AOOD Final Project for Juniors, Option 2

From Mr. McLaughlin: These challenges are three geocaching puzzles that I am curious to see if anyone can solve. I have solved the first one and can tell you that the decrypted text is English-language words that will make sense to you if you decrypt them correctly. A bunch of the words will be spelling out numbers because all geocaches have a GPS location and geocaching puzzles almost always simplify to the GPS location. I did it with a JavaScript program more than two years ago and I was a much worse coder then, so I don't know that my method was good and I don't remember everything I did. I have ideas about how to solve the second one but I haven't given it my full effort before. I'm not sure that my ideas would be enough to solve it even if I gave it my full effort. I have literally no idea how someone would go about solving the third one. I'd love it if you were able to solve any of them and to teach me how you solved the second and third ones!

Kerckhoffs (part 1)

As a young kid Cacher Craig set out to create his own method to encode data, as one does. Of course he didn't yet know about the design principles of proper encryption algorithms like AES or ECDH or whatever, instead he had simple things like Caesar Ciphers as his model. In an effort to create the most complicated variation of this possible he came up with:

1. Each letter maps to a string of digits (called a "codeword"). These codewords have different lengths. The first digit tells you how long the codeword is. (For example "52381" would be a valid codeword because it starts with 5 and is five digits long).
2. After you replace a letter with a codeword the entire mapping shifts (letters stay in place, codewords shift down). The amount that it shifts is given by the last digit of the codeword. (For example, using the key below, if the first letter of the plaintext is "A" it would map to the codeword "89411894". If the second letter were "S" it would now map to "57643" since the entire key has shifted by four). This shift is cumulative. Codewords that shift off the bottom go back on the top.

Cacher Craig had various other tricks that would make this even more confusing. The same letter could appear multiple times in the mapping with different codewords. The letters might not appear in alphabetical order in the mapping. Other symbols like punctuation or whitespace could also have entries in the mapping. Finally shorter codewords could "hide" inside longer codewords (such as having both codewords "321" and "53214") to confuse frequency analysis. None of these additional countermeasures will be employed for these puzzles (at least intentionally, all keys have been generated randomly).

A	89411894
B	52381
C	88527391
D	946320122
E	923921735
F	4254
G	4504
H	7171031
I	692473

J	971559793
K	638440
L	930424404
M	84524991
N	87445918
O	57643
P	7004062
Q	376
R	29
S	4468
T	85053600
U	361
V	636187
W	20
X	23
Y	53177
Z	4502

```
850536007171031946320122450263618737670040626384405764363618771710319715597 93
```

```
8505360071710319463201224502636187376700406263844057643636187717103197155979 3
```

```
85053600717103194632012245026361873767004062638440576436361877171031971559793
36129523819304244044504450237692392173589411894450245029304244048505360071710
31717103170040627004062446845024468700406292392173553177446884524991209715597
93450437693042440444688505360063618787445918450288527391717103144688505360045
02361450445048941189423450488527391923921735294468894118948852739144686384404
50269247384524991717103142544468638440971559793450242547004062576436384402087
44591857643361450288527391636187923921735576432997155979369247337623361717103
18505360020850536007171031930424404238505360063844063618787445918450288527391
71710314468850536004502361971559793850536008452499152381576435317737689411894
45024254638440376700406269247369247323692473946320122946320122450445025238163
84404468930424404576436361876384409715597937171031425457643376971559793700406
288527391946320122
```

Kerckhoffs (part 2)

Kerckhoffs's principle states that a properly designed cryptosystem should be secure even if an adversary knows everything about its workings except for the particular key used.

So much of the complexity of Cacher Craig's cryptosystem lies in details that are not part of the key. The differing lengths of the codewords and the shifting of the mapping are part of the algorithm and the exact details of both can be easily extracted from the ciphertext when the full algorithm is known.

