

Solving CM Bifids (and others) Using the Equivalence Class Method

PELKABO

August 19, 2023



Presentation Outline



Solving Conjugate Matrix Bifids

- Basics of CM Bifids
- Organizing information from the crib
- Reconstructing primary/secondary keysquares
- Problem for you to work on
- Extending the method to other cipher types

8/19/23

CM Bifid Encryption

Primary

	1	2	3	4	5
1	e	x	t	r	a
2	k	l	m	p	o
3	h	w	z	q	d
4	g	v	u	s	i
5	f	c	b	y	n

Secondary

	1	2	3	4	5
1	N	C	D	R	S
2	O	B	F	Q	U
3	V	A	G	P	W
4	E	Y	H	M	X
5	L	T	I	K	Z

t	h	e	e	a	r	l		y	b	i	r	d	g	e
1	3	1	1	1	1	2		5	5	4	1	3	4	1
3	1	1	1	5	4	2		4	3	5	4	5	1	1
D	N	N	F	N	S	Y		Z	E	P	R	W	X	N

CM Bifid Decryption: known keysquares

	1	2	3	4	5
1	e	x	t	r	a
2	k	l	m	p	o
3	h	w	z	q	d
4	g	v	u	s	i
5	f	c	b	y	n

	1	2	3	4	5
1	N	C	D	R	S
2	O	B	F	Q	U
3	V	A	G	P	W
4	E	Y	H	M	X
5	L	T	I	K	Z

S	E	P	Z	W	X	Z
1	5	4	1	3	4	5
5	3	5	4	5	5	5
a	b	i	r	d	i	n

D	D	S	G	N	S	Z
1	3	1	3	1	5	3
3	1	1	1	5	5	5
t	h	e	h	a	n	d

Known plaintext for a given block of ciphertext

S	E	P	Z	W	X	Z
S1	S2	E1	E2	P1	P2	Z1
Z2	W1	W2	X1	X2	Z1	Z2

 $=$

a	b	i	r	d	i	n
a1	b1	i1	r1	d1	i1	n1
a2	b2	i2	r2	d2	i2	n2

S1 = a1

Z2 = a2

S2 = b1

W1 = b2

.

.

Z2 = n2

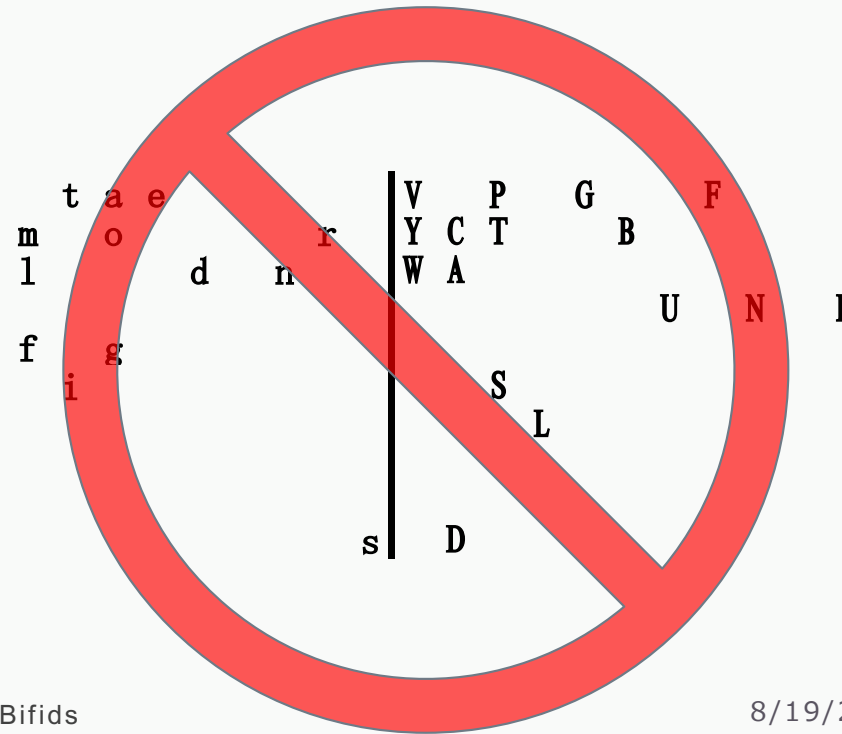
etc.

