Examples of Solving Cm Cons*



Solving E-8 from Sample *Cm* Checkerboard Cipher

* "*Cm* Cons" means "cipher constructions in *The Cryptogram*" -- the bi-monthly publication for members of the American Cryptogram Association (ACA) -- <u>www.cryptogram.org</u>

Examples of Solving

This series shows specific examples of solving ACA ciphers. It tries to give successive hints of what to look at, then follows through by using each hint, building to the solution.

- Try to solve the cipher on your own, using as many hints as you need, or just read along.
- Please report errors or send suggestions to <u>nudge@cryptogram.org</u>

References

• <u>The ACA and You</u>, Ch. 4, How to Solve a Problem in *The Cryptogram*.

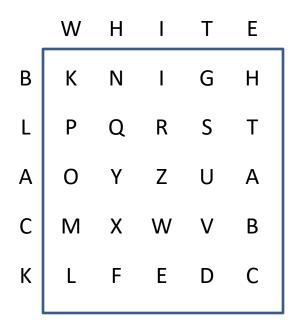
What is a Checkerboard Cipher?

- Checkerboard uses a 5x5 Polybius key square in which I&J share a space. (ACA Guideline: The plaintext should be 60-90 letters)
- A five letter keyword is chosen (no repeated letters) to label rows, and another for columns.
- The ciphertext for each plaintext letter is comprised of two letters: the key letters of its row and column, written as a digraph.

Checkerboard Cipher Example

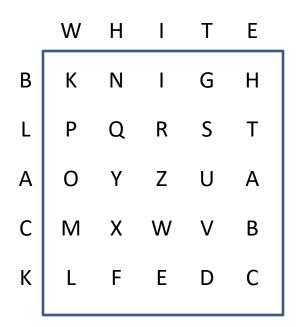
Keywords BLACK & WHITE were chosen for the Row and Column keywords. KNIGHT is the alphabet key, and the keyed alphabet has been

written into the keysquare using a clockwise spiral.



Checkerboard Cipher Example

Plaintext: "repeated letters cause repeated digraphs." The ciphertext digraph for R is LI, for E is KI, for P is LW, etc.

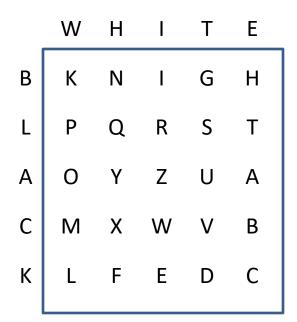


r	е	р	е	а	t	е	d
LΙ	ΚI	LW	ΚI	AE	LΕ	ΚI	ΚT

KI appears 3 times above. E appears 3 times in REPEATED.

Checkerboard Cipher Example

Plaintext: "repeated letters cause repeated digraphs."



Ciphertext:

LΙ	ΚI	LW	ΚI	AE	LΕ	ΚI	ΚT	KW	ΚI
LΕ	LΕ	ΚI	LΙ	LT	KE	AE	AT	LT	ΚI
LΙ	ΚI	LW	ΚI	AE	LΕ	ΚI	ΚT	ΚT	ΒI
ΒT	LΙ	AE	LW	ΒE	LT.	•			

Checkerboard: Getting Started

- Start by looking at the set of letters that start the digraphs. Try to guess those keywords.
- L,K,A,B start our digraphs, and I,W,E,T end them. Only 4 letters each... BLEAK? BLANK? BLACK? TWINE? WHITE? WRITE?

LE KT KT T.W ΚT AF ΚW ΚT **T**.F. T.F. ΚT KΤ AT LT T.T KE АF ΚT LI KI MT ΚT ΑE .T.F. BI BT LI AE LW KΤ BE Τ_ΓΤ,

Checkerboard: Getting Started

- Guessing keywords... BLEAK? BLANK? BLACK? TWINE? WHITE? WRITE? Do any words form a likely pair? Perhaps BLACK & WHITE?
- (Caution: there might be up to ten letters each for Row or Column keyword letters if the constructor used double keywords.)

Checkerboard: Getting Started 2

- If there is a crib, find a place for it and see how the alphabet letters fit into the keysquare.
- If the Row/Column keywords are correct, it might help reveal the route used to write the keyed alphabet into the square.
- If the Row/Column keywords might not be right, try a different pair and copy alphabet letters to a new keysquare.