Prove Kerckhoffs right by breaking the following message without the key, thereby showing that Cacher Craig's cryptosystem is indeed insecure.

```
65265521707328176144355570955709795448179544815570989447709404555709652655504
61641971557095920789447709781153976998555212330889447709308769985565265539140
45781153994543228677566596058587906967605858521237811539920376451775665965265
```

```
52033879544816419717080686790696721769985533876144352179069676419714045775665
```

Kerckhoffs (part 3)

With the benefit of more experience Cacher Craig realized that some of the design features of his cryptosystem that were meant to aid a human doing the decryption by hand don't really make sense now when computers can simply do it all for you!

There is no reason the first digit of a codeword needs to tell you the length of the codeword. As long as no codeword is a prefix of another codeword (for example you couldn't have both "123" and "1234" as codewords) you can still uniquely determine the boundaries if you know the key. With this change all codewords will still have a length between 2 and 9, but the first digit no longer has any meaning.

There is also no reason the last digit of a codeword needs to tell you the shift applied after that codeword is used. These shifts can also be secret values that are part of the key. With this change all codewords have a secret shift between 0 to 25 (inclusive) with the last digit no longer having any meaning. Some shift values can be repeated and some may not be used at all.

After these two changes Cacher Craig has become overconfident. He is convinced there is no way anyone can break the code now!

```
86096972781418871646243255912860798333763800541880920926222146337946294413243
```

```
56338877378194629441331707793418860809209260952531707724325591278114246243255
91287164641863388773969723170776103003595419106489462944131424686014246930952
53763800502733515954191222146337243255912156978143261860243255912027335196972
79833871646860095255954191064830027335144439615697815697886218360273351871646
96972317077969729462944131424661030033170772221463376338877379833306338877387
16468621836937813763800521679483170770952561030038601424624325591230306103003
14326102733518716462432559124443968092092644439694629441363388773095252221463
37243255912798334189697224325591280920926064814246156978934189462944139697215
69780648798336338877344439641806483170779462944132221463376338877396972142469
32432559120273351798337983341806488621836303763800506487983387164693932167948
14326196972862183686093935954191376380058092092609525781633887735954191936338
87737813763800578180920926595419186218368716460952531707793862183686218361424
61424686094629441306487983302733519697287164602733519697214246064821679481432
61142461432615954191143261317077143261095259697224325591221679488092092602733
51317077222146337156978969724189462944138092092609525860444396969722221463370
95254182432559122221463374443969697280920926860027335159541911432611432616103
00314246946294413809209266103003376380056103003216794879833444396871646143261
14326163388773095253059541910648860142467983380920926418946294413969727983380
92092614246862183615697886024325591294629441302733512432559124443968092092680
92092622214633714326122214633714326115697822214633731707706483170775954191610
30033763800587164606482221463374443968604187983393143261064886087164686014246
41863388773610300359541916338877386218361569788606338877378137638005216794878
18092092602733519361030033763800530633887734188608621836027335144439663388773
86002733519393595419178122214633787164693216794863388773781862183602733519341
88621836860633887739697279833809209266338877386094629441386087164609525156978
14246142463086218368608621836243255912969729337638005301569782432559128092092
62221463371569789697214326187164615697831707741894629441380920926610300393216
79484443963763800521679489697221679480952515697830317077317077143261871646317
07724325591214246809209267818716461424622214633780920926143261243255912243255
91287164624325591286002733512432559120648798337983386002733513170771432610952
51424663388773860309341893595419180920926860095252167948809209261424679833871
64614246860633887730273351809209269363388773303170778716462221463373763800586
08602167948798336103003064887164644439686218360648376380050952580920926860781
24325591278122214633778141859541917812167948027335121679482167948027335115697
81432619462944138092092641822214633786218364184182167948444396095257983314326
11432617983394629441359541918092092686079833633887732167948376380059697221679
48304187813170772167948969723170777983396972946294413222146337064886218364183
17077871646809209261569781569783024325591222214633722214633744439
6
```