Where:

1 refers to row coordinate

2 refers to column coordinate

Objective was to avoid tableaus like this



Sample CM Bifid Con

Known period, placed crib:

CKNNTDRU BKQMIKCW AHGFFYRX CYBUTGNB CDIGHVZW AYGERVCE WVHCAMNR

ETCLICVK QYQYVEXH OVIAHDWX MNXBASCV YKARVDZW EYMFLVNE CONEZHXL

QFTFXGFG CKMGOKYU KNKNDUDR HKVAUCTD AQAAZHMR CKHANDDR BREYZWLV
asignal thatthem apshaveb eenmade

MBDTNHUF CGCLVZXA HVCODDOH IXB

Write ciphertext and crib in coordinate form

CKMGOKYU KNKNDUDR HKVAUCTD AQAAZHMR
 asignal thatthem apshaveb eenmade

C1	C2	K1	K2	M1	M2	G1	G2	K1	K2	N1	N2	K1	K2	N1	N2	H1	H2	K1	K2	V1	V2	A1	A2	A1	A2	Q1	Q2	A1	A2	A1	A2
O1	O2	K1	K2	Y1	Y2	U1	U2	D1	D2	U1	U2	D1	D2	R1	R2	U1	U2	C1	C2	T1	T2	D1	D2	Z1	Z2	H1	H2	M1	M2	R1	R2
*	a1	s1	i1	g1	n1	a1	l1	t1	h1	a1	t1	t1	h1	e1	m1	a1	p1	s1	h1	a1	v1	e1	b1	e1	e1	n1	m1	a1	d1	e1	*
*	a2	s2	i2	g2	n2	a2	l2	t2	h2	a2	t2	t2	h2	e2	m2	a2	p2	s2	h2	a2	v2	e2	b2	e2	e2	n2	m2	a2	d2	e2	*

Where:
 1 refers to row coordinate
 2 refers to column coordinate

Write out the equivalences

C1	C2	K1	K2	M1	M2	G1	G2
O1	O2	K1	K2	Y1	Y2	U1	U2

*	a1	s1	i1	g1	n1	a1	l1
*	a2	s2	i2	g2	n2	a2	l2

C2 = a1 M1 = g1
 O2 = a2 Y1 = g2
 K1 = s1 M2 = n1
 K1 = s2 Y2 = n2
 K2 = i1 G1 = a1
 K2 = i2 U1 = a2
 G2 = l1
 U2 = l2

K1	K2	N1	N2	K1	K2	N1	N2
D1	D2	U1	U2	D1	D2	R1	R2

t1	h1	a1	t1	t1	h1	e1	m1
t2	h2	a2	t2	t2	h2	e2	m2

K2 = t1 K1 = t1
 D1 = t2 D2 = t2
 K2 = h1 K2 = h1
 D2 = h2 D2 = h2
 N1 = a1 N1 = e1
 U1 = a2 R1 = e2
 N2 = t1 N2 = m1
 U2 = t2 R2 = m2

H1	H2	K1	K2	V1	V2	A1	A2
U1	U2	C1	C2	T1	T2	D1	D2

a1	p1	s1	h1	a1	v1	e1	b1
a2	p2	s2	h2	a2	v2	e2	b2

H1 = a1 V1 = a1
 U1 = a2 T1 = a2
 H2 = p1 V2 = v1
 U2 = p2 T2 = v2
 K1 = s1 A1 = e1
 C1 = s2 D1 = e2
 K2 = h1 A2 = b1
 C2 = h2 D2 = b2

A1	A2	Q1	Q2	A1	A2	A1	A2
Z1	Z2	H1	H2	M1	M2	R1	R2

e1	e1	n1	m1	a1	d1	e1	*
e2	e2	n2	m2	a2	d2	e2	*

A1 = e1 A1 = a1
 Z1 = e2 M1 = a2
 A2 = e1 A2 = d1
 Z2 = e2 M2 = d2
 Q1 = n1 A1 = e1
 H1 = n2 R1 = e2
 Q2 = m1
 H2 = m2

