MATH 75: Cryptography **Spring 2022**

PSET 8 — Final Cipher Challenge

Prof. Asher Auel ***Student: Amittai Siavava***

Credit Statement

I worked on these problems alone, with reference to class notes and the following books:

(a) ***The Code Book*** by **Simon Singh**.
(b) ***Cryptography*** by **Simon Rubinsen-Salzedo**

Problems

1. Substitution cipher.

```
OVDKLJOODKBPLABZGUFVDKLACVQLKBZVWLJJVGVLYBZVZUJJQLKBZVJLYVSUYVDTL
FVZVKDYOBZVJLRDJLYVCIZLJLFVZVKGUFVDKLACVGUFVDKLACVIUBZDIUJJQLKBZV
CLYCLQLJOODKBPLABZQLKBZVODAGZBVKCLQODKBPLABZBZLAGZKLAYOBZVGUKOJVO
VDKBZBZVRKLDPZVKCSVJJLYBZVPKVPDUYCBZVRZDFVBZVCBUJJYLKBZUYBZVUKZVD
KBCBZVZUJJIUYOCUYBZVUKFVUYCDYOBZVGKDYUBVLQYVIZDPSCZUKVUYBZVUKPACW
JVCDYOBZVUKTKDUYCDZUYBQLKWUSZVKCUHUCBZVLKOVKLQQUFVPLOAJLSUCCPDJJ
```

O — d
V — e
D — a
K — r
L — o
J — l

I used this website to check word and letter frequencies:
https://www3.nd.edu/~busiforc/handouts/cryptography/Letter%20Frequencies.html
For a start, we can analyze the frequencies of different letters in the ciphertext.

Standard English frequencies:

letter	percentage frequency
e	12.702
t	9.056
a	8.087
o	7.507
i	6.966
n	6.749
s	6.234
h	6.094
r	5.987
d	4.253
l	4.094
c	2.781
u	2.758
m	2.587
w	2.36
f	2.228
g	2.015
y	1.974
p	1.929
b	1.493
v	0.978
k	0.772
j	0.153
x	0.15
q	$9.6e-2$
z	$7.4e-2$

Ciphertext frequencies:

letter	percentage frequency	plaintext
v	12.853470437017995	e
z	10.025706940874036	h
l	8.740359897172237	a
b	8.483290488431876	t
k	8.483290488431876	i
u	7.455012853470437	
d	6.169665809768637	
j	5.912596401028278	
c	5.3984575835475574	
y	5.3984575835475574	
o	4.113110539845758	
a	2.827763496143959	
p	2.570694087403599	
q	2.570694087403599	
f	2.056555269922879	
g	2.056555269922879	
i	1.2853470437017995	
s	1.2853470437017995	
r	0.7712082262210797	
w	0.7712082262210797	
t	0.5141388174807198	
h	0.2570694087403599	

We expect similarities in the frequencies.

For a sure start, we know the most-common 3-letter word in English is 'the'. We can use this to find the most-common 3-gram in the ciphertext, substitute it with 'the', and check how it matches up to our table above.

```
ghci> frequencies $ ngrams 3 ciphertext
  BZV: 4.651162790697675
  KBZ: 1.550387596899225
  VDK: 1.550387596899225
```

The highest frequency is 'BZV', matching to the English word 'the'. We would expect 'B' to match to 't', 'Z' to match to 'h', and 'V' to match to 'e'. This appears a bit off from the single-letter frequencies, but all letters matched are still in the top letters in the frequency tables.
After substitution:

```
OeDKLJOODKtPLAthGUFeDKLACeQLKtheWLJJeGeLYthehUJJQLKtheJLYeSUYeDTL
FeheKDYOtheJLRDJLYeCIhLJLFeheKGUFeDKLACeGUFeDKLACeIUthDIUJJQLKthe
CLYCLQLJOODKtPLAthQLKtheODAGhteKCLQODKtPLAththLAGhKLAYOtheGUKOJeO
eDKththeRKLDPheKCSeJJLYthePKePDUYCtheRhDFetheCtUJJYLKthUYtheUKheD
KtCthehUJJIUYOCUYtheUKFeUYCDYOtheGKDYUteLQYeIhDPSChUKeUYtheUKPACW
JeCDYOtheUKTKDUYCDhUYtQLKWUSheKCUHUCtheLKOeKLQQUFePLOAJLSUCCPDJJ
```

