Science Olympiad — Captains Tryouts 2019 - Parkland High School 2019

Timed Question **[200 points]** Solve this Aristocrat, a quote said by Cookie Monster. When you have solved it, raise your hand so that the time can be recorded and the solution checked.

BCSGO WR ZNAA ANDR NE BUR WCWREB, QEARTT NB'T
TODAY ME WILL LIVE IN THE MOMENT, UNLESS IT'S

QEYARGTGEB, NE ZUNKU KGTR N ZNAA RGB G KCCLNR!
UNPLEASANT, IN WHICH CASE I WILL EAT A COOKIE!

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

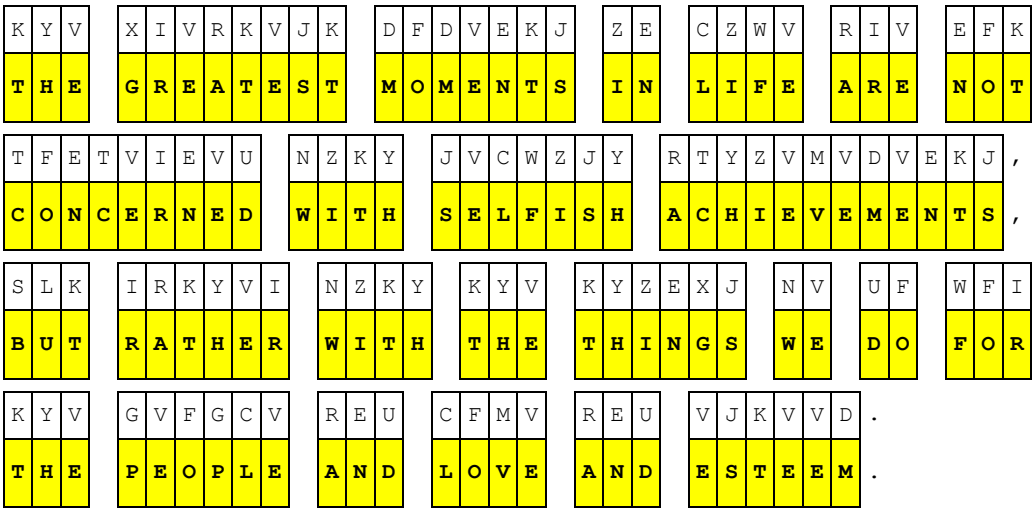
1) **[275 points]** Solve this Aristocrat, a quote by David Alan Grier pertaining to body image.

GFEU MNAG V PRVDI V XFFI IVDM FW TZPU, QZP FPRUJ
SOME DAYS I THINK I LOOK KIND OF CUTE, BUT OTHER

MNAG V PJA PF NYFVM PRU EVJJFJ.
DAYS I TRY TO AVOID THE MIRROR.

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

2) **[125 points]** Decode this quote by Walt Disney which has been encoded using an unknown shift of the Caesar cipher.



How to solve

Since there are no single letter words we look for the double letter words and find ZE and NV and UF.

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 Z and AI with a key of N and AL with a key of U

Using the beginning letter B gives BG with a key of Y and BJ with a key of M and BM with a key of T

Using the beginning letter I gives a common word IN with a key of R and IQ with a key of F a common word and IT with a key of M

Using the beginning letter M gives MR with a key of N a common word and MU with a key of B and MX with a key of I

Using the beginning letter O gives OT with a key of L and OW with a key of Z and OZ with a key of G

Using the beginning letter U gives UZ with a key of F and UC with a key of T and UF with a key of A

Using the ending letter O gives 'JO' with a key of Q a common word and 'GO' with a key of H a common word and 'DO' with a key of R

Using the ending letter E gives 'ZE' with a key of A a common word and 'WE' with a key of R and 'TE' with a key of B

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

Using the R row to decode the first long word 'XIVRKVJK', it comes out as 'GREATEST'

Using the H row to decode the first long word 'XIVRKVJK', it comes out as 'QBOKDOCD'

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

3) **[215 points]** Decode this affine, which is a *punny* quote from the children's TV show *Bubble Guppies.* The first two letters are IM.

Z	P	V	N	E	T	B	I	J		L	X	V		T		F	V	J	N	E	Z	X	G	.		K	V	E		Z	'	Y	Y
I	**M**	**U**	**S**	**T**	**A**	**C**	**H**	**E**		**Y**	**O**	**U**		**A**		**Q**	**U**	**E**	**S**	**T**	**I**	**O**	**N**	.		**B**	**U**	**T**		**I**	'	**L**	**L**

N	I	T	M	J		Z	E		A	X	W		Y	T	E	J	W	.
S	**H**	**A**	**V**	**E**		**I**	**T**		**F**	**O**	**R**		**L**	**A**	**T**	**E**	**R**	.

How to solve

Using the given value of $\mathrm{a} = 17$ and $\mathrm{b} = 19$ we can calcuate using the formula $a * x + b \mod 26$

Z	P	V	N	E	T	B	I	J	L	X	V	T	F	V	J	N	E	Z	X	G	K	V	E	Z	Y	Y	N	I	T	M	J	Z	E	A	X	W	Y	T	E	J	W

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

$$
\begin{array}{lcrcrcl}
E(4) & \rightarrow & 4 * 17 + 19 & \rightarrow & 87 \mod 26 & \rightarrow & J(9) \\
T(19) & \rightarrow & 19 * 17 + 19 & \rightarrow & 342 \mod 26 & \rightarrow & E(4) \\
A(0) & \rightarrow & 0 * 17 + 19 & \rightarrow & 19 \mod 26 & \rightarrow & T(19) \\
O(14) & \rightarrow & 14 * 17 + 19 & \rightarrow & 257 \mod 26 & \rightarrow & X(23) \\
I(8) & \rightarrow & 8 * 17 + 19 & \rightarrow & 155 \mod 26 & \rightarrow & Z(25) \\
N(13) & \rightarrow & 13 * 17 + 19 & \rightarrow & 240 \mod 26 & \rightarrow & G(6)
\end{array}
$$