Split into equivalence classes

C2 = a1	M1 = g1	K2 = t1	K1 = t1	H1 = a1	V1 = a1	A1 = e1	A1 = a1
O2 = a2	Y1 = g2	D1 = t2	D2 = t2	U1 = a2	T1 = a2	Z1 = e2	M1 = a2
K1 = s1	M2 = n1	K2 = h1	K2 = h1	H2 = p1	V2 = v1	A2 = e1	A2 = d1
K1 = s2	Y2 = n2	D2 = h2	D2 = h2	U2 = p2	T2 = v2	Z2 = e2	M2 = d2
K2 = i1	G1 = a1	N1 = a1	N1 = e1	K1 = s1	A1 = e1	Q1 = n1	A1 = e1
K2 = i2	U1 = a2	U1 = a2	R1 = e2	C1 = s2	D1 = e2	H1 = n2	R1 = e2
	G2 = l1	N2 = t1	N2 = m1	K2 = h1	A2 = b1	Q2 = m1	
	U2 = l2	U2 = t2	R2 = m2	C2 = h2	D2 = b2	H2 = m2	

C2, a1, h2, G1, N1, H1, V1, A1, D2, e1, n2, b2, A2, Y2, b1, d1

List splits into eleven classes

a: a1, b1, b2, d1, e1, h2, n2, A1, A2, C2, D2, G1, H1, N1, V1, Y2 (16)

b: e2, l2, p2, t2, D1, R1, U2, Z1, Z2 (9)

c: m1, s1, s2, t1, C1, K1, N2, Q2 (8)

d: a2, g1, M1, O2, T1, U1 (6)

e: d2, n1, M2, Q1 (4)

f: m2, p1, H2, R2 (4)

g: h1, i1, i2, K2 (4)

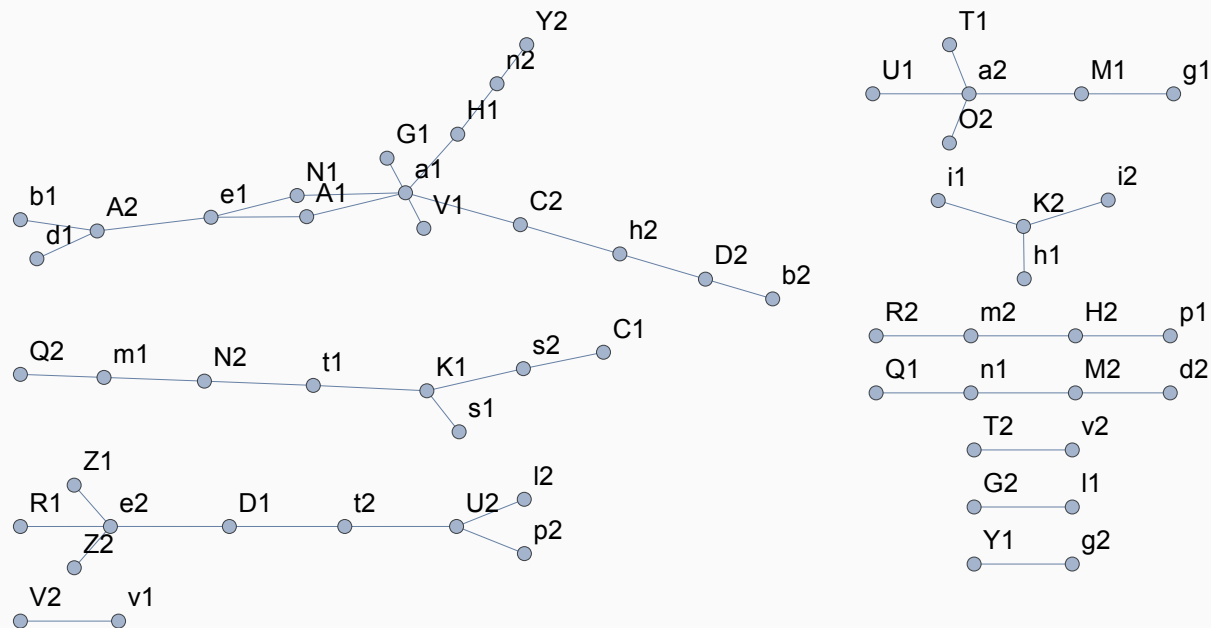
h: l1, G2 (2)

i: g2, Y1 (2)

j: v2, T2 (2)

k: v1, V2 (2)