E-8. Checkerboard. A thought from Parker Hitt. (analysis) ARTEMIS LC YC UP UP LT LC LC CC YC LY UT LT UP CP KY CY LT UC KC LT KR KT KR LT LT UT LC KY LT UC LC LT LP LT UC UR KR UP LT UR KR UR LY YP LC CP LC CP KR KT YC CP KT CP LR KR UR KR UT LY YC UP CT.

What does the first line tell us?

Cipher ID: E-8.

- Type: Checkerboard cipher.
- Title: A thought from Parker Hitt.

Crib: analysis. (Word appears in plaintext. Has 2 letter repeats!) Created by ACA member ARTEMIS

E-8. Checkerboard. A thought from Parker Hitt. (analysis) ARTEMIS LC YC UP UP LT LC LC CC YC LY UT LT UP CP KY CY LT UC KC LT KR KT KR LT LT UT LC KY LT UC LC LT LP LT UC UR KR UP LT UR KR UR LY YP LC CP LC CP KR KT YC CP KT CP LR KR UR KR UT LY YC UP CT.

What are the first or leading letters in the digraphs? What are second or trailing letters in the digraphs?

E-8. Checkerboard. A thought from Parker Hitt. (analysis) ARTEMIS LC YC UP UP LT LC LC CC YC LY UT LT UP CP KY CY LT UC KC LT KR KT KR LT LT UT LC KY LT UC LC LT LP LT UC UR KR UP LT UR KR UR LY YP LC CP LC CP KR KT YC CP KT CP LR KR UR KR UT LY YC UP CT.

What are the first or leading letters in the digraphs? L,Y,U,C,K What are second or trailing letters in the digraphs? C,P,T,Y,R

Can you guess at Row/Column keywords for the square?

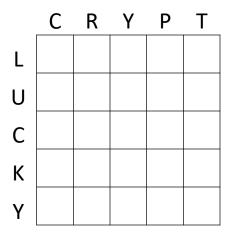
E-8. Checkerboard. A thought from Parker Hitt. (analysis) ARTEMIS LC YC UP UP LT LC LC CC YC LY UT LT UP CP KY CY LT UC KC LT KR KT KR LT LT UT LC KY LT UC LC LT LP LT UC UR KR UP LT UR KR UR LY YP LC CP LC CP KR KT YC CP KT CP LR KR UR KR UT LY YC UP CT.

What are the first or leading letters in the digraphs? L,Y,U,C,K What are second or trailing letters in the digraphs? C,P,T,Y,R

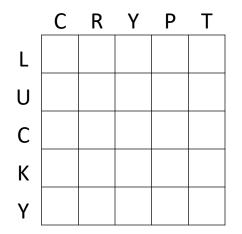
Can you guess at Row/Column keywords for the square? Maybe LUCKY and CRYPT?

E-8. Checkerboard. A thought from Parker Hitt. (analysis) ARTEMIS LC YC UP UP LT LC LC CC YC LY UT LT UP CP KY CY LT UC KC LT KR KT KR LT LT UT LC KY LT UC LC LT LP LT UC UR KR UP LT UR KR UR LY YP LC CP LC CP KR KT YC CP KT CP LR KR UR KR UT LY YC UP CT.

Start a keysquare labeled with LUCKY and CRYPT. We fill it in as we go.



The crib is "analysis". Find the locations that fit a pattern word like this.

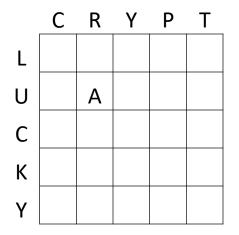


E-8	B.Cł	nec]	kerk	ooai	rd.	A t	thou	ıght	: fi	rom	Pai	ckei	r Hi	itt.	. (a	ana	Lysi	Ls)	AR	FEMIS
LC	YС	UP	UP	LT	LC	LC	СС	YС	LY	UT	LT	UP	СР	ΚY	СҮ	LT	UC	KC	LT	KR
—	—	-	_	-	_	-	-	-	_	-	-	-	_	-	-	-	-	_	-	-
ΚT	KR	LT	LT	UT	LC	ΚY	LT	UC	LC	LT	LΡ	LT	UC	UR	KR	UP	LT	UR	KR	UR
—	—	-	_	-	_	-	-	-	_	-	-	-	_	-	-	-	-	_	-	-
LY	ΥP	LC	СР	LC	СР	KR	ΚT	YC	СР	ΚT	СР	LR	KR	UR	KR	UT	LΥ	YC	UP	СТ
-	-	-	_	-	_	-	-	-	-	-	-	_	_	_	_	-	_	_	-	-

The crib is "analysis". Find the locations that fit a pattern word like this.

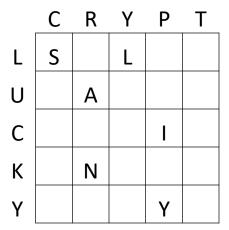
There is only one location, on lines 2 & 3.

Next, add the letters found into the keysquare. For example, A goes in UR.



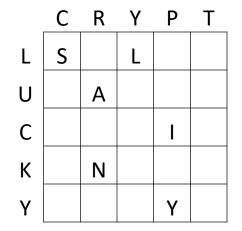
E-	8.Cl	necl	ker	boai	rd.	A t	thou	ıght	c fi	rom	Par	rkei	r Hi	itt.	. (a	anal	Lysi	is)	ART	FEMIS
LC	YC	UΡ	UP	LT	LC	LC	СС	YC	LY	UT	LT	UP	СР	ΚY	СҮ	LT	UC	KC	LT	KR
-	-	-	-	-	_	-	-	-	-	_	-	_	_	-	-	-	-	_	-	-
KT	KR	LT	LT	UT	LC	ΚY	LT	UC	LC	LT	LΡ	LT	UC	UR	KR	UP	LT	UR	KR	UR
-	-	-	-	-	_	-	-	-	_	-	-	_	_	-	-	-	-	а	n	a
LY	ΥP	LC	СР	LC	СР	KR	KΤ	YC	СР	ΚT	СР	LR	KR	UR	KR	UT	LΥ	YС	UP	СТ
1	У	S	i	S	_	_	-	-	-	_	_	_	_	_	-	-	-	_	_	-

Now that the crib is placed and the keysquare has been updated, fill in letters for known digraphs.



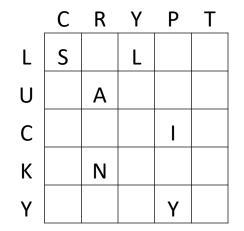
E-8	B.Cł	necl	ker	poar	rd.	A t	zhou	ıght	: fi	rom	Par	rkei	r Hi	itt	. (a	ana	Lys	is)	AR	FEMIS
LC	YС	UP	UP	LT	LC	LC	СС	YС	LΥ	UT	LT	UP	СР	ΚY	СҮ	LT	UC	KC	LT	KR
S	_	_	_	_	S	S	_	_	1	_	_	_	i	_	_	_	_	_	_	n
KT	KR	LT	LT	UT	LC	ΚY	LT	UC	LC	LT	LΡ	LT	UC	UR	KR	UP	LT	UR	KR	UR
-	n	_	_	_	S	-	-	-	S	—	—	_	_	а	n	-	—	а	n	a
LY	ΥP	LC	СР	LC	СР	KR	ΚT	YС	СР	ΚT	СР	LR	KR	UR	KR	UT	LΥ	YС	UP	СТ
1	У	S	i	S	i	n	-	_	i	—	i	_	n	а	n	-	1	—	_	_

What might the first word be? Which digraphs are more numerous?



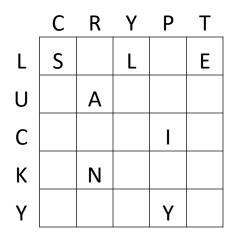
E-8	B.Cł	necl	kerk	boai	rd.	A t	thou	ıght	: fi	com	Par	rkei	r Hi	itt	. (a	ana	Lys	is)	AR	[EMIS
LC	YC	UP	UP	LT	LC	LC	СС	YC	LY	UT	LT	UP	СР	ΚY	СҮ	LT	UC	KC	LT	KR
S	_	_	_	_	S	S	_	-	l	_	_	_	i	_	_	_	_	_	_	n
ΚT	KR	LT	LT	UT	LC	ΚY	LT	UC	LC	LT	ΓЬ	LT	UC	UR	KR	UP	LT	UR	KR	UR
-	n	_	_	_	S	_	_	_	S	_	_	_	_	а	n	_	_	а	n	а
LY	ΥP	LC	СР	LC	СР	KR	ΚT	YC	СР	ΚT	СР	LR	KR	UR	KR	UT	LΥ	YС	UP	СТ
1	У	S	i	S	i	n	-	_	i	_	i	_	n	а	n	-	1	_	_	-

What might the first word be? Which digraphs are more numerous? LT occurs 10 times – could it be E?