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

Z	P	V	N	E	T	B	I	J	L	X	V	T	F	V	J	N	E	Z	X	G	K	V	E	Z	Y	Y	N	I	T	M	J	Z	E	A	X	W	Y	T	E	J	W
I				**T**	**A**			**E**		**O**		**A**			**E**		**T**	**I**	**O**	**N**			**T**	**I**				**A**		**E**	**I**	**T**		**O**			**A**	**T**	**E**	

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

$$
\begin{array}{lcrcrcl}
S(18) & \rightarrow & 18 * 17 + 19 & \rightarrow & 325 \mod 26 & \rightarrow & N(13) \\
R(17) & \rightarrow & 17 * 17 + 19 & \rightarrow & 308 \mod 26 & \rightarrow & W(22) \\
H(7) & \rightarrow & 7 * 17 + 19 & \rightarrow & 138 \mod 26 & \rightarrow & I(8) \\
L(11) & \rightarrow & 11 * 17 + 19 & \rightarrow & 206 \mod 26 & \rightarrow & Y(24) \\
D(3) & \rightarrow & 3 * 17 + 19 & \rightarrow & 70 \mod 26 & \rightarrow & S(18)
\end{array}
$$

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

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

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

$$
\begin{array}{lcrcrcl}
C(2) & \rightarrow & 2 * 17 + 19 & \rightarrow & 53 \mod 26 & \rightarrow & B(1) \\
U(20) & \rightarrow & 20 * 17 + 19 & \rightarrow & 359 \mod 26 & \rightarrow & V(21) \\
M(12) & \rightarrow & 12 * 17 + 19 & \rightarrow & 223 \mod 26 & \rightarrow & P(15) \\
F(5) & \rightarrow & 5 * 17 + 19 & \rightarrow & 104 \mod 26 & \rightarrow & A(0) \\
P(15) & \rightarrow & 15 * 17 + 19 & \rightarrow & 274 \mod 26 & \rightarrow & O(14)
\end{array}
$$

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

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

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

$$
\begin{array}{lcrcrcl}
G(6) & \rightarrow & 6*17+19 & \rightarrow & 121 & \mod 26 & \rightarrow & R(17) \\
W(22) & \rightarrow & 22*17+19 & \rightarrow & 393 & \mod 26 & \rightarrow & D(3) \\
Y(24) & \rightarrow & 24*17+19 & \rightarrow & 427 & \mod 26 & \rightarrow & L(11) \\
B(1) & \rightarrow & 1*17+19 & \rightarrow & 36 & \mod 26 & \rightarrow & K(10) \\
V(21) & \rightarrow & 21*17+19 & \rightarrow & 376 & \mod 26 & \rightarrow & M(12)
\end{array}
$$

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

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

We will convert the remaining 5 letters **KXJQZ**.

$$
\begin{array}{lcrcrcl}
K(10) & \rightarrow & 10*17+19 & \rightarrow & 189 & \mod 26 & \rightarrow & H(7) \\
X(23) & \rightarrow & 23*17+19 & \rightarrow & 410 & \mod 26 & \rightarrow & U(20) \\
J(9) & \rightarrow & 9*17+19 & \rightarrow & 172 & \mod 26 & \rightarrow & Q(16) \\
Q(16) & \rightarrow & 16*17+19 & \rightarrow & 291 & \mod 26 & \rightarrow & F(5) \\
Z(25) & \rightarrow & 25*17+19 & \rightarrow & 444 & \mod 26 & \rightarrow & C(2)
\end{array}
$$

The remaining 5 letters we know are (HUQFC), so we will fill those in.

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

The solution is now complete!

---

4) **[200 points]** Encode this quote by Rumi using the Vigenère cipher and using the keyword, WORDS.

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

W	O	R	D	S	W	O	R	D	S	W	O	R	D	S	W	O	R	D	S	W
R	O	W	S	F	L	O	W	E	R	S	N	O	T	T	H	U	N	D	E	R
N	C	N	V	X	H	C	N	H	J	O	B	F	W	L	D	I	E	G	W	N

5) **[325 points]** Solve this quote by Dmitri Mendeleev, which has been encoded with a K1 alphabet. However, when being encoded, the machine made some mistakes, so keep on the lookout for those!

QWQ TXL SF X ZVQXR X UXYEQ LPQVQ XEE UPQ QEQRQFUT
EYE SAW IN A DREAM A TABLE WHERE ALL THE ELEMENTS

AQEE SFUG HEXOQ XT VQIJSVQZ. XLXDQFSFB, QWQ
FELL INTO PLACE AS REQUIRED. AWAKENING, EYE

SRRQZSXUQEW LVGUQ SU ZGLF GF X HQXOQ GA HXHQV
IMMEDIATELY WROTE IT DOWN ON A PEACE OF PAPER

K1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	2	1		1	8	7	5	4	1	1		5			2	2	23	4	7	3	7	6	3	14	1	4
Replacement	F	G	J	K	L	N	O	P	Q	U	V	W	X	Z	C	H	E	M	I	S	T	R	Y	A	B	D

6) **[300 points]** Solve this baconian, a quote by Michelle Obama.