Equivalence Graph



Find coordinates of pt and ct letters

a: a_1 , b_1 , b_2 , d_1 , e_1 , h_2 , n_2 , A_1 , A_2 , C_2 , D_2 , G_1 , H_1 , N_1 , V_1 , Y_2

b: e_2 , l_2 , p_2 , t_2 , D_1 , R_1 , U_2 , Z_1 , Z_2

c: m_1 , s_1 , s_2 , t_1 , C_1 , K_1 , N_2 , Q_2

d: a_2 , g_1 , M_1 , O_2 , T_1 , U_1

e: d_2 , n_1 , M_2 , Q_1

f: m_2 , p_1 , H_2 , R_2

g: h_1 , i_1 , i_2 , K_2

h: l_1 , G_2

i: g_2 , Y_1

j: v_2 , T_2

k: v_1 , V_2

primary

$a = (a, d)$

$b = (a, a)$

etc.

secondary

$A = (a, a)$

$C = (c, a)$

etc.

Make a table for each keysquare

Primary keysquare

	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
row	<i>a</i>	<i>a</i>		<i>a</i>	<i>a</i>		<i>d</i>	<i>g</i>	<i>g</i>		<i>h</i>	<i>c</i>	<i>e</i>		<i>f</i>			<i>c</i>	<i>c</i>		<i>k</i>				
col	<i>d</i>	<i>a</i>		<i>e</i>	<i>b</i>		<i>i</i>	<i>a</i>	<i>g</i>		<i>b</i>	<i>f</i>	<i>a</i>		<i>b</i>			<i>c</i>	<i>b</i>		<i>j</i>				

Secondary keysquare

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
row	<i>a</i>		<i>c</i>	<i>b</i>			<i>a</i>	<i>a</i>		<i>c</i>		<i>d</i>	<i>a</i>			<i>e</i>	<i>b</i>		<i>d</i>	<i>d</i>	<i>a</i>			<i>i</i>	<i>b</i>
col	<i>a</i>		<i>a</i>	<i>a</i>			<i>h</i>	<i>f</i>		<i>g</i>		<i>e</i>	<i>c</i>	<i>d</i>		<i>c</i>	<i>f</i>		<i>j</i>	<i>b</i>	<i>k</i>			<i>a</i>	<i>b</i>

Reconstruct the keysquares

Primary keysquare

	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
row	a	a		a	a		d	g	g		h	c	e		f			c	c		k				
col	d	a		e	b		i	a	g		b	f	a		b			c	b		j				

$a=2, b=5, e=4, d=1, c=4, g=3$, etc.

Secondary keysquare

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
row	a		c	b			a	a		c		d	a			e	b		d	d	a			i	b
col	a		a	a			h	f		g		e	c	d		c	f		j	b	k			a	b

	1	2	3	4	5
1					
2	a	b	c	d	e
3		h	i		
4				s	t
5					

	1	2	3	4	5
1		Y		M	
2		A		N	
3					
4		C	K		
5		D			Z

Can also reconstruct some plaintext

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
<i>a</i>	<i>a</i>		<i>a</i>	<i>a</i>		<i>d</i>	<i>g</i>	<i>g</i>		<i>h</i>	<i>c</i>	<i>e</i>		<i>f</i>			<i>c</i>	<i>c</i>		<i>k</i>				
<i>d</i>	<i>a</i>		<i>e</i>	<i>b</i>		<i>i</i>	<i>a</i>	<i>g</i>		<i>b</i>	<i>f</i>	<i>a</i>		<i>b</i>			<i>c</i>	<i>b</i>		<i>j</i>				

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
<i>a</i>		<i>c</i>	<i>b</i>			<i>a</i>	<i>a</i>		<i>c</i>		<i>d</i>	<i>a</i>			<i>e</i>	<i>b</i>		<i>d</i>	<i>d</i>	<i>a</i>			<i>i</i>	<i>b</i>
<i>a</i>		<i>a</i>	<i>a</i>			<i>h</i>	<i>f</i>		<i>g</i>		<i>e</i>	<i>c</i>	<i>d</i>		<i>c</i>	<i>f</i>		<i>j</i>	<i>b</i>	<i>k</i>			<i>a</i>	<i>b</i>