We can expect L to map to either 'a' or 'o', depending on frequencies.
Next, if we print the 4-grams we see

```
"Ythe": 1.2953367875647668
"oKth": 1.2953367875647668
"Kthe": 1.0362694300518134
"Othe": 1.0362694300518134
"QoKt": 1.0362694300518134
"YOth": 1.0362694300518134
"eDKo": 1.0362694300518134
"heUK": 1.0362694300518134
"theU": 1.0362694300518134
"Cthe": 0.7772020725388601
```

"aKth" or "oKth" occurs frequently. We would expect this to be 'r', as in the sequence "arth" or 'orth", which is common in English.
Thus, we can replace 'K' → 'r'

```
OeDroJOODrtPoAthGUFeDroACeQortheWoJJeGeoYthehUJJQortheJoYeSUYeDTo
FeherDYOtheJoRDJoYeCIhoJoFeherGUFeDroACeGUFeDroACeIUthDIUJJQorthe
CoYCoQoJOODrtPoAthQortheODAGhterCoQODrtPoAththoAGhroAYOtheGUrOJeO
eDrththeRroDPherCSeJJoYthePrePDUYCtheRhDFetheCtUJJYorthUYtheUrheD
rtCthehUJJIUYOCUYtheUrFeUYCDYOtheGrDYUteoQYeIhDPSChUreUYtheUrPACW
JeCDYOtheUrTrDUYCDhUYtQorWUSherCUHUCtheorOeroQQUFePoOAJoSUCCPDJJ
```

Looking at the tri-grams again:

```
"the": 4.651162790697675
"eDr": 1.550387596899225
"rth": 1.550387596899225
"Drt": 1.2919896640826873
"Qor": 1.2919896640826873
"Yth": 1.2919896640826873
"ort": 1.2919896640826873
"Dro": 1.0335917312661498
```

```
"Oth": 1.0335917312661498
"UFe": 1.0335917312661498
```

We see 'D' occurs in "eDr", "Drt", and "Dro". One letter unused that makes sense in all these contexts is 'a'. Thus, we can swap 'D' → 'a'.

```
OearoJOOartPoAthGUFearoACeQortheWoJJeGeoYthehUJJQortheJoYeSUYeaTo
FeheraYOtheJoRaJoYeCIhoJoFeherGUFearoACeGUFearoACeIUthaIUJJQorthe
CoYCoQoJOOartPoAthQortheOaAGhterCoQOartPoAththoAGhroAYOtheGUrOJeO
earththeRroaPherCSeJJoYthePrePaUYCtheRhaFetheCtUJJYorthUYtheUrhea
rtCthehUJJIUYOCUYtheUrFeUYCaYOtheGraYUteoQYeIhaPSChUreUYtheUrPACW
JeCaYOtheUrTraUYCahUYtQorWUSherCUHUCtheorOeroQQUFePoOAJoSUCCPaJJ
```

We now see the sequence "Oear". This should be either "bear", "dear", "hear", "fear", "near", "pear", or "wear". Of those, "dear" tends to occur more often at the beginning of letters or addressed messeges. Thus, we can swap 'O' → 'd'.

```
dearoJddartPoAthGUFearoACeQortheWoJJeGeoYthehUJJQortheJoYeSUYeaTo
FeheraYdtheJoRaJoYeCIhoJoFeherGUFearoACeGUFearoACeIUthaIUJJQorthe
CoYCoQoJddartPoAthQorthedaAGhterCoQdartPoAththoAGhroAYdtheGUrdJed
earththeRroaPherCSeJJoYthePrePaUYCtheRhaFetheCtUJJYorthUYtheUrhea
rtCthehUJJIUYdCUYtheUrFeUYCaYdtheGraYUteoQYeIhaPSChUreUYtheUrPACW
JeCaYdtheUrTraUYCahUYtQorWUSherCUHUCtheorderoQQUFePodAJoSUCCPaJJ
```

We have "dearoJd". This should probably be "dear old", So we can replace 'J' → 'l'.
Looking at the ciphertext, We have the sequence "the order oQ". This is most-likely "the order of", so we can replace 'Q' → 'f'.

```
dearolddartPoAthGUFearoACefortheWolleGeoYthehUllfortheloYeSUYeaTo
FeheraYdtheloRaloYeCIholoFeherGUFearoACeGUFearoACeIUthaIUllforthe
CoYCofolddartPoAthforthedaAGhterCofdartPoAththoAGhroAYdtheGUrdled
earththeRroaPherCSelloYthePrePaUYCtheRhaFetheCtUllYorthUYtheUrhea
rtCthehUllIUYdCUYtheUrFeUYCaYdtheGraYUteofYeIhaPSChUreUYtheUrPACW
leCaYdtheUrTraUYCahUYtforWUSherCUHUCtheorderoffUFePodAloSUCCPall
```

