TECHNICAL REPORT 1937-213C

THE SPYCLIST CIPHER CLOCK
(THIRD ADDENDUM)

Prepared for

OFFICE OF THE DIRECTOR,
BUREAU OF SECURITY AND SIGNALS INTELLIGENCE

CONTENTS

5. CRYPTANALYSIS OF THE SPYCLIST CIPHER CLOCK

C. CRYPTANALYSIS BY COUNTING DIGRAMS

The rationale behind this attack is that if the text is long enough, then when we encipher the next letter of a text, then the hands on the cipher clock move at most 26 steps. Since there are two more characters in the ciphertext alphabet, there are no double letters in the ciphertext and the other missing digrams indicate what letter(s) is found on the key just before the last ciphertext letter that we wrote down.

To show how it works, we will work through an example in two methods. Here is the ciphertext:

XAYIHVBS+URMXE#+WBQPSTGXECXCXPA#OCATLXVBEQSZYB#DTAJSNEKGJDVWEAXA#G
BNGQWJQXOJEGPXJLFXFESFMWDOWEKEJFPWE#CABSYUWSKOLZDMH+BIBYTJQYUECVAU
EOCSPKWLGM#HIEWNEJKCUBSXMSEQVALMNTUBSNBMD+OJEQGADBPGYPHYQJVHBHIBTD
KTAPCEUMI+WEHNGZIDVQXZENWAQBPFHJKMSYOBUORLGNBLZ#+QAWPRIEOVY+#RVYUF
CHO#UZJ+DVUNAT+NF#UPXKOPYRSZ#STJHKNSMPRDVXTGEKITAPLUEJ+OVR+SUPJPZK
GNGDWCXIPJDIXCPBYOQMSLZUJVNXED+QG+WENUGCN#OFEPATLMPDWLCDEOATAP#D+Z
+CFORQLUZPXQ+ZGOKTA#NKMPG+MQLZUJVNB#ADBNALQ#E#KLND+XUF#BL+E#GOBHDA
#DTAGXPXIYUVBCYOJ#TQD+WDLIO+NJKB+TDRUZRNG#H+JW+PSE#NRD+XUSLHZSRNXS
DXZGKIJEUYXCPVOMHGHSLNULRZPU+UNO#EGEAPEXUFWEACWJYIEMLHJXNOWLIQYXKV
XV+GRCMPYKOJDP#DJZGVPOVUBIQGAZIHUYX#RLWBSL#DSGTBEV+PSKEDLGRLORQYVJ
QWBGBZMDAWCUQ+IKET#PISD#QPVSZGTLTDZODTUO+MEKO#FXOMXCOGZIDVUNAXKREN
OQ#FHVAW#UIVPSKGJVRNGQVMDJYBPQBQ#FHOMSFECWORYQSZLMK+ZFPSIJQCEHXSED
HNJQJGZOBPSBQMGUJOMSFECWORYQSZLMK+ZFPSIJQCEHXUJ#MHMPAEGBNXEIDUWCDK
+OQYXKMSIVOPBZKQDRGWZSHBYTAPLXB#CSF#SMAYMEJPTHJWGNBYN+UCZMBL+WCSMT
GYJOUBHJQZF+ILIESECK#FXIVRXMSENJGQJQDVXECSJU+UKSPAUFBOYVJVJMRVJ+BW
CUQKXEJPA#ELVJS+QR#VSEASOGUIMCGDEUYXVYJYLNETQEZO#PQRO+NKMXZOSVASNK
LZJFAPWCE+FJVGMKMXDZ#RXMSNSMJNB#XB+JEMNDI#YSKWAP#SRU#H+JABHNQEOLED
ASYTCPYOSGMIVGOJQAKUCLXJRNUCPAIHVBDU#LMR+OTLGIZUF+KGXNRDLUMIDZLCOB
GZIJHGCYPEGTJ#DUAVAVH+MJRJEYQDRGLHXT+BVF#KSREJCXC#RV+RLGBQNBYTAPDN
DKMXSLHUJHKHJBDGIUNTWBV+KTAJVGMK#AUYFZSNOGKRHBTXUJNKDT#JRFEUMIHOBX
AEILWTCZSJ+KTAPGIFI#GD#FS+VZLZGJBTCXB+JEMNDUPKXEVL+E+MDWDGHIEWTAPG
AZVR+SUGL+EYSWTBI+JZFAVFV#N#R#FSFPJOWJ#ILMIXVZOPBPS#PA#+KBSZ#GPELO
ROXOHYNEHTJZ#T+J#TPKVZDBPD#OJHEJDHDGQEAWGNBJ#OPCMKBR+IVSCOHYQJUGQ+
XZKDGEGXGAZVR+SUXAEYGZIULT+XNXBPJNFUI+UTGLGKOYBLJWMKDFJWBVDRE#FHVY
BLSCSZSNK#XHQDEAGNBTJDVZUZF+EUVYPKBSDJXAGAYSLUZG+VIAOHESYJT+HIWOXB
CLVQNR#AXUXZNPBRQ#XFHIEWDA#QUDHIXYFZS+JYSPKBDHJSNOACE#KECUIHVYDNHV
JDWXHMKDYPGEN#FHJBEVCXUOELYJWMKDTETDSAUCUIECXF#CXPHSZLV+KVUXBJ+EKP
KDHLH+PX+TGWTK+HBLXECTJO#VZSVAWQJAUSZKXHSIJOZF+EW#UNKP+XQJUJEYLMNP
SWIWBUSPFJUBDVZVFTXCFEGWP#SNBMDWBC+QNPHOBJRTBPUZJHCGQJBZ+DTQYXCKMX
DGRMPYJRLRNG#DJZVLICVHEJKPAVF#EM+VYQDUBDXUJWBYDUGYXFCOFEBLGJHUYQJH
LT#DTETPRI#PJFC#VF#RVXAHUY#WQEUGWCJ#EIAGVB#AIDORQYOQZLGMLVQXYXTXBQ
YNRDJ#BZ+FZSY#LZOTLMDAPILIPYUI#HBFSR+RVAV#L+OMKVUZENUAQBPFHDIVXDJS
UYFOROSXMATLGXPZ#DSCLUXUIMPKECUGTLRXSTYGZIF+PEWPIFYGOIJVAWDVL+UZPO
WDLHEXZT+EQLXCZDJUVCOPBHYMBZBZHXGEUGPNDW#HSE#MXJRBSRNDGZH+JQCPE+SU
IMNDKVEXUFCPTLDHMB#V#GW+UAPXNSZPGSAYPVHYXJWMLFZF+#Y#+CUZI+ACVBSMAY
QJVUGQMDXBPECUQ+NJVXVGBCP#LIUWSZYXTQYUJ#LXCVCWOUZT+IZJBNYSBDIPSXCZ
TXLEMNYQJVLIEANOKEBQYXFCXYVQWPDOALM+NGTJFPYBLIPGCKMJDWEALHPHOROVGH
IEWDYJNDUZSYOS+DLXMAJHJL+OMK+CDECD+KTFPDXCOMPVHC#YSMOKSZRXLTHJOE+U
PKRUCGLUXBEAORXPHEQSHRXMKL#IS#TDUG+PCDIVAI+WZ#BMJ#LSROUKL#I#LOXQTJ

