Timed Question [250 points] Solve this Aristocrat. No hints are provided. When you have solved it, raise your hand so that the time can be recorded and the solution checked.

HDM HU EWM Ohte UPSTEPIEFDJ UMMZFJDJT FD EWM BHPZX FT
ONE OF THE MOST FRUSTRATING FEELINGS IN THE WORLD IS

QMFDJ TOIPE MDHSJW EH VDHB EWM PM'I I QMEE MP BIK EH
BEING SMART ENOUGH TO KNOW THERE'S A BETTER WAY TO

XH THOMEWFJDJ, QSE DHE TOIPE MDHSJW EH FDGMDE I BIK
DO SOMETHING, BUT NOT SMART ENOUGH TO INVENT A WAY

EH XH FE.
TO DO IT.
1) [350 points] Solve this Aristocrat. The word drive appears at least once.

MJ ZQV ISMWG QWGS C BCDECFG MU OQQFT PQSG OMFG C
IF YOU DRIVE OVER A PANCAKE IT LOOKS MORE LIKE A

XCJJOG, MJ ZQV ISMWG QWGS C XCJJOG MU OQQFT PQSG
WAFFLE, IF YOU DRIVE OVER A WAFFLE IT LOOKS MORE

OMFG C BCDECFG.
LIKE A PANCAKE.

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

2) [350 points] Solve this Aristocrat. E is not the most common vowel.

HK ZLR HF WDA LYYLFHWA LK YUL HF ZLREUAFF WDA
IF CON IS THE OPPOSITE OF PRO IS CONGRESS THE

LYYLFHWA LK YULEUAFF?
OPPOSITE OF PROGRESS?

| 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 | 2 | 2 | 8 | 5 | 3 | 10 | 2 | 4 | 4 | 6 | 2 |
| Replacement | E | Q | M | H | G | S | L | I | B | Z | F | O | Y | W | U | V | K | N | X | A | R | J | T | D | P | C |
3) [275 points] Solve this Aristocrat regarding justice. It is supposed to be a joke.

OQMVNBG NM XGMV MGALGK BDHK. XGBPQMGM NW NV ZPM
JUSTICE IS BEST SERVED COLD. BECAUSE IF IT WAS
MGALGK ZPAR, NV ZDQHK XG OQMV-ZPVGA.
SERVED WARM, IT WOULD BE JUST-WATER.

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

4) [275 points] Solve this joke regarding your eyes. It is an Aristocrat.

IBMZ AEL YHM, VBM FGDV QGWV EX AELW TEYA VE DVEQ
WHEN YOU DIE, THE LAST PART OF YOUR BODY TO STOP
IEWRHZU GWM AELW QLQHFD. VBMA YHFGVM.
WORKING ARE YOUR PUPILS. THEY DILATE.

| 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 | 3 | 8 | 3 | 4 | 4 | 2 | 4 | 6 | 4 | 1 | 1 | 1 | 7 | 5 | 1 | 3 | 2 |
| Replacement | Y | H | V | S | O | L | A | I | W | X | C | U | E | J | Z | Q | P | K | M | B | G | T | R | F | D | N |
5) **[200 points]** Solve this Aristocrat from Macbeth. It has been slightly altered. It was encoded with a K1 alphabet with the keyword Macbeth.

```
DAYU AJ R VRDU VFDX TO RE AXAFV, YKDD FY JFKEX REX
LIFE IS A TALE TOLD BY AN IDIOT, FULL OF SOUND AND
YKIO, JAZEAYOAEZ EFVWAEZ.
FURY, SIGNIFYING NOTHING.
```

| 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 | 8 | 5 | 7 | 5 | 1 | 3 | 3 | 3 | 3 | 4 | 1 | 2 | 4 | 1 | 4 | 5 | 3 |

6) **[125 points]** Solve this Aristocrat.

```
AWSSJAA BA QDV GQ DRVBDQ. BV BA GQ DHEBLGVBDQ.
SUCCESS IS NOT AN OPTION. IT IS AN OBLIGATION.
```

| K4 | 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 | 6 | 5 | 1 | 3 | 1 | 1 | 1 | 5 | 1 | 2 | 4 | 1 |
| Replacement | S | I | Z | O | L | Y | A | B | D | E | F | G | H | J | K | M | N | P | Q | R | T | U | V | W | X |
7) [200 points] Solve this Aristocrat by Einstein. There is no frequency table.

```
NZBRUZR XBSDFW ERCBJBDU BNCHLR
SCIENCES WITHOUT RELIGION IS LAME,
ERCBJBDU XBSDFW NZBRUZR BNQCBUI
RELIGION WITHOUT SCIENCE IS BLIND.
```

8) [275 points] Solve this Aristocrat with errors by Plato. All words are still real English words.

```
RUVNO NL EQPH UFOA NQ OVGVFRNQC FQ CPT RUNQC
THEIR IS KNOW HARM IN REPEATING AN GOD THING
```

```
|     | 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 | 3 | 1 | 1 | 1 | 5 | 3 | 2 | 5 | 3 | 1 | 3 | 3 | 1 | 3 | 3 | 1 | 3 | 3 | 1 | 3 | 3 |
| Replacement | M | V | G | Z | K | A | P | W | F | B | X | S | Q | I | R | O | N | T | Y | D | H | E | C | U | L | J |
```
9) [375 points] Solve this Xenocrypt.

