CS1653
ASSIGNMENT #1
CIPHERTEXT

C O V I D C O V I D C O V I D C

ECI OUCH PTDVWJVV DM YMFTMKBLPU OPLU
AZAVCUZ GRW VVDH ECHXOGHZL VVSK WQG CA BXKG
VAVKUIUHPH OW FQAKTHVS OPH PSSB VVSK WI VVZ 36
IVUWBUPGBO GRW APAW UIVULV HCM FQRZ WI VVZ 35
BRQZN GRW INMG VC YMFTMKB WJWN UHUGVOH KB V 35
OLVVPJ UGDJALVCMG BQI PAHF O FIVKGFQ H2OHQQCHDWQ 42
CBY BXGB V JUWHZ NRTQZ WQ CZG SHAG JN WJS XQVECQMUGR 42
GMQIHC A VWPHQW VVZ KRFS TWX WGZL IQF WWWJ CA 36
BKGGZ AWGDN BRC DMQYCHZ OLVVPJ UGDJALVCMG QCAZL 41
FU1653 JDOHPSMM DDQ123 RPHTS VJF123 KG TWXT DDBW 31
WGZZQCAZ AHROMIUG HCM ZQFYA ZKHC IDUVZA VJOMM 39
WJWN ZHRCNQWQFT ELVV OPH VO QQFVCMHKB WA GRW 36 37
GJTYGR NBHR CIM XUW1O HPHDZHNM KMQ CBY XDRSM AFCB 41
TWXT VVVGYF DBWGB YWFWAZVW CBY AXDADB LV UI MLVVZZ 42
FCGZ AXDADB D TSVLPG TDTH FSNKUKPDVJ ACPZ DRDMVDEV 43
DN BQI CIYG ZDBVNS YWFWAZVWCHDWQ CPJGW AGZZ 37
VQZPBLQB TWX OOT KKQCNM VQ WHXOGAVVW C PVALE YVALVYD 11
MACADVDVWJV WQ SIAXTS OPDV MJC JGH ACON DJQQVG JV
WJWN AWGD JN WJS VAVKUIUHPH

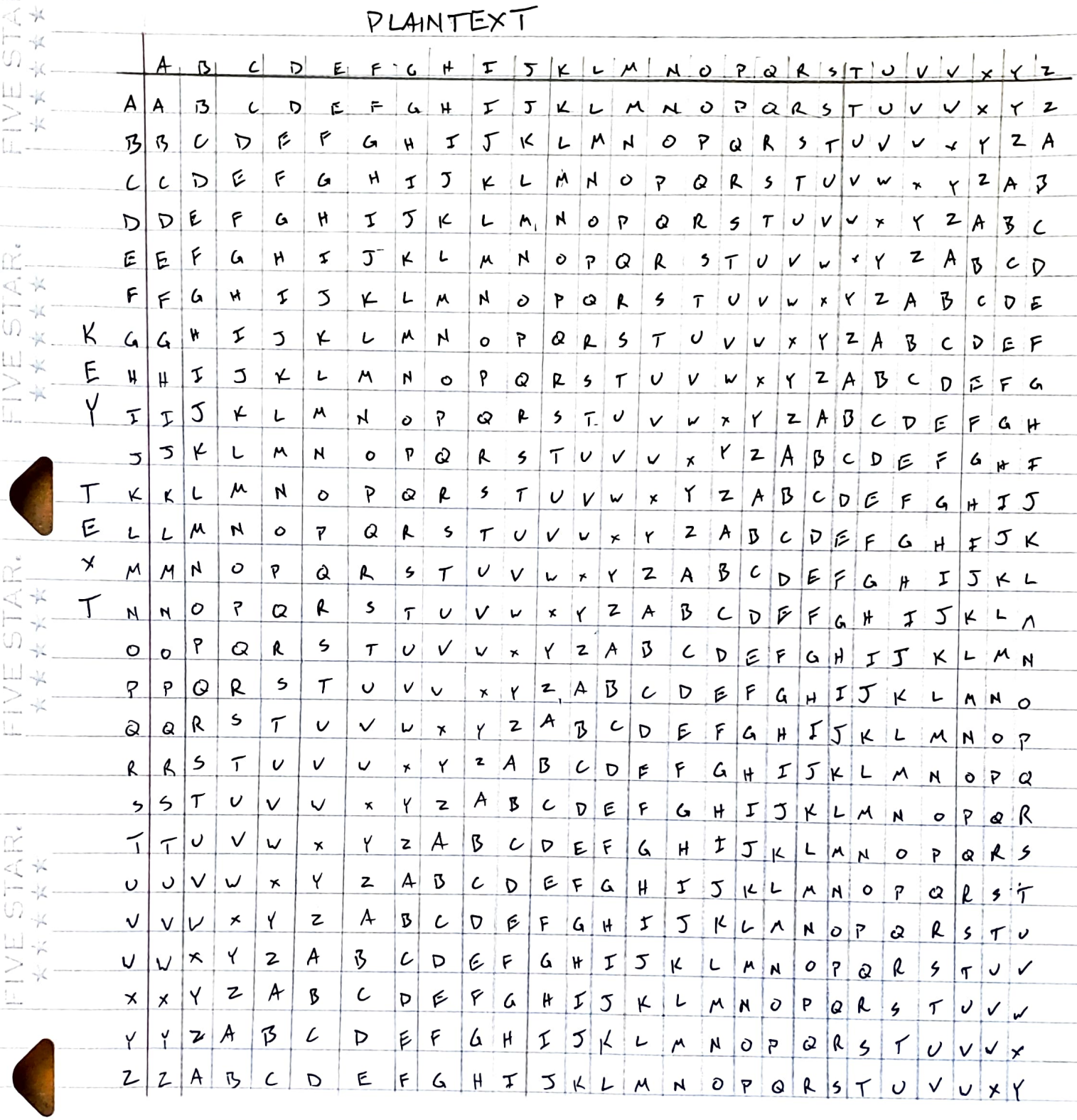
Assumptions:
- Ignore whitespace
- Ignore non-alphabetic characters
- We know that FU (ciphertext) maps to CS (plaintext) → FU1653 = CS1653
- Distance is counted starting at 1st char after 1st instance of substring thru last char of 2nd instance of substring
- Can likely assume ddq123 → abc123 because all of CS department formats their submission instructions the same way, usually "abc123 where abc123 is your..."