E-8	8.Cł	necl	ker	boai	rd.	A t	zhou	ıght	: fi	com	Pai	rkei	r Hi	itt	. (a	anal	Lysi	Ls)	AR	FEMIS
LC	YC	UP	UP	LT	LC	LC	СС	YС	LY	UT	LT	UP	СР	ΚY	СҮ	LT	UC	KC	LT	KR
S	_	_	_	_	S	S	_	_	1	_	_	_	i	_	_	_	_	_	_	n
ΚT	KR	LT	LT	UT	LC	ΚY	LT	UC	LC	LT	LΡ	LT	UC	UR	KR	UP	LT	UR	KR	UR
-	n	—	_	_	S	-	—	-	S	_	—	_	—	а	n	_	_	а	n	a
LY	ΥP	LC	СР	LC	СР	KR	KΤ	YC	СР	ΚT	СР	LR	KR	UR	KR	UT	LΥ	YC	UP	СТ
l	У	S	i	S	i	n	-	-	i	—	i	—	n	а	n	-	1	-	—	-

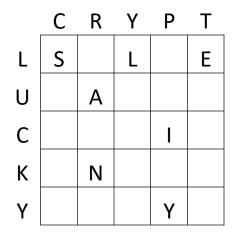
What might the first word be?Which digraphs are more numerous?LT occurs 10 times – could it be E?E has been filled in.



E-3	8.Cl	necl	kerl	ooai	rd.	A 1	thou	ıght	t fi	rom	Pa	rkei	r Hi	itt	. (a	ana	lys	is)	AR	FEMIS
LC	YC	UP	UP	LT	LC	LC	CC	YС	LY	UT	LT	UP	СР	ΚY	СҮ	LT	UC	KC	LT	KR
S	_	_	_	е	S	S	_	_	1	_	е	_	i	_	_	е	_	_	е	n
ΚT	KR	LT	LT	UT	LC	ΚY	LT	UC	LC	LT	LΡ	LT	UC	UR	KR	UP	LT	UR	KR	UR
-	n	е	е	_	S	_	е	—	S	е	_	е	_	а	n	_	е	а	n	а
LY	ΥP	LC	СР	LC	СР	KR	ΚT	YС	СР	ΚT	СР	LR	KR	UR	KR	UT	LΥ	YС	UP	СТ
1	У	S	i	S	i	n	_	—	i	_	i	_	n	а	n	_	1	_	_	_

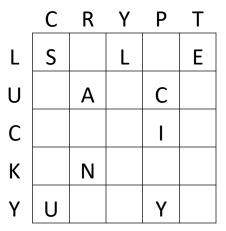
What might the first word be?

Was the keysquare filled by columns? By rows?



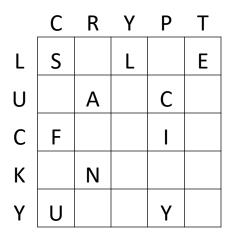
E-3	8.Cl	necl	kerl	ooai	rd.	At	thou	ıght	c fi	rom	Par	rkei	r Hi	itt	. (a	ana	lys	is)	AR	FEMIS
LC	YC	UP	UP	LT	LC	LC	CC	YС	LΥ	UT	LT	UP	СР	ΚY	СҮ	LT	UC	KC	LT	KR
S	-	-	-	е	S	S	-	_	1	_	е	_	i	_	_	е	_	-	е	n
ΚT	KR	LT	LT	UT	LC	ΚY	LT	UC	LC	LT	ΓЬ	LT	UC	UR	KR	UP	LT	UR	KR	UR
-	n	е	е	_	S	_	е	_	S	е	_	е	_	а	n	—	е	а	n	а
LY	ΥP	LC	СР	LC	СР	KR	ΚT	YC	СР	ΚT	СР	LR	KR	UR	KR	UT	LΥ	YС	UP	СТ
l	У	S	i	S	i	n	-	_	i	—	i	_	n	а	n	—	1	_	_	_

What might the first word be? Looks like YC is a vowel, followed by UP UP, a doubled consonant. Was the keysquare filled by columns? By rows? It looks like it was filled by rows. So YC should be a letter late in the alphabet. Maybe U, and the doubled consonant could be C to make SUCCESS?



