

Timed Question **[150 points]** Solve this quote by former President JFK. A K2 alphabet type has been used with a keyword of "Kennedy." When you have solved it, raise your hand so that the time can be recorded and the solution checked.

OHH HEOKG RK KGAHT ODK XHFEHLO HE HIYGYHG RYODHPO  
 TOO OFTEN WE ENJOY THE COMFORT OF OPINION WITHOUT

ODK ZYMXHFEHLO HE ODHPNDO.  
 THE DISCOMFORT OF THOUGHT.

Replacement	V	W	X	Z	K	E	N	D	Y	A	B	C	F	G	H	I	J	L	M	O	P	Q	R	S	T	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			5	5	2	4	14	1		5	2	1	1	10	2		2		1				2	4	1

1) [200 points] Here is an obligatory Star Wars quote from Shmi Skywalker.

**DTX KFS'W BWTU WOH KOFSNH, FSD RTIH WOFS DTX KFS  
YOU CAN'T STOP THE CHANGE, ANY MORE THAN YOU CAN**

**BWTU WOH BXSB MITR BHWPSN.  
STOP THE SUNS FROM SETTING.**

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

2) [200 points] Decode this Hill cipher with the keyword HILLCIPHE

$$\begin{pmatrix} H & I & L \\ L & C & I \\ P & H & E \end{pmatrix} \equiv \begin{pmatrix} 7 & 8 & 11 \\ 11 & 2 & 8 \\ 15 & 7 & 4 \end{pmatrix} \quad \text{Decode} \begin{pmatrix} H & I & L \\ L & C & I \\ P & H & E \end{pmatrix}^{-1} \equiv \begin{pmatrix} 12 & 5 & 22 \\ 20 & 5 & 13 \\ 11 & 5 & 12 \end{pmatrix}$$

S	C	N	K	N	D	S	G	T	A	B	D	T	C	Z
<b>S</b>	<b>T</b>	<b>A</b>	<b>R</b>	<b>S</b>	<b>D</b>	<b>O</b>	<b>N</b>	<b>O</b>	<b>T</b>	<b>S</b>	<b>P</b>	<b>I</b>	<b>N</b>	<b>Z</b>

3) [125 points] Affina! Solve this Affine cipher with an A value of 3 and a B value of 2.

C	R	R	A	P	O	A	E	A	P	H	O	B	O	E	H	A	P	U
A	F	F	I	N	E	I	S	I	N	T	E	R	E	S	T	I	N	G

4) [10 points] I hope you know your basics! Encode this Vigenère with a key of AAA

A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	A	.		
T	H	E	S	T	E	G	O	S	A	U	R	U	S	O	F	Z	Z	Y	Z	X	H	A	D	S	I	X	L	E	G	S	.
T	H	E	S	T	E	G	O	S	A	U	R	U	S	O	F	Z	Z	Y	Z	X	H	A	D	S	I	X	L	E	G	S	.

5) [175 points] E-tastic! Solve this Aristocrat written my me with a whole bunch of E!

XOF LFMFTWFRFW EFFGFFHFI EFXAFFT XOF HFJKFGFFHFIW  
 THE DEFENSELESS BEEKEEPER BETWEEN THE PEACEKEEPERS

JTL XOF UZFIFJNFI FTNPFFI ERFWWFL OPW EFFI JTL OPW  
 AND THE OVEREAGER ENGINEER BLESSED HIS BEER AND HIS

EFFW.  
 BEES.

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				5	32	2	3	6	4	1	4	1	2	5	3		2		6	1		9	4		1
Replacement	W	X	Y	Z	B	E	K	P	R	A	C	D	F	G	H	I	J	L	M	N	O	Q	S	T	U	V

6) [150 points] A quote has been encoded using the Morbit Cipher for you to decode. You are told that 1=xx, 2=--, 3=x●, 4=●-, 5=-x, 6=●●. Bonus Hint: What does two consecutive numbers at the beginning of the Morbit cipher imply?