/{\]}[{1|/]}\[{]1|}[{]/\}[1{]}|[{]}[/{\]1}[{|]}[{]/}[
BABAAAABBBAABAAABBAAAABBAABAAABAAAAABABABAAABAAAAABAA
W H E N G I R L S A R

{]}[\{]}[1{]}[{|/\]}1|[{]/}[{]}[\{]1}[{|]}[{]/\1}[|{]
AAAABAAAABAAAAABBBAABBAAABAAAAAABAABAAABAAAAABBBAABAA
E E D U C A T E D T

}/\1[{|]}[/{]}\[{]}[{]1}[|/{\1]}|/[\1{]|}[/{\]}[{]1}[
ABBBAABAAABAAABAAAAAAABAABBABBAABBABBAABAABABAAAAABAA
H E I R C O U N T R I

{]}|[{/]}[\{]}[1{]|}[{]}/[{\1]|}/[\1{]|}[/{]}\1[{|]/}
AAABAABAAABAAAABAABAAAAABAABBABABABBAABAABAAABBAABABA
E S B E C O M E S T

[{]}\1[|{/\]}[{1|]}[/{]\}[{]}[{]}[1|{]}[{/\]1}|/[\1{|
AAAABBABABBAAAABBAAABAABAAAAAAAAAABBAAAAABBABABBABBAB
R O N G E R A N D M O

/]}[{]}\[{]1|/}\[{]}[1|{/\]}[1{|/\]}[1{]|}[{]}/\[1|{]
BAAAAAABAAABBBABAAAAABBABBAAABABBBAAABAABAAAAABBABBAA
R E P R O S P E R O U

/\1}[{|
BBBAAAB
S

When girls are educated, their countries become stronger and more prosperous.

The A letters are represented by '{]}[' and the B letters by '/\I|'

7) **[375 points]** Solve this quote by Dr. Seuss, which has been encoded into Spanish using a K2 Alphabet with an English keyword.

OP KGBT AKIK KWWK, OP KGBT AKIK KWWK, SKH ÑMCKC
DE AQUI PARA ALLA, DE AQUI PARA ALLA, HAY COSAS

OTDPILTOKC PY LMOKC AKILPC
DIVERTIDAS EN TODAS PARTES

Replacement	K	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	M	A	G	I	C	L	B	D	E	F	H	J
K2	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	3	2	5	1			2	1	4		15	3	2		1	5	5			1	4			4		1	

Translation: *From there to here, from here to there, funny things are everywhere*

8) **[175 points]** Decrypt this word below, which had been encoded using the keyword "PINT"

$$\begin{pmatrix} P & I \\ N & T \end{pmatrix} \equiv \begin{pmatrix} 15 & 8 \\ 13 & 19 \end{pmatrix}$$

F	L	P	L	V	Q	C	N	A	H
T	**E**	**L**	**E**	**P**	**H**	**O**	**N**	**E**	**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

$$\begin{pmatrix} 15 & 8 \\ 13 & 19 \end{pmatrix}^{-1} = (15 * 19 - 8 * 13)^{-1} \begin{pmatrix} 19 & -8 \\ -13 & 15 \end{pmatrix}$$

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

$$(15 * 19 - 8 * 13) \mod 26 = 181 \mod 26 = 25$$

Looking up 25 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 25 which we substitute into the formula to compute the matrix:

$$(15 * 19 - 8 * 13)^{-1} \begin{pmatrix} 19 & -8 \\ -13 & 15 \end{pmatrix} \equiv 25 \begin{pmatrix} 19 & -8 \\ -13 & 15 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 25 * 19 & 25 * -8 \\ 25 * -13 & 25 * 15 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} 475 & -200 \\ -325 & 375 \end{pmatrix}$$
$$\mod 26 \equiv \begin{pmatrix} 475 \mod 26 & -200 \mod 26 \\ -325 \mod 26 & 375 \mod 26 \end{pmatrix} \equiv \begin{pmatrix} 7 & 8 \\ 13 & 11 \end{pmatrix}$$

With the inverse matrix we can now decode

$$\begin{pmatrix} H & I \\ N & L \end{pmatrix} * \begin{pmatrix} F \\ L \end{pmatrix} \equiv \begin{pmatrix} 7 & 8 \\ 13 & 11 \end{pmatrix} * \begin{pmatrix} 5 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 7 * 5 + 8 * 11 \\ 13 * 5 + 11 * 11 \end{pmatrix} \equiv \begin{pmatrix} 123 \\ 186 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 4 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} T \\ E \end{pmatrix}$$
$$\begin{pmatrix} H & I \\ N & L \end{pmatrix} * \begin{pmatrix} P \\ L \end{pmatrix} \equiv \begin{pmatrix} 7 & 8 \\ 13 & 11 \end{pmatrix} * \begin{pmatrix} 15 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 7 * 15 + 8 * 11 \\ 13 * 15 + 11 * 11 \end{pmatrix} \equiv \begin{pmatrix} 193 \\ 316 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 4 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} L \\ E \end{pmatrix}$$
$$\begin{pmatrix} H & I \\ N & L \end{pmatrix} * \begin{pmatrix} V \\ Q \end{pmatrix} \equiv \begin{pmatrix} 7 & 8 \\ 13 & 11 \end{pmatrix} * \begin{pmatrix} 21 \\ 16 \end{pmatrix} \equiv \begin{pmatrix} 7 * 21 + 8 * 16 \\ 13 * 21 + 11 * 16 \end{pmatrix} \equiv \begin{pmatrix} 275 \\ 449 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 7 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} P \\ H \end{pmatrix}$$
$$\begin{pmatrix} H & I \\ N & L \end{pmatrix} * \begin{pmatrix} C \\ N \end{pmatrix} \equiv \begin{pmatrix} 7 & 8 \\ 13 & 11 \end{pmatrix} * \begin{pmatrix} 2 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 7 * 2 + 8 * 13 \\ 13 * 2 + 11 * 13 \end{pmatrix} \equiv \begin{pmatrix} 118 \\ 169 \end{pmatrix} \equiv \begin{pmatrix} 14 \\ 13 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} O \\ N \end{pmatrix}$$
$$\begin{pmatrix} H & I \\ N & L \end{pmatrix} * \begin{pmatrix} A \\ H \end{pmatrix} \equiv \begin{pmatrix} 7 & 8 \\ 13 & 11 \end{pmatrix} * \begin{pmatrix} 0 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 7 * 0 + 8 * 7 \\ 13 * 0 + 11 * 7 \end{pmatrix} \equiv \begin{pmatrix} 56 \\ 77 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 25 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} E \\ Z \end{pmatrix}$$