C	K	N	N	T	D	R	U
<i>c</i>	<i>a</i>	<i>c</i>	<i>g</i>	<i>a</i>	<i>c</i>	<i>a</i>	<i>c</i>
<i>d</i>	<i>j</i>	<i>b</i>	<i>a</i>	<i>b</i>	<i>f</i>	<i>d</i>	<i>b</i>
?	?	<i>t</i>	<i>h</i>	<i>e</i>	<i>m</i>	<i>a</i>	<i>t</i>

B	K	Q	M	I	K	C	W
?	?	<i>c</i>	<i>g</i>	<i>e</i>	<i>c</i>	<i>d</i>	<i>e</i>
?	?	<i>c</i>	<i>g</i>	<i>c</i>	<i>a</i>	?	?
?	?	<i>s</i>	<i>i</i>	?	?	?	?

A	H	G	F	F	Y	R	X
<i>a</i>	<i>a</i>	<i>a</i>	<i>f</i>	<i>a</i>	<i>h</i>	?	?
?	?	<i>i</i>	<i>a</i>	<i>b</i>	<i>f</i>	?	?
?	?	?	?	<i>e</i>	?	?	?

C	Y	B	U	T	G	N	B
<i>c</i>	<i>a</i>	<i>i</i>	<i>a</i>	?	?	<i>d</i>	<i>b</i>
<i>d</i>	<i>j</i>	<i>a</i>	<i>h</i>	<i>a</i>	<i>c</i>	?	?
?	?	?	?	?	?	?	?

C	D	I	G	H	V	Z	W
<i>c</i>	<i>a</i>	<i>b</i>	<i>a</i>	?	?	<i>a</i>	<i>h</i>
<i>a</i>	<i>f</i>	<i>a</i>	<i>k</i>	<i>b</i>	<i>b</i>	?	?
?	?	?	?	?	?	?	?

One to practice on

EX-1 CM Bifid. Cape Canaveral before NASA.

PELKABO

BGSGCPALP YCYWFWWUT WDWVGNWAI EPVMGSHUG PWQPPHQKQ TPAZOFBZK GVOVCSCDS ZSDGVCAA0
VWWSQYQCZ KVWWDIAUR QYPHXTPTV VCPVSTNT0 SXVVCAMXW YPHCHSHSN VMEYLSPLL BZCDEWXHY
XYPCATNOQ GHVGOTCBB HVFIM (begins: imagineforamomentadesolate)

B	G	S	G	C	P	A	L	P		Y	C	Y	W	F	W	W	U	T		W	D	W	V	G	N	W	A	I	
B1	B2	G1	G2	S1	S2	G1	G2	C1		Y1	Y2	C1	C2	Y1	Y2	W1	W2	F1		W1	W2	D1	D2	W1	W2	V1	V2	G1	
C2	P1	P2	A1	A2	L1	L2	P1	P2		F2	W1	W2	W1	W2	U1	U2	T1	T2		G2	N1	N2	W1	W2	A1	A2	I1	I2	
i	m	a	g	i	n	e	f	o		r	a	m	o	m	e	n	t	a		d	e	s	o	l	a	t	e	?	
i1	m1	a1	g1	i1	n1	e1	f1	o1		r1	a1	m1	o1	m1	e1	n1	t1	a1		d1	e1	s1	o1	l1	a1	t1	e1		
i2	m2	a2	g2	i2	n2	e2	f2	o2		r2	a2	m2	o2	m2	e2	n2	t2	a2		d2	e2	s2	o2	l2	a2	t2	e2		

~~B1~~=i1 Y1 = m1
B2 = m1 Y2 = e1
G1 = a1 W1 = n1
G2 = g1 W2 = t1
~~S1~~=i1 F1 = a1
S2 = n1 F2 = r2
G1 = e1 W1 = a2
G2 = f1 W2 = m2
C1 = o1 W1 = o2
C2 = i2 W2 = m2
P1 = m2 U1 = e2
P2 = a2 U2 = n2
A1 = g2 T1 = t2
A2 = i2 T2 = a2
L1 = n2 W1 = d1
L2 = e2 W2 = e1
P1 = f2 D1 = s1
P2 = o2 D2 = o1
Y1 = r1 W1 = l1
Y2 = a1 W2 = a1
C1 = m1 V1 = t1
C2 = o1 V2 = e1

a B1, i1, S1
b _____
c _____
d _____
e _____
f _____
g _____
h _____
i _____
j _____

