

# Science Olympiad — SSSS Codebusters - builderguy135

## Exam Preparation

You will need:

1. Folders for each of the teams to hold the tests
2. Sufficient copies of the test for all teams. They don't need to be stapled.
3. Multiple timers which have a lap function on them - ideally one per volunteer. The timer app on an iPhone or Android Phone that has a stopwatch function with lap function is sufficient.

Before the event begins:

1. Practice starting the timers and using the lap function to record the times. Make sure volunteers understand how to use the lap function and are not accidentally stopping the timer completely.
2. Memorize the answer to the timed question.
3. Check to make sure that this key matches the test you are proctoring.
4. Place one copy of the test for each team in the provided folders with the first page outside the folder.
5. Adjust desks and chairs – teams may have up to 3 students for this event.

## Running the Event

1. When the students enter the room, instruct them to sit down, DO NOT OPEN THE FOLDER, and put their names, school name and school number on the first page.
2. Encourage them to write their team number on all the other pages AFTER they begin the test. This way if their papers gets separated from each other we can make sure to give them credit.
3. **CRITICAL:** Check to see that students have ONLY brought
  - i. Something to write with (pencils, pens, erasers)
  - ii. Five function calculators (addition, subtraction, multiplication, division, and usually square root). The calculator can have a simple memory store/recall function but must not have a modulus or other scientific and programmable functions. If their calculator doesn't meet these requirements, they may not use it.
  - iii. If there are spare calculators in the kit, you may loan up to one per team to use for the test.
  - iv. If the student has a smart watch (Apple watch, Samsung Gear, etc.) they will need to put it away.
4. Instruct the students that if they answer the timed question within 10 minutes, they can be awarded a bonus if they solve the timed question with no more than 2 letters incorrect.
  - i. When they have a solution for the cryptogram they should raise their hand.
  - ii. Let them know that you will announce when the 10-minute time is up. After the first 10 minutes, no additional bonus points will be awarded.
  - iii. When you see a team raise their hand, hit the LAP function and head to the team.
  - iv. Determine if their answer is correct (see next page for grading), If so, write the time on their score sheet.
  - v. If their score is incorrect (more than 2 letters incorrect), tell the team that the answer is wrong, but DO NOT tell them what is wrong. They can continue to work on the question and raise their hand again to be checked. A team has an unlimited number of attempts during the 10-minute bonus.
5. Tell the teams that they do not have to fill in the frequency table. It is simply there as an aid to them solving the cryptogram. It will not be graded.
6. Some students may never have used a non-scientific calculator. You should have them enter a simple formula on their calculator:  $1 / 26 = * 26 = ..$  Most will be surprised to see that the answer is not rounded to 1 as they expected but .9999999999

7. When the timers hit the 10-minute point, announce that no bonus points will be awarded and put away the timers. The students may continue to work on the question, but they may not receive any extra points.
8. A team is not restricted to only the timed question during the 10 minutes. They can move on or split up the work if they would like, but it is in their best interest to try for the bonus.
9. When time is up, have the students put writing instruments down and put their answer pages back into the folder in the correct order.

## How to grade

1. Teams can have up to two incorrect letters total on their cryptogram and still be correct. The frequency of the incorrect letter is irrelevant. See the example below.

If the cryptogram was as shown:

**KZBAOF KFXMFXYP**  
**SAMPLE SENTENCE**

and the students answered (underlined letters indicate mistakes)

**SAMPLE SENTENCE**

then it counts as four mistakes (even though the mistake was only in the letter E) and the answer DOES NOT count. However, if they put

**SAMPUL SENTENCE**

It is considered correct with two letter mistakes.

