CSIGNMENT #1 CIPHERTEXT

1 1 1 1 0 0 1 1 0 C 0 1 1 0 C -ECI YOUCH PIDVUJVV -DM YMFTMKBLPU -OPLU AZAVČUZ CRŮ NUDH ECHXOGHZL NVSK NQG CA TXKG VAVKUÍUHPH OÙ FOAKTHŮS OPH PSSBUŬSK WIJVZ 36 FVUVBUPGBOKRUTAPAN VINULV HEM FÄRZ VITWI 35 BROZN GRW INMG VC YMFTMKB WSWN WHUGVOH KBV 35 OLAVUP OCO ALVEMG BOT PAHE TO FIVEGER HZOHOROCHOWA 42 CBY TXGBN JUNHZ MRTQZ NO CZG SHAG ON NJS YQVECQMUCR CGMQTHC A VWPHQW WYZIKRFS TUX WGZL FQFNWWS CA 42 BKOGGZ AUGDY ÉRC DMQYCHZ OLVUPS UGDSALVCMG QCAZL ॐ FUIGS JOHPSMM DDQIZZ RPHTS USFIZZ KG TWXT DDBW WGZZQCAZ MA AHROMIUG HCM ZQFYA ZXHC IDÜVZA USOMM MOW WJWN ZHRCHQWAFT ELVV OPH VO QQFVCMHKB WA GRU 41 31 39 MGSTYGR MBHR CIM XUNIO HTHDZHMM KMQ CBY XDRSM AFZIS 36 37 TWAT VVV GYFDBWGB YVFWAZVW CBY AXDADB LY UT MLYVZZ 41 FLGZ AXDADIS D TSVLPG TOTH FSMKUKPDW ACPZ DEDMUDEV 42 DN BOI CITY ZDBUNS YNFWALVINCHONG COSCW ACTZ 43 VÖZPBLABTUX ÖNT KKÁCHM VÁ WHXOCALUW É PVÁLE YVALÚYD II MAČADVÖVWJV VÁ STAXTS OPDV MJC JEH ACON DJAQVG JV NJUN AWGD JN WJS VAVKUJUHPH

Assumptions: . Ignore whitespace

· Ignere non-alphabetic characters

· We know That FU (ciphertext) maps to CS (plaintext) > FU1653 = CS1653

Distance is counted starting at 15th char offer 15Th instance of substring thru lost char of 2nd instance of substring

· Can likely assume ddq123 -> abc123 because all of CS department formats their submission instructions three same way, usually "abc123 where abc123 is your..."

- ~	Substang	# Occurrences		tun consecutive instance	(ts)
\checkmark \star	LVV	5	1-2:121, 2-3:	140, 3-4:105, 4-5:100	
0 *	VVZ	4	1-2: 35, 2-3:1	35, 3.4: 250	
LUK	TUX	4	1-2:80, 2-3:1	ás, 5-4: 130	
2 ×	DBW	3	,		
Colons	AZV	3			
	AZVW	3			
- <u>~</u>	VUC	3			
X X	AZVINC	3			
10 ×	GRU	4	1-2:75, 2-3:30	3-4:295	
— Д *	VWS	3			
		\vee	າ		
	Distances	Factors (20)	Most Common Factors	Freq
	295	5		5	la
_ č	250	5, 10		10	6
4 *	140	4,5,7,10,14	,20	4	3
0 *	135	3,5,9,15		7	3
U.X.	130	5,10,13		<i>-</i> 3	3
	125	5			
	105	3, 5, 7, 15	/		
	100	4,5,10,20			
e C	90	4, 5, 8, 10, 1	6	Highly likely	that
- F 4	75	3,5,15		kay length	73 5
₩.	35	5,7			
	30	5,6,10,15			
L	121		rendong data, a	26sume 121 to be an	author
) - '		

