

# Examples of Solving *Cm* Cons\*



Solving E-7 from Sample *Cm*  
Complete Columnar Transposition

\* “*Cm* Cons” means “cipher constructions in *The Cryptogram*” -- the bi-monthly publication for members of the American Cryptogram Association (ACA) -- [www.cryptogram.org](http://www.cryptogram.org)

# 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 [nudge@cryptogram.org](mailto:nudge@cryptogram.org)

# References

- The ACA and You, Ch. 4, How to Solve a Problem in *The Cryptogram*.

# What is a Complete Columnar Transposition?

- This is a transposition cipher, based on a rectangular block. (ACA Guideline: The block should have 8-15 rows)
- Plaintext letters are written by rows into the block. All rows must be complete.
- Ciphertext is formed by taking off the rows of the block in an order determined by a key.

# Complete Columnar Transposition Example

Plaintext: Come at once and bring your brotherX  
Length is 30. We'll use 5 columns, key=STAGE.

# Complete Columnar Transposition Example

Plaintext: Come at once and bring your brotherX  
Length is 30. We'll use 5 columns, key=STAGE.

s t a g e

4 5 1 3 2

C	O	M	E	A
T	O	N	C	E
A	N	D	B	R
I	N	G	Y	O
U	R	B	R	O
T	H	E	R	X

# Complete Columnar Transposition Example

Plaintext: Come at once and bring your brotherX

s t a g e

4 5 1 3 2

C	O	M	E	A
T	O	N	C	E
A	N	D	B	R
I	N	G	Y	O
U	R	B	R	O
T	H	E	R	X

Reorder the columns

1 2 3 4 5

M	A	E	C	O
N	E	C	T	O
D	R	B	A	N
G	O	Y	I	N
B	O	R	U	R
E	X	R	T	H

# Complete Columnar Transposition Example

Plaintext: Come at once and bring your brotherX

s t a g e

4 5 1 3 2

C	O	M	E	A
T	O	N	C	E
A	N	D	B	R
I	N	G	Y	O
U	R	B	R	O
T	H	E	R	X

Reorder the columns

1 2 3 4 5

M	A	E	C	O
N	E	C	T	O
D	R	B	A	N
G	O	Y	I	N
B	O	R	U	R
E	X	R	T	H

Take off  
Ciphertext by  
columns

Ciphertext: MNDGB EAERO OXECB YRRCT AIUTO ONNRH



# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

What does the first line tell us?

Cipher ID: E-7.

Type: Complete Columnar Transposition.

Title: No title.

Crib: ball. (word appears in the plaintext.)

Created by ACA member WALRUS

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

There are 84 letters which must fill a rectangular block. But what is the size of that block?

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

There are 84 letters which must fill a rectangular block. But what is the size of that block? The factors of 84 are:  $2 \times 2 \times 3 \times 7$ .

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

There are 84 letters which must fill a rectangular block. But what is the size of that block? The factors of 84 are:  $2 \times 2 \times 3 \times 7$ . The block could be 6 cols x 14 rows, or 7 cols x 12 rows. Both sizes are within the ACA guidelines (8-15 rows).

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

Try 7 x 12. Fill in the block by columns.  
(Strips of paper with the column letters  
also work well.)

E	T	L	E	H	A	A
C	E	O	S	B	S	E
T	V	A	T	S	Y	H
P	I	P	S	U	L	H
S	T	N	R	H	C	E
T	O	T	I	T	U	E
A	O	E	O	O	Y	O
A	A	E	H	T	E	A
N	W	Y	P	R	D	A
E	B	T	W	E	D	E
L	U	T	T	H	E	H
N	R	L	H	L	T	P

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

Try 7 x 12. Fill in the block by columns.  
Search for the crib: ball. There are two Bs.