**ZFP UOD RXPYX AOK TKX RX MFPUKIMX, KR TGKUZPK JOKRJK**
**POR MUY LARGA QUE SEA LA TORMENTA, EL SIEMPRE VUELVE**

**X WPGRRXP KIMPK RXT IOWKT.**
**A BRILLAR ENTRE LAS NUBES.**

| 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 | 1 | 2 | 2 | 3 | 2 | 1 | 1 | 3 | 4 | 7 | 7 | 4 | 3 | 2 | 8 | 1 | 2 |   |   |   |   |   |   |   |   |

Translation: *However long the storm, the sun will always shine again amongst the clouds.*

10) [325 points] Solve this Xenocrypt about being a good person.

**AM ÑLDNS AHJR MMADS NA QLADRH BAPHSDRH. HO DS MRH**
**EL MUNDO ESTA LLENO DE BUENAS PERSONAS. SI NO LAS**

**ADTLADJPRH, HA LDR NA AMMRH.**
**ENCUENTRAS, SE UNA DE ELLAS.**

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

Translation: *The world is full of good people. If you can’t find one, become one.*
11) [400 points] Solve this Patristocrat about a specific instrument. Encrypted K1 with the keyword being the name of that instrument.

**LIXXV JOWFH IJKLM NOAXW NOLWN AJMQL OTLMV LDXMQ**
**ILOOK ATMYC LARIN ETSOM ETIME SANDI THINK IWOND**

**NKDTJ OASXL MSOXH XWNBX OXROT NKNX MLSTO FXBMN**
**ERWHA TSGOI NGTOC OMEOU TOFTH ERETO NIGHT YOUNE**

**CNKVM XD**
**VERKN OW**

I look at my clarinet sometimes and I think, I wonder what's going to come out of there tonight? You never know.

| 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 | 3 | 2 | 1 | 3 | 2 | 2 | 4 | 4 | 8 | 8 | 9 | 10 | 2 | 1 | 3 | 4 | 3 | 4 | 12 | |
| Replacement | S | U | V | W | X | Y | Z | C | L | A | R | I | N | E | T | B | D | F | G | H | J | K | M | O | P | Q |

12) [450 points] Solve this Patristocrat. No hints.

**KQSJV NQSVW JNUCU ZWKKW IRJVO QIRSU TDQTVU CUWZF**
**SOLID GOLDT IGERE ATSST UPIDC OUPLE WHOWE RETAK**

**JPNRD QWQKQ GJWJTJ WDWDU JCOZX UCZRD QPU**
**INGPH OTOSO FITWI THTHE IRCAM ERAPH ONE**

Solid gold tiger eats stupid couple who were taking photos of it with their camera phone.

| 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 | 4 | 5 | 1 | 1 | 2 | 7 | 4 | 3 | 2 | 2 | 8 | 4 | 3 | 3 | 8 | 3 | 8 | 1 | 4 |
| Replacement | Y | V | R | H | B | K | F | J | U | I | S | Z | X | G | C | N | O | P | L | W | E | D | T | M | Q | A |
13) [300 points] Solve this Patristocrat based on the sound of the English language. Encoded K1 with a keyword of English.

TNTHY DWKYF CYKYK JKL MN OPOZJ QWJBO JKL MN OPOYD
DIDYO UKNOW TONON ENGLI SHSPE AKERS ENGLI SHSOU

KTOMN WJJKL MNOP
NDSLI KEENG LISH

Did you know to non English speakers English sounds like English?

| 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 | 2 | 1 | 1 | 6 | 7 | 3 | 4 | 5 | 7 | 3 | 1 | 3 | 3 | 5 | 1 |
| Replacement | Q | R | T | U | V | W | X | Y | Z | ENGL | ISH | H | A | B | C | D | F | J | K | M | O | P |

14) [75 points] Solve this. This is an atbash cipher.