Print out the
handout and try
it for yourself

VPQB	FXHKQ	FFUYC	LRCXX	EDWXP	PYLGF	ZFPHE	SFRKK	OVITS
TXEMO	WHXNE	WGKCD	GXEAO	PPRIR	DNBJV	PEFYS	ZYPRS	XSWPR
JYVTH	SSXKI	WXMZS	QQYOG	SJCTN	CCBJY	ZSPAC	QCLQF	OSAME
YQWMS	IDEEU	ZLUAW	LVLAV	JIHMA	UHTDS	CKCMK	AKJUQ	GOWOT
WFLIO	WBRAA	ZOONA	NINZN	RCLSO	XIHPK	WLFCC	YLIGA	MNOHU
JAGNG	RHHFO	ZHRNC	OYCJZ	XOUMJ	XMCIK	USDMJ	FQQZX	TDPFT
WRYYN	IESMW	PCHCR	QGBTK	EDJYV	IDLEH	FVUEJ	TACBP	HTWBT
SRCUL	PZFYT	GVABU	DDWOP	JJXJV	TPUCT	RSOTP	FTZCR	SHGXA
IYYMW	LDEBO	VBJFF	SULLC	UHLUH	XNPNT	ROJTM	CZZEC	TWEOH
SUUPC	VFRRV	WQCGB	VRUGE	XXMPR	OTBYG	JLYDH	BEGFZ	ILTJP
VBXDR	YSZZT	DFIRQ	CUNDQ	KUFGS	AJDVQ	FJZUM	YQLWY	FRIEY
PRLZQ	QHXZI	ABCTB	OLJRY	VHDM	BLOQF	WJZZJ	YCMYD	EVDYU
ZJENF	TBXLI	CMUMP	KKRBL	NZDAG	NQJDR	NGOLF	QYOXG	OYKNV
DGRFX	ZZKRC	XFXAD	EXENB	GIIXS	IMDIC	ADKFP	GHRQZ	TJEOZ
DPDUW	RVWRJ	VOTMS	VYUBZ	OLELL	ZCWEI	DDMIS	HBTSV	HASMW
EINCH	XVATJ	RLBMK	MWMFN	NSFTJ	WZXPP	UHJVB	WIFNL	BFSPF
JZZGW	PYEXB	FQEV	BULFJ	FCSXZ	YYSFW	PEYPF	ROOEX	SGRGA
UFZHG	GFIBZ	HKQWH	TTYJY	HVBFK	ZXEUD	VEEAB	EJDWI	TSXYK
IMONR	UKKPH	OSYVU	HYIPM	IEPMU	XVEPN	LMYWH	OSCAI	DDLYK
QOWXS	TVDUS	FYVXP	AKFOR	SOEYO	KILIV	FCMPI	JOAVR	COTYK

Using this method for other cipher types

Same process works for Bifid

IUEMMKX BADTADV QLEURMN EYMCLOR FTEENFK UMTGIBH IBFMNHC OTDAHIZ
 OTLOHNR ELXRNRI TOANOKN BKTKAU Y OFETYE H ENDINGB FBTYXFT LDMOHC I
 yandedd icatedt

OTTPPNO LFENHNL OYUGUIF UEGKFNB SUMEL

E1	E2	N1	N2	D1	D2	I1
I2	N1	N2	G1	G2	B1	B2

F1	F2	B1	B2	T1	T2	Y1
Y2	X1	X2	F1	F2	T1	T2

CT

Y1	A1	N1	D1	D1	E1	D1
Y2	A2	N2	D2	D2	E2	D2

I1	C1	A1	T1	E1	D1	Y1
I2	C2	A2	T2	E2	D2	Y2

PT

A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
c	c	c	b	a	b	a		b				d						a				f	a	
d	a	f	a	c	c	a		e				b						b				d	e	

...And for Trifids

YUESEAVDK YSDDFFNNJ NINCKIB#G TKLPENNVW SSTSFFIGN RUNAGSHOY TFOFDINJH FBTADL
codebreak ingisthem