UGCX#SR#CPYTLQDUBZDEVLI#FHFLFAEBSTPY+UK#OWJLTDJZF+QP#LUEHXVMCWJYQJ
NB#+WGBCTQGKUGLPFXOASABRZ#KMKDZTXSTAPYXJFXAEBSNGZIB#IBFPSIPQUIJBJ#
HFCPNVEJ#YJHSEXBEQEQ+RVKXYVFSY+U+OQRMVWDQBWQUQPY+LNR#FXEOJWJALFJGT
#SL+TABIE+FNREJKVXPIV+RTXNOHJLSZJBDKVHIBTAIUQNUIPA#ORQRZLDUBTHZOXS
MJQYXCZPIEOJWJALSXHDHMGCJQZF+ME+BIFECUSYOTQXAVUZDTAG#HTBTCUKOQGDLF
ZC#SMNEQSHFJMKL#+XGWJUXSURVKX#CEGMAUILWOSGAWOWCENO#FHJKPYR#EMZDVZ#
+NOVB#HIBY+UY+PFNA#+SY

i. BY TABULATION

The first step in the attack is to tabulate all of the digrams in the ciphertext. Remember to count *all* of them. The first four letters are XAYI; from them we get XA and AY and YI; don't forget that one in the middle. We don't need to count the digrams, just make a table of all the ones that exist.