8 8 3 9 4 8 3 6 9 9 4 9 3 2 3 9 4 6 3 8 9 3 4 3 6  
 -●-●x●●x●--●x●●●●x●x●-●xx●--x●●x●-●●x●-●●xx●●-x●●●  
 C I P H E R / W I L L / U S

3 4 3 5 4 6 3 8 9 8 2 1 6 9 5 4 3 8 7 1 4 5 6 7 3 6 9  
 x●●-x●-x●-●●x●-●●x●-●--xx●●●x-x●-x●-●x-xx●--x●●x-x●●●●x  
 U A L L Y / S T A R T / W I T H

3 3 9 5 6 6 3 3 8 1 4 1 8 8 1 2 5 4 9 3 6 9  
 x●x●●x-x●●●●x●x●-●xx●-xx-●-●xx---x●-●xx●●●●x  
 / E I T H E R / A / C / O R / H

7) [650 points] Solve this Patristocrat which includes the word "cash" in it.

YFLWO ZZWIV FTMPF LSHFT ZZYIS EIVFT WOGIO POAVF  
 HOWLI TTLEY OUKNO WABOU TTHEA GEYOU LIVEI NIFYO

TZYOP MZYSZ YFPIV OCCLI IZINZ YSPRS CYOPY SPB  
 UTHIN KTHAT HONEY ISSWE ETERT HANCA SHINH AND

*How little you know about the age you live in if you think that honey is sweeter than cash in hand.*

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

8) [200 points] More Star Wars! Solve this Aristocrat.

QS MTS AVS BXMTE PW VPXS, AVMA QJOO OJUVA AVS WJTS,  
 WE ARE THE SPARK OF HOPE, THAT WILL LIGHT THE FIRE,

AVMA QJOO YNTE AVS WJTBA PTCST CPQF  
 THAT WILL BURN THE FIRST ORDER DOWN

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

9) [600 points] Solve this Patristocrat.

SZBPK BGSBW SRHGV VPQHS WQWSZ BTRUB KSRBW SQIGS  
 THEGR EATES TOFAL LGIFT SISTH EPOWE RTOES TIMAT

BSZQM PWGSS ZBQKS KLBUR KSZ  
 ETHIN GSATT HEIRT RUEWO RTH

*The greatest of all gifts is the power to estimate things at their true worth*

	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					4	2	1		5	1	1			3	5	4	13	1	2	2	5			5
<b>Replacement</b>	Z	E	J	Q	K	X	A	F	M	Y	R	U	N	C	B	G	I	O	T	P	W	L	S	V	D	H

10) [125 points] Encode this Caesar cipher with an offset of 15.

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

11) [500 points] Homophonez! I hop u lik dis aristo w errors. I took out a few homophones to make this slightly easier.

PXP JLPX RVI FPZR MPPL FZMP VIG CGAESR, IL QPZ SZAL  
EYE PREY TWO MEAT DEER MADE WON KNIGHT, OR SEA HAIR

NZLP QARP, DZAM AG QTF HPPOS HTX VSAGP HTR CGIV JAP,  
FARE SITE, LAID IN SUM BEECH BUY WHINE BUT KNOW PIE,

FILGAGE NITL FP VPZL GIGP FARP SPLP.  
MORNING FOUR ME WEAR NONE MITE HERE.

Replacement	Z	H	O	M	P	N	E	S	A	B	C	D	F	G	I	J	K	L	Q	R	T	U	V	W	X	Y
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	9		2	1	2	6	9	3	7	2		9	3	2	1	20	3	6	5	4		5		3		7

12) [200 points] A quote has been encoded using the Pollux Cipher for you to decode. You are told that the quote starts with POLL.

12215222512115121151125211255115111551115115225122151211  
●---●x---x●-●●x●-●●x●●-x-●●-xx●●x●●●xx●●●x●●x--x●--●x●-●●  
P O L L U X I S S I M P L

52122551252175615817110651913151178025636952253825121  
x-●---xx●-x-●xx●●x-●x●●-●x●x●-●x●●x---x●-●xx--x---x●-●  
Y A N I N F E R I O R M O R

7061154498  
x-●●●x●●x-  
B I T

13) [300 points] Haha, enjoy these word patterns. Solve this nonsensical Aristocrat written by me.