9) **[150 points]** A quote adapted from a famous saying by Benjamin Franklin, has been encoded using the Morbit Cipher for you to decode. You are told that **9**=●×, **2**=–●, **1**=–×, **8**=—, **3**=×●, **7**=●●

```
9 5 3 2 3 2 9 2 8 6 1 8 1 4 7 9 9 2 9 3 3 1 5 9 5 7 4 5 1
●×●–×●–●×●–●●×–●––××–×–––××–●●●×●×–●●××●×●–×●–●×●–●●×–●––×
E A  R   L    Y   / T O   /B    E D   /E A  R   L    Y

4 4 8 6 5 1 5 4 5 3 6 8 3 1 2 1 9 7 9 3 1 3 2 9 5 4 7
×–×–––××●––×●–×–●–×●××––×●–×–●–×●×●●●××●–××●–●●×●–×–●●
/T O  / W   A  K   E/ M  A  K   E S   /A  /L   A  D

4 5 1 3 7 4 1 5 3 2 4 6 5 2 3 2 3 4 4 4 5 1 3 1 2 4 7
×–●––××●●●×––×●–×●–●×–××●––●×●–●×●×–×–×–●––××●–×–●×–●●
 Y    /S   M  A  R   T/ P    R   E T T Y    /A  N  D

6 8 9 5 9 9 5 4
××––●×●–●×●×●–×–
/ G   R   E A  T
```

How to solve

Since we are told the mapping of 921837 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 5 3 2 3 2 9 2 8 6 1 8 1 4 7 9 9 2 9 3 3 1 5 9 5 7 4 5 1
●×  ×●–●×●–●●×–●––  –×–––×  ●●●×●×–●●××●×●–×  ●×  ●●    –×
E    R   L            O        E D  / E A

4 4 8 6 5 1 5 4 5 3 6 8 3 1 2 1 9 7 9 3 1 3 2 9 5 4 7
    ––    –×      ×●  ––×●–×–●–×●×●●●××●–××●–●●×    ●●
                        A  K   E S  / A / L

4 5 1 3 7 4 1 5 3 2 4 6 5 2 3 2 3 4 4 4 5 1 3 1 2 4 7
    –××●●●  –×  ×●–●      –●×●–●×●        –××●–×–●  ●●
     /                    R           / A

6 8 9 5 9 9 5 4
  ––●×  ●×●×
          E
```

At this point in time, 3 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 95 where we know that 9 ends with × which means that 5 cannot be ××, so we can eliminate that possibility. Also,we find the sequence 14 where we know that 1 ends with × which means that 4 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:

```
9 5 3 2 3 2 9 2 8 6 1 8 1 4 7 9 9 2 9 3 3 1 5 9 5 7 4 5 1
●× –×●–●×●–●●×–●––  –×–––× –●●●×●×–●●××●×●–× –●× –●● – ––×
E    R   L            O        E D  / E A
```

```
4 4 8 6 5 1 5 4 5 3 6 8 3 1 2 1 9 7 9 3 1 3 2 9 5 4 7
 – ---   --x – – –x●  --x●–x–●–x●x●●●xx●–xx●–●●x – –●●
                        A  K   E S  / A / L

4 5 1 3 7 4 1 5 3 2 4 6 5 2 3 2 3 4 4 4 5 1 3 1 2 4 7
 – --xx●●● --x –x●–● –   --●x●–●x● – – – --xx●–x–● –●●
    /                      R            / A

6 8 9 5 9 9 5 4
  --●x –●x●x – –
         E
```

At this point in time, 3 ciphertext characters still need to be mapped. Looking for unique mappings, 6 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:

```
9 5 3 2 3 2 9 2 8 6 1 8 1 4 7 9 9 2 9 3 3 1 5 9 5 7 4 5 1
●x –x●–●x●–●●x–●––xx–x–––x –●●●x●x–●●xx●x●–x –●x –●● – ––x
E   R   L   Y   / T O         E D  / E A

4 4 8 6 5 1 5 4 5 3 6 8 3 1 2 1 9 7 9 3 1 3 2 9 5 4 7
 – ---xx --x – – –x●xx––x●–x–●–x●x●●●xx●–xx●–●●x – –●●
    /            E/ M  A  K   E S  / A / L

4 5 1 3 7 4 1 5 3 2 4 6 5 2 3 2 3 4 4 4 5 1 3 1 2 4 7
 – --xx●●● --x –x●–● –xx --●x●–●x● – – – --xx●–x–● –●●
    /                /     R            / A

6 8 9 5 9 9 5 4
××––●x –●x●x – –
 / G       E
```

At this point in time, 2 ciphertext characters still need to be mapped. Looking for unknowns next to ×× which would result in three in a row, we find the sequence 65 where we know that 6 is ×× which means that 5 cannot start with ×, so we can eliminate those possibilities That leaves ●– as the only option for 5, so we eliminate it from all the other options. Eliminating ●– as an option for 4 means that 4 must be ×–. Also,we find the sequence 65 where we know that 6 is ×× which means that 5 cannot start with ×, so we can eliminate those possibilities That leaves ●– as the only option for 5, so we eliminate it from all the other options.

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

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

```
9 5 3 2 3 2 9 2 8 6 1 8 1 4 7 9 9 2 9 3 3 1 5 9 5 7 4 5 1
●x●–x●–●x●–●●x–●––xx–x–––xx–●●●x●x–●●xx●x●–x●–●x●–●●x–●––x
E A  R   L   Y   / T O  / B    E D  / E A  R   L   Y

4 4 8 6 5 1 5 4 5 3 6 8 3 1 2 1 9 7 9 3 1 3 2 9 5 4 7
x–x–––xx●––x●–x–●–x●xx––x●–x–●–x●x●●●xx●–xx●–●●x●–x–●●
  T O  / W   A  K   E/ M  A  K   E S  / A / L   A  D

4 5 1 3 7 4 1 5 3 2 4 6 5 2 3 2 3 4 4 4 5 1 3 1 2 4 7
x–●––xx●●●x––x●–x●–●x–xx●––●x●–●x●x–x–x–●––xx●–x–●x–●●
  Y   / S   M  A  R   T/ P    R   E T T Y   / A  N  D