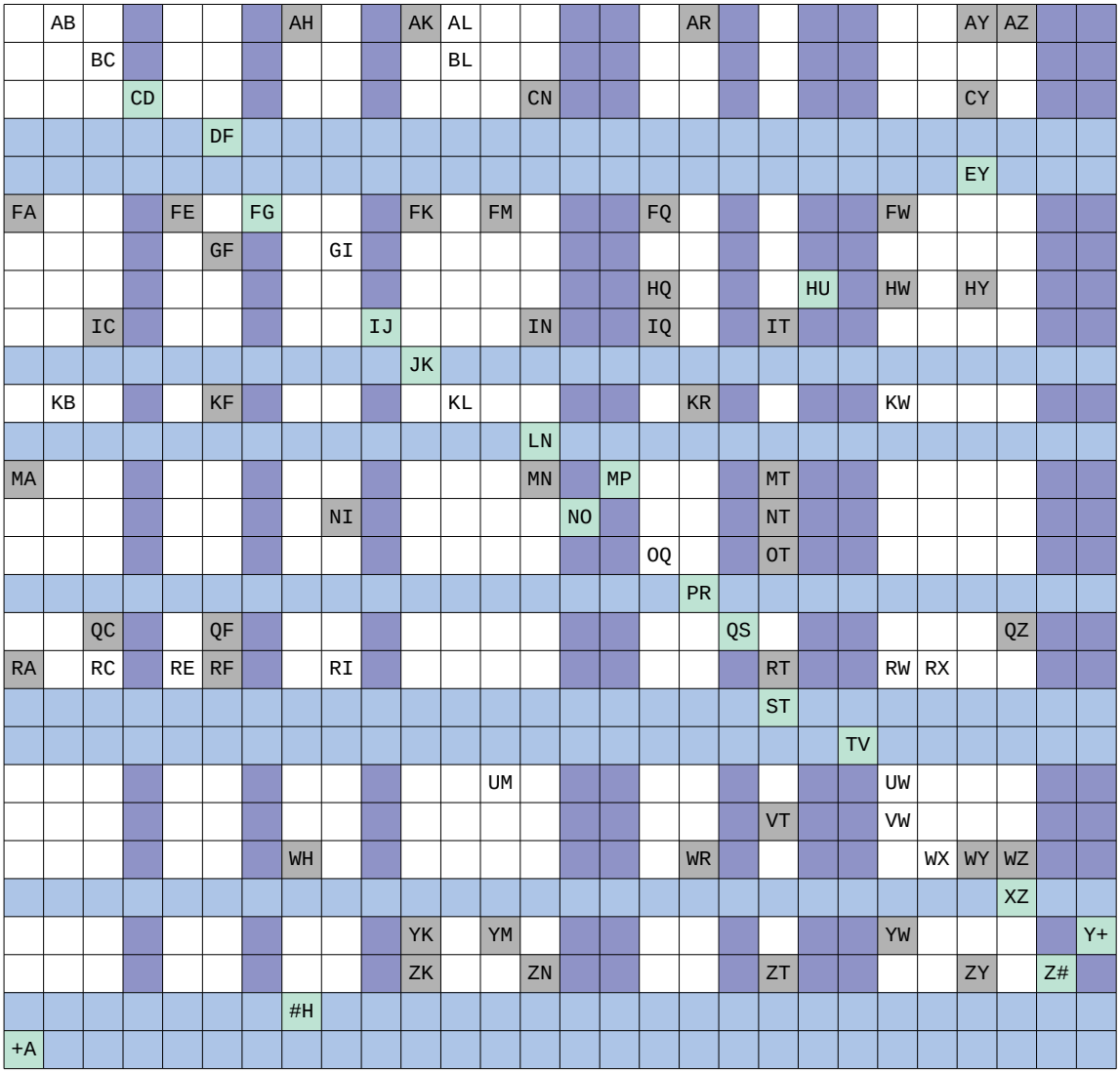
AB			DB	EB	FB	GB	HB	IB	JB	KB		MB	NB	OB	PB	QB	RB	SB	TB	UB	VB	WB	XB	YB	ZB	#B	+B
AC	BC			EC	FC	GC	HC	IC	JC	KC	LC	MC		OC	PC	QC	RC	SC	TC	UC	VC	WC	XC		ZC	#C	+C
AD	BD	CD		ED		GD	HD	ID	JD	KD	LD	MD	ND	OD	PD	QD	RD	SD	TD	UD	VD	WD	XD	YD	ZD	#D	+D
AE	BE	CE	DE		FE	GE	HE	IE	JE	KE	LE	ME	NE	OE	PE	QE	RE	SE	TE	UE	VE	WE	XE		ZE	#E	+E
	BF	CF	DF				HF	IF	JF		LF		NF	OF	PF		RF	SF	TF	UF	VF		XF	YF	ZF	#F	+F
AG	BG	CG	DG	EG			HG		JG	KG	LG	MG	NG	OG	PG	QG	RG	SG	TG	UG	VG	WG	XG	YG	ZG	#G	+G
AH	BH	CH	DH	EH	FH	GH		IH	JH	KH	LH	MH	NH	OH	PH		RH	SH	TH		VH		XH	YH	ZH	#H	+H
AI	BI		DI	EI	FI	GI	HI			KI	LI	MI		OI	PI		RI	SI		UI	VI	WI	XI	YI	ZI	#I	+I
AJ	BJ	CJ	DJ	EJ	FJ	GJ	HJ	IJ			LJ	MJ	NJ	OJ	PJ	QJ	RJ	SJ	TJ	UJ	VJ	WJ	XJ	YJ	ZJ	#J	+J
AK		CK	DK	EK		GK	HK	IK	JK			MK	NK	OK	PK	QK		SK	TK	UK	VK		XK	YK	ZK	#K	+K
AL	BL	CL	DL	EL	FL	GL	HL	IL	JL	KL		ML		OL	PL	QL	RL	SL	TL	UL	VL	WL	XL	YL	ZL	#L	+L
	BM	CM	DM	EM	FM	GM	HM	IM	JM	KM	LM			OM		QM	RM	SM		UM	VM	WM	XM	YM	ZM	#M	+M
AN	BN	CN	DN	EN	FN	GN	HN		JN	KN	LN	MN			PN	QN	RN	SN		UN	VN	WN	XN	YN	ZN	#N	+N
AO	BO	CO	DO	EO	FO	GO	HO	IO	JO	KO	LO	MO	NO		PO		RO	SO		UO	VO	WO	XO	YO	ZO	#O	+O
AP	BP	CP	DP	EP	FP	GP	HP	IP	JP	KP	LP	MP	NP	OP		QP		SP	TP	UP	VP	WP	XP	YP	ZP	#P	+P
AQ	BQ		DQ	EQ		GQ	HQ	IQ	JQ	KQ	LQ	MQ	NQ	OQ	PQ		RQ		TQ	UQ	VQ	WQ	XQ	YQ		#Q	+Q
	BR		DR			GR	HR		JR	KR	LR	MR	NR	OR	PR	QR		SR		UR	VR			YR	ZR	#R	+R
AS	BS	CS	DS	ES	FS	GS	HS	IS	JS	KS	LS	MS	NS	OS	PS	QS	RS			US	VS	WS	XS	YS	ZS	#S	+S
AT	BT	CT	DT	ET	FT	GT	HT	IT	JT	KT	LT	MT	NT	OT	PT	QT	RT	ST		UT		WT	XT	YT	ZT	#T	+T
AU	BU	CU	DU	EU	FU	GU	HU	IU	JU	KU	LU		NU	OU	PU	QU	RU	SU	TU		VU		XU	YU	ZU	#U	+U
AV	BV	CV	DV	EV	FV	GV	HV	IV	JV	KV	LV	MV	NV	OV	PV	QV	RV	SV		UV			XV	YV	ZV	#V	+V
AW	BW	CW	DW	EW	FW	GW		IW	JW	KW	LW	MW	NW	OW	PW	QW		SW	TW	UW	VW					#W	+W
AX	BX	CX	DX	EX	FX	GX	HX	IX	JX	KX	LX	MX	NX	OX	PX	QX	RX	SX	TX	UX	VX	WX		YX		#X	+X
AY	BY	CY	DY	EY	FY	GY	HY	IY	JY		LY		NY	OY	PY	QY	RY	SY	TY	UY	VY		XY		ZY	#Y	
AZ	BZ	CZ	DZ	EZ	FZ	GZ	HZ	IZ	JZ		LZ	MZ		OZ	PZ	QZ	RZ	SZ		UZ	VZ	WZ	XZ				+Z
A#	B#	C#	D#	E#	F#	G#		I#	J#	K#	L#	M#	N#	O#	P#	Q#	R#	S#	T#	U#	V#	W#	X#	Y#	Z#		+#
	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+	#+	

What is important to us now is which digrams are missing. Of course, all of the diagonal entries are missing, since double letters cannot occur in the ciphertext for a device with this configuration. But look at the J column. The digram for JI is the only other one missing. Therefore, we know that I comes immediately before J in the key.