2. For questions which have a numeric answer (such as determining the a= and b= values), no mistakes are allowed.
3. Teams do NOT have to fill in the frequency table. It is simply there as an aid to them solving the cryptogram. It WILL NOT be graded. It is included in the answer key as an aid to the grader.
4. When scoring the Baconian ciphers (with strange text or symbols), they can write the answer under the Baconian symbols or on the line provided. Note that you will see lots of As and Bs, but they are not graded as the answer, only what they put on the answer line.
5. As you score each question, if correct, put the number of incorrect letters (0, 1, or 2) next to the question number on the scoring page. Also, put the value for the question into the score column. If they get more than 2 letters wrong, subtract 100 points from the score until it would be zero. If a question is worth 240 points and they get 4 letters wrong, you would start with 240 points (for up to 2 letters wrong) and then subtract 100 points for the next two letters wrong ending up with a final score of 40 points for that question. If they had gotten 5 or more letters wrong on a 240 point question, they would receive 0 points for that question. With a 650 point question, they could get 8 letters wrong and receive 50 points (2 free letters then  $6 \times 100 = 600$  points off). Just put the incorrect cost deduction on the score sheet and subtract it from the value for the question. Under no circumstance should the score for any question be less than zero. Note that while the timed question must have 2 or fewer letters incorrect in order to get the timing bonus, a team solving the timed question after the 10 minutes passed would be accepted as correct with 3 incorrect letters receiving 100 points for the timed question.
6. If they correctly answered the timed question in 10-minutes or less with 2 or fewer letters incorrect, you need to compute the bonus time. Take the value for the minute from this first table below

0:xx	2,160	1:xx	1,920	2:xx	1,680	3:xx	1,440	4:xx	1,200
5:xx	960	6:xx	720	7:xx	480	8:xx	240	9:xx	0

and then add the seconds value from this table:

X:00	240	X:01	236	X:02	232	X:03	228	X:04	224	X:05	220
X:06	216	X:07	212	X:08	208	X:09	204	X:10	200	X:11	196
X:12	192	X:13	188	X:14	184	X:15	180	X:16	176	X:17	172
X:18	168	X:19	164	X:20	160	X:21	156	X:22	152	X:23	148

X:24	144
X:30	120
X:36	96
X:42	72
X:48	48
X:54	24

X:25	140
X:31	116
X:37	92
X:43	68
X:49	44
X:55	20

X:26	136
X:32	112
X:38	88
X:44	64
X:50	40
X:56	16

X:27	132
X:33	108
X:39	84
X:45	60
X:51	36
X:57	12

X:28	128
X:34	104
X:40	80
X:46	56
X:52	32
X:58	8

X:29	124
X:35	100
X:41	76
X:47	52
X:53	28
X:59	4

For example if they solved the time question at the 6:46 mark, you would add 720 (from the 6:xx entry in the first table) to 56 (from the X:46 entry in the second table) to get a bonus of 776. If they had solved it in exactly 4:00 minutes, you would add 1200 and 240 to get a bonus of 1440.

7. Add up all the scores and put the total on the bottom of score sheet.
8. You must break all ties. Indicate the tie breaker by adding .1 to the score of the team ahead. With multiple teams tied, you will add more. I.e. if five teams all scored 200 points, the final scores that you would enter on the score sheet would be 200.4, 200.3, 200.2, 200.1 and 200.
9. To determine how to break the tie, you need to look at the correctly answered questions in the order from the table below. If both teams answered the same (i.e. they answered the question with zero mistakes) then you go on to the next question. If one team had no mistakes and the other team had one mistake, then the team with no mistakes is ahead. For example, if one team answered question #8 (which is the highest value question) and another team didn't, the first team will be ahead.

Tie Breaker Order	Question #
1	11
2	30
3	19
4	10
5	9
6	29
7	8
8	7
9	Timed
10	24
11	6
12	27
13	23
14	21
15	5
16	4
17	18
18	17
19	3
20	26
21	22
22	20
23	25
24	16
25	15
26	13
27	28
28	14
29	12
30	2

<b>Tie Breaker Order</b>	<b>Question #</b>
--------------------------	-------------------

31

1

0. If there is still a tie (typically when you have teams which answered either zero, one or two questions) then you will need to look at the tie breaker questions again and count the number of correctly answered letters. The team with the most correctly matched letters is to be ahead.

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

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

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

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

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

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

T	G	L	J	Q	G	V	A	S	D
<b>B</b>	<b>O</b>	<b>T</b>	<b>R</b>	<b>Y</b>	<b>O</b>	<b>D</b>	<b>I</b>	<b>A</b>	<b>L</b>

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

E	N	C	O	D	E	T	H	I	S	W	I	T	H	A	C	A	E	S	A	R	S	H	I	F	T	O	F
<b>Q</b>	<b>Z</b>	<b>O</b>	<b>A</b>	<b>P</b>	<b>Q</b>	<b>F</b>	<b>T</b>	<b>U</b>	<b>E</b>	<b>I</b>	<b>U</b>	<b>F</b>	<b>T</b>	<b>M</b>	<b>O</b>	<b>M</b>	<b>Q</b>	<b>E</b>	<b>M</b>	<b>D</b>	<b>E</b>	<b>T</b>	<b>U</b>	<b>R</b>	<b>F</b>	<b>A</b>	<b>R</b>

  

N	I	N	E	T	Y	.
<b>Z</b>	<b>U</b>	<b>Z</b>	<b>Q</b>	<b>F</b>	<b>K</b>	.

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

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

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

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

ORB) .  
 PAM) .

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

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

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

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

K1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	1	3	10	1		4		1	2	2			9	3		1			7	3	3	5	2	5	2	5
Replacement	B	D	E	F	G	H	J	K	L	M	P	Q	T	W	X	Y	Z	C	O	R	N	A	V	I	U	S

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

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

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

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

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

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

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

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



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

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

BZJJVRZJ LJS DR XHQFKVDVCQJSJ KZXIDSG LZJ AEH  
MESSAGES USING CRYPTANALYSIS TECHNIQUES FOR

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

Replacement	V	W	X	Y	Z	A	R	I	S	T	O	C	B	D	E	F	G	H	J	K	L	M	N	P	Q	U
K2	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	1	3	5	9	4	4	1	7	3	10	6	2	1	1			5	2	7		1	11		8	8	13

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

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

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

V'G VKFWKM HGWX  
I'M INSANE LMAO

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

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

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

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

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

K1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency		1		1	7	4	8	3	3	2	1	9	1	4	1	1	3	9		1			5	6	2	2
Replacement	X	Y	Z	C	A	N	T	L	O	U	P	E	B	D	F	G	H	I	J	K	M	Q	R	S	V	W

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

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

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

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

K1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency			6	10	6	3	3	4	3	5	8	1	3	2	1	5			1	7	2		4		3	
Replacement	Y	Z	N	E	T	H	R	L	A	D	S	B	C	F	G	I	J	K	M	O	P	Q	U	V	W	X

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

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

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

JXLTI LDXXK SFB  
CETHA TFEEL ING

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

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

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

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

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

P	K	W	Y	N	K	R	S	E	S	P	R	K	X	E
<b>B</b>	<b>A</b>	<b>S</b>	<b>I</b>	<b>L</b>	<b>A</b>	<b>R</b>	<b>M</b>	<b>E</b>	<b>M</b>	<b>B</b>	<b>R</b>	<b>A</b>	<b>N</b>	<b>E</b>

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

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

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

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

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

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

E	E	G	E	E	G	E	E	G	E	E	G	E	E	G	E	E	G	E	E	G			
I	P	K	G	X	X	S	I	T	G	I	V	L	E	R	S	X	U	K	V	G	T	L	E
<b>E</b>	<b>L</b>	<b>E</b>	<b>C</b>	<b>T</b>	<b>R</b>	<b>O</b>	<b>E</b>	<b>N</b>	<b>C</b>	<b>E</b>	<b>P</b>	<b>H</b>	<b>A</b>	<b>L</b>	<b>O</b>	<b>T</b>	<b>O</b>	<b>G</b>	<b>R</b>	<b>A</b>	<b>P</b>	<b>H</b>	<b>Y</b>

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

4235672894357235678924357623578235947236578235729345723  
 BAAABAABBBAABAAAABABBABAAABAAAABAAABBAABAABAAAABABAAAA  
 S H A M I R S S E C R  
 5762385792435762389457235672357823579423576829357423567  
 AABAABAABABAAABAABBBAABAAAABAAAABAAAABBAABBAABAAABA  
 E T S H A R I N G S C  
 23894576235879423657  
 AABBBAAABAAABABBAABAA  
 H E M E

Shamir's secret sharing scheme

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

APPLY AFTER FEWER BEADS ABOUT CAKES ALARM CAUSE AWAKE  
 ABBBA ABBAB BAAAB BAABA ABAAB AAAAA ABABA AAAAA AAAAA  
 P O S T K A L A A  
 DEPTH AWAKE BOOKS EGYPT GERMS BEAMS ADAPT ISAAC ALIBI  
 BABBB AAAAA BAAAA AAABB AABAA BAAAA ABABB AAAAA ABABA  
 Z A R D E R M A L  
 ALONE MOVIE IDEAS TIGER WALTZ GRUNT MESSY INDIA CROOK  
 ABABA AABAA ABAAA BAAAB AABBB ABABB AAAAA ABBAA ABAAA  
 L E I/J S H M A N I/J  
 SMOKE JOKER CRAIG TWIST  
 AAAAA BAAAB ABAAA BAAAB  
 A S I/J S

post kala azar dermal leishmaniasis

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

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

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

XAFSAOWYUALY  
 SIGNIFICATIVA

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

4 6 4 2 3 8 7 5 3 8 5 1 2 9 6 7 2 6 7 2 3 2 7 6 8 1  
 ●--x●-●x●●x-x●xx●●x-xx-●●x---xx●●x-xx●●x●●●xx●-xx--●  
 W R I T E/ I T/ D O /I T /I S /A /G

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

8 2 9 2 2 8 6 1 9 5 9 7 2 1 8 3  
 x-●x--●x●xx--x-●---xx--x●●x-●x-●●  
 N G E /M Y / M I N D

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

521501592295192919251905221010219259252209522195215912  
●-●●x●●x--x●●x-x●x-●●xx●--●x●x-●x-●x-●--xx●--●x●-●●x●-  
L I M I T E D P E N N Y P L A

92105  
x-●x●  
N E

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

480902403008803204100920230039028088024803890801203231  
--x●x--x●xx--x●-x-●xx●-x-●xx●●x--x--x---x●-●x-x●-x●-●●  
M E M E M A N A N I M M O R T A L

00213103013021028900919103009101390030333801092108922  
xx-●●●x●x●●x-●x--●xx●●●●x●xx●●x●●●xx●●●●-x●x●-●x-●--  
B E I N G H E I S E V E R Y

038203191030123010023110318040018038190331022800890882  
x●--x●●●●x●x●-●x●xx-●●●x●●-x-xx●-x●-●●x●●●x---xx-●x---  
W H E R E B U T A L S O N O

09820319103018103  
x●--x●●●●x●x●-●x●  
W H E R E

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

50453425961493459014366195374166308904881213132419018016  
 -●---x---x●●-xx--x●●-x●●●x-xx-●●●x●xx●-xx●-●x●x--●x●●x●●●  
 Y O U M U S T B E A R E G I S

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

32528040300535237574229307261310948705569128556903111  
 x---x●-●x●●-x--xx-x---xx●x-●●x●●x-xx●--●x●-x--●x●x●●●  
 O R U M T O E D I T P A G E S

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

$$\begin{aligned} n &= 20016863 & q &= 2039 \\ p &= 9817 & d &= 18819931 \\ \phi &= 20005008 & e &= 7516195 \end{aligned}$$

Likewise, Brooklin also generates RSA keys resulting in the values

$$\begin{aligned} d &= 21336781 & p &= 5923 \\ n &= 30675217 & \phi &= 30664116 \\ q &= 5179 & e &= 18266425 \end{aligned}$$

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

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

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

<b>30675217</b>	<b>18266425</b>	
-----------------	-----------------	--

*These two numbers can be in either order.*

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

<b>20016863</b>	<b>7516195</b>	
-----------------	----------------	--

*These two numbers can be in either order.*

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

<b><math>2205 \wedge 18266425 \bmod 30675217</math></b>
---------------------------------------------------------

---

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

$$p = 347$$

$$q = 337$$

$$n = 116939$$

$$\phi = 116256$$

$$e = 110077$$

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

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

**75541**

---

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

$$n = 38609821 \quad e = 6315131$$

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

$$38609821 = 8923 * 4327$$

Compute the value of their private key:

Enter the computed private key:

**21408179**