Assignment #2

CPEN 442

September 27

Kaibo Ma (32400129)
Department of Electrical and Computer Engineering
University of British Columbia
Vancouver, Canada

I. PROBLEM #1

Cypher Text:
GXMLKTALSMSEIKXIHUGPKTWEHRKVJKWH
MLGEGLTEUWHUJSXHQKELKWQHOGYBYKJ
JGMLHAKKUJGEYLHHWVTXXRYKJNXSHUU
KMKEYHJKWHMLHEHSALOKWQGEUVWSHE
UQAGMLHWHUGOKTMMLHAWGIHKVEGEYR
LGEBQYKJJGGEULHWQKEVKTEUYKJVKWM
SEMLHSWQRJNGMLRGEUMLHSWNWHQHEY
HUKMMLHQNKMCLHWHXSEYKXEQJKMLH
WXSHQSQEKCHEYXKQHUCSMLSEGLSALSW
KEVHEYHUKMGMMLHLHGUKVMLHAWGIHG
CLSMHQMKEHYKJJGQSJNXHYKJJGTEGVVH
YMHUYKJJGGEUSEBHHNSEACSMLMLHQTW
WKTEUSEAQYKJJGLGQOHHENXGYHUUKMS
MOHGWQMLHVKXXKCSEASEQYWSNMSKEE
GEYRLGEBQXSEYKXEYKJJGJKMLHWKVNW
HQSUHEMXSEYKXEYKJJGUSHUKYMKOHWV
SIHYKJJGG

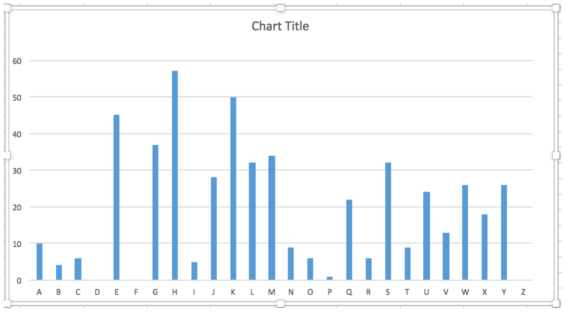
Plain Text:
ALTHOUGH IT INVOLVED A JOURNEY OF MORE THAN A HUNDRED MILES ON HORSEBACK COMMA THE GOOD MAN CHEERFULLY COMPLIED DOT ONCE MORE THE NEIGHBORS AND FRIENDS GATHERED ABOUT THE GRAVE OF NANCY HANKS COMMA AND HER SON FOUND COMFORT IN THEIR SYMPATHY AND THEIR PRESENCE DOT THE SPOT WHERE LINCOLNS MOTHER LIES IS NOW ENCLOSED WITH IN A HIGH IRON FENCE DOT AT THE HEAD OF THE GRAVE A WHITE STONE COMMA SIMPLE COMMA UNAFFECTED COMMA AND IN KEEPING WITH THE SURROUNDINGS COMMA HAS BEEN PLACED DOT IT BEARS THE FOLLOWING INSCRIPTION NANCY HANKS LINCOLN COMMA MOTHER OF PRESIDENT LINCOLN COMMA DIED OCTOBER FIVE COMMA A

Plain Text with Punctuation:
ALTHOUGH IT INVOLVED A JOURNEY OF MORE THAN A HUNDRED MILES ON HORSEBACK, THE GOOD MAN CHEERFULLY COMPLIED. ONCE MORE THE NEIGHBORS AND FRIENDS GATHERED ABOUT THE GRAVE OF NANCY HANKS, AND HER SON FOUND COMFORT IN THEIR SYMPATHY AND THEIR PRESENCE. THE SPOT WHERE LINCOLNS MOTHER LIES IS NOW ENCLOSED WITH IN A HIGH IRON FENCE. AT THE HEAD OF THE GRAVE A WHITE STONE, SIMPLE, UNAFFECTED, AND IN KEEPING WITH THE SURROUNDINGS, HAS BEEN PLACED. IT BEARS THE FOLLOWING INSCRIPTION NANCY HANKS LINCOLN, MOTHER OF PRESIDENT LINCOLN, DIED OCTOBER FIVE, A

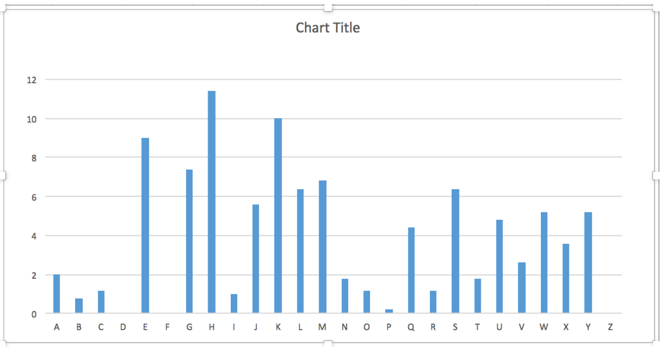
Alphabet: abcdefghijklmnopqrstuvwxyz
Key: goyuhvalspbxjeknzwqmticfrd

Procedure:
The first method I used to decrypt the cypher was to see if it was a Caesar Cypher. I wrote a javascript that spat out all possible 26 shifts. From which I learned that the cypher text was not Caesar. Next I used frequency analysis to figure out if it might be a monoalphabetical cypher.