Looking at the five-grams:

```
"Ydthe": 1.0389610389610389
"forth": 1.0389610389610389
"orthe": 1.0389610389610389
"theUr": 1.0389610389610389
"Fearo": 0.7792207792207793
"GUFea": 0.7792207792207793
"PoAth": 0.7792207792207793
"UFear": 0.7792207792207793
"UYthe": 0.7792207792207793
"YtheU": 0.7792207792207793
```

We see "theUr" occur frequently. This is most likely "their". Thus, we can replace 'U' → 'i'.
Looking at the tri-grams

```
"the": 4.651162790697675
"ear": 1.550387596899225
"rth": 1.550387596899225
"Qor": 1.2919896640826873
"Yth": 1.2919896640826873
"art": 1.2919896640826873
"ort": 1.2919896640826873
```

```
"Ydt": 1.0335917312661498
"aro": 1.0335917312661498
"dth": 1.0335917312661498
```

We see “Qor” as one of the most-common 3-letter sequences. This is most-likely “for”.
Thus, we can swap ‘Q’ $\rightarrow$ ‘f’.

```
dearolddartPoAthGiFearoACefortheWolleGeoYthehillfortheloYeSiYeaTo
FeheraYdtheloRaloYeCIholoFeherGiFearoACeGiFearoACeIithaIillforthe
CoYCofolddartPoAthforthedaAGhterCofdartPoAththoAGhroAYdtheGirdled
earththeRroaPherCSelloYthePrePaiYCtheRhaFetheCtillYorthiYtheirhea
rtCthehillIiYdCiYtheirFeiYCaYdtheGraYiteofYeIhaPSChireiYtheirPACW
leCaYdtheirTraiYCahiYtforWiSherCiHiCtheorderoffiFePodAloSiCCPall
```

We have the sequence “WolleGe”, which could correspond to “college”
Thus, we can replace ‘W’ $\rightarrow$ ‘c’ and ‘G’ $\rightarrow$ ‘g’.

```
dearolddartPoAthgiFearoACeforthecollegeoYthehillfortheloYeSiYeaTo
FeheraYdtheloRaloYeCIholoFehergiFearoACegiFearoACeIithaIillforthe
CoYCofolddartPoAthforthedaAghterCofdartPoAththoAghroAYdthegirdled
earththeRroaPherCSelloYthePrePaiYCtheRhaFetheCtillYorthiYtheirhea
rtCthehillIiYdCiYtheirFeiYCaYdthegraYiteofYeIhaPSChireiYtheirPACc
leCaYdtheirTraiYCahiYtforciSherCiHiCtheorderoffiFePodAloSiCCPall
```

We have ‘the college oY the hill’. ‘Y’ is most likely ‘n’.
We can also guess that, since we are talking about a college, “dartPoAth” should be “dartmouth”.
Thus, we can replace ‘Y’ *rightarrow* ‘n’, ‘P’ $\rightarrow$ ‘m’, and ‘A’ *rightarrow* ‘u’.

```
dearolddartmouthgiFearouCeforthecollegeonthehillfortheloneSineaTo
FeherandtheloRaloneCIholoFehergiFearouCegiFearouCeIithaIillforthe
ConCofolddartmouthforthedaughterCofdartmouththoughroundthegirdled
earththeRroamherCSellonthemremainCtheRhaFetheCtillnorthintheirhea
rtCthehillIindCintheirFeinCandthegraniteofneIhamSChireintheirmuCc
leCandtheirTrainCahintforciSherCiHiCtheorderoffiFemoduloSiCCmall
```

We have the sequence “dear old dartmouth giFe arouCe for the college on the hill...”
We can guess that ‘F’ should be ‘v’ and ‘C’ should be ‘s’, so that we have “dear old dartmouth give a rouse for the college on the hill”.
We also have “neI hamSshire”, which should likely be “new hampshire”. We can replace ‘I’ $\rightarrow$ ‘w’ and ‘S’ $\rightarrow$ ‘p’.
We can also guess that “aTove” should be “above”, and “the loRal ones” should be “the loyal ones”.
Finally, a number “siH” is probably “six”.

```
dearolddartmouthgivearouseforthecollegeonthehillforthelonepineabo
veherandtheloyaloneswholovehergivearousegivearousewithawillforthe
sonsofolddartmouthforthedaughtersofdartmouththoughroundthegirdled
earththeyroamherspellonthemremainstheyhavethestillnorthintheirhea
rtsthehillwindsintheirveinsandthegraniteofnewhampshireintheirmusc
lesandtheirbrainsahintforciphersixistheorderoffivemodulopissmall
```