EUBNDEG IWANSCA ANU WJGADJA ANDA JSANWJK UVWGAG,  
PERHAPS WITHOUT THE INSTANT THAT NOTHING EXISTS,

EUSEFU LCBANUB RUXSQU TUDT.  
PEOPLE FURTHER BECOME DEAD.

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

14) [300 points] Solve this Bacon that is a bit more complicated. Be careful! Spaces are included and stand for A.

\ / | - \_ \_ / - - - / \_ - \_ - \_ \_ / | \_ ! \_ // \ \_ \_ - \_ - / - - | \_ \_ - - / ! \ / \_ \_ \_ -  
BAABAAABBBAABAABAAAAABAAABAAABAAABABBAAABBABBAAAAABA  
T H E R E I S N O R I

/ | \_ - - // - - - ! \_ \_ \ \_ - - \_ / | \_ \_ / - / - - \_ - \_ ! \_ \_ \ - - / | \_ - - - - / ! \  
AAAABBAAABBBBAABABABAAAAAABABBABAABAABBABAAABBABBABB  
G H T W A Y T O D O

/ \_ \_ - - - - - ! / | \ \_ \_ - // - \_ \_ - - - - \_ / | ! \ \_ \_ // - - - - - \_ \_ /  
AAABABBABABABBAABAABAABAABBBABAAAABBAAAABBABABAABAAA  
S O M E T H I N G W R

| \_ - ! \_ \ / - - / \_ \_ - -  
AABBABABBAAAABBA  
O N G

There is no right way to do something wrong.



15) [300 points] Solve this Patristocrat written by me that is meant to be easy.

**TXTHK SUZMI ZVBYB OSBMG MESUZ MIZVB MEJZM ZEMSE  
EVERY THING IS AFA CTAND NOTHI NGISA NOPIN IONTO**

**FBHGV VROOT VV  
WARDS SUCCE SS**

*Everything is a fact and nothing is an opinion towards success.*

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

16) [200 points] Solve this Aristocrat. It is a Chinese proverb pertaining to a type of plant.

**OAR YRNO OBGR OJ KFXIO X OMRR SXN OSRIOV VRXMN XHJ,  
THE BEST TIME TO PLANT A TREE WAS TWENTY YEARS AGO,**

**OAR NRZJIT YRNO OBGR BN IJS.  
THE SECOND BEST TIME IS NOW.**

Replacement	X	Y	Z	T	R	E	H	A	B	C	D	F	G	I	J	K	L	M	N	O	P	Q	S	U	V	W
<b>K2</b>	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>	2	3				1	2	1	4	4	1		2	6	11			11	3	1		2		5	2	1

17) [150 points] Here is a easier Aristocrat from Randy Pausch.

**OVJOXLOYBO LG UPFI ATE MOI UPOY ATE ZLZY'I MOI UPFI  
EXPERIENCE IS WHAT YOU GET WHEN YOU DIDN'T GET WHAT**

**ATE UFYI  
YOU WANT**

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

18) [300 points] The following quote has been encoded with the Vigenère Cipher using a very common word for the key. The 31st through 35th cipher characters (**NEWUC**) decode to be **YMYCR**.

P	S	Y	S	L	P	S	Y	S	L	P	S	Y	S	L	P	S	Y	S	L	P	S	Y	S	L	P	S	Y					
H	Z	W	Y	J	E	K	W	K	W	N	D	W	K	A	G	Q	J	Q	E	G	Q	Q	L	M	N	E	W	U	C	N	H	R
S	H	Y	G	Y	P	S	Y	S	L	Y	L	Y	S	P	R	Y	L	Y	T	R	Y	S	T	B	Y	M	Y	C	R	Y	P	T

19) [450 points] Solve this Xenocrypt which is a Google Translated quote by Kurt Lewin. This is a K2 alphabet with a keyword of "Translate."

**KS JTWBCTDMT IÑSTJTK TDMTDZTJ WBAG, SDMTDMW  
SI REALMENTE QUIERES ENTENDER ALGO, INTENTA**

**YWCXSWJBG.  
CAMBIARLO.**

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

Translation: *If you want truly to understand something, try to change it.*

20) [150 points] Decode this Bacon cipher.