I found that out of the 500 characters in my text file, some characters appeared more than others, which is a tall tail sign of a monoalphabetical cypher (Fig 1, Fig 2).

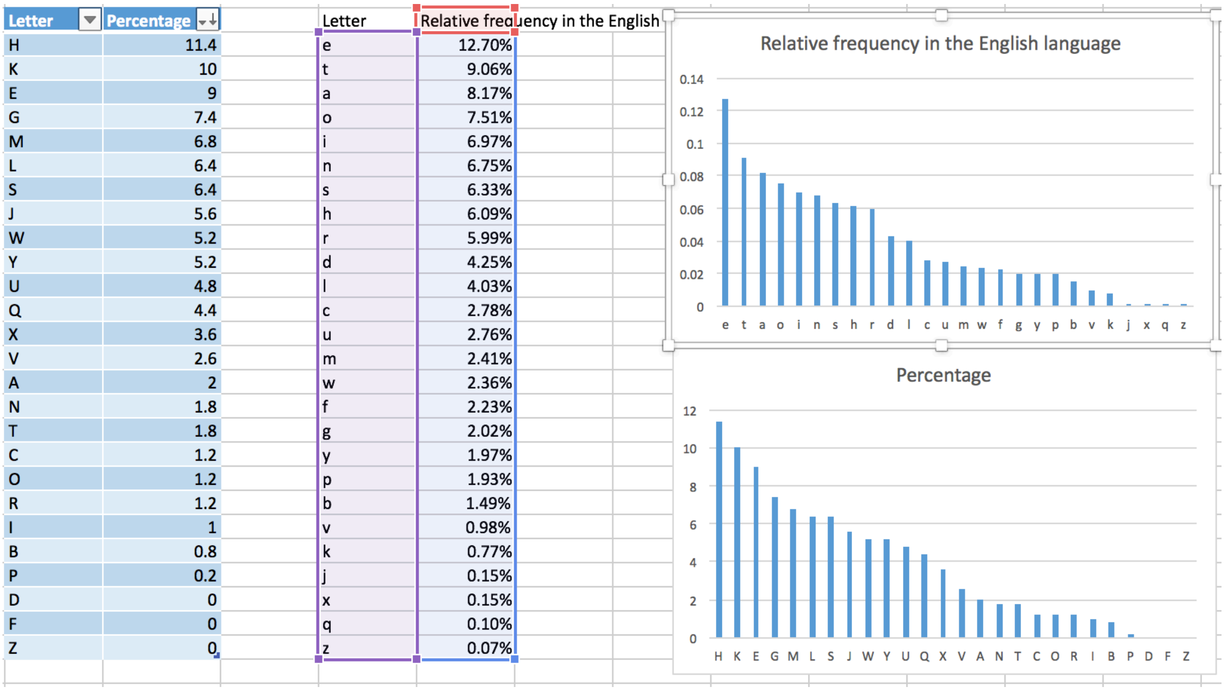


(Fig. 1) Number of Occurrences of Letters



(Fig. 2) Percentage of occurances

Next, I compared to side by side with the English natural frequency occurances (Fig 3). From there I found the letter "E" and common digrams and trigrams like "the". From there I found that there was a common 5 letter combination that kept on repeating which later I found out it was the phrase "COMMA". Now I knew that punctuation was spelt out. There I found common trigrams which was a candidate for "DOT" as I already found "O" and "T". From there I found words like "their" and "gather". With trial and error I finally completed the decryption.



Letter	Percentage
H	11.4
K	10
E	9
G	7.4
M	6.8
L	6.4
S	6.4
J	5.6
W	5.2
Y	5.2
U	4.8
Q	4.4
X	3.6
V	2.6
A	2
N	1.8
T	1.8
C	1.2
O	1.2
R	1.2
I	1
B	0.8
P	0.2
D	0
F	0
Z	0

Letter	Relative frequency in the English
e	12.70%
t	9.06%
a	8.17%
o	7.51%
i	6.97%
n	6.75%
s	6.33%
h	6.09%
r	5.99%
d	4.25%
l	4.03%
c	2.78%
u	2.76%
m	2.41%
w	2.36%
f	2.23%
g	2.02%
y	1.97%
p	1.93%
b	1.49%
v	0.98%
k	0.77%
j	0.15%
x	0.15%
q	0.10%
z	0.07%

Relative frequency in the English language
0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
e t a o i n s h r d l c u m w f g y p b v k j x q z
Percentage
12
10
8
6
4
2
0
H K E G M L S J W Y U Q X V A N T C O R I B P D F Z

(Fig. 3) cypher text sorted next to the letter statistics of English.