When spaced out, the above reads:

```
dear old dartmouth, give a rouse
for the college on the hill
for the lone pine above her
and the loyal ones who love her
give a rouse, give a rouse with a will
for the sons of old dartmouth
for the daughters of dartmouth
though round the girdled earth they roam
her spell on them remains
they have the still north in their hearts
the hill winds in their veins
and the granite of new hampshire in their muscles and their brains
a hint for cipher six is the order of five modulo p is small.
```

2. Vigènere cipher.

```
hcbxpcjlemyzlgjwagtfjhtnvvriarrqzvuqbipjrqhggrzwtfnahgkqfesrqszvo
dyabgcwafvvrotsotdreoaqnbnfzgcbqetqloafvvnpapnqvzrzvyarnrpzgoashy
cwzvvwaphmbssvvhyammusjhnsfwnbbhbshhuwtkjylhrangemwsjnvprdatnrpsh
```

First, we can analyze coincidences when the message is shifted to try and guess the key length.

Key Length	**Coincidences**
1	14
2	9
3	10
4	12
5	11
6	6
7	11
8	15
9	9
10	15

The highest coincidences are with key lengths 8 and 10.

Next, let's consider the recurrence of 3-grams and 4-grams, whose difference of occurrence should generally be a multiple of the key-length.

n-gram	Occurrence	Difference
afv	72, 102	30
cbq	94, 231	137
fvv	73, 103	30
hcb	0, 230	230
jnv	182, 222	40
loa	100, 240	140
nrp	120, 190	70
nvv	23, 223	200
vvr	24, 74	50
afvv	72, 102	30

Thus, we can guess the key length to be 10, since most of the n-grams recur at multiples of 10.

Next, let's divide the ciphertext into blocks corresponding to the first, second, on to the tenth letter of the ciphertext.

```
hyjrrnqconlnncbubjwnuanhlr
czhqqaswtfoqrwsshysrmcocor
bltzhhzadzavpzsjbljpayjbal
xgnvggvfrgfzzvvhshnsbgnqvn
pjvugkovecvrgvvnhrvhcjvgj
cwvqrqdvobvzowhshapsbovto
jarbzfyraqnvaayfunrebgbvi
lgiiweaoqepyspawwgdapisja
etaptsbtntaahhmnteanhaden
mfrjfrgsbqprymmbkmtrcimym
```

```
1.
    'n': 23.076923076923077
    'r': 11.538461538461538
    'b': 7.6923076923076925
    'c': 7.6923076923076925
    'h': 7.6923076923076925
    'j': 7.6923076923076925
    'l': 7.6923076923076925
    'u': 7.6923076923076925
    'a': 3.8461538461538463
    'o': 3.8461538461538463
    'q': 3.8461538461538463
    'w': 3.8461538461538463
    'y': 3.8461538461538463
2.
    's': 15.384615384615385
    'c': 11.538461538461538
    'o': 11.538461538461538
    'q': 11.538461538461538
    'r': 11.538461538461538
    'h': 7.6923076923076925
    'w': 7.6923076923076925
    'a': 3.8461538461538463
    'f': 3.8461538461538463
    'm': 3.8461538461538463
    't': 3.8461538461538463
    'y': 3.8461538461538463
    'z': 3.8461538461538463
3.
    'a': 15.384615384615385
    'z': 15.384615384615385
    'b': 11.538461538461538
    'j': 11.538461538461538
    'l': 11.538461538461538
    'h': 7.6923076923076925
    'p': 7.6923076923076925
    'd': 3.8461538461538463
    's': 3.8461538461538463
    't': 3.8461538461538463
    'v': 3.8461538461538463
    'y': 3.8461538461538463
4.
    'g': 19.23076923076923
    'v': 19.23076923076923
    'n': 15.384615384615385
    'f': 7.6923076923076925
    'h': 7.6923076923076925
    's': 7.6923076923076925
    'z': 7.6923076923076925
    'b': 3.8461538461538463
    'q': 3.8461538461538463
    'r': 3.8461538461538463
    'x': 3.8461538461538463
5.
    'v': 28.0
    'g': 12.0
    'j': 12.0
    'c': 8.0
    'h': 8.0
    'r': 8.0
    'e': 4.0
    'k': 4.0
    'n': 4.0
    'o': 4.0
    'p': 4.0
    'u': 4.0
6.
    'o': 16.0
    'v': 16.0
    'b': 8.0
    'h': 8.0
    'q': 8.0
    's': 8.0
    'w': 8.0
    'a': 4.0
    'c': 4.0
    'd': 4.0
    'p': 4.0
    'r': 4.0
    't': 4.0
    'z': 4.0
7.
    'a': 16.0
    'b': 12.0
    'r': 12.0
    'f': 8.0
    'n': 8.0
    'v': 8.0
    'y': 8.0
    'e': 4.0
    'g': 4.0
    'i': 4.0
    'j': 4.0
    'q': 4.0
    'u': 4.0
    'z': 4.0
8.
    'a': 16.0
    'i': 12.0
    'p': 12.0
    'w': 12.0
    'e': 8.0
    'g': 8.0
    's': 8.0
    'd': 4.0
    'j': 4.0
    'l': 4.0
    'o': 4.0
    'q': 4.0
    'y': 4.0
9.
    'a': 20.0
    't': 20.0
    'n': 16.0
    'e': 12.0
    'h': 12.0
    'b': 4.0
    'd': 4.0
    'm': 4.0
    'p': 4.0
    's': 4.0
10.
    ‘m': 24.0
    'r': 16.0
    'b': 8.0
    'f': 8.0
    'y': 8.0
    'c': 4.0
    'g': 4.0
    'i': 4.0
    'j': 4.0
    'k': 4.0
    'p': 4.0
    'q': 4.0
    's': 4.0
    't': 4.0
```