**BBBBABBBBBBBBABBAABABAABBBBBBBBABBBBBBBBABBAABABAABBBBBB  
AAAABAAAAAABAABBABABBAAAAAABAAAAAAABAABBABABBAAAAA  
B A C O N B A C O N B**

**BABBBBBBBBABBAABABAABBBBBBBBAABBBBBBAABBABBBBAABBBAABA  
ABAAAAAABAABBABABBAAAAAABBAAAAABBAAABAABBAABBAB  
A C O N A N D E G G**

**BBBA  
AAAB  
S**

**Bacon, Bacon, Bacon and eggs.**

21) [600 points] Solve this Xenocrypt, which was created using Google Translate.

FZSZY FJTJUZY AZYDHDXDSBSJY MNJ TZ GZTZGJUZY.  
 TODOS TENEMOS POSIBILIDADES QUE NO CONOCEMOS.

AZSJUZY KBGJÑ GZYBY MNJ TD YDMNDJÑB YZQBUZY MNJ  
 PODEMOS HACER COSAS QUE NI SIQUIERA SOÑAMOS QUE

AZSJUZY KBGJÑ  
 PODEMOS HACER

	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	6		6		2	5	1		12	2		4	4	3			1		5	4	5			1	12	15
Replacement	P	A	X	I	Y	T	C	B	J	E	H	F	Q	U	R	Z	W	Ñ	V	D	N	M	K	G	L	S	O

Translation: *We all have possibilities we don't know about. We can do things we don't even dream we can do.*

22) [100 points] Decode this Caesar cipher which is the name of a city.

M	V	O	F	O	V	K	X	N
C	L	E	V	E	L	A	N	D

23) [400 points] Aristocrats are fun, challenging ones more so. Here is a challenging Aristocrat by Lord Byron.

PX FXZG QG FGGI HP WXPAGZ SXQGZN RSNGPYG BRN FRAG FG  
NO MORE WE MEET IN YONDER BOWERS ABSENCE HAS MADE ME

LZXPG IX ZXTHPJ; SKI XOAGZ, MHZFGZ BGRZIN IBRP XKZN,  
PRONE TO ROVING; BUT OLDER, FIRMER HEARTS THAN OURS,

BRTG MXKPA FXPXIXPW HP OXTHPJ  
HAVE FOUND MONOTONY IN LOVING

	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>	4	4				6	15	5	6	2	3	1	2	5	2	12	2	6	3	3			2	14	1	10
<b>Replacement</b>	D	H	J	X	Z	M	E	I	T	G	U	P	F	S	L	N	W	A	B	V	K	Q	Y	O	C	R

24) [250 points] Solve this interesting Affine cipher. You are given that the plaintext S corresponds to the ciphertext Y and vice-versa.

S	M	X	M	Q	Z	X	J	I	Y	I	D	N	M	M	N	B	W	Z	B	F	M	.
Y	E	T	E	A	R	T	H	I	S	I	N	D	E	E	D	P	U	R	P	L	E	.

25) **[100 points]** Isabella 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:

$$e = 790753 \quad \phi = 10391068$$

$$q = 3467 \quad d = 6587761$$

$$p = 2999 \quad n = 10397533$$

As it comes to pass, Sarah is on vacation in Hawaii, and Isabella 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. Isabella needs to tell Sarah his/her public key, knowing well that it can be read by untrustworthy parties. List the minimum set of numbers that Isabella needs to email to Sarah in order for Sarah to be able to decode the message.

Additionally, Sarah wants to transmit the combination to the safe (which is 812) in the response email, but encrypted with RSA. What should formula should Sarah compute in order to know the ciphertext to transmit?

Enter the minimum values to transmit:

<b>10397533</b>	<b>790753</b>	
-----------------	---------------	--

*These two numbers can be in either order.*

Enter the formula (using correct numbers) to transmit:

<b><math>812 \wedge 790753 \bmod 10397533</math></b>
--