II. PROBLEM #2

Cypher Text:

```
HSOLGRRELZDBWMXOLIYKVDRVQVKIUVKOVZHGF
UTAMDOHQPQDDBWNFUPGVAOUCHOIBDDWAKHX
APTAAZVACVAKBHVAOUCOVQOITAKQFKIHVZDCO
HQPQDOUZCFWUVKOOIKOTOILTZVXMGAVEVGWT
LOUXOFVGRVZBODWOUXCXOFUZRHFOHQPQDTHIV
LIDVVIXOVYQVDWQTOUILWVAVUKGBDLQDOQEHS
FVQAZVFXOHSLIHVZUATTBVQCHCMTULCTWYSEN
DLLDDNQOOCHVZUSLXPCHLRTHLSWYVMPOCZVQ
KVCVTAVZHDDWILZROUILXERIXOREYDIGGWEGCX
TKUTPGOUCHMOHVWZEMDVIHOHQPQDCXILFWVR
OHQPQDDBONDBOMIHYWQZLZIROUDVHPIMEIIHDC
DHOHQPQDVLZRZVGRDCFCOUCLOQAETLVBICEHSP
YCVQTHDWOUPLOUDVVGOIUVLCFDLCGIOLVQRWP
GTHLICZWVAVOUCHMOCQHZOUDVHPKOYCKATHV
ASFKDQERHVKVLBDLPYDHUILZOLCOHQPLDCPOIF
GTDCUTHHILHMOFUPCRGRHTLTQPHOCYDSFEXKV
CVDBTVLCZEBWHKXZLCMVKVDWOUZCCEEHUHLC
EWILOPKIHIUVKODUCLDBVMTHDWCDUMVLOQEHS
FRLEXDWUVVCSHLHOILGDLQDDBWNLIOZDWOUZC
WYOPIRVDDWOHQPQDHPLIOUZHGDOQHZWPDBOZ
EHMGDQPCVUOUDVOUPLAVLCLVZULCXECSOZPCO
UOCYDSFNUTHMOKOOIVGOIYDLCAKNGVAHSBHUK
PCLCGLEXAPTADUERREAYZOLCKVLPPGOUZLFUSF
PHERFOLCIMEIPOVFXOHSLIHVZUATTBOQKDGUCX
OUCOLCDXVFZRECHVZULCTDGNZLVLPHERQLDHH
VLTSFSPQEEHMNDVOZMGVPBPCPMIQOOZKGILDBC
ITDCAOIOUCOSEPDZCZECOIHTLOUICLIDVPGOUZCX
OIRDUTEILTEILTEILADDWATWMERFOLCUKZVCOW
ZHUZVUOLCCVMOIGQDDWOUXCXOFUZRHFCVMOR
QDHILPGRGOPTAVUZXGEIHWYWBDHDWAVOHQPQ
DOUDVTHIRVQOKXVCPWGDHGQXOSXGWLCILRECS
OUXOFVPOCPKIHVRUZEIGOYDLQDCXBOLIZFQEFCL
PDWPOOHQPQDDBVWVAATWZDCKAQVBHZOOHQP
QDDBAPTWUVPODCFCNGOUCEDTCTZULCLHSHXZE
GUFLIOLPGDTVCOUDVOLPGDTVCOUDVVLBDLPYD
UVLCCXVMAEDLTLFNZFMGGRLCOMATVGYCWVAV
ZVGRDKSEOZTANVAVZVHICZKGFHPOAVZVWGVHX
EKVOPREBOOZLIONDLQDSPOUWIAVWVAVZVHKXO
VPWIVXYMHFFCILCOOYDLQDZVHIPZLIKIRGDCGRD
QXVGXREUTBOQIIGPOVAOIIVCHRZQNCOERZVNTA
VPVDCAVDTRPLIZVFNHIQRTAOYDCRGOPLITDKVH
DQSTLVQOYDLQDPRTBKVGZVZQIIGVDOZWRPOAV
OUTHCSOFIHURIGPCVWEXILDVZVOHQPQDDBOPOI
DPCFDBOMDTCUILHIQRKOWGADWPGIDVEVYMVLZ
VOHQPQDDBOPEBSHIHZVWILIHIYBXCTULCGELGW
FUVDBOCOUDVLCQVWYVYDOXEAZVALCMVAVYK
VZYDHDIXLVIXLVCZVQUVPRXEVZWRVLZOKODNL
VAKCQZOKOAZOUDVTANSERQCPOSYWZRLDLHVLP
UKILCHLVOUILOHQPQDRPYWRGVUECVROHQPQDD
BWMZVSEVUVDERGQAHPCOHQPQDDBWMERQCIHH
ETMVLHEONSEBDOHQPQDDBWNFUPGVBQOKIHGK
APGZOTAVDDWZXDEECSPQEMEVKRGVFTHDWOHQ
PQDDBTDWPGIXEVTAVOUZCSPQEQCIHVFHYQATUL
CHDDWILZFMOXZOUTLOUCOHETHLVYDLCCDHIOH
QPQDDBVWZXYHQOOZVKVALHKNXOFUZRHFOUXC
ZVTLOUZOVXFOKOVZHRVHDYATTHYAKDWVAVHP
OHQPQDPGOUGRVBCODLQDTACDVUXPZOLCCXTK
UTTLOUDVTANVAVHPVQZOAETLDQERXVMSZVSEV
TAVZVGRREHXOUIHWYHIVDDWOUIHVDIRHPVQPC
AVDKPONGOUXELQAOCEPGIHKGCOTKHIOUZCVQC
ODLLDYDAETHLICZWVAVHVZVGRSPOUOUDVOLPG
DTVCTAVZYDHDDUHCGVUOXECSDZCHEMPHERRCS
HLHOIIGVTAVOUPLKQPGCVRUHYWOVCHUERELDO
XCCODLXOEHUVVQVTAVTHMVIHOCDWDBVUSPQE
MHDCOPLSDHHPVPVPOYDLQDDBVWTBLHHNECOI
MSPHILPOAVHPHKOQQCILZLILLITVHEAOPGCRBTU
VLHHIVIDBTAMOVQVZUVUVKOUZEHSFGRLCVPYD
LCGPCPOZPCOUOCYDSFGBDLQDDBWNLVTWOCTVL
HHIOLPGDTVCWVAVOUIHDQEMILOUDVOUXPCEOP
UVTDSYUOILVPTDVUOLAEHESPQEQCIHEDHXCDQT
UVDXIHVFCTZULCSGYOVLXVCPQVOHQPQDDBANX
OQFVHDZIGOCECKIKI
```