6 8 9 5 9 9 5 4
××––●x●–●x●x●–x–
 / G   R   E A  T
```

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

EARLY TO BED EARLYTO WAKE MAKES A LADY SMART PRETTY AND GREAT

---

10) **[450 points]** Solve this patristocrat, which is a quote by Maya Angelou which has been encoded using a K1 Alphabet.

UTJZF SZOEX UWQDZ YQEMU OPLMN OPQUE UTJZF LNOEL
IFYOU DONTL IKESO METHI NGCHA NGEIT IFYOU CANTC

MNOPQ UELMN OPQJZ FCNEE UEFSQ
HANGE ITCHA NGEYO URATT ITUDE

If you don't like something, change it. If you can't change it, change your attitude.

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

11) **[200 points]** The following quote by Shakespeare has been encoded with the Vigenère Cipher using a very common word for the key. The 21st through 24th cipher characters (**HEGM**) decode to be **OWNO**

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

12) **[200 points]** Special Agent, Samantha, has the following RSA public key:

`n = 132823  e = 46501`

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

```
132823 = 317 * 419
```

Compute the value of their private key:

Enter the computed private key:

58589

How to solve

To find the private key, First we need to find Φ using the formula:
$\Phi = (p-1) * (q-1)$
$\Phi = (317-1) * (419-1) = 316 * 418 = 132088$
We now know that we know that $\Phi = 132088$

Second, we use the extended Euclidean Algorithm (https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm) using 46501 and 132088

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):

$r_0 = 132088$	$s_0 = 1$	$t_0 = 0$
$r_1 = 46501$	$s_1 = 0$	$t_1 = 1$

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: $r_0 = 132088, s_0 = 1, t_0 = 0$
... and the second set of values for them: $r_1 = 46501, s_1 = 0, t_1 = 1$
The quotient for this step is computed from $q_i = \lfloor 132088 \div 46501 \rfloor = 2$

$r_2 = r_0 - (q_1 * r_1)$	$s_2 = s_0 - (q_1 * s_1)$	$t_2 = t_0 - (q_1 * t_1)$
$r_2 = 132088 - (2 * 46501)$	$s_2 = 1 - (2 * 0)$	$t_2 = 0 - (2 * 1)$
$r_2 = 132088 - 93002$	$s_2 = 1 - 0$	$t_2 = 0 - 2$
$r_2 = 39086$	$s_2 = 1$	$t_2 = -2$

Iteration 2 ...

Start with first set of values for the remainder and coefficients: $r_1 = 46501, s_1 = 0, t_1 = 1$
... and the second set of values for them: $r_2 = 39086, s_2 = 1, t_2 = -2$
The quotient for this step is computed from $q_i = \lfloor 46501 \div 39086 \rfloor = 1$

$r_3 = r_1 - (q_2 * r_2)$	$s_3 = s_1 - (q_2 * s_2)$	$t_3 = t_1 - (q_2 * t_2)$
$r_3 = 46501 - (1 * 39086)$	$s_3 = 0 - (1 * 1)$	$t_3 = 1 - (1 * -2)$
$r_3 = 46501 - 39086$	$s_3 = 0 - 1$	$t_3 = 1 - (-2)$
$r_3 = 7415$	$s_3 = -1$	$t_3 = 3$

Iteration 3 ...

Start with first set of values for the remainder and coefficients: $r_2 = 39086, s_2 = 1, t_2 = -2$
... and the second set of values for them: $r_3 = 7415, s_3 = -1, t_3 = 3$
The quotient for this step is computed from $q_i = \lfloor 39086 \div 7415 \rfloor = 5$

$r_4 = r_2 - (q_3 * r_3)$ $r_4 = 39086 - (5 * 7415)$ $r_4 = 39086 - 37075$ $r_4 = 2011$	$s_4 = s_2 - (q_3 * s_3)$ $s_4 = 1 - (5 * -1)$ $s_4 = 1 - (-5)$ $s_4 = 6$	$t_4 = t_2 - (q_3 * t_3)$ $t_4 = -2 - (5 * 3)$ $t_4 = -2 - 15$ $t_4 = -17$

Iteration 4 ...

Start with first set of values for the remainder and coefficients: $r_3 = 7415, s_3 = -1, t_3 = 3$
... and the second set of values for them: $r_4 = 2011, s_4 = 6, t_4 = -17$
The quotient for this step is computed from $q_i = \lfloor 7415 \div 2011 \rfloor = 3$

$r_5 = r_3 - (q_4 * r_4)$ $r_5 = 7415 - (3 * 2011)$ $r_5 = 7415 - 6033$ $r_5 = 1382$	$s_5 = s_3 - (q_4 * s_4)$ $s_5 = -1 - (3 * 6)$ $s_5 = -1 - 18$ $s_5 = -19$	$t_5 = t_3 - (q_4 * t_4)$ $t_5 = 3 - (3 * -17)$ $t_5 = 3 - (-51)$ $t_5 = 54$

Iteration 5 ...

Start with first set of values for the remainder and coefficients: $r_4 = 2011, s_4 = 6, t_4 = -17$
... and the second set of values for them: $r_5 = 1382, s_5 = -19, t_5 = 54$
The quotient for this step is computed from $q_i = \lfloor 2011 \div 1382 \rfloor = 1$

$r_6 = r_4 - (q_5 * r_5)$ $r_6 = 2011 - (1 * 1382)$ $r_6 = 2011 - 1382$ $r_6 = 629$	$s_6 = s_4 - (q_5 * s_5)$ $s_6 = 6 - (1 * -19)$ $s_6 = 6 - (-19)$ $s_6 = 25$	$t_6 = t_4 - (q_5 * t_5)$ $t_6 = -17 - (1 * 54)$ $t_6 = -17 - 54$ $t_6 = -71$

Iteration 6 ...

Start with first set of values for the remainder and coefficients: $r_5 = 1382, s_5 = -19, t_5 = 54$
... and the second set of values for them: $r_6 = 629, s_6 = 25, t_6 = -71$
The quotient for this step is computed from $q_i = \lfloor 1382 \div 629 \rfloor = 2$

$r_7 = r_5 - (q_6 * r_6)$ $r_7 = 1382 - (2 * 629)$ $r_7 = 1382 - 1258$ $r_7 = 124$	$s_7 = s_5 - (q_6 * s_6)$ $s_7 = -19 - (2 * 25)$ $s_7 = -19 - 50$ $s_7 = -69$	$t_7 = t_5 - (q_6 * t_6)$ $t_7 = 54 - (2 * -71)$ $t_7 = 54 - (-142)$ $t_7 = 196$