Looking at the highest frequencies (which we would expect to map to the same letters), we see that:
In the first position, ‘e’ likely shifted to ‘n’, so the shift would be by 9 corresponding to ‘j’.
in the second position, ‘e’ shifted to ‘s’, so the shift would be by 14 corresponding to ‘o’.

Continuing this way, we find the key 'JOHNCONWAY', which decrypts the message to give:

```
YOUKNOWPEOPLETHINKTHATMATHEMATICSISCOMPLICATEDMATHEMATICSISTHESIMPLEBITITSTHESTUFFWE
CANUNDERSTANDITSCATSTHATARECOMPLICATEDIMEANWHATISITINTHOSELITTLEMOLECULESANDSTUFF
THATMAKEUPMAKEONECATBEHAVEDIFFERENTLYTOANOTHERORTHATMAKEACATHOWDOYOUDEFINEACATIHAVE
NOIDEA
```

hHen spaced out, the above reads:

```
YOU KNOW PEOPLE THINK THAT MATHEMATICS IS COMPLICATED
MATHEMATICS IS THE SIMPLE BIT
ITS THE STUFF WE CAN UNDERSTAND
ITS CATS THAT ARE COMPLICATED
I MEAN WHAT IS IT IN THOSE LITTLE MOLECULES AND STUFF
THAT MAKE UP MAKE ONE CAT BEHAVE DIFFERENTLY TO ANOTHER
OR THAT MAKE A CAT
HOW DO YOU DEFINE A CAT
I HAVE NO IDEA
```

3. Affine cipher

```
6917141364293641, 5044493105177484, 10208794241351887, 16394322558427148,
11758121930809893, 15571898457877977, 7672722015089403, 13661070158473411,
17999297470735005, 12313955920676335, 5960590266677512, 1613421779734456,
1750819096862416, 3118598423638319, 14816640742963862, 4952241931583899,
12257144082730227, 7862771476786858, 5006500927265261, 11323114722137903,
22833602100630408, 8963415721169565, 15595638667025459, 8028339051359388,
3385708046121353, 12190779082257523, 8983375210790796, 15571898457877977,
15147654701575566, 16361132341028484, 5962327355151718, 8901193427034701,
5179568152435730, 3672045789372412, 23610469115026974, 1577294047287513,
15642317927380556, 15571898457877977, 10282634434851196, 10749617216933305,
17838746455253440, 21499666401460178, 1037344909841996, 17413814796435480,
16269186929768054, 10449344135634668, 24087490685235750, 10768725190149571,
6484888204271905, 22185358129776042, 19377417029468988, 16267449841293848,
16555381474675390, 21520574190817628, 14140526597210259, 19733309797334806,
16283129124025650, 16538093542757166, 24098448719654436, 16798515250649044,
13879801264995293, 10264930014031131, 7946076055449771, 18258106201941864,
423054714981679, 17458353983971638, 9294184051519018, 19030921054252445
```

Using enhanced mind-reading techniques, Eve was able to able to extract the following information: Alice uses a general affine cipher, and the plaintext alphabet consists of blocks of five letters written as ASCII bytes (extended ASCII) and then interpreted as an integer modulo n. Apparently, even the coefficients of the affine cipher transformation are ASCII byte encodings of important codewords. (See strtoint and inttostr in final.sage for the precise encoding used.) The first part of the corresponding plaintext was also recovered: 314077111660, 464400513312, 495875089509 Unfortunately, Bob's mind went dark and he could not disclose n.