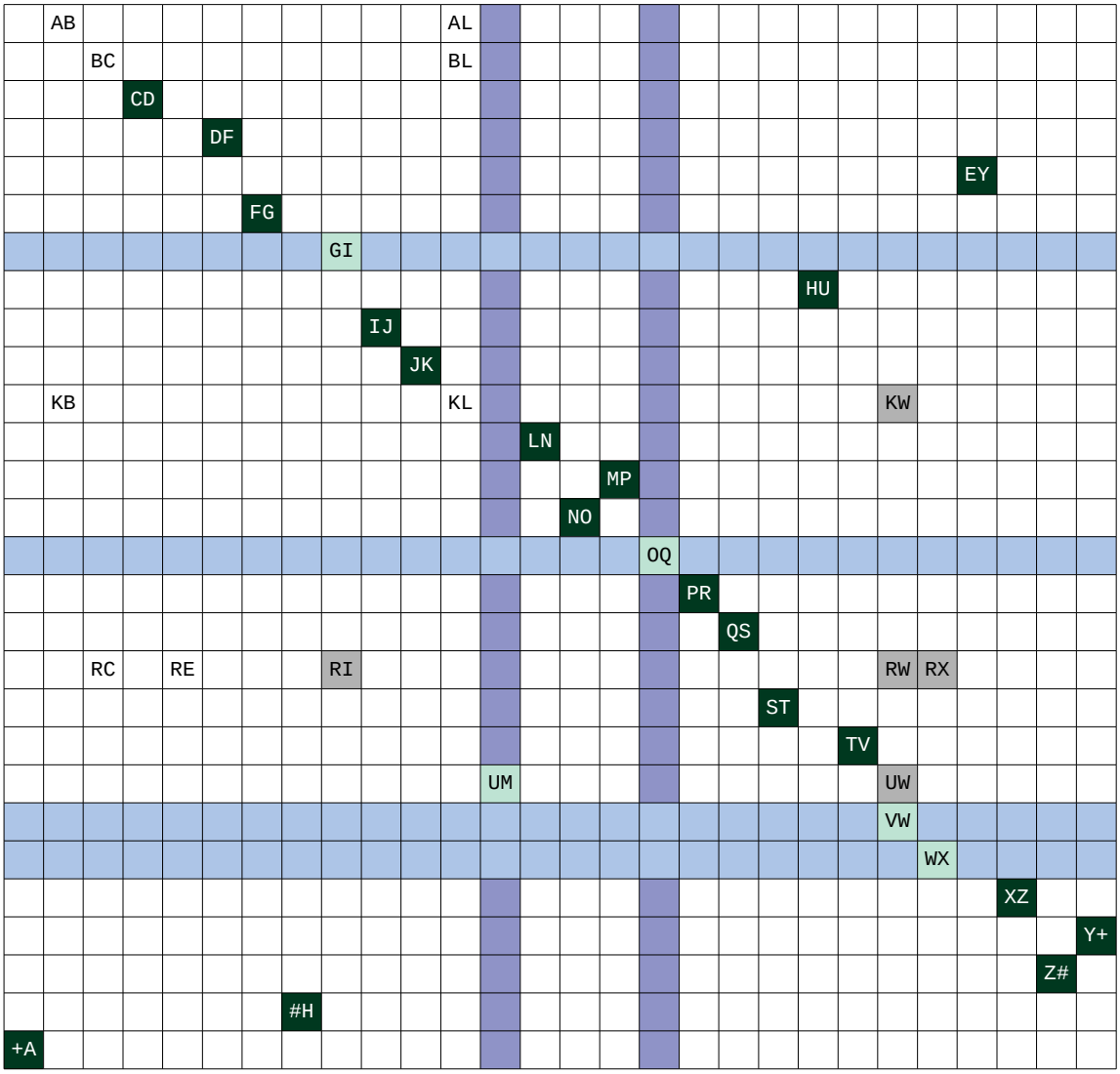
Here are all of the missing digrams, except for the doubles:

	BA						HA			KA	LA						RA							YA	ZA		
		CB									LB																
			DC										NC											YC			
					FD																						
																								YE			
AF				EF		GF				KF		MF				QF						WF					
					FG			IG																			
																QH				UH		WH		YH			
		CI							JI				NI			QI			TI								
										KJ																	
	BK				FK						LK						RK					WK					
													NL														
AM													NM		PM				TM								
								IN						ON					TN								
																QO			TO								
																	RP										
		CQ			FQ													SQ						ZQ			
AR		CR		ER	FR			IR											TR			WR	XR				
																			TS								
																					VT						
												MU										WU					
																			TV			WV					
							HW										RW						XW	YW	ZW		
																									ZX		
										KY		MY										WY					+Y
										KZ			NZ						TZ					YZ		#Z	
							H#																				
A+																											