Iteration 7 ...

Start with first set of values for the remainder and coefficients: $r_6 = 629, s_6 = 25, t_6 = -71$
... and the second set of values for them: $r_7 = 124, s_7 = -69, t_7 = 196$
The quotient for this step is computed from $q_i = \lfloor 629 \div 124 \rfloor = 5$

$r_8 = r_6 - (q_7 * r_7)$ $r_8 = 629 - (5 * 124)$ $r_8 = 629 - 620$ $r_8 = 9$	$s_8 = s_6 - (q_7 * s_7)$ $s_8 = 25 - (5 * -69)$ $s_8 = 25 - (-345)$ $s_8 = 370$	$t_8 = t_6 - (q_7 * t_7)$ $t_8 = -71 - (5 * 196)$ $t_8 = -71 - 980$ $t_8 = -1051$

Iteration 8 ...

Start with first set of values for the remainder and coefficients: $r_7 = 124, s_7 = -69, t_7 = 196$
... and the second set of values for them: $r_8 = 9, s_8 = 370, t_8 = -1051$
The quotient for this step is computed from $q_i = \lfloor 124 \div 9 \rfloor = 13$

$r_9 = r_7 - (q_8 * r_8)$ $r_9 = 124 - (13 * 9)$ $r_9 = 124 - 117$ $r_9 = 7$	$s_9 = s_7 - (q_8 * s_8)$ $s_9 = -69 - (13 * 370)$ $s_9 = -69 - 4810$ $s_9 = -4879$	$t_9 = t_7 - (q_8 * t_8)$ $t_9 = 196 - (13 * -1051)$ $t_9 = 196 - (-13663)$ $t_9 = 13859$

Iteration 9 ...

Start with first set of values for the remainder and coefficients: $r_8 = 9, s_8 = 370, t_8 = -1051$
... and the second set of values for them: $r_9 = 7, s_9 = -4879, t_9 = 13859$
The quotient for this step is computed from $q_i = \lfloor 9 \div 7 \rfloor = 1$

$r_{10} = r_8 - (q_9 * r_9)$ $r_{10} = 9 - (1 * 7)$ $r_{10} = 9 - 7$ $r_{10} = 2$	$s_{10} = s_8 - (q_9 * s_9)$ $s_{10} = 370 - (1 * -4879)$ $s_{10} = 370 - (-4879)$ $s_{10} = 5249$	$t_{10} = t_8 - (q_9 * t_9)$ $t_{10} = -1051 - (1 * 13859)$ $t_{10} = -1051 - 13859$ $t_{10} = -14910$

Iteration 10 ...

Start with first set of values for the remainder and coefficients: $r_9 = 7, s_9 = -4879, t_9 = 13859$
... and the second set of values for them: $r_{10} = 2, s_{10} = 5249, t_{10} = -14910$
The quotient for this step is computed from $q_i = \lfloor 7 \div 2 \rfloor = 3$

$r_{11} = r_9 - (q_{10} * r_{10})$ $r_{11} = 7 - (3 * 2)$ $r_{11} = 7 - 6$ $r_{11} = 1$	$s_{11} = s_9 - (q_{10} * s_{10})$ $s_{11} = -4879 - (3 * 5249)$ $s_{11} = -4879 - 15747$ $s_{11} = -20626$	$t_{11} = t_9 - (q_{10} * t_{10})$ $t_{11} = 13859 - (3 * -14910)$ $t_{11} = 13859 - (-44730)$ $t_{11} = 58589$

Success!

$d = 58589$
Therefore, let's check that $d \cdot e = 1 \mod \Phi$
$58589 \cdot 46501 = 1 \mod 132088$
$2724447089 = 1 \mod 132088$
$1 + 2724447088 = 1 \mod 132088$
$1 + (20626 \cdot 132088) = 1 \mod 132088$

Hence 58589 and 132088 are inverses of each other

13) **[275 points]** Encode the word **animation** below using the keyword TYPEWRITE.

$$\begin{pmatrix} T & Y & P \\ E & W & R \\ I & T & E \end{pmatrix} \equiv \begin{pmatrix} 19 & 24 & 15 \\ 4 & 22 & 17 \\ 8 & 19 & 4 \end{pmatrix}$$

A	N	I	M	A	T	I	O	N
Q	**G**	**T**	**T**	**H**	**Q**	**H**	**P**	**S**

How to solve

$$\begin{pmatrix} T & Y & P \\ E & W & R \\ I & T & E \end{pmatrix} * \begin{pmatrix} A \\ N \\ I \end{pmatrix} \equiv \begin{pmatrix} 19 & 24 & 15 \\ 4 & 22 & 17 \\ 8 & 19 & 4 \end{pmatrix} * \begin{pmatrix} 0 \\ 13 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 19*0+24*13+15*8 \\ 4*0+22*13+17*8 \\ 8*0+19*13+4*8 \end{pmatrix} \equiv \begin{pmatrix} 432 \\ 422 \\ 279 \end{pmatrix} \equiv \begin{pmatrix} 16 \\ 6 \\ 19 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} Q \\ G \\ T \end{pmatrix}$$

$$\begin{pmatrix} T & Y & P \\ E & W & R \\ I & T & E \end{pmatrix} * \begin{pmatrix} M \\ A \\ T \end{pmatrix} \equiv \begin{pmatrix} 19 & 24 & 15 \\ 4 & 22 & 17 \\ 8 & 19 & 4 \end{pmatrix} * \begin{pmatrix} 12 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 19*12+24*0+15*19 \\ 4*12+22*0+17*19 \\ 8*12+19*0+4*19 \end{pmatrix} \equiv \begin{pmatrix} 513 \\ 371 \\ 172 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 7 \\ 16 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} T \\ H \\ Q \end{pmatrix}$$

$$\begin{pmatrix} T & Y & P \\ E & W & R \\ I & T & E \end{pmatrix} * \begin{pmatrix} I \\ O \\ N \end{pmatrix} \equiv \begin{pmatrix} 19 & 24 & 15 \\ 4 & 22 & 17 \\ 8 & 19 & 4 \end{pmatrix} * \begin{pmatrix} 8 \\ 14 \\ 13 \end{pmatrix} \equiv \begin{pmatrix} 19*8+24*14+15*13 \\ 4*8+22*14+17*13 \\ 8*8+19*14+4*13 \end{pmatrix} \equiv \begin{pmatrix} 683 \\ 561 \\ 382 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 15 \\ 18 \end{pmatrix} \mod 26 \equiv \begin{pmatrix} H \\ P \\ S \end{pmatrix}$$

14) **[200 points]** A quote from *The Hunger Games* has been encoded using the Pollux Cipher for you to decode. You are told that the quote has **THEB** in it corresponding to the encoded text **2212787828221**.