Key: ‘FRLQMZIEXPYGCBNTVOADUSHKW’,
'NYGCBDTVOAWUSHKMFRLQPZIEX'

Found two keys with same output text with the same score of -11976.949219.

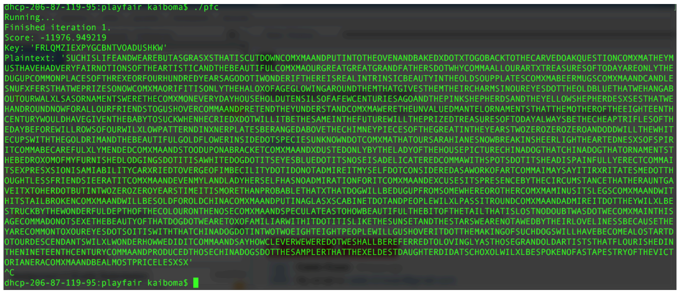
Plaintext:

```
'SUCHISLIFEANDWEAREBUTASGRASXSTHATISCUTD
OWNCOMXMAANDPUTINTOTHEOVENANDBAKEDXD
OTXTOGOBACKTOTHECARVEDOAKQUESTIONCOMX
MATHEYMUSTHAVEHADVERYFAIRNOTIONSOFTHE
ARTISTICANDTHEBEAUTIFULCOMXMAOURGREATG
REATGRANDFATHERSDOTWHYCOMMAALLOURART
XTREASURESOFTODAYAREONLYTHEDUGUPCOMM
ONPLACESOFTHREXEORFOURHUNDREDYEARSAGO
DOTIWONDERIFTHEREISREALINTRINSICBEAUTYINT
HEOLDSOUPPLATESCOMXMABEERMUGSCOMXMAA
NDCANDLESNUFXFERSTHATWEPRIZESONOWCOMX
MAORIFITISONLYTHEHALOXOFAGEGLOWINGAROU
NDTHEMTHATGIVESTHEMTHEIRCHARMSINOUREYE
SDOTTHEOLDBLUETHATWEHANGABOUTOURWALX
LSASORNAMENTSWERETHECOMXMONEVERYDAYH
OUSEHOLDUTENSILSOFAFEWCENTURIESAGOANDT
HEPINKSHEPHERDSANDTHEYELLOWSHEPHERDESX
SESTHATWEHANDROUNDNOWFORALLOURFRIENDS
TOGUSHOVERCOMMAANDPRETENDTHEYUNDERST
ANDCOMXMAWERETHEUNVALUEDMANTELORNAM
ENTSTHATTHEMOTHEROFTHEEIGHTEENTHCENTUR
YWOULDHAVEGIVENTHEBABYTOSUCKWHENHECRI
EDXDOTWILLITBETHESAMEINTHEFUTUREWILLTHE
PRIZEDTREASURESOFTODAYALWAYSBETHECHEAP
TRIFLESOFTHEDAYBEFOREWILLROWSOFOURWILXL
OWPATTERNDINXNERPLATESBERANGEDABOVETHE
CHIMNEYPIECESOFTHEGREATINTHEYEARSTWOZER
OZEROZEROANDODDWILLTHEWHITECUPSWITHTHE
GOLDRIMANDTHEBEAUTIFULGOLDFLOWERINSIDED
OTSPECIESUNKNOWNDOTCOMXMATHATOURSARA
```

```
HIANESNOWBREAKINSHEERLIGHTHEARTEDNESXSO
FSPIRITCOMMABECAREFULXLYMENDEDCOMXMAA
NDSTOODUPONABRACKETCOMXMAANDXDUSTEDO
NLYBYTHELADYOFTHEHOUSEPICTURECHINADOGT
HATCHINADOGTHATORNAMENTSTHEBEDROXOMOF
MYFURNISHEDLODGINGSDOTITISAWHITEDOGDOTI
TSEYESBLUEDOTITSNOSEISADELICATEREDCOMMA
WITHSPOTSDOTITSHEADISPAINFULLYERECTCOMM
AITSEXPRESXSIONISAMIABILITYCARXRIEDTOVERG
EOFIMBECILITYDOTIDONOTADMIREITMYSELFDOTC
ONSIDEREDASAWORKOFARTCOMMAIMAYSAYITIRX
RITATESMEDOTTHOUGHTLESSFRIENDSIEERATITCO
MXMAANDEVENMYLANDLADYHERSELFHASNOAD
MIRATIONFORITCOMXMAANDEXCUSESITSPRESENC
EBYTHECIRCUMSTANCETHATHERAUNTGAVEITXTO
HERDOTBUTINTWOZEROZEROYEARSTIMEITISMORE
THANPROBABLETHATXTHATDOGWILLBEDUGUPFR
OMSOMEWHEREOROTHERCOMXMAMINUSITSLEGSC
OMXMAANDWITHITSTAILBROKENCOMXMAANDWI
LLBESOLDFOROLDCHINACOMXMAANDPUTINAGLA
SXSCABINETDOTANDPEOPLEWILXLPASSITROUNDC
OMXMAANDADMIREITDOTTHEYWILXLBESTRUCKB