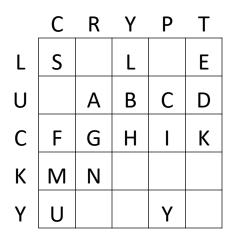
E-8	B.Cł	necl	kerk	boai	rd.	A t	zhou	ıght	c fi	com	Pai	rkei	r Hi	itt.	. (a	ana	lys	is)	AR	[EMIS
LC	YС	UP	UP	LT	LC	LC	СС	YС	LΥ	UT	LT	UP	СР	ΚY	СҮ	LT	UC	KC	LT	KR
S	u	С	С	е	S	S	_	u	1	_	е	С	i	_	_	е	_	_	е	n
ΚT	KR	LT	LT	UT	LC	ΚY	LT	UC	LC	LT	ΓЬ	LT	UC	UR	KR	UP	LT	UR	KR	UR
—	n	е	е	_	S	_	е	-	S	е	—	е	-	а	n	С	е	а	n	а
LY	ΥP	LC	СР	LC	СР	KR	ΚT	YC	СР	KΤ	СР	LR	KR	UR	KR	UT	LΥ	YС	UP	СТ
1	У	S	i	S	i	n	-	u	i	_	i	_	n	а	n	_	1	u	С	_

What might the first word be? Now it looks like SUCCESSFUL, giving us one more letter. UR, UP, CC, CP, and KR contain letters in proper Alphabetic order with the right spacing to fill in the blanks since L & E are already filled in.



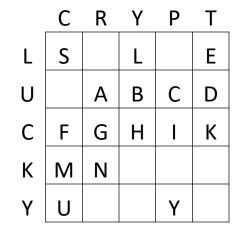
E-8.Checkerboard. A thought from Parker Hitt. (analysis) ARTEMIS UP LT LC LC CC YC LY UT LT UP CP KY CY LT UC KC LT KR T.C. YC IJΡ f C ρ S S 11 е С S 11 ρ n Т.Т UC ЪС Т.Т Τ.P UR KR UR KR Т.Т TT TIT ЪС KΥ Т.Т UC UR KR ΠP Т.Т S е а YC CP T.C CP KR KТ CP KТ CΡ T.R KR IIR KR IJΨ ΠP СТ 1 S i i n V S Ť. n u Í. а n

What might the first word be? Now it looks like SUCCESSFUL, giving us one more letter. UR, UP, CC, CP, and KR contain letters in proper Alphabetic order with the right spacing to fill in the blanks since L & E are already filled in.



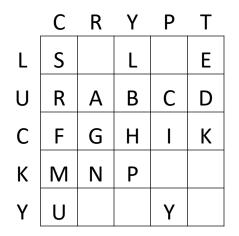
E-8.Checkerboard. A thought from Parker Hitt. (analysis) ARTEMIS T.C. YC ΠP Т.T UC KC LT KR IJΡ f 1 d C ρ S S 11 е C S 11 ٦ m ρ n UC UΡ Т.Т LC KΥ LTЪС Т.Т Τ.P KR Т.Т KR UR KR ΠŢ Т.Т UC UR UR d е а T,Y CP T.C CP KR YC CP KТ CΡ T.R KR UR KR UΤ YC ΠP СТ 1 S i i d k V S Ť. n u n а n 11

What might the second word be?