WRW BLF PMLD GSZG GSIVZ IVZLYFG GVMB
DID YOU KNOW THAT THERE ARE ABOUT TEN

JFRMG ROORL MRMWERWZF O RMHVXGH ZOREV ZG
QUINTILLION INDIVIDUAL INSECTS ALIVE AT

ZMB TREV NLNVMG
ANY GIVEN MOMENT?
15) **[125 points]** Decode this Caesar Cipher. It is somebody's name.

```
E P I G X R Z
PAT R I C K
```

16) **[150 points]** Solve this quote by Dumbledore. This is an affine cipher, given BP=PB.

```
O N E C A N N E V E R H A V E E N O U G H S O C K S
```
17) [200 points] Encode this Affine with A=7 and B=1.


18) [200 points] Encode this Vigenère given that the keyword is Homer.


S: H U T U P, B R A I N, O R I'LL S T A B Y O U W I T H A


E - R H O !
Q - T I P !
U - K P D !
19) [175 points] Solve this Vigenère given that the first two words are I've been.

```
U'GLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYU,
GLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYUGLYU,
C'BPZKYKUAURWCXARJS,VFEOMWWZARJS,
I'VEBEENCALLEDUGLY,PUGUGLY,FUGLY,
```

```
GLYUGLYUGLYUGLYUGLYUGLYUGLY,
VFEZARJS,HFRHKGCLARJSARJS,
PUGFUGLY,BUTNEVERUGLYUGLY
```

20) [225 points] Solve this Bacon. First two words are how many.

```
MONTHUNDERHETOOTOINALLOGOOSEALLEYFOLLYMAINE
AABBABABBABABAAAABABAAABAAA
HOMANAYC
```

```
AMIGOCLUBSUPFORDERLEWISCRIESMARIEPSYCHSUCKS
AAAAAABABAABBABAAAAAABAAABAABABA
ALARORIJESAS
```

```
JAMIEKILOSINUSEOFHIMSAUCESAILSPOUNDSWEET
BAAAAAABAAABAABAAAABAAAABAAABAABAAA
REIJNAACU/VB
```

```
INWAYMAILSIRONYINWAYMANDYWORLDBEADSFELLA
ABAAAABABAABAAAABAAABAABBBBAABAABABA
IJCLIJ/GHTY
```

```
AMBOYGOSAYLUCKYSTRAPCOLORWAISTPOUNDBYITS
AABAAAAAAABAAAABBABABABAABAAAABABBBBAABABA
EAROFBU/ VT
```

```
HOWLSISTAYHICKS
BAABAAABAAA
TEER
```

How many calories are in a cubic light year of butter?
21) [100 points] Solve this Bacon.

BAAABAAAABAAAAABABABABABABABAABABAABABABABABABABABABABAB
BAAABAAAABABAABABADDABABABABABABAABABAABABABABABABABABAB
S   C   I   O   L   Y   S   U   M   M   E

AABAAAABAAAABABABAABABADDABABABABABABAABABAABABABABABABABABA
AABAAAABAAAABABABAABABADDABABABABABABAABABAABABABABABABABABA
R   S   T   U   D   Y   S   E   S   S

BAAAABBABABBBAA
BAAAABBABABBBAA
I   O   N

Scioly Summer Study Session

22) [600 points] William has faithfully followed the steps of the RSA key-generation algorithm. Here are the results:

\[
\begin{align*}
p &= 193 \\
q &= 283 \\
n &= 54619 \\
\phi &= 54144 \\
e &= 25079
\end{align*}
\]

Unfortunately, William 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.

5447
23) [575 points] Jasmine and Hannah are accountants for a very large bank, and have started a friendship. They communicate via email, because they live thousands of miles apart. Hannah gets curious and asks Jasmine the year that they were born. Jasmine doesn’t mind telling Hannah, but they know that the bank monitors all employee emails, and is afraid of being the victim of age discrimination. Therefore, Hannah suggests that they use RSA, and they provides their public key: (5963, 2665). Jasmine replies with the ciphertext 5490. Hannah’s private key is 4921. In what year was Jasmine born?

Enter the answer: 1955

24) [275 points] Encode this Hill cipher

\[
\begin{pmatrix}
H & I & J \\
K & C & B \\
V & D & P
\end{pmatrix}
\equiv
\begin{pmatrix}
7 & 8 & 9 \\
10 & 2 & 1 \\
21 & 3 & 15
\end{pmatrix}
\]

H Y D R O X Y C H L O R O Q U I N E
I R E W N Q N R E Z I Q K S O G H
25) **[50 points]** Compute the decryption matrix.

\[
\begin{pmatrix}
F & Q \\
C & B
\end{pmatrix} = \begin{pmatrix}
5 & 16 \\
2 & 1
\end{pmatrix}
\]

\[
\begin{array}{cc}
25 & 16 \\
2 & 21 \\
\end{array}
\]

26) **[475 points]** Given that HILL encodes to FBLA, find the decryption matrix.

\[
\begin{array}{cc}
1 & 2 \\
1 & 3 \\
\end{array}
\]