**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](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) or [ECDH](https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman) or whatever, instead he had simple things like [Caesar Ciphers](https://en.wikipedia.org/wiki/Caesar_cipher) 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 |

8505360071710319463201224502636187376700406263844057643636187717103197155979336129523819304244044504450237692392173589411894450245029304244048505360071710317171031700406270040624468450244687004062923921735531774468845249912097155979345043769304244044468850536006361878744591845028852739171710314468850536004502361450445048941189423450488527391923921735294468894118948852739144686384404502692473845249917171031425444686384409715597934502425470040625764363844020874459185764336145028852739163618792392173557643299715597936924733762336171710318505360020850536007171031930424404238505360063844063618787445918450288527391717103144688505360045023619715597938505360084524991523815764353177376894118944502425463844037670040626924736924732369247394632012294632012245044502523816384404468930424404576436361876384409715597937171031425457643376971559793700406288527391946320122

Kerckhoffs (part 2)

[Kerckhoffs's principle](https://en.wikipedia.org/wiki/Kerckhoffs%27s_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.

65265521707328176144355570955709795448179544815570989447709404555709652655504616419715570959207894477097811539769985552123308894477093087699855652655391404578115399454322867756659605858790696760585852123781153992037645177566596526552033879544816419717080686790696721769985533876144352179069676419714045775665934150461215920721453078115395920740457699855504613917073281769985570806867756659920376451341338391920376451920376451775665979544815570952123338781153976998557614435781153950461605858453045306419718944770930821708068639164197120769985578115397756659920376451920376451391769985540456419718944770939192037645120708068634192037645194543228620391557093086058583085920721404550461652655945432286795448179069677906967341652655641971592072065265564197194543228665265534176144357614435761443570732813083915570955709212045305920789447709391557094530920376451708068639189447709708068689447709769985545302059207338308795448165265533845306058586419717073281894477097811539945432286453060585845302021894477096419718944770952123775665934165265534120453055709795448120761443576998557906967453021308592077073281338775665934121707328145305920760585878115394530652655338945432286592077614435707328130870732816058585570960585892037645140457614435945432286945432286557095570921761443530865265545307756659945432286391214045404533833876144355046121557093389454322862089447709761443552123557097080686308215046192037645121769985579544814530214530521235046177566597073281945432286920376451920376451391769985540455920792037645189447709795448133892037645179544817073281605858641971641971708068650461781153989447709203384045790696740453412055709894477094530557097614435391214530920376451945432286391504615920734134164197155709404540452059207652655521233082079544817756659605858308781153952123775665960585876144353917954481

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](https://en.wikipedia.org/wiki/Prefix_code) 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!

86096972781418871646243255912860798333763800541880920926222146337946294413243255912610300306489462944138092092630317077243255912064863388773156978969721569783044439661030039314326179833142468092092644439631707731707759541912167948376380053763800514246376380054443962221463377983324325591202733511569788621836860142466103003860095258716468621836610300322214633741893781610300361030030648933015697815697887164686061030037812221463374184443966103003798336103003095256338877378194629441331707793418860809209260952531707724325591278114246243255912871646418633887739697231707761030035954191064894629441314246860142469309525376380050273351595419122214633724325591215697814326186024325591202733519697279833871646860095255954191064830027335144439615697815697886218360273351871646969723170779697294629441314246610300331707722214633763388773798333063388773871646862183693781376380052167948317077095256103003860142462432559123030610300314326102733518716462432559124443968092092644439694629441363388773095252221463372432559127983341896972243255912809209260648142461569789341894629441396972156978064879833633887734443964180648317077946294413222146337633887739697214246932432559120273351798337983341806488621836303763800506487983387164693932167948143261969728621836860939359541913763800580920926095257816338877359541919363388773781376380057818092092659541918621836871646095253170779386218368621836142461424686094629441306487983302733519697287164602733519697214246064821679481432611424614326159541911432613170771432610952596972243255912216794880920926027335131707722214633715697896972418946294413809209260952586044439696972222146337095254182432559122221463374443969697280920926860027335159541911432611432616103003142469462944138092092661030033763800561030032167948798334443968716461432611432616338877309525305954191064886014246798338092092641894629441396972798338092092614246862183615697886024325591294629441302733512432559124443968092092680920926222146337143261222146337143261156978222146337317077064831707759541916103003376380058716460648222146337444396860418798339314326106488608716468601424641863388773610300359541916338877386218361569788606338877378137638005216794878180920926027335193610300337638005306338877341886086218360273351444396633887738600273351939359541917812221463378716469321679486338877378186218360273351934188621836860633887739697279833809209266338877386094629441386087164609525156978142461424630862183686086218362432559129697293376380053015697824325591280920926222146337156978969721432618716461569783170774189462944138092092661030039321679484443963763800521679489697221679480952515697830317077317077143261871646317077243255912142468092092678187164614246222146337809209261432612432559122432559128716462432559128600273351243255912064879833798338600273351317077143261095251424663388773860309341893595419180920926860095252167948809209261424679833871646142468606338877302733518092092693633887733031707787164622214633737638005860860216794879833610300306488716464443968621836064837638005095258092092686078124325591278122214633778141859541917812167948027335121679482167948027335115697814326194629441380920926418222146337862183641841821679484443960952579833143261143261798339462944135954191809209268607983363388773216794837638005969722167948304187813170772167948969723170777983396972946294413222146337064886218364183170778716468092092615697815697830243255912222146337222146337444396