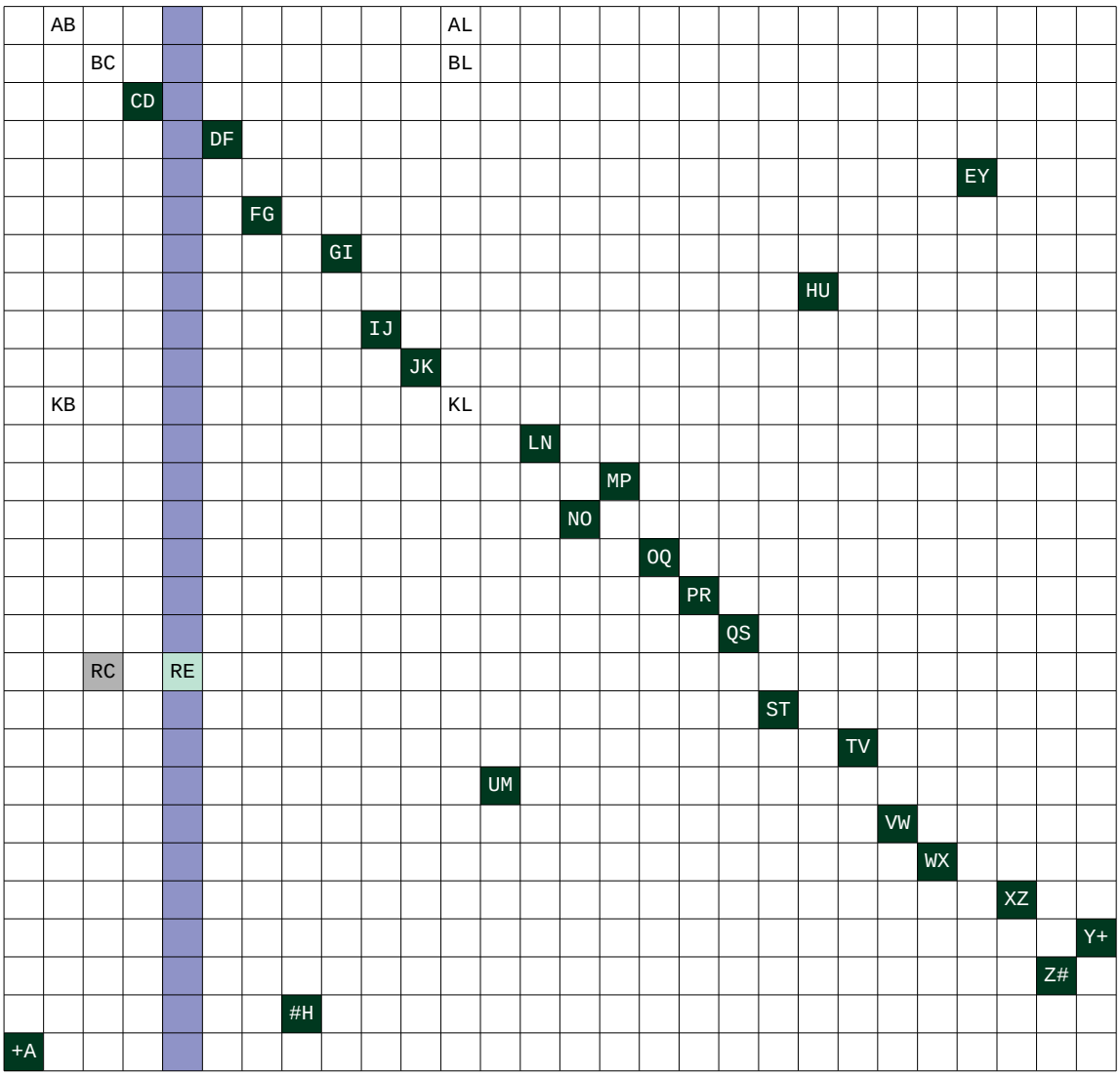
Now don't get confused, but to make things easier, we reverse each missing digram so that it is written in the way it might appear in the key. Here is the new table:



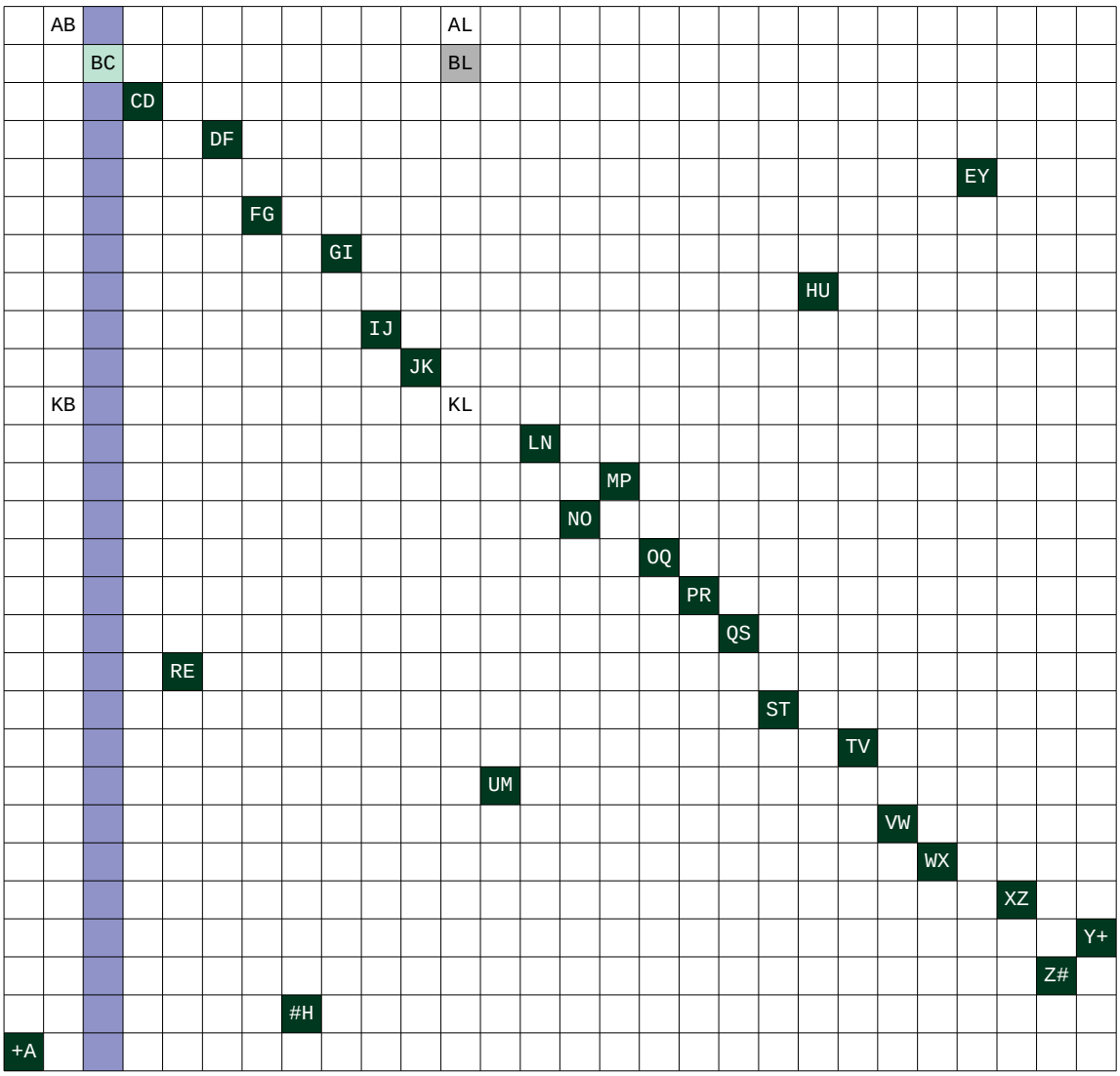
Now we look for any digram that appears alone in a row or column. Such a digram must be in the key. We find CD, FG, IJ, NO, MP, QS, HU, TV, Z#, Y+, DF, EY, JK, LN, PR, ST, XZ, #H, and +A. Once we decide to keep a digram in a row, we can eliminate the other digrams in its column; similarly, once we keep a digram in a column, we can eliminate the others in the same row. We can also eliminate the reversal of any digram that we keep. Here is what is left after we make those deletions:



Now we play the same game and look for digrams that are alone on a row or column in what remains in the table. We find GI, OQ, UM, VW, and WX. Eliminate those rows and columns to get an even smaller table:



Now we get RE and eliminate RC. One more time:



Now we keep BC and eliminate BL. One more elimination won't gain us anything, so we stop.