Since this an affine cipher, we know that $\exists\ x, y \in \mathbb{Z}$ such that $c = p \cdot x + y$.
First, we need to recover the base of the affine cipher, n.

We know from the structure of the affine cipher that:

$$
\begin{aligned}
c_i &= p \cdot x_i + y \pmod n \\
c_i &= p \cdot x_i + y - n_i \cdot n \\
c_1 &= p \cdot x_1 + y - n_1 \cdot n \\
c_2 &= p \cdot x_2 + y - n_2 \cdot n \\
c_3 &= p \cdot x_3 + y - n_3 \cdot n
\end{aligned}
$$

$$
\begin{aligned}
c_1 - c_2 &= p(x_1 - x_2) - (n_1 - n_2) \cdot n \\
c_2 - c_3 &= p(x_2 - x_3) - (n_2 - n_3) \cdot n
\end{aligned}
$$

To get rid of p we calculate:

$$(x_2 - x_3)(c_1 - c_2) - (x_1 - x_2)(c_2 - c_3)$$

Giving:

$$((x_2 - x_3)(n_1 - n_2) - (m_1 - m_2)(n_2 - n_3))p = (x_2 - x_3)(c_1 - c_2) - (x_1 - x_2)(c_2 - c_3)$$

Meaning, n is a factor of $(x_2 - x_3)(c_1 - c_2) - (x_1 - x_2)(c_2 - c_3) = -83525612426675561226062868 5$
Taking the factors of the absolute value, we have:
$835256124266755612260628685 = 5 \cdot 167051224853351122452125737$
We can use 24610808569754243 as out n, since it's the smallest value that is greater than all the ciphertext.
Using the recovered plaintext, we can recover the coefficients of the affine cipher.

$$
\begin{aligned}
6917141364293641 &= 314077111660 \cdot x + y \pmod n \\
5044493105177484 &= 464400513312 \cdot x + y \pmod n \\
10208794241351887 &= 495875089509 \cdot x + y \pmod n
\end{aligned}
$$

$$
\begin{array}{c|c|c|}
 & 6917141364293641 & = 314077111660 \cdot x + y \pmod n \\
- & 5044493105177484 & = 464400513312 \cdot x + y \pmod n \\
\hline
 & 1872648259116157 & = -150323401652 \cdot x \\
\hline
\hline
 & 1872648259116157 & \equiv 24610658246352591 \cdot x \pmod n \\
\hline
\end{array}
$$

Thus:

$$x \equiv 1872648259116157 \cdot 24610658246352591^{-1} \pmod{24610808569754243}$$
$$x \equiv 1872648259116157 \cdot 2956863623047174 \pmod{24610808569754243}$$
$$x \equiv 289514745701 \pmod{24610808569754243}$$

$$6917141364293641 = 314077111660 \cdot 289514745701 + y \pmod{n}$$
$$y \equiv 5044493105177484 \cdot 289514745701 + y \pmod{n}$$
$$y \equiv 24610808569754212 \pmod{n}$$

$$c = 289514745701 \cdot p + 24610808569754212 \pmod{24610808569754243}$$
$$p = (c - 24610808569754212) \cdot 6618130068783420 \pmod{24610808569754243}$$

Finally, we can decrypt the entire message:

```
314077111660, 464400513312, 495875089509, 474400107552,
147495347566,139476301088,444083740788,448378660128,
457135256352,499967423520,521560989800,418598166626,
435493412979,477284692585,465675313518,500036083828,
491260571237,430040313714,189522408819,498760574317,
435626861938,139391951220,139476301170,139358200172,
139224637984,452903072872,418560108902,139476301088,
418531057766,491327400992,521560989806,435492757620,
477284954725,434336132973,435443164281,139140559717,
198107482470,139476301088,448311747872,495790679328,
482906432882,189523060837,472991231861,490170117986,
139208106100,477284887920,478744506912,495790679394,
478427029605,465792478752,138855082355,139208106094,
478689651317,495869518112,444300616237,422540943459,
418463906080,444016190766,146567877736,434333118057,
444216713330,452823839604,435610744174,442925215602,
139106807912,435706410016,452903062867,305716535328
```

by converting back to text, we get:

```
I tell my students, ‘‘When you get these jobs that
you have been so brilliantly trained for, just remember
that your real job is that if you are free, you need to
free somebody else. If you have some power, then your job
is to empower somebody else. This is not just a grab-bag candy  game.’’
The Enigma ringstellung for cipher 4 is MSG.
```