E	T	L	E	H	A	A
C	E	O	S	B	S	E
T	V	A	T	S	Y	H
P	I	P	S	U	L	H
S	T	N	R	H	C	E
T	O	T	I	T	U	E
A	O	E	O	O	Y	O
A	A	E	H	T	E	A
N	W	Y	P	R	D	A
E	B	T	W	E	D	E
L	U	T	T	H	E	H
N	R	L	H	L	T	P

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

Try 7 x 12. Fill in the block by columns.  
Search for the crib: ball. There are two Bs.  
Neither B has the letters ALL on the same  
line or the subsequent line.  
This must be the wrong size.

E	T	L	E	H	A	A
C	E	O	S	B	S	E
T	V	A	T	S	Y	H
P	I	P	S	U	L	H
S	T	N	R	H	C	E
T	O	T	I	T	U	E
A	O	E	O	O	Y	O
A	A	E	H	T	E	A
N	W	Y	P	R	D	A
E	B	T	W	E	D	E
L	U	T	T	H	E	H
N	R	L	H	L	T	P

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

Try 6 x 14. Fill in the block by columns.  
Search for the crib: ball.

E	V	N	O	R	E
C	I	T	H	E	T
T	T	E	P	H	A
P	O	E	W	L	E
S	O	Y	T	A	H
T	A	T	H	S	H
A	W	T	H	Y	E
A	B	L	B	L	E
N	U	E	S	C	O
E	R	S	U	U	A
L	L	T	H	Y	A
N	O	S	T	E	E
T	A	R	O	D	H
E	P	I	T	D	P



# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

Try 6 x 14. Fill in the block by columns.

Search for the crib: ball.

This block has both Bs in row 8, along with  
A, L, L, and E. The crib must be in row 8.

E	V	N	O	R	E
C	I	T	H	E	T
T	T	E	P	H	A
P	O	E	W	L	E
S	O	Y	T	A	H
T	A	T	H	S	H
A	W	T	H	Y	E
A	B	L	B	L	E
N	U	E	S	C	O
E	R	S	U	U	A
L	L	T	H	Y	A
N	O	S	T	E	E
T	A	R	O	D	H
E	P	I	T	D	P

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

Looking only at the first 9 rows...

What does the crib tell us about the original order of the columns?

	1	2	3	4	5	6
E	V	N	O	R	E	
C	I	T	H	E	T	
T	T	E	P	H	A	
P	O	E	W	L	E	
S	O	Y	T	A	H	
T	A	T	H	S	H	
A	W	T	H	Y	E	
A	B	L	B	L	E	
N	U	E	S	C	O	

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

Looking only at the first 9 rows...

What does the crib tell us about the original order of the columns? Some combination of four columns must spell BALL.

	1	2	3	4	5	6
E	V	N	O	R	E	
C	I	T	H	E	T	
T	T	E	P	H	A	
P	O	E	W	L	E	
S	O	Y	T	A	H	
T	A	T	H	S	H	
A	W	T	H	Y	E	
A	B	L	B	L	E	
N	U	E	S	C	O	

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

Looking only at the first 9 rows...

What does the crib tell us about the original order of the columns? Some combination of four columns must spell BALL. Then the key order must contain 2 or 4 (B), 1 (A), and followed by either 35 or 53 (LL). Which of these will be correct?

	1	2	3	4	5	6
E	V	N	O	R	E	
C	I	T	H	E	T	
T	T	E	P	H	A	
P	O	E	W	L	E	
S	O	Y	T	A	H	
T	A	T	H	S	H	
A	W	T	H	Y	E	
A	B	L	B	L	E	
N	U	E	S	C	O	

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

We'll look at it bit by bit. There are only  
Two choices for the columns with "ALL"  
in row 8: 153 and 135. Look at  
These two combinations to see  
which looks more promising.