```
7722033210920322122300270208212202900228938200927732 7
●●××–●●×–––×–●××–××●––×●–×–●×–××–×–––××●–●●×–––×●●●×●
I   D   O   N   T   W   A   N   T   T O   L   O   S   E

221278782822177829912031922309273212387822123733272208 38
××–×●●●●×●××–●●●×–––×–●––××●––×●●×–×●●●●××–×●●●●×●××–●●●
  T H   E  B   O   Y   W   I  T H   T H   E  B

2707282812937
×●–●×●×●–×–●●
 R  E A  D
```

How to solve

With the crib of theb mapped to the ciphertext 2212787828221 we now know the mapping of 4 characters. Since we are told the mapping of 2178 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:

```
7722033210920322122300270208212202900228938200927732 7
●●××   ×–  ×  ××–××   ×● × ●×–×× ×   ××●  ●×   ×●● ×●
I /          / T/          T/     /           E

221278782822177829912031922309273212387822123733272208 38
××–×●●●●×●××–●●●×  –×  – ××   ×● ×–× ●●●××–× ●  ×●×× ● ●
/ T H   E/ B          /       T    / T     E/

2707282812937
×● ●×●×●–×  ●
    E A
```

At this point in time, 3 ciphertext characters still need to be mapped. Looking at the ciphertext, we see the sequence 220 which would result in three ×s in a row if 0 were an ×. Also, we see the sequence 332 which would result in three ×s in a row if 3 were an ×. Also, we see the sequence 922 which would result in three ×s in a row if 9 were an ×.

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

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

```
7722033210920322122300270208212202900228938200927732 7
●●××???×–??×??××–××???×●?×?●×–××?×???××●??●×???×●●?×●
I /          / T/          T/     /           E

221278782822177829912031922309273212387822123733272208 38
××–×●●●●×●××–●●●×??–×??–?××???×●?×–×?●●●××–×?●??×●××?●?●
/ T H   E/ B          /       T    / T     E/

2707282812937
×●?●×●×●–×??●
    E A
```

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

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

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

```
77220332109203221223002702082122029002289382009277327
●●××?●●×–??×?●××–××●??×●?×?●×–××?×???××●?●●×???×●●●×●
I /           / T/           T/     /          S   E

221278782822177829912031922309273212387822123733272208 38
××–×●●●●×●××–●●●×??–×?●–?××●??×●●×–×●●●●××–×●●●●×●××?●●●
/ T H    E/ B           /     I  T H   / T H    E/

2707282812937
×●?●×●×●–×?●●
     E A
```

At this point in time, 2 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: ITH THE HSEA. Trying – for 0 gives us a chunk: ITH THE BREA. 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:

```
77220332109203221223002702082122029002289382009277327
●●××–●●×––?×–●××–××●––×●–×–●×–××–×?––××●?●●×––?×●●●×●
I / D       N / T/ W   A  N  T/ T    /          S   E

221278782822177829912031922309273212387822123733272208 38
××–×●●●●×●××–●●●×??–×–●–?××●–?×●●×–×●●●●××–×●●●●×●××–●●●
/ T H    E/ B           /     I  T H   / T H    E/ B

2707282812937
×●–●×●×●–×?●●
 R   E A
```

At this point in time, 1 ciphertext characters still need to be mapped. Since 9 can still map to ●– 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: I DGN T WANT TW HGSE THE BUC RITH THE BREA. Trying – for 9 gives us a chunk: I DON T WANT TO LOSE THE BOY WITH THE BREA. Which means we know that 9 must map to –

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

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

```
77220332109203221223002702082122029002289382009277327
●●××–●●×–––×–●××–××●––×●–×–●×–××–×–––××●–●●×–––×●●●×●
I / D   O   N / T/ W   A  N  T/ T O  / L    O   S   E

221278782822177829912031922309273212387822123733272208 38
××–×●●●●×●××–●●●×–––×–●––××●––×●●×–×●●●●××–×●●●●×●××–●●●
/ T H    E/ B    O   Y   / W   I  T H   / T H    E/ B

2707282812937
×●–●×●×●–×–●●
 R   E A  D
```

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

I DON T WANT TO LOSE THE BOY WITH THE BREAD

15) **[275 points]** Solve this aristocrat quote by Audrey Hepburn. As a hint, X=S

CEW ABNPGOCPH BDBX, HEEF NG GLB VEEU OQ EGLBWX; CEW
FOR BEAUTIFUL EYES, LOOK AT THE GOOD IN OTHERS; FOR

ABNPGOCPH HOMX, XMBNF EQHD REWUX EC FOQUQBXX; NQU
BEAUTIFUL LIPS, SPEAK ONLY WORDS OF KINDNESS; AND

CEW MEOXB, RNHF ROGL GLB FQERHBUVB GLNG DEP NWB
FOR POISE, WALK WITH THE KNOWLEDGE THAT YOU ARE

QBKBW NHEQB.
NEVER ALONE.

	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	16	6	3	15	5	9	8			1	5	3	9	7	5	8	4			5	2	7	8		
Replacement	B	E	F	Y	O	K	T	L	C	M	V	H	P	A	I	U	N	W	Z	Q	D	G	R	S	X	J

16) **[600 points]** Solve this patristocrat, a quote by Barack Obama. A hint to get you started is G=I.

GSGDO KLSQT OKLAC FARIT FVUTD DFSQT FVSSQ TZKDS
ITISY OUTHE YOUNG ANDFE ARLES SATHE ARTTH EMOST

RGMTV DTFAR TRLYF STRCT ATVFS GKAGA KLVQG DSKVO
DIVER SEAND EDUCA TEDGE NERAT IONIN OURHI STORY

JQKSQ TAFSG KAGDJ FGSGA CSKIK UUKJ
WHOTH ENATI ONISW AITIN GTOFO LLOW

It is you, the young and fearless at heart, the most diverse and educated generation in our history, who the nation is waiting to follow.

	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		3	7		9	10		2	3	11	4	1		3		6	5	13	12	3	6			1	1
Replacement	N	P	G	S	J	A	I	Q	F	W	O	U	V	B	Y	K	H	D	T	E	L	R	X	Z	C	M

17) **[275 points]** Solve this baconian, a quote said by Bubbles from the old show, *The Powerpuff Girls.*

```
@$%&)@#%*(@#%*(@$^&(@#%*)@$%*)!$^*(!$^*(@$%&)!$^*)@$^*)@$
AABBAABBABABBABAAABBABBAAAABAABAAABBAAABAABBABAAAAAAAAAA
  G     O     O     D     N     E     S     S     G     R     A

^&)@#^*)@#%*(!$^&(!$^*(!$^*(@#^*)!$^*)!$%&)@#%*(!$^&(@$^*
ABAABAAAABBABBAABBBAAABBAAABABAAABAAAABABBAABBABBAABBAAAA
C     I     O     U     S     S     I     R     Y     O     U     A

)!$^*)@$%*)@$^*(@$%*)@#^*)@#%*)@$%&)!$^*(@#^&)@#%*(!$%*)@
ABAAAAAABAAAAAABAABAAABAAAABBAAAABBABAAABABABAABBABBABAAA
   R     E     B     E     I     N     G     S     L     O     W

#^&)!$%&)@$^&(@#^*)@$%&)@$%*)!$^*(!$^&)@$%*)@$^&(!$%*)@$%
BABABABBAAAABBABAAAAABBAAABAABAAABBAABAAABAAAAABBBABAAAAB
 L     Y     D     I     G     E     S     T     E     D     W     E

*)@#%*)@$%*)@$%*)@$^&(!$^&)@#%*(@$%&)@$%*)!$^&)!$%&)@#%*(
AAABBAAAABAAAABAAAAABBBAABAABBABAABBAAABAABAABABABBAABBAB
    N     E     E     D     T     O     G     E     T     Y     O

!$^&(!$^&)@#%*(@$^*)@$%&(@#%*(!$^*(@#%&)@#^*)!$^&)@$^*)@#
BAABBBAABAABBABAAAAAAABBBABBABBAAABABBBAABAAABAABAAAAAAB
  U     T     O     A     H     O     S     P     I     T     A

^&)
ABA
L

Goodness gracious! Sir, you are being slowly digested. We need to get you to
a hospital.
```

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

18) **[100 points]** Emma and Andrew want to communicate with each other using RSA for encryption. Emma generates RSA keys obtaining the following values:

n = 55665229 e = 29342143

q = 8209 d = 27256447

Φ = 55650240 p = 6781

Likewise, Andrew also generates RSA keys resulting in the values

p = 5197 q = 7717

n = 40105249 d = 15190219

Φ = 40092336 e = 10021699

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 Emma needs to calculate in order to decrypt the value 25805 from Andrew

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

40105249	**10021699**	

These two numbers can be in either order.

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

55665229	**29342143**	

These two numbers can be in either order.

Write the formula Emma needs to calculate in order to decrypt the value 25805 from Andrew

25805 ^ 27256447 mod 55665229

How to solve

Andrew needs to send only their public key (*e*=10021699, *n*=40105249) to Emma
Emma needs to send only their public key (*e*=29342143, *n*=55665229) to Andrew
Emma needs to use their own private key (n = 55665229, d = 27256447) because Andrew had to encode it using Emma's public key of (55665229,29342143).

In order to decrypt the value 25805, Emma must use the formula: `value ^ d mod n`

19) **[375 points]** Solve this aristocrat, a quote by Pablo Picasso.

QM KCV IQN JQHVDG QM KCV, CVP QM KCV'J IQN JQHVDG QM
HE CAN WHO THINKS HE CAN, AND HE CAN'T WHO THINKS HE

KCV'J. JQHG HG CV HVMRNBCUYM, HVPHGXLJCUYM YCI.
CAN'T. THIS IS AN INEXORABLE, INDISPUTABLE LAW.

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

20) **[515 points]** Solve this xenocrypt quote by J.K. Rowling, which has been translated into Spanish.

SI HOÑIADZ EI FQL ZEVQHLS SZBL, UHSI EI FQL UL
NO IMPORTA LO QUE ALGUIEN NACE, SINO LO QUE SE

BISJHLADL LS ULA.
CONVIERTE EN SER.

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

Translation: *It matters not what someone is born, but what they grow to be.*