Substring	# Occurrences	Distances (btwn consecutive instances)
LVV	5	1-2: 121, 2-3: 140, 3-4: 105, 4-5: 100
VVZ	4	1-2: 35, 2-3: 135, 3-4: 250
TWX	4	1-2: 80, 2-3: 125, 3-4: 130
DBW	3	
AZV	3	
AZVW	3	
VVC	3	
AZVWC	3	
GRV	4	1-2: 75, 2-3: 30, 3-4: 295
VWS	3	

Distances	Factors (>2, <20)
295	5
250	5, 10
140	4, 5, 7, 10, 14, 20
135	3, 5, 9, 15
130	5, 10, 13
125	5
105	3, 5, 7, 15
100	4, 5, 10, 20
80	4, 5, 8, 10, 16
75	3, 5, 15
35	5, 7
30	5, 6, 10, 15
121	Based on trending data, assume 121 to be an outlier

Most Common Factors	Freq
5	12
10	6
4	3
7	3
3	3

Highly likely that key length is 5


PLAINTEXT
KEY
TEXT
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

KNOWN: · FU maps to CS
· Those will relate to consecutive letters of the key
· Assume 5 letter key

F=D, U=C

Possible keys: DC___ 1
_DC__ 2
__DC_ 3
___DC 4
C___D 5

1 E C I O U C H P T D V W J V V D M Y M F T M K B L P U
B A _ __ Z F ___ S U ___ A K ___ Q K ___ M S

2 E C I O U C H P T D V W J V V D M Y M F T M K B L P U
_ Z G ___ E N___ T H__ _ J W___ J I___ R

3 E C I O U C H P T D V W J V V D M Y M F T M K B L P U
__ F M_ __ MR___ G T_ __ V K___ H Z___

4 E C I O U C H P T D V W J V V D M Y M F T M K B L P U
___ L S__ _ Q B_ __ S T __ _ J D___ Y A__

5 E C I O U C H P T D V W J V V D M Y M F T M K B L P U
C__ _ R A_ __ A T___ S B_ __ C R___ I N_

Based on 1-5, 1/2/3 look pretty unlikely due to the number of Z's distributed throughout. Going to check 4/5 against ddq123... vjf123 ⇔ abc123... abc123

Plaintext	ABC ~~DDQ~~ 123 WHERE ABC123 IS YOUR
Ciphertext	DDQ123 RPHTS VJF123 KG TWXT
Key	DCO VIDCO VID, COVIDC

COVID

KEY IS LIKELY COVID

Decryption:

GRV = YOU LVV = ITH

VVZ = THE TWX = YOU

CON GRAT ULATIONS BY DECRYPTING THIS MESSAGE YOU HAVE COMPLETED STEP ONE OF THIS ASSIGNMENT TO COMPLETE THE NEXT STEP OF THE ASSIGNMENT YOU MUST SUBMIT THE CODE OF THE TOOLS YOU ~~MUST SUBMIT THIS~~ USED TO DECRYPT THIS MESSAGE IN A GITHUB REPOSITORY YOU USED A KASISKI EXAMINATION AND THEN A BRUTE FORCE ON ALL KEYS OF THE DISCOVERED LENGTH S SUBMIT THE CODE YOU USED FOR BOTH OF THESE STEPS TO A PRIVATE GITHUB REPOSITORY NAMED CS1653 VIGINERE ABC123 WHERE ABC123 IS YOUR PITT USERNAME SEPARATE THE WORDS WITH DASHES SHARE THIS REPOSITORY WITH THE TA VICTORZHZ IF YOU SOLVED STEP ONE USING ENTIRELY PEN AND PAPER SCAN YOUR HANDWRITTEN DOCUMENT AND SUBMIT IT IN EITHER CASE SUBMIT A README FILE DESCRIBING YOUR APPROACH IF YOU HAVE LITTLE DOCUMENTATION ABOUT YOUR SOLUTION YOU MAY CHOOSE TO IMPLEMENT A BASIC KASISKI EXAMINATION TO ENSURE THAT YOU GET FULL POINTS ON THIS STEP OF THE ASSIGNMENT