Here are all of the key's digrams that we have found to definitely belong:

BC CD DF EY FG GI HU IJ JK LN MP NO OQ
PR QS RE ST TV UM VW WX XZ Y+ Z# #H +A

But remember that AB, AL, KB, and KL are still possibilities.

If we chain the definte key digrams together, we get these key fragments:

BCDFGIJK
LNOQSTVWXZ#HUMPREY+A

There are two ways to combine them, but it doesn't matter, since the key goes on a ring. So now we know that the key is something like

LNOQSTVWXZ#HUMPREY+ABCDFGIJK

To find the final key, we need to roll this key to each possible position on the ring and decipher the ciphertext. When we find a recognizably English plaintext, then we have found the correct key. It turns out that the correct key is

#HUMPREY+ABCDFGIJKLNOQSTVWXZ

and the plaintext is (broken into words)

ALL THESE SORROWS ARE PAST MY GLANCING AT THEM MAY NOT BE WITHOUT ITS USE FOR IT MAY HELP IN SOME MEASURE TO EXPLAIN WHY I HAVE ALL MY LIFE BEEN ATTACHED TO THE INANIMATE OBJECTS THAT PEOPLE MY CHAMBER AND HOW I HAVE COME TO LOOKUP ON THEM RATHER IN THE LIGHT OF OLD AND CONSTANT FRIENDS THAN AS MERE CHAIRS AND TABLES WHICH A LITTLE MONEY COULD REPLACE AT WILL CHIEF AND FIRST AMONG ALL THESE IS MY CLOCK MY OLD CHEERFUL COMPANIONABLE CLOCK HOW CAN I EVER CONVEY TO OTHERS AN IDEA OF THE COMFORT AND CONSOLATION THAT THIS OLD CLOCK HAS BEEN FOR YEARS TO ME IT IS ASSOCIATED WITH MY EARLIEST RECOLLECTIONS IT STOOD UPON THE STAIRCASE AT HOME I CALL IT HOME STILL MECHANICALLY NIGH SIXTY YEARS AGO I LIKE IT FOR THAT BUT IT IS NOT ON THAT ACCOUNT NOR BECAUSE IT IS A QUAINT OLD THING IN A HUGE OAKEN CASE CURIOUSLY AND RICHLY CARVED THAT I PRIZE IT AS I DO I INCLINE TO IT AS IF IT WERE ALIVE AND COULD UNDERSTAND AND GIVE ME BACK THE LOVE I BEAR IT AND WHAT OTHER THING THAT HAS NOT LIFE COULD CHEER ME AS IT DOES WHAT OTHER THING THAT HAS NOT LIFE I WILL NOT SAY HOW FEW THINGS THAT HAVE COULD HAVE PROVED THE SAME PATIENT TRUE UNTIRING FRIEND HOW OFTEN HAVE IS AT IN THE LONG WINTER EVENINGS FEELING SUCH SOCIETY IN ITS CRICKET VOICE THAT RAISING MY EYES FROM MY BOOK AND LOOKING GRATEFULLY TOWARDS IT THE FACE REDDENED BY THE GLOW OF THE SHINING FIRE HAS SEEMED TO RELAX FROM ITS STAID EXPRESSION AND TO REGARD ME KINDLY HOW OFTEN IN THE SUMMER TWILIGHT WHEN MY THOUGHTS HAVE WANDERED BACK TO A MELANCHOLY PAST HAVE ITS REGULAR WHISPERINGS RECALLED THEM TO THE CALM AND PEACEFUL PRESENT HOW OFTEN IN THE DEAD TRANQUILLITY OF NIGHT HAS ITS BELL BROKEN THE OPPRESSIVE SILENCE AND SEEMED TO GIVE ME ASSURANCE THAT THE OLD CLOCK WAS STILL A FAITHFUL WATCHER AT MY CHAMBER DOOR MY EASY CHAIR MY DESK MY ANCIENT FURNITURE MY VERY BOOKS I CAN SCARCELY BRING MYSELF TO LOVE EVEN THESE LAST LIKE MY OLD CLOCK IT STANDS IN A SNUG CORNER MIDWAY BETWEEN THE FIRESIDE AND A LOW ARCHED DOOR LEADING TO MY BEDROOM ITS FAME IS DIFFUSED SO EXTENSIVELY THROUGHOUT THE NEIGHBOURHOOD THAT I HAVE OFTEN THE SATISFACTION OF HEARING THE PUBLICAN OR THE BAKER AND SOMETIMES EVEN THE PARISH CLERK PETITIONING MY HOUSEKEEPER OF WHOM IS HALL HAVE