PLAINTEXT 2 I JKLM NOPQRSITUVXXX E FIG H [5] D LU K A 13 I Parstuvvx D 7 K M O 7 Z 4 H N 13 1 T Μ ZA 3 \mathcal{C} ワ G I ĸ P 5 T J H L H O Q 4 1 E H ۴ 7 D G W Н O v w C I K L 7 Q R 5 Τ U A 3 ٢ E ۶ I 7 0 D G H K Н R T VY 2 L M P Q 5 V O 3 C F E T J_ L E G H K И Z A M 0 7 Q R 5 T U CD B F F 6 H I 3 - K ۴ L М И O PQ 4 T U 4 В K V × c DE K 4 H I 3 K M M 4 L U Z 0 P Q R 5 T × ٢ A В V V C 0 EF E H I J γ H L М P И 2 U BC O Q R 5 T V W × 4 FFG D 5 I 4 I L М Ч 7 Q R 5 T. U Z A ß CD 0 ን V W E FGH K 7 L M r И 3 0 P Q R 5 T v V 2 Α V BC D E M T И 5 K P K L 0 Q R T U Y Z A B COE V W × F H I 5 E L M H 0 Q R 5 Z L 7 A DEF T U V v 4 B ۴ C G × M И 0 M P Q R T U B C 5 2 Α V * 4 E 7 W D I JK L G T R 5 0 7 Z M Q H T U V × 4 A B C V E F 5 D H I 8 5 Q R V 3 T U ZA CD 0 V 4 0 × E F GH IJ KLMN R 5 T ZAB 8 P 0 U V XY D F IJ C E G H K MM R 5 T A V ✓ 2 Q Q $\boldsymbol{\nu}$ Y 3 C IJK ۲ D E F GH MNO 5 2 Α T v V V 4 Β CD GH R B * ۴ ٤ I JK L Μ OPQ N 5 T U A Y B 5 V V × 2 C D E F G H IJKLMN Q R OP 1 U V A B T W Y C IJK × Z D EF 6 H LMN QR5 0 P o V A \mathfrak{V} W Y Z U Х C 巨 F D G H I 5 KL MM 0 7 R 5 T Q A Z V V × 4 B C D E ٧ F T 5 K 6 G H ٨ N OP R Q STU × 4 2 A 飞 C V D E F 6 5 H I K L M 0 7 R 4 N JV Q T Z A C Y B × E F I × P 6 H 5 K L P UVV M N 0 Q R 4 T A B L 5 K V 2 D F F 6 H I R 3 N Q 1 0 ٦ U VVX 2 A E D JKL 4 H I MN OPORST VUXY U

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

F=D, U=C

Possible keys: DC _ _ _ 1
_ _ DC _ _ 2
_ _ DC _ _ 3
_ _ _ DC _ 4
_ _ DC _ 4

BA _ _ ZF _ _ SU _ _ AK _ _ _ QK _ _ MS

LECF OUCH PT DV WJVV DM YMFTMKBLPU -ZG _-E N__-TH__ J W___JI__R

JECF OUCH PTDVWJVV DM YMFTMKBLPU -- F M--- MR---GT- -- VK--- HZ---

4 ECT OUCH PTDVWJVV DM YMFTMKBLPU

SECT OUCH PTDVWJVV DM YMFTMKBLPU

--- -RA- --AT---S B_ --CR___IN_

Bused on 1-5, 1/2/3 look pretty unlikely due to the number of Z's distributed throughout. @ Giving to check 4/5 against ddq123...vjf123 = abc 123...abc 123

Plaintext ABC DDQ 123 WHERE ABC 123 IS YOUR Cophertext DDQ 123 RPHTS VJF 123 KG TWXT Key DCO VID, COVIDC COVIDC

KEY IS LIKELY COVID

Decrypton:

GRU = 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 LODE OF THE TOOLS YOU MUST SORMET THE USED TO DECRYPT THIS MESSAGE IN A GITHUB REPOSITORY YOU USED A KASISKI EXAMINATION AND THEN A BRUTE FURLE ON ALL KEYS OF THE DISCOVERED LENGTH S SUBMIT THE CODE YOU USED FOR BOTH OF THESE STEPS TO A PRIVATE GITHUR REPOSITORY NAMED CS1653 VIGINERE ABC123 WERE ABC123 IS YOUR PITT USERNAME SEPARATE THE VORDS 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