YTHEWONDERFULDEPTHOFTHECOLOURONTHENOS
ECOMXMAANDSPECULATEASTOHOWBEAUTIFULTH
EBITOFTHETAILTHATISLOSTNODOUBTWASDOTWEC
OMXMAINTHISAGECOMMADONOTSEXETHEBEAUTY
OFTHATDOGDOTWEARETOXOFAMILIARWITHITDOT
ITISLIKETHESUNSETANDTHESTARSWEARENOTAWE
DBYTHEIRLOVELINESSBECAUSETHEYARECOMMON
TOXOUREYESDOTSOITISWITHTHATCHINADOGDOTI
NTWOTWOEIGHTEIGHTPEOPLEWILLGUSHOVERITD
OTTHEMAKINGOFSUCHDOGSWILLHAVEBECOMEAL
OSTARTDOTOURDESCENDANTSWILXLWONDERHO
WWEDIDITCOMMAANDSAYHOWCLEVERWEWERED
OTWESHALLBEREFERREDTOLOVINGLYASTHOSEGR
ANDOLDARTISTSTHATFLOURISHEDINTHENINETEEN
THCENTURYCOMMAANDPRODUCEDTHOSECHINAD
OGSDOTTHESAMPLERTHATTHEXELDESTDAUGHTER
DIDATSCHOXOLWILXLBESPOKENOFASTAPESTRYOF
THEVICTORIANERACOMXMAANDBEALMOSTPRICEL
ESXSX'
```

Procedure:

First I performed Caesar and Frequency analysis but the outputs were gibberish. Thus I then attempted Playfair as it was in class lecture. I first tried to do it by hand by following some online resources but got nowhere. Then I googled how to decrypt Playfair and I did some research about Hill Climbing algorithms and fitness functions. I found and followed an algorithm that computes Playfair. Then I based my code off this algorithm (http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-playfair/). After attempting to decrypt the message. My code kept on getting stuck on certain randomly generated keys because those keys would be a local maximum for the Hill Climbing Technique. I looked further into how to get unstuck and came across Simulated Annealing. Simulated Annealing allows the code to become unstuck. It allows my randomly generated keys to accept lower scoring values than the local maximum that it gets stuck on. Thus I am able to achieve a different maximum which potentially is the global maximum for the fitness function. In other words, I am able to find the correct key instead of an incorrect key that could also score well in the fitness function. Soon I was able to modify my parameters to achieve the plain text faster. I have been able to reproduce the solution with two different keys. They both score the same fitness output of -11976.949219. My program can be found here: https://github.com/kiddo122/Decryption-Programs/tree/master/playfair