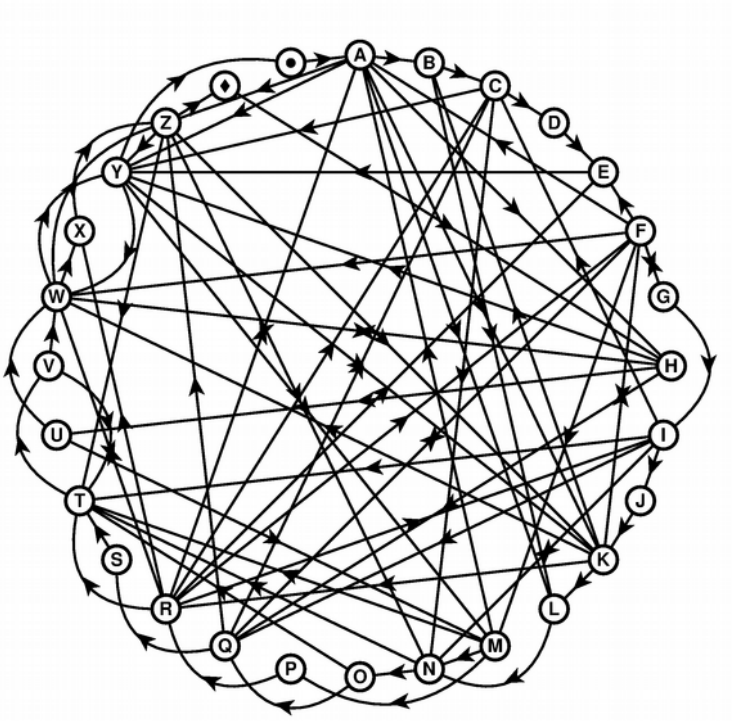
MUCH TO SAY BY AND BY TO IN FORM HIM THE EXACT TIME BY
MASTER HUMPHREYS CLOCK MY BARBER TO WHOM I HAVE REFERRED
WOULD SOONER BELIEVE IT THAN THE SUN NOR ARE THESE ITS
ONLY DISTINCTIONS IT HAS ACQUIRED I AM HAPPY TO SAY
ANOTHER INSEPARABLY CONNECTING IT NOT ONLY WITH MY
ENJOYMENTS AND REFLECTIONS BUT WITH THOSE OF OTHER MEN

You might recognize the text from *Master Humphrey's Clock* by Charles Dickens.

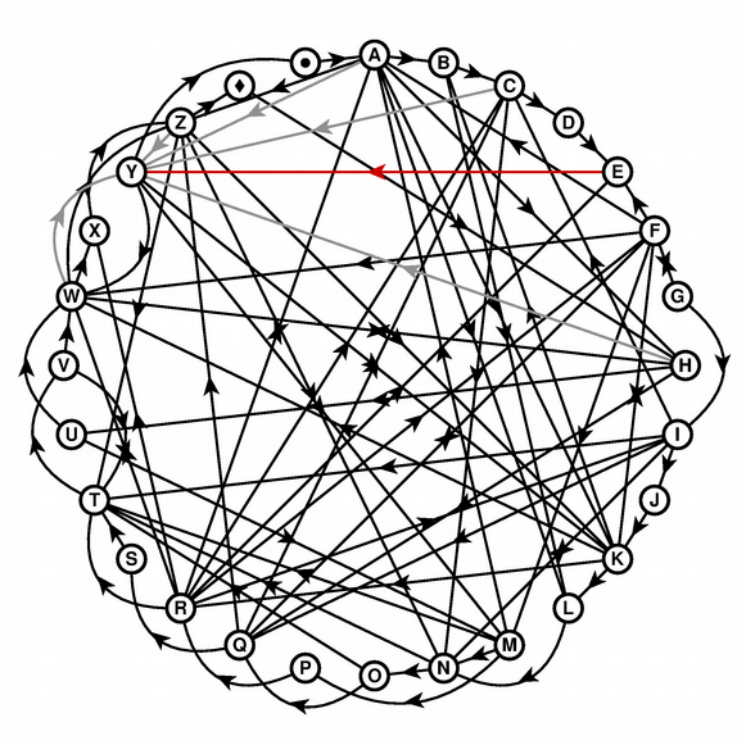
ii. By directed graph

When working with pen and paper, it may be easier to do this attack with a directed graph. A directed graph is a graph whose edges are directed (have a direction). A graph is a set of vertices and a set of edges. A *vertex* is a point, but it can be drawn anywhere; we don't care about coordinates in this kind of graph, and vertices can be slid around on the page. An edge is a line from one vertex to another. In a directed graph, each of those lines has an arrow on it to show its direction. Think of a map in which cities are connected by one-way roads.

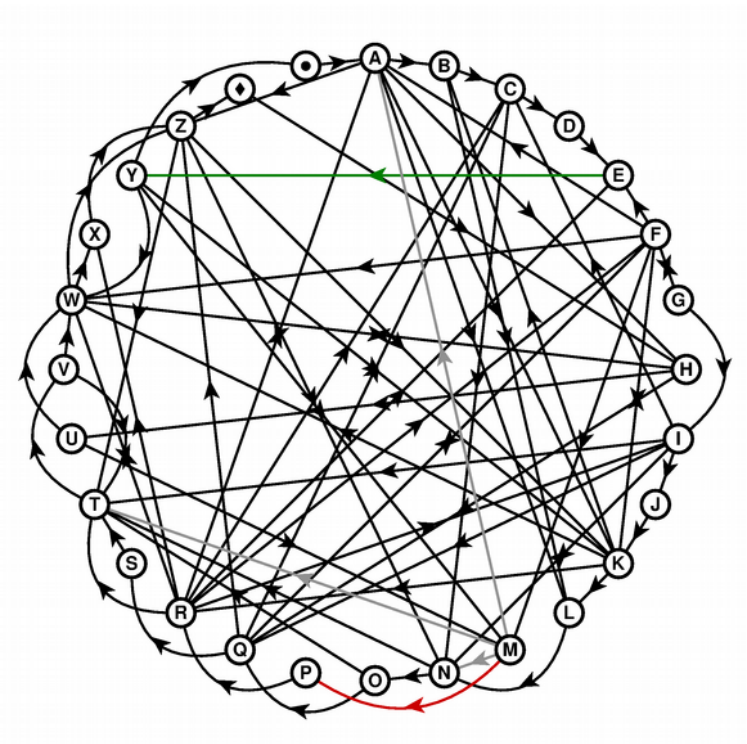
Let's redo the example with a directed graph. If we take the reversed missing digrams and use each to define a directed edge, we have this graph:



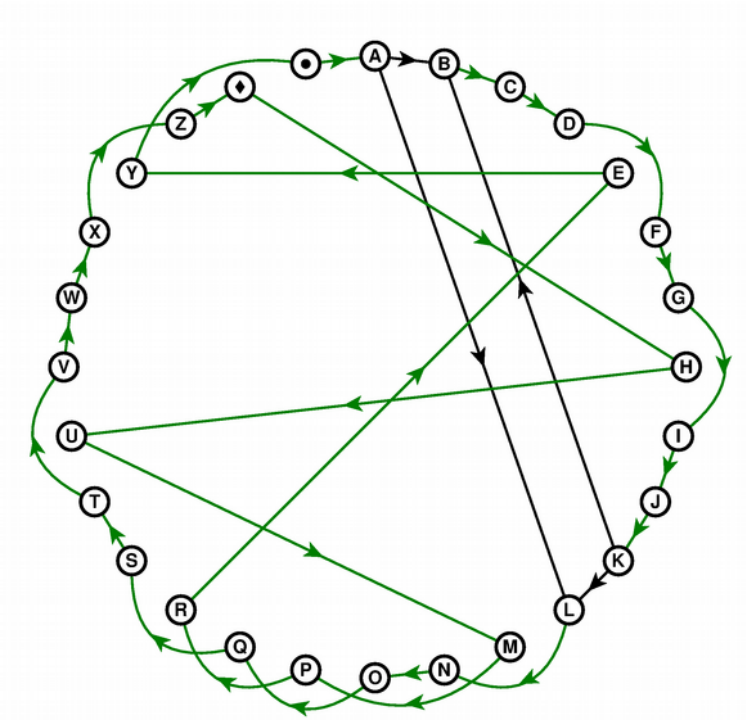
It is quite a mess. But notice that E has only one line directed outward from it. That line ends on Y. Since E must come immediately before Y in the key, we know that no other letter comes immediately before Y, so all other lines that end on Y can be removed.



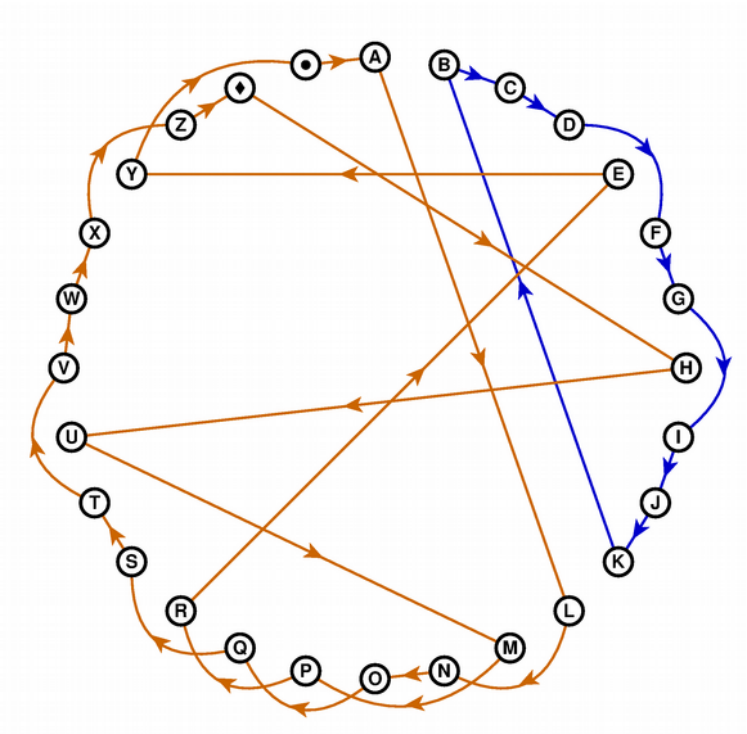
Also notice that P has only one edge that ends on it, from M. Therefore all other lines that start on M can be removed.



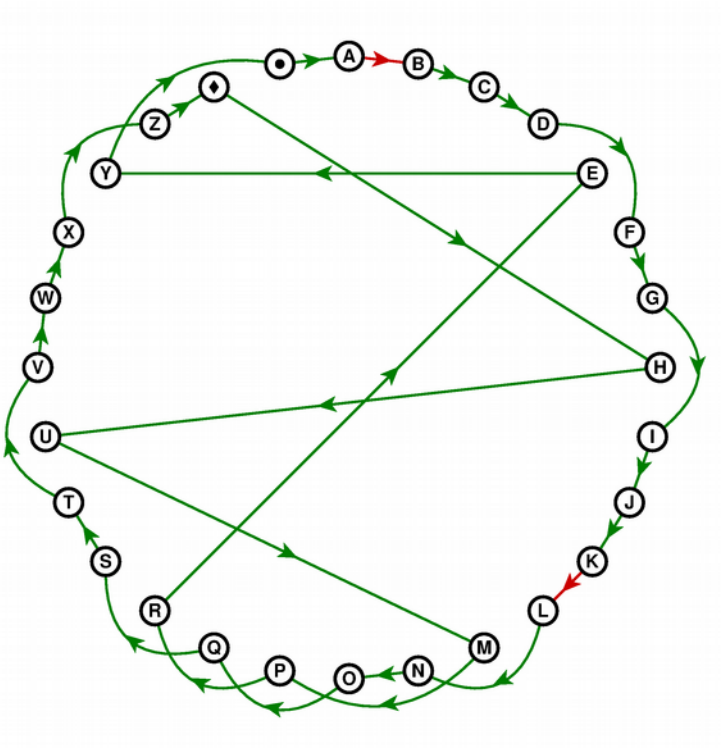
After a lot of this sort of work, we eventually get to the following graph, in which we can make no more eliminations. Did I say "pen and paper"? I meant "pencil." The kind with an eraser.



At this point, we have a choice to make. Either we keep A to B and K to L, or A to L and K to B. If we choose A to L and K to B, we see that the graph has two separate circuits (loops):



We can't have two loops, since we want one key to fit on the outer ring of the cipher clock. With the other choice, we get that one loop:



If we untangle the graph (remember that coordinates of vertices don't matter, and so vertices can be slid around), we see the key just as it would be set into the ring of the device: