = 179$

Iteration 5 ...

Start with first set of values for the remainder and coefficients: $r_4 = 1048, s_4 = 19, t_4 = -20$
... and the second set of values for them: $r_5 = 455, s_5 = -170, t_5 = 179$
The quotient for this step is computed from $q_i = \lfloor 1048 \div 455 \rfloor = 2$

$r_6 = r_4 - (q_5 * r_5)$	$s_6 = s_4 - (q_5 * s_5)$	$t_6 = t_4 - (q_5 * t_5)$
$r_6 = 1048 - (2 * 455)$	$s_6 = 19 - (2 * -170)$	$t_6 = -20 - (2 * 179)$
$r_6 = 1048 - 910$	$s_6 = 19 - (-340)$	$t_6 = -20 - 358$
$r_6 = 138$	$s_6 = 359$	$t_6 = -378$

Iteration 6 ...

Start with first set of values for the remainder and coefficients: $r_5 = 455, s_5 = -170, t_5 = 179$
... and the second set of values for them: $r_6 = 138, s_6 = 359, t_6 = -378$
The quotient for this step is computed from $q_i = \lfloor 455 \div 138 \rfloor = 3$

$r_7 = r_5 - (q_6 * r_6)$	$s_7 = s_5 - (q_6 * s_6)$	$t_7 = t_5 - (q_6 * t_6)$
$r_7 = 455 - (3 * 138)$	$s_7 = -170 - (3 * 359)$	$t_7 = 179 - (3 * -378)$
$r_7 = 455 - 414$	$s_7 = -170 - 1077$	$t_7 = 179 - (-1134)$
$r_7 = 41$	$s_7 = -1247$	$t_7 = 1313$

Iteration 7 ...

Start with first set of values for the remainder and coefficients: $r_6 = 138, s_6 = 359, t_6 = -378$
... and the second set of values for them: $r_7 = 41, s_7 = -1247, t_7 = 1313$
The quotient for this step is computed from $q_i = \lfloor 138 \div 41 \rfloor = 3$

$r_8 = r_6 - (q_7 * r_7)$	$s_8 = s_6 - (q_7 * s_7)$	$t_8 = t_6 - (q_7 * t_7)$
$r_8 = 138 - (3 * 41)$	$s_8 = 359 - (3 * -1247)$	$t_8 = -378 - (3 * 1313)$
$r_8 = 138 - 123$	$s_8 = 359 - (-3741)$	$t_8 = -378 - 3939$
$r_8 = 15$	$s_8 = 4100$	$t_8 = -4317$

Iteration 8 ...

Start with first set of values for the remainder and coefficients: $r_7 = 41, s_7 = -1247, t_7 = 1313$
... and the second set of values for them: $r_8 = 15, s_8 = 4100, t_8 = -4317$
The quotient for this step is computed from $q_i = \lfloor 41 \div 15 \rfloor = 2$

$r_9 = r_7 - (q_8 * r_8)$	$s_9 = s_7 - (q_8 * s_8)$	$t_9 = t_7 - (q_8 * t_8)$
$r_9 = 41 - (2 * 15)$	$s_9 = -1247 - (2 * 4100)$	$t_9 = 1313 - (2 * -4317)$
$r_9 = 41 - 30$	$s_9 = -1247 - 8200$	$t_9 = 1313 - (-8634)$
$r_9 = 11$	$s_9 = -9447$	$t_9 = 9947$

Iteration 9 ...

Start with first set of values for the remainder and coefficients: $r_8 = 15, s_8 = 4100, t_8 = -4317$
... and the second set of values for them: $r_9 = 11, s_9 = -9447, t_9 = 9947$
The quotient for this step is computed from $q_i = \lfloor 15 \div 11 \rfloor = 1$

$r_{10} = r_8 - (q_9 * r_9)$	$s_{10} = s_8 - (q_9 * s_9)$	$t_{10} = t_8 - (q_9 * t_9)$
$r_{10} = 15 - (1 * 11)$	$s_{10} = 4100 - (1 * -9447)$	$t_{10} = -4317 - (1 * 9947)$
$r_{10} = 15 - 11$	$s_{10} = 4100 - (-9447)$	$t_{10} = -4317 - 9947$
$r_{10} = 4$	$s_{10} = 13547$	$t_{10} = -14264$

Iteration 10 ...

Start with first set of values for the remainder and coefficients: $r_9 = 11, s_9 = -9447, t_9 = 9947$
... and the second set of values for them: $r_{10} = 4, s_{10} = 13547, t_{10} = -14264$
The quotient for this step is computed from $q_i = \lfloor 11 \div 4 \rfloor = 2$

$r_{11} = r_9 - (q_{10} * r_{10})$ $r_{11} = 11 - (2 * 4)$ $r_{11} = 11 - 8$ $r_{11} = 3$	$s_{11} = s_9 - (q_{10} * s_{10})$ $s_{11} = -9447 - (2 * 13547)$ $s_{11} = -9447 - 27094$ $s_{11} = -36541$	$t_{11} = t_9 - (q_{10} * t_{10})$ $t_{11} = 9947 - (2 * -14264)$ $t_{11} = 9947 - (-28528)$ $t_{11} = 38475$

Iteration 11 ...

Start with first set of values for the remainder and coefficients: $r_{10} = 4, s_{10} = 13547, t_{10} = -14264$
... and the second set of values for them: $r_{11} = 3, s_{11} = -36541, t_{11} = 38475$
The quotient for this step is computed from $q_i = \lfloor 4 \div 3 \rfloor = 1$

$r_{12} = r_{10} - (q_{11} * r_{11})$ $r_{12} = 4 - (1 * 3)$ $r_{12} = 4 - 3$ $r_{12} = 1$	$s_{12} = s_{10} - (q_{11} * s_{11})$ $s_{12} = 13547 - (1 * -36541)$ $s_{12} = 13547 - (-36541)$ $s_{12} = 50088$	$t_{12} = t_{10} - (q_{11} * t_{11})$ $t_{12} = -14264 - (1 * 38475)$ $t_{12} = -14264 - 38475$ $t_{12} = -52739$

Success!

Since the value for *d* is negative, add the modulus 196692
$-52739 + 196692 = 143953$
$d = 143953$
Therefore, let's check that $d \cdot e = 1 \mod \Phi$
$143953 \cdot 186805 = 1 \mod 196692$
$26891140165 = 1 \mod 196692$
$1 + 26891140164 = 1 \mod 196692$
$1 + (136717 \cdot 196692) = 1 \mod 196692$
Hence 143953 and 196692 are inverses of each other

9) **[305 points]** John and Kaitlyn are accountants for a very large bank, and have started a friendship. They communicate via email, because they live thousands of miles apart. Kaitlyn gets curious and asks John the year that they were born. John doesn't mind telling Kaitlyn, but they know that the bank monitors all employee emails, and is afraid of being the victim of age discrimination. Therefore, Kaitlyn suggests that they use RSA, and they provides their public key: (12629063, 250219). John replies with the ciphertext 5405012. Kaitlyn's private key is 1803547. In what year was John born?

Enter the answer:

1982

How to solve

In order to decode, we need to use the function: $value^d \mod n$. Because of the size of the values, we have to use the Rapid Modular Exponentation (https://en.wikipedia.org/wiki/Modular_exponentiation) method, also known as the method of repeated squaring (https://en.wikipedia.org/wiki/Exponentiation_by_squaring).

First we need to convert Kaitlyn's private key *d* to binary which will tell us how many operations we will need to do

$d = 1803547 = binary(110111000010100011011)$

We need to compute the following powers: 5405012^{1}, 5405012^{2}, 5405012^{8}, 5405012^{16}, 5405012^{256}, 5405012^{1024}, 5405012^{32768}, 5405012^{65536}, 5405012^{131072}, 5405012^{524288} and $5405012^{1048576}$

$5405012^{1} = 5405012$

Since this is the first powers we start our result: $result = 5405012$

$5405012^{2} \equiv 5405012^{2} \equiv 5405012^{2} \mod 12629063 \equiv 29214154720144 \mod 12629063 \equiv 12622583$

We need this power, so accumulate it: $result = (5405012 * 12622583) \mod 12629063 = 68225212585996 \mod 12629063 = 8543002$

$5405012^{4} \equiv 12622583^{2} \equiv 12622583^{2} \mod 12629063 \equiv 159329601591889 \mod 12629063 \equiv 4103211$

$5405012^{8} \equiv 4103211^{2} \equiv 4103211^{2} \mod 12629063 \equiv 16836340510521 \mod 12629063 \equiv 6204575$

We need this power, so accumulate it: $result = (8543002 * 6204575) \mod 12629063 = 53005696634150 \mod 12629063 = 3735590$

$5405012^{16} \equiv 6204575^{2} \equiv 6204575^{2} \mod 12629063 \equiv 38496750930625 \mod 12629063 \equiv 7575867$

We need this power, so accumulate it: $result = (3735590 * 7575867) \mod 12629063 = 28300333006530 \mod 12629063 = 4649523$

$5405012^{32} \equiv 7575867^{2} \equiv 7575867^{2} \mod 12629063 \equiv 57393760801689 \mod 12629063 \equiv 11560338$

$5405012^{64} \equiv 11560338^{2} \equiv 11560338^{2} \mod 12629063 \equiv 133641414674244 \mod 12629063 \equiv 667905$

$5405012^{128} \equiv 667905^{2} \equiv 667905^{2} \mod 12629063 \equiv 446097089025 \mod 12629063 \equiv 696676$

$5405012^{256} \equiv 696676^{2} \equiv 696676^{2} \mod 12629063 \equiv 485357448976 \mod 12629063 \equiv 9928823$

We need this power, so accumulate it: $result = (4649523 * 9928823) \mod 12629063 = 46164290901429 \mod 12629063 = 1382166$

$5405012^{512} \equiv 9928823^{2} \equiv 9928823^{2} \mod 12629063 \equiv 98581526165329 \mod 12629063 \equiv 7567054$

$5405012^{1024} \equiv 7567054^{2} \equiv 7567054^{2} \mod 12629063 \equiv 57260306238916 \mod 12629063 \equiv 8306286$

We need this power, so accumulate it: $result = (1382166 * 8306286) \mod 12629063 = 11480666095476 \mod 12629063 = 1681255$

$5405012^{2048} \equiv 8306286^{2} \equiv 8306286^{2} \mod 12629063 \equiv 68994387113796 \mod 12629063 \equiv 9988787$

$5405012^{4096} \equiv 9988787^{2} \equiv 9988787^{2} \mod 12629063 \equiv 99775865731369 \mod 12629063 \equiv 4016121$

$5405012^{8192} \equiv 4016121^{2} \equiv 4016121^{2} \mod 12629063 \equiv 16129227886641 \mod 12629063 \equiv 7447128$

$5405012^{16384} \equiv 7447128^{2} \equiv 7447128^{2} \mod 12629063 \equiv 55459715448384 \mod 12629063 \equiv 6172979$

$5405012^{32768} \equiv 6172979^{2} \equiv 6172979^{2} \mod 12629063 \equiv 38105669734441 \mod 12629063 \equiv 10573604$

We need this power, so accumulate it: $result = (1681255 * 10573604) \mod 12629063 = 17776924593020 \mod 12629063 = 2932960$

$5405012^{65536} \equiv 10573604^{2} \equiv 10573604^{2} \mod 12629063 \equiv 111801101548816 \mod 12629063 \equiv 10222787$

We need this power, so accumulate it: $result = (2932960 * 10222787) \mod 12629063 = 29983025359520 \mod 12629063 = 648393$

$5405012^{131072} \equiv 10222787^{2} \equiv 10222787^{2} \mod 12629063 \equiv 104505374047369 \mod 12629063 \equiv 4012999$

We need this power, so accumulate it: $result = (648393 * 4012999) \mod 12629063 = 2602000460607 \mod 12629063 = 9352591$

$5405012^{262144} \equiv 4012999^{2} \equiv 4012999^{2} \mod 12629063 \equiv 16104160974001 \mod 12629063 \equiv 9224543$

$5405012^{524288} \equiv 9224543^{2} \equiv 9224543^{2} \mod 12629063 \equiv 85092193558849 \mod 12629063 \equiv 4474008$

We need this power, so accumulate it: $result = (9352591 * 4474008) \mod 12629063 = 41843566954728 \mod 12629063 = 8243403$

$5405012^{1048576} \equiv 4474008^{2} \equiv 4474008^{2} \mod 12629063 \equiv 20016747584064 \mod 12629063 \equiv 11084702$

We need this power, so accumulate it: $result = (8243403 * 11084702) \mod 12629063 = 91375665720906 \mod 12629063 = 1982$

Since we have computed all the powers, we see that the result is 1982

10) **[300 points]** Brett, has faithfully followed the steps of the RSA key-generation algorithm. Here are the results:

p = 1439
q = 2099
n = 3020461
Φ = 3016924
e = 2729827

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

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

2621231

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 $e = 2729827$ and $\Phi = 3016924$ 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):

$r_0 = 3016924$	$s_0 = 1$	$t_0 = 0$
$r_1 = 2729827$	$s_1 = 0$	$t_1 = 1$

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: $r_0 = 3016924, s_0 = 1, t_0 = 0$
... and the second set of values for them: $r_1 = 2729827, s_1 = 0, t_1 = 1$
The quotient for this step is computed from $q_i = \lfloor 3016924 \div 2729827 \rfloor = 1$

$r_2 = r_0 - (q_1 * r_1)$ $r_2 = 3016924 - (1 * 2729827)$ $r_2 = 3016924 - 2729827$ $r_2 = 287097$	$s_2 = s_0 - (q_1 * s_1)$ $s_2 = 1 - (1 * 0)$ $s_2 = 1 - 0$ $s_2 = 1$	$t_2 = t_0 - (q_1 * t_1)$ $t_2 = 0 - (1 * 1)$ $t_2 = 0 - 1$ $t_2 = -1$

Iteration 2 ...

Start with first set of values for the remainder and coefficients: $r_1 = 2729827, s_1 = 0, t_1 = 1$
... and the second set of values for them: $r_2 = 287097, s_2 = 1, t_2 = -1$
The quotient for this step is computed from $q_i = \lfloor 2729827 \div 287097 \rfloor = 9$

$r_3 = r_1 - (q_2 * r_2)$ $r_3 = 2729827 - (9 * 287097)$ $r_3 = 2729827 - 2583873$ $r_3 = 145954$	$s_3 = s_1 - (q_2 * s_2)$ $s_3 = 0 - (9 * 1)$ $s_3 = 0 - 9$ $s_3 = -9$	$t_3 = t_1 - (q_2 * t_2)$ $t_3 = 1 - (9 * -1)$ $t_3 = 1 - (-9)$ $t_3 = 10$

Iteration 3 ...

Start with first set of values for the remainder and coefficients: $r_2 = 287097, s_2 = 1, t_2 = -1$
... and the second set of values for them: $r_3 = 145954, s_3 = -9, t_3 = 10$
The quotient for this step is computed from $q_i = \lfloor 287097 \div 145954 \rfloor = 1$

$r_4 = r_2 - (q_3 * r_3)$ $r_4 = 287097 - (1 * 145954)$ $r_4 = 287097 - 145954$ $r_4 = 141143$	$s_4 = s_2 - (q_3 * s_3)$ $s_4 = 1 - (1 * -9)$ $s_4 = 1 - (-9)$ $s_4 = 10$	$t_4 = t_2 - (q_3 * t_3)$ $t_4 = -1 - (1 * 10)$ $t_4 = -1 - 10$ $t_4 = -11$

Iteration 4 ...

Start with first set of values for the remainder and coefficients: $r_3 = 145954, s_3 = -9, t_3 = 10$
... and the second set of values for them: $r_4 = 141143, s_4 = 10, t_4 = -11$

The quotient for this step is computed from $q_i = \lfloor 145954 \div 141143 \rfloor = 1$

$r_5 = r_3 - (q_4 * r_4)$	$s_5 = s_3 - (q_4 * s_4)$	$t_5 = t_3 - (q_4 * t_4)$
$r_5 = 145954 - (1 * 141143)$	$s_5 = -9 - (1 * 10)$	$t_5 = 10 - (1 * -11)$
$r_5 = 145954 - 141143$	$s_5 = -9 - 10$	$t_5 = 10 - (-11)$
$r_5 = 4811$	$s_5 = -19$	$t_5 = 21$

Iteration 5 ...

Start with first set of values for the remainder and coefficients: $r_4 = 141143, s_4 = 10, t_4 = -11$
... and the second set of values for them: $r_5 = 4811, s_5 = -19, t_5 = 21$
The quotient for this step is computed from $q_i = \lfloor 141143 \div 4811 \rfloor = 29$

$r_6 = r_4 - (q_5 * r_5)$	$s_6 = s_4 - (q_5 * s_5)$	$t_6 = t_4 - (q_5 * t_5)$
$r_6 = 141143 - (29 * 4811)$	$s_6 = 10 - (29 * -19)$	$t_6 = -11 - (29 * 21)$
$r_6 = 141143 - 139519$	$s_6 = 10 - (-551)$	$t_6 = -11 - 609$
$r_6 = 1624$	$s_6 = 561$	$t_6 = -620$

Iteration 6 ...

Start with first set of values for the remainder and coefficients: $r_5 = 4811, s_5 = -19, t_5 = 21$
... and the second set of values for them: $r_6 = 1624, s_6 = 561, t_6 = -620$
The quotient for this step is computed from $q_i = \lfloor 4811 \div 1624 \rfloor = 2$

$r_7 = r_5 - (q_6 * r_6)$	$s_7 = s_5 - (q_6 * s_6)$	$t_7 = t_5 - (q_6 * t_6)$
$r_7 = 4811 - (2 * 1624)$	$s_7 = -19 - (2 * 561)$	$t_7 = 21 - (2 * -620)$
$r_7 = 4811 - 3248$	$s_7 = -19 - 1122$	$t_7 = 21 - (-1240)$
$r_7 = 1563$	$s_7 = -1141$	$t_7 = 1261$

Iteration 7 ...

Start with first set of values for the remainder and coefficients: $r_6 = 1624, s_6 = 561, t_6 = -620$
... and the second set of values for them: $r_7 = 1563, s_7 = -1141, t_7 = 1261$
The quotient for this step is computed from $q_i = \lfloor 1624 \div 1563 \rfloor = 1$

$r_8 = r_6 - (q_7 * r_7)$	$s_8 = s_6 - (q_7 * s_7)$	$t_8 = t_6 - (q_7 * t_7)$
$r_8 = 1624 - (1 * 1563)$	$s_8 = 561 - (1 * -1141)$	$t_8 = -620 - (1 * 1261)$
$r_8 = 1624 - 1563$	$s_8 = 561 - (-1141)$	$t_8 = -620 - 1261$
$r_8 = 61$	$s_8 = 1702$	$t_8 = -1881$

Iteration 8 ...

Start with first set of values for the remainder and coefficients: $r_7 = 1563, s_7 = -1141, t_7 = 1261$
... and the second set of values for them: $r_8 = 61, s_8 = 1702, t_8 = -1881$
The quotient for this step is computed from $q_i = \lfloor 1563 \div 61 \rfloor = 25$

$r_9 = r_7 - (q_8 * r_8)$	$s_9 = s_7 - (q_8 * s_8)$	$t_9 = t_7 - (q_8 * t_8)$
$r_9 = 1563 - (25 * 61)$	$s_9 = -1141 - (25 * 1702)$	$t_9 = 1261 - (25 * -1881)$
$r_9 = 1563 - 1525$	$s_9 = -1141 - 42550$	$t_9 = 1261 - (-47025)$
$r_9 = 38$	$s_9 = -43691$	$t_9 = 48286$

Iteration 9 ...

Start with first set of values for the remainder and coefficients: $r_8 = 61, s_8 = 1702, t_8 = -1881$
... and the second set of values for them: $r_9 = 38, s_9 = -43691, t_9 = 48286$
The quotient for this step is computed from $q_i = \lfloor 61 \div 38 \rfloor = 1$

$r_{10} = r_8 - (q_9 * r_9)$	$s_{10} = s_8 - (q_9 * s_9)$	$t_{10} = t_8 - (q_9 * t_9)$
$r_{10} = 61 - (1 * 38)$	$s_{10} = 1702 - (1 * -43691)$	$t_{10} = -1881 - (1 * 48286)$
$r_{10} = 61 - 38$	$s_{10} = 1702 - (-43691)$	$t_{10} = -1881 - 48286$
$r_{10} = 23$	$s_{10} = 45393$	$t_{10} = -50167$

Iteration 10 ...

Start with first set of values for the remainder and coefficients: $r_9 = 38, s_9 = -43691, t_9 = 48286$
... and the second set of values for them: $r_{10} = 23, s_{10} = 45393, t_{10} = -50167$
The quotient for this step is computed from $q_i = \lfloor 38 \div 23 \rfloor = 1$

$r_{11} = r_9 - (q_{10} * r_{10})$ $r_{11} = 38 - (1 * 23)$ $r_{11} = 38 - 23$ $r_{11} = 15$	$s_{11} = s_9 - (q_{10} * s_{10})$ $s_{11} = -43691 - (1 * 45393)$ $s_{11} = -43691 - 45393$ $s_{11} = -89084$	$t_{11} = t_9 - (q_{10} * t_{10})$ $t_{11} = 48286 - (1 * -50167)$ $t_{11} = 48286 - (-50167)$ $t_{11} = 98453$

Iteration 11 ...

Start with first set of values for the remainder and coefficients: $r_{10} = 23, s_{10} = 45393, t_{10} = -50167$
... and the second set of values for them: $r_{11} = 15, s_{11} = -89084, t_{11} = 98453$
The quotient for this step is computed from $q_i = \lfloor 23 \div 15 \rfloor = 1$

$r_{12} = r_{10} - (q_{11} * r_{11})$ $r_{12} = 23 - (1 * 15)$ $r_{12} = 23 - 15$ $r_{12} = 8$	$s_{12} = s_{10} - (q_{11} * s_{11})$ $s_{12} = 45393 - (1 * -89084)$ $s_{12} = 45393 - (-89084)$ $s_{12} = 134477$	$t_{12} = t_{10} - (q_{11} * t_{11})$ $t_{12} = -50167 - (1 * 98453)$ $t_{12} = -50167 - 98453$ $t_{12} = -148620$

Iteration 12 ...

Start with first set of values for the remainder and coefficients: $r_{11} = 15, s_{11} = -89084, t_{11} = 98453$
... and the second set of values for them: $r_{12} = 8, s_{12} = 134477, t_{12} = -148620$
The quotient for this step is computed from $q_i = \lfloor 15 \div 8 \rfloor = 1$

$r_{13} = r_{11} - (q_{12} * r_{12})$ $r_{13} = 15 - (1 * 8)$ $r_{13} = 15 - 8$ $r_{13} = 7$	$s_{13} = s_{11} - (q_{12} * s_{12})$ $s_{13} = -89084 - (1 * 134477)$ $s_{13} = -89084 - 134477$ $s_{13} = -223561$	$t_{13} = t_{11} - (q_{12} * t_{12})$ $t_{13} = 98453 - (1 * -148620)$ $t_{13} = 98453 - (-148620)$ $t_{13} = 247073$

Iteration 13 ...

Start with first set of values for the remainder and coefficients: $r_{12} = 8, s_{12} = 134477, t_{12} = -148620$
... and the second set of values for them: $r_{13} = 7, s_{13} = -223561, t_{13} = 247073$
The quotient for this step is computed from $q_i = \lfloor 8 \div 7 \rfloor = 1$

$r_{14} = r_{12} - (q_{13} * r_{13})$ $r_{14} = 8 - (1 * 7)$ $r_{14} = 8 - 7$ $r_{14} = 1$	$s_{14} = s_{12} - (q_{13} * s_{13})$ $s_{14} = 134477 - (1 * -223561)$ $s_{14} = 134477 - (-223561)$ $s_{14} = 358038$	$t_{14} = t_{12} - (q_{13} * t_{13})$ $t_{14} = -148620 - (1 * 247073)$ $t_{14} = -148620 - 247073$ $t_{14} = -395693$

Success!

Since the value for *d* is negative, add the modulus 3016924
$-395693 + 3016924 = 2621231$
$d = 2621231$
Therefore, let's check that $d \cdot e = 1 \mod \Phi$
$2621231 \cdot 2729827 = 1 \mod 3016924$
$7155507157037 = 1 \mod 3016924$
$1 + 7155507157036 = 1 \mod 3016924$
$1 + (2371789 \cdot 3016924) = 1 \mod 3016924$

Hence 2621231 and 3016924 are inverses of each other