E-8	8.C1	necl	kerl	ooai	rd.	A 1	thou	ıght	c fi	rom	Par	rkei	r Hi	itt	. (a	ana	lys	is)	AR	CEMIS
LC	YC	UP	UP	LT	LC	LC	СС	YС	LY	UT	LT	UP	СР	ΚY	СҮ	LT	UC	KC	LT	KR
S	u	С	С	е	S	S	f	u	l	d	е	С	i	_	h	е	_	m	е	n
ΚT	KR	LT	LT	UT	LC	ΚY	LT	UC	LC	LT	LΡ	LT	UC	UR	KR	UP	LT	UR	KR	UR
-	n	е	е	d	S	_	е	_	S	е	_	е	_	а	n	С	е	а	n	a
LY	ΥP	LC	СР	LC	СР	KR	ΚT	YC	СР	ΚT	СР	LR	KR	UR	KR	UT	LΥ	YС	UP	СТ
1	У	S	i	S	i	n	_	u	i	_	i	_	n	а	n	d	1	u	С	k

What might the second word be? It might be DECIPHERMENT, giving us P and R. The remaining letters are quickly guessed.

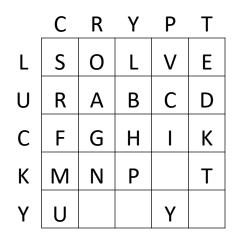


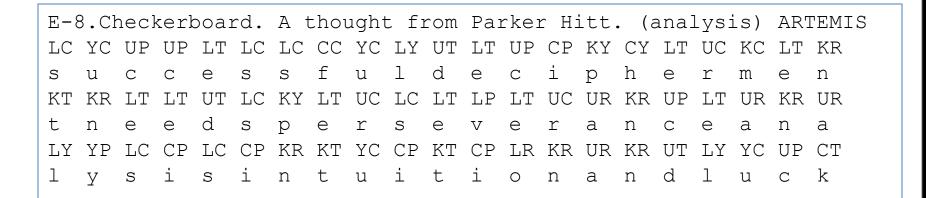
E-3	8.Cl	hecl	ker	ooai	rd.	A t	thou	ıght	c fi	rom	Par	rkei	r Hi	itt	. (a	ana	Lys	is)	ART	[EMIS
LC	YC	UP	UP	LT	LC	LC	СС	YС	LY	UT	LT	UP	СР	ΚY	СҮ	LT	UC	KC	LT	KR
S	u	С	С	е	S	S	f	u	l	d	е	С	i	р	h	е	r	m	е	n
ΚT	KR	LT	LT	UT	LC	ΚY	LT	UC	LC	LT	LΡ	LT	UC	UR	KR	UP	LT	UR	KR	UR
-	n	е	е	d	S	р	е	r	S	е	_	е	r	а	n	С	е	а	n	a
LY	ΥP	LC	СР	LC	СР	KR	ΚT	YC	СР	ΚT	СР	LR	KR	UR	KR	UT	LΥ	YС	UP	СТ
1	У	S	i	S	i	n	_	u	i	_	i	_	n	а	n	d	1	u	С	k

The remaining letters are quickly guessed.

That gives us O, T, and V.

Decipher is complete. The remaining letters in the keysquare can easily be filled in.





The keysquare is now complete.

Record the solution so you could later submit

it for credit. We can give the key and plaintext.

	С	R	Υ	Ρ	Т
L	S	0	L	V	Ε
U	R	А	В	С	D
С	F	G	н	I	К
К	Μ	Ν	Р	Q	Т
Y	U	W	Х	Y	Z

E-8 LUCKY/CRYPT/SOLVER successful decipherment needs perseverance, analysis, intuition, and luck

E-8.Checkerboard. A thought from Parker Hitt. (analysis) ARTEMIS YC UP UP LT LC LC CC YC LY UT LT UP CP KY CY LT UC KC LT KR ЪС s s f u l d e c с е i h р е 11 S r m е n LT UT LC KY LT UC LC LT LP LT UC UR KR UP LT UR KR KR LT UR d е е е r t S р е S V е r а n а CP LC CP KR KT YC CP KT UT LY YP LC CP T.R KR UR KR YC ΠP СТ i n t u i t i V i S Ο n а d k S n 11

The digraphs of Checkerboard ciphers help in guessing letters, especially if you correctly guessed the Row/Column keywords.

Good Solving!



Thank you. Try another. Try the ACA!

The American Cryptogram Association (ACA) is a non-profit organization dedicated to promoting the hobby and art of cryptanalysis – learning to break ciphers. And we write ciphers, too. Our Sample Issue and all its solution tutorials are available on our website:

www.cryptogram.org/resource-area/sample-issue-cryptogram/