When we decrypt the key, we get:

```
Chloe Wofford
```

4. Enigma

Captain! We managed to get partial information about the daily settings.

```
Walzenlage: I II IV
Ringstellung: ?? ?? ??
Steckerverbindungen: ST AX UV FQ BM OP WY CD ?? ??
Kenngruppen: QZE TRF IOU TGB

SOP HIE = IOUTO XLIVE QVUAN MMGNC OMOUU GIHWR UKVIZ KBRQK IPIJU
          BWBTO ZHFNT BBZEU KCFRT IXOHJ AMKOE POYFV UFUQF ZTNGO
          LWAQK DQTVG INUFT NPZQH VMHCQ DVIDV GVLZA SNSOK FQD
```

If we could get the ring settings, the next tent over says we should be able figure out the rest of the plugboard.

Use first half of key (SOP) as starting position to decrypt second part (EJF) to get (KEH)
Use decryption of second part (KEH) as new starting position to decrypt message.
We get:

```
bytho wcani descl ibemy astot ishmw ntfnd admcl
ation bnsee inumy estye medcx llesp onden tmons reulr
kbran cmeta molph ospdi ntoth iscer ebrbt edpel son
```

Looking at our decryption, we have "desclibe" which should be "describe". Thus, we can guess the plugboard setting 'LR'.

We now have:

```
butho wcani descr ibemy aston ishmw ntand admcr
ation bnsee inumy estee medcx rresp onden tmons leurl
eblan cmeta morph ospdi ntoth iscel ebrbt edper son
```

Looking at our plaintext again, the first error is "astonishmwnt" which should be "astonishment". Thus, we need a way of mapping 'w' to 'e'.
However, we have already used 'w' on the plugboard. Let's find a way of mapping the encrypted form of 'W', in this specific position, which is 'Z', to a letter that routes it to 'E'.
After a little trial-and-error, we see that mapping 'ZJ' fixes the message.

We now have:

```
butho wcani descr ibemy aston ishme ntand admir
ation onsee ingmy estee medco rresp onden tmons ieurl
eblan cmeta morph osedi ntoth iscel ebrat edper son
```

Which, when spaced out properly, reads:

```
but how can i describe my astonishment and admiration
on seeing my esteemed correspondent monsieur leblanc
metamorphosed into this celebrated person
```

5. RSA

```
alice> heya bob, how ar u
bob> im gr8
bob> you reT?
bob> n = 24907363464921047217297225673350762575281464933167781569819743
7363162214936770864263301292885652120647173264628224337396O731
alice> soo kewl that we hav the same modulus, soo much more secure
alice> i usu just ask sophie to make some more primes for me <33
bob> no prob alie
alice> e = 65537 for me
bob> f = 1000003 for me
charlie> hi y'all, just came outa meeting! stuff is going down, so act fast
charlie> alice: 117593034210606527105028325031030941931648
                815630540152029044354860203580828326210173
                429212200536739479721725911690334195608 6
charlie> bob: 179930614739269660678231086701062190445253
              840132173573802352450775824950968612040118
              663497344113724004618578500551561498 7681
charlie> btw i just strtoint'ed the whole thing, no blocks or anything fancy pantsy
eve> lolh smh
```

$$
\begin{aligned}
e &= 65537 \\
f &= 1000003 \\
n &= 24907363464921047217297225673350762575281464933167781569819743 \\
&\quad 73631622149367708642633012928856521206471732646282243373960731 \\
m_a = m^e &= 11759303421060652710502832503103094193164881563054015202904435 \\
&\quad 48602035808283262101734292122005367394797217259116903341956086 \\
m_b = m^f &= 179930614739269660678231086701062190445253840132173573802352450775824 95 \\
&\quad 0968612040118663497344113724004618578500551561498 7681 \\
\gcd(e, f) &= 1 \\
e \cdot x + f \cdot y &\equiv 1 \pmod{n} \\
x &\equiv 295788 \pmod{n} \\
y &\equiv -19385 \pmod{n} \\
m_a^x \cdot m_b^y &\equiv m^{e \cdot x + f \cdot y} = m^1 = m \pmod{n} \\
m &= 1482878568381413441093954225925874186699333036099796714625982563913650 8 \\
&\quad 3697606202170869585351243553
\end{aligned}
$$

Running it through strtoint gives:

`Elona Musk is pulling out, sell TWTR now!`

6. RSA

```
n = 16653052943296534009927166682117653018853597228304609699601636
4234771423224878910478932117699610350618246947860042343417159
e = 65537
y = 14944140254560528408209463017103768683741055494303520438904279
7718540079485257006113787250895354916689260854817821121453874
```

The plaintext is encoded as an integer in base 26 (modulo n), with 'digits'

```
A = 0, B = 1, . . . , Z = 25
```

$$
\begin{aligned}
n &= 16653052943296534009927166682117653018853597228304609699601636 \\
&\quad 4234771423224878910478932117699610350618246947860042343417159 \\
e &= 65537 \\
e^{-1} &\equiv 508279320116515204846991951328866767377402849318365362804417937277 \\
&\quad 34881147087355424965028798253793847992240038067422171393 \\
p = y^{e^{-1}} &= 5634262806810528583441449525122235691095 8 \\
p \text{ (base 26)} &= [13, 14, 0, 7, 18, 0, 24, 18, 12, 20, 11, 19, 8, 15, 11, 24, 8, 13, 1, 0, 18, 4, 17, 0, 8, 13, 1, 14, 22] \\
&= \text{“NOAHSAYSMULTIPLYINBASERAINBOW”}
\end{aligned}
$$

Relevant code (based sage, based on stuff done in class):

```
....:
....: def pollard_pminus_1(n, a):
....:     i = 1
....:     a = Integers(n)(a)
....:     while gcd(Integers()(a)-1, n) == 1:
....:         i += 1
....:         a = a^i
....:     return gcd(Integers()(a)-1, n)
....:
....: n = 16653052943296534009927166682117653018853597228304609699601636
....:     64234771423224878910478932117699610350618246947860042343417159
....:
....: p = pollard_pminus_1(n, 5)
....:
....: q = n / p
....:
....: l = lcm(p-1, q-1)
....: ring = IntegerModRing(l)
....: print(ring(65537)^-1)
....:

508279320116515204846991951328866767377402849318365362804417937277
34881147087355424965028798253793847992240038067422171393
```

The decryption reads "Noah says multiply in base rainbow"

7. 7. Diffie–Hellman

```
alice> p = 1600774441581334219780600000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000432209099226960239340763
bob> Yahoo! What's going on with your prime!? Oh well, g = 2 as always!
alice> g^a = 115916852703688593321785760893301236896991672430420707679222309
282509317751229144270012266510200309346808149667382577787878633
0002771542293766114467228890040575216761614423950398825418437936
bob> g^b = 575888213681660770475128571088550295674623296573691479085064213
967623740013786721669248908515706185159465035805440862621304296
869839120646574688710399284505691846199112507789898432268180523
alice> Let's just add our common secret to the message like a one-time pad
bob> Yeah! I don't trust ASCII--I think it's rigged.
alice> I'm just going to write my message as an integer like
alice> h e l l o = 07 04 11 11 14 = 704111114
alice> Heading your way!
alice> m: 620945601844830146411372829211407124029166699782737399787363634
438224667948005628550729901067384508056258649925961457566814249
100027830822531155426663083200685298415308333701929015786144937
bob> You said it girl!
```

I got stuck on this problem.

8. Elliptic curve ElGamel

lliptic curve ElGamal is used with the following parameters:

$$p = 2^{31} - 1 = 2147483647$$
$$E : y2 = x3 + x + 1 \text{ over } \mathbb{F}_p$$
$$G = (2120200592, 1037835596) \in E(\mathbb{F}_p)$$

Bob sends the point $(502702028, 397327625) \in E(\mathbb{F}_p)$. Alice takes her message, encodes it as the x-coordinate of a point on E using strtoint, and she sends the pair of points $(1271659322, 1653304), (86041769, 166781836)$. Use baby step–giant step to solve the discrete logarithm problem on E and discover the message.

Bob picks secret b and sends $bG = (502702028, 397327625)$ to Alice.
Alice returns $(aG, x + abG) = ((1271659322, 1653304), (86041769, 166781836))$.
Bob recomputes $x = (x + abG) - (b \cdot aG)$.

$x = (86041769, 166781836) - b(1271659322, 1653304)$

If we find b, we can recover x.

Let $m = \sqrt{p} = 46341$

Computing the discrete log, we using the baby-step giant-step, we find the common element (2120200592 : 1037835596 : 1)

Thus, $g^1 \equiv$

I know the common element should be used to find the discrete log, but I'm not sure how the SAGE elliptic curve works.