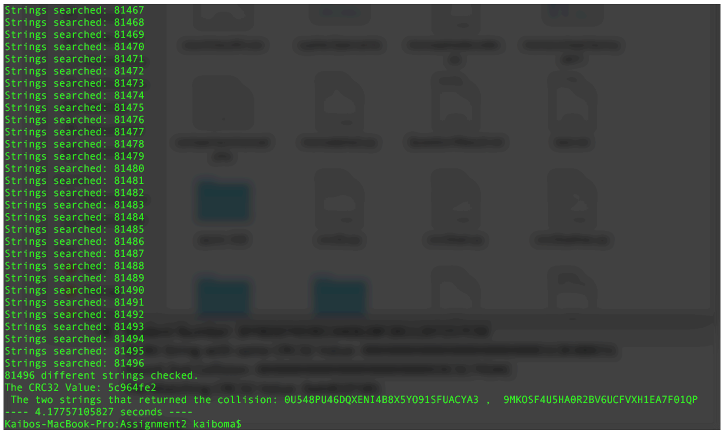


```
dhcp-206-87-119-95:playfair kaiboma$ ./pfc
Running...
Finished iteration 1.
Score: -11976.949219
Key: 'FRLQMZIEXPYGCBNTVOADUSHKW'
Plaintext: 'SUCHISLIFEANDWEAREBUTASGRASXSTHATISCUTDOWNCOMXMAANDPUTINTOTHEOVENANDBAKEDXDOTXTOGOBACKTOTHECARVEDOAKQUESTIONCOMXMATHEYM
USTHAVEHADVERYFAIRNOTIONSOFTHEARTISTICANDTHEBEAUTIFULCOMXMAOURGREATGREATGRANDFATHERSDOTWHYCOMMAALLOURARTXTREASURESOFTODAYAREONLYTHE
DUGUPCOMMONPLACESOFTHREXEORFOURHUNDREDYEARSAGODOTIWONDERIFTHEREISREALINTRINSICBEAUTYINTHEOLDSOUPPLATESCOMXMABEERMUGSCOMXMAANDCANDLE
SNUFXFERSTHATWEPRIZESONOWCOMXMAORIFITISONLYTHEHALOXOFAGEGLOWINGAROUNDTHEMTHATGIVESTHEMTHEIRCHARMSINOUREYESDOTTHEOLDBLUETHATWEHANGAB
OUTOURWALXLSASORNAMENTSWERETHECOMXMONEVERYDAYHOUSEHOLDUTENSILSOFAFEWCENTURIESAGOANDTHEPINKSHEPHERDSANDTHEYELLOWSHEPHERDESXSESTHATWE
HANDROUNDNOWFORALLOURFRIENDSTOGUSHOVERCOMMAANDPRETENDTHEYUNDERSTANDCOMXMAWERETHEUNVALUEDMANTELORNAMENTSTHATTHEMOTHEROFTHEEIGHTEENTH
CENTURYWOULDHAVEGIVENTHEBABYTOSUCKWHENHECRIEDXDOTWILLITBETHESAMEINTHEFUTUREWILLTHEPRIZEDTREASURESOFTODAYALWAYSBETHECHEAPTRIFLESOFTH
EDAYBEFOREWILLROWSOFOURWILXLOWPATTERNDINXNERPLATESBERANGEDABOVETHECHIMNEYPIECESOFTHEGREATINTHEYEARSTWOZEROZEROZEROANDODDWILLTHEWHIT
ECUPSWITHTHEGOLDRIMANDTHEBEAUTIFULGOLDFLOWERINSIDEDOTSPECIESUNKNOWNDOTCOMXMATHATOURSARAHIANESNOWBREAKINSHEERLIGHTHEARTEDNESXSOFSPIR
ITCOMMABECAREFULXLYMENDEDCOMXMAANDSTOODUPONABRACKETCOMXMAANDXDUSTEDONLYBYTHELADYOFTHEHOUSEPICTURECHINADOGTHATCHINADOGTHATORNAMENTST
HEBEDROXOMOFMYFURNISHEDLODGINGSDOTITISAWHITEDOGDOTITSEYESBLUEDOTITSNOSEISADELICATEREDCOMMAWITHSPOTSDOTITSHEADISPAINFULLYERECTCOMMAI
TSEXPRESXSIONISAMIABILITYCARXRIEDTOVERGEOFIMBECILITYDOTIDONOTADMIREITMYSELFDOTCONSIDEREDASAWORKOFARTCOMMAIMAYSAYITIRXRITATESMEDOTTH
OUGHTLESSFRIENDSIEERATITCOMXMAANDEVENMYLANDLADYHERSELFHASNOADMIRATIONFORITCOMXMAANDEXCUSESITSPRESENCEBYTHECIRCUMSTANCETHATHERAUNTGA
VEITXTOHERDOTBUTINTWOZEROZEROYEARSTIMEITISMORETHANPROBABLETHATXTHATDOGWILLBEDUGUPFROMSOMEWHEREOROTHERCOMXMAMINUSITSLEGSCOMXMAANDWIT
HITSTAILBROKENCOMXMAANDWILLBESOLDFOROLDCHINACOMXMAANDPUTINAGLASXSCABINETDOTANDPEOPLEWILXLPASSITROUNDCOMXMAANDADMIREITDOTTHEYWILXLBE
STRUCKBYTHEWONDERFULDEPTHOFTHECOLOURONTHENOSECOMXMAANDSPECULATEASTOHOWBEAUTIFULTHEBITOFTHETAILTHATISLOSTNODOUBTWASDOTWECOMXMAINTHIS
AGECOMMADONOTSEXETHEBEAUTYOFTHATDOGDOTWEARETOXOFAMILIARWITHITDOTITISLIKETHESUNSETANDTHESTARSWEARENOTAWEDBYTHEIRLOVELINESSBECAUSETHE
YARECOMMONTOXOUREYESDOTSOITISWITHTHATCHINADOGDOTINTWOTWOEIGHTEIGHTPEOPLEWILLGUSHOVERITDOTTHEMAKINGOFSUCHDOGSWILLHAVEBECOMEALOSTARTD
OTOURDESCENDANTSWILXLWONDERHOWWEDIDITCOMMAANDSAYHOWCLEVERWEWEREDOTWESHALLBEREFERREDTOLOVINGLYASTHOSEGRANDOLDARTISTSTHATFLOURISHEDIN
THENINETEENTHCENTURYCOMMAANDPRODUCEDTHOSECHINADOGSDOTTHESAMPLERTHATTHEXELDESTDAUGHTERDIDATSCHOXOLWILXLBESPOKENOFASTAPESTRYOFTHEVICT
ORIANERACOMXMAANDBEALMOSTPRICELESXSX'
^C
dhcp-206-87-119-95:playfair kaiboma$
```

(Fig. 4) Program output.

III. PROBLEM #3

81496 different strings checked.
The CRC32 Value: 5c964fe2
The two strings that returned the collision:
X: 0U548PU46DQXENI4B8X5YO91SFUACYA3
Y: 9MKOSF4U5HA0R2BV6UCFVXH1EA7F01QP
---- 4.17757105827 seconds ----



```
Strings searched: 81467
Strings searched: 81468
Strings searched: 81469
Strings searched: 81470
Strings searched: 81471
Strings searched: 81472
Strings searched: 81473
Strings searched: 81474
Strings searched: 81475
Strings searched: 81476
Strings searched: 81477
Strings searched: 81478
Strings searched: 81479
Strings searched: 81480
Strings searched: 81481
Strings searched: 81482
Strings searched: 81483
Strings searched: 81484
Strings searched: 81485
Strings searched: 81486
Strings searched: 81487
Strings searched: 81488
Strings searched: 81489
Strings searched: 81490
Strings searched: 81491
Strings searched: 81492
Strings searched: 81493
Strings searched: 81494
Strings searched: 81495
Strings searched: 81496
81496 different strings checked.
The CRC32 Value: 5c964fe2
 The two strings that returned the collision: 0U548PU46DQXENI4B8X5YO91SFUACYA3 ,  9MKOSF4U5HA0R2BV6UCFVXH1EA7F01QP
---- 4.17757105827 seconds ----
Kaibos-MacBook-Pro:Assignment2 kaiboma$
```

(Fig. 5) Output for program

Procedure:

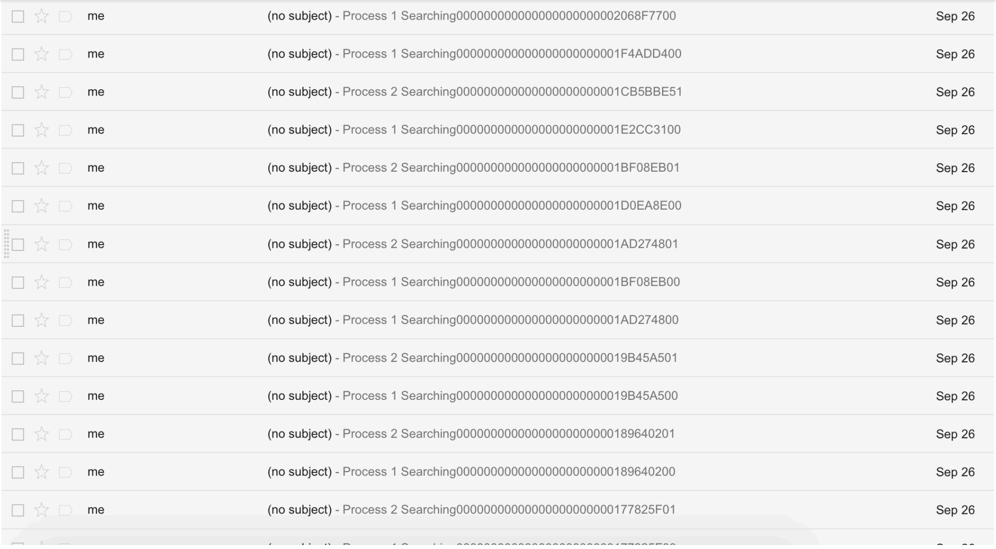
I utilized zilb.crc32() instead of pycrc because it ran with less machine cycles. I took the alphabet and randomly generated 32 letter long strings. It would then hash it with crc32 and I will store it in a python dictionary. This will keep on running until we hash another different randomly generated 32 letter long string that has the same crc32 hash value of the collision. The program will check if there is already another value for the dictionary and will output the two strings that caused the same hash value collision. Lastly I would check if the two strings are correct by using the pycrc script to double check the values. (Program can be found here: (https://github.com/kiddo122/Decryption-Programs/blob/master/crc32.py).

IV. PROBLEM #4

Student Number: 3FF8D07459EC440628F2811207257C9E
32 Bit String: 000000000000000000000001CB5BBE51
Found 2nd Collision:000000000000000000000003C5C743AC
The Matching CRC32 Value: 0xA402F581

Run Time:
- 7hours, 21mins on a single process that ran 5.1 billion combinations.
- Then 56 minutes on a multiprocess search that ran to 2.6 billion more combinations.
- Second Collision Occurred 1 hour and 33 minutes after the first collision.

Procedure:
First I ran a search algorithm based off of question 3 that compared my CRC32 value of my MD5 Student Number with a randomly generated 32-bit Hex String. After about 5 hours, I gave up on the algorithm because using random is not efficient as it can have repeated strings tested. Then I changed my algorithm go increment from 0x00000000000000000000000000000000 to 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF. I ran this search over night for around 7 hours and 21minutes with no collision. Then I made my search algorithm search with multiple processes. It took just under an hour to search 2.6 billion more combinations from where I left off with the previous algorithm that ran 5.1 billion combinations. After about 13 hours of machine searching, I was able to design a faster algorithm to search for collisions that match my MD5 Student Number. Because the search took a long time, I utilized my desktop at home which computes much faster. Because I am at school, I set up email notifications periodically to reassure the search did not crash and once it finished it emails the time and string that caused the collision. Lastly I would check if the two strings are correct by using the pycrc script to double check the values. Single Processed Program can be found here: https://github.com/kiddo122/Decryption-Programs/blob/master/crc32q4hex.py



☐ ☆	me	(no subject) - Process 1 Searching000000000000000000000002068F7700	Sep 26
☐ ☆	me	(no subject) - Process 1 Searching000000000000000000000001F4ADD400	Sep 26
☐ ☆	me	(no subject) - Process 2 Searching000000000000000000000001CB5BBE51	Sep 26
☐ ☆	me	(no subject) - Process 1 Searching000000000000000000000001E2CC3100	Sep 26
☐ ☆	me	(no subject) - Process 2 Searching000000000000000000000001BF08EB01	Sep 26
☐ ☆	me	(no subject) - Process 1 Searching000000000000000000000001D0EA8E00	Sep 26
☐ ☆	me	(no subject) - Process 2 Searching000000000000000000000001AD274801	Sep 26
☐ ☆	me	(no subject) - Process 1 Searching000000000000000000000001BF08EB00	Sep 26
☐ ☆	me	(no subject) - Process 1 Searching000000000000000000000001AD274800	Sep 26
☐ ☆	me	(no subject) - Process 2 Searching0000000000000000000000019B45A501	Sep 26
☐ ☆	me	(no subject) - Process 1 Searching0000000000000000000000019B45A500	Sep 26
☐ ☆	me	(no subject) - Process 2 Searching00000000000000000000000189640201	Sep 26
☐ ☆	me	(no subject) - Process 1 Searching00000000000000000000000189640200	Sep 26
☐ ☆	me	(no subject) - Process 2 Searching00000000000000000000000177825F01	Sep 26

(Fig 6.) Email notifications while I was away from my home desktop showing two processes checking odd and even respectively.

REFERENCES

[1] *"Cryptanalysis of the Playfair Cipher." Practical Cryptography. James Lyon, n.d. Web. 26 Sept. 2016. <http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-playfair/>.*

[2] *Ma, Kaibo. "Decryption Programs." Git Hub. GitHub, Inc., 28 Sept. 2016. Web. 28 Sept. 2016. <https://github.com/kiddo122/Decryption-Programs>.*