Y1	Y2	Y3	U1	U2	U3	E1	E2	E3
S1	S2	S3	E1	E2	E3	A1	A2	A3
V1	V2	V3	D1	D2	D3	K1	K2	K3

Y1	Y2	Y3	S1	S2	S3	D1	D2	D3
D1	D2	D3	F1	F2	F3	F1	F2	F3
N1	N2	N3	N1	N2	N3	J1	J2	J3

C1	O1	D1	E1	B1	R1	E1	A1	K1
C2	O2	D2	E2	B2	R2	E2	A2	K2
C3	O3	D3	E3	B3	R3	E3	A3	K3

I1	N1	G1	I1	S1	T1	H1	E1	M1
I2	N2	G2	I2	S2	T2	H2	E2	M2
I3	N3	G3	I3	S3	T3	H3	E3	M3

Y1=C1 Y3=D1 U2=B1
S1=C2 S3=D2 E2=B2
V1=C3 V3=D3 D2=B3
Y2=O1 U1=E1 U3=R1
S2=O2 E1=E2 E3=R2
V2=O3 D1=E3 D3=R3

... etc.

Trifids (continued)

a: {A1,C1,E1,I1,S1,T1,U1,Y1,B2,C2,D2,E2,F2,N2,O2,S2,B3,G3,N3,S3,T3}

b: {D1,F1,G1,H1,K1,H2,I2,J2,R2,E3,Y3}

c: {M1,G2,D3,R3,V3}

d: {N1,O1,Y2,I3}

e: {M2,T2,F3}

f: {R1,U3}

g: {K2,A3}

h: {J3,M3}

i: {V2,O3}

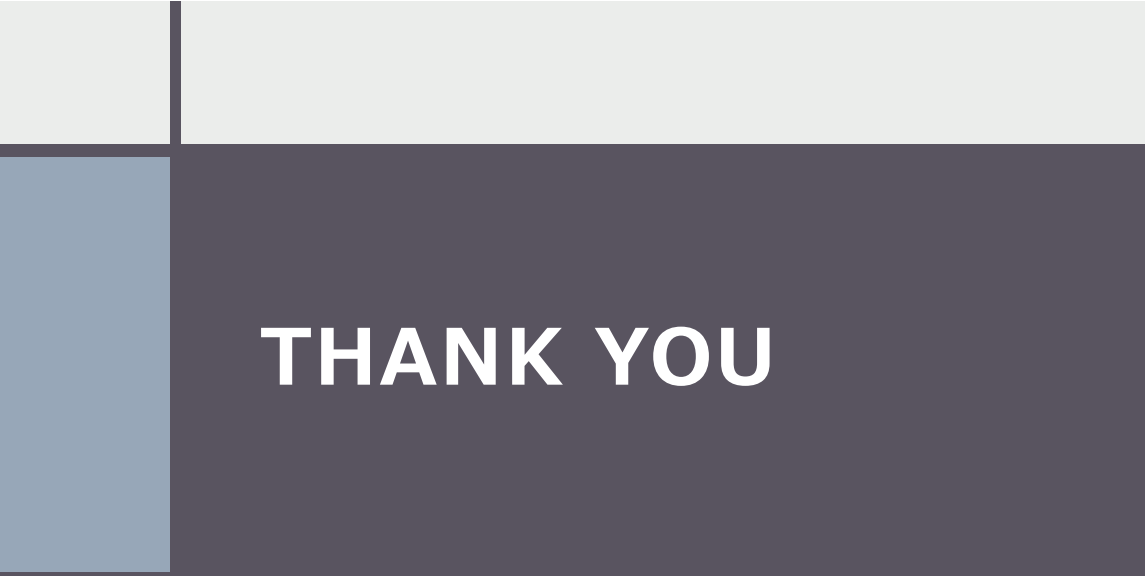
j: {K3}

k: {A2}

	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	#
1	a		a	b	a	b	b	b	a		b		c	d	d			f	a	a	a				a		
2	k	a	a	a	a	a	c	b	b	b	g		e	a	a			b	a	e		i			d		
3	g	a		c	b	e	a		d	h	j		h	a	i			c	a	a	f	c			b		

Other cipher types

- **6x6 Bifid (try AC-1353)**
- **6x6 CM Bifid**
- **Twin Bifid**
- **Twin Trifid**
- **Two-square and four-square**
- **Digrafid – a bit more complicated but same idea**



THANK YOU

A black and white photograph of a modern interior space featuring a staircase and several large, circular light fixtures hanging from the ceiling.

PELKABO
jashonder@gmail.com

Solving Conjugate Matrix Bifids