1	3	5	1	5	3
E	N	R	E	R	N
C	T	E	C	E	T
T	E	H	T	H	E
P	E	L	P	L	E
S	Y	A	S	A	Y
T	T	S	T	S	T
A	T	Y	A	Y	T
A	L	L	A	L	L
N	E	C	N	C	E

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
 ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP  
 WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

Of the two choices to form “ALL” in  
 row 8, rows 1, 3, 5, and 6 look a bit more  
 English-like in the 153 version. We will  
 assume 153 is correct. Now which  
 B column fits better in front of 153: 2 or 4?

1	3	5		1	5	3
E	N	R	*	E	R	N
C	T	E		C	E	T
T	E	H	*	T	H	E
P	E	L		P	L	E
S	Y	A	*	S	A	Y
T	T	S	*	T	S	T
A	T	Y		A	Y	T
A	L	L		A	L	L
N	E	C		N	C	E

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

These are the two choices to add “B” to  
“ALL”. Which choice looks like it makes  
better English?

2	4	1	5	3
V	O	E	R	N
I	H	C	E	T
T	P	T	H	E
O	W	P	L	E
O	T	S	A	Y
A	H	T	S	T
W	H	A	Y	T
B	B	A	L	L
U	S	N	C	E

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

These are the two choices to add “B” to  
“ALL”. Which choice looks like it makes  
better English? Look at rows 1, 2, 6, and 9.  
The combinations made with 4+153 seem  
unlikely, whereas the combinations with  
2+153 seem more likely.  
We’ll guess it’s 2153.

2		4	1	5	3
V	*	O	E	R	N
I	*	H	C	E	T
T		P	T	H	E
O		W	P	L	E
O		T	S	A	Y
A	*	H	T	S	T
W		H	A	Y	T
B		B	A	L	L
U	*	S	N	C	E



# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

With 2153 known, only two columns  
remain to be placed. Where will  
columns 4 & 6 fit best?

4	6	2	1	5	3
O	E	V	E	R	N
H	T	I	C	E	T
P	A	T	T	H	E
W	E	O	P	L	E
T	H	O	S	A	Y
H	H	A	T	S	T
H	E	W	A	Y	T
B	E	B	A	L	L
S	O	U	N	C	E

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
 ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP  
 WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

With 2153 known, only two columns remain to be placed. Where will columns 4 & 6 fit best? Rows 3 & 4 point the way.

4	6	2	1	5	3
O	E	V	E	R	N
H	T	I	C	E	T
P	A	T	T	H	E
W	E	O	P	L	E
T	H	O	S	A	Y
H	H	A	T	S	T
H	E	W	A	Y	T
B	E	B	A	L	L
S	O	U	N	C	E

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

With 2153 known, only two columns remain to be placed. Where will columns 4 & 6 fit best? Look at 6-2153 and row 4 contains EOPLE. If we follow with 4, then rows 3 & 4 give us AT THE PEOPLE. This looks very good.

4	6	2	1	5	3
O	E	V	E	R	N
H	T	I	C	E	T
P	A	T	T	H	E
W	E	O	P	L	E
T	H	O	S	A	Y
H	H	A	T	S	T
H	E	W	A	Y	T
B	E	B	A	L	L
S	O	U	N	C	E

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP. 6 2 1 5 3 4

Put the columns together with order

621534 for a last check to see if it still looks good.

E	V	E	R	N	O
T	I	C	E	T	H
A	T	T	H	E	P
E	O	P	L	E	W
H	O	S	A	Y	T
H	A	T	S	T	H
E	W	A	Y	T	H
E	B	A	L	L	B
O	U	N	C	E	S
A	R	E	U	S	U
A	L	L	Y	T	H
E	O	N	E	S	T
H	A	T	D	R	O
P	P	E	D	I	T

# Solving E-7 from Sample Cm

E-7. Complete Columnar Transposition. (ball) WALRUS  
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EYTT LESTS RIOHP  
WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

Record the solution so you could later submit it for credit. We give the column order and the beginning of the text. (WEASEL, VICTIM, YOGURT as a key would each give the same column order.)

**E-7 621534** ever notice that the people who say

	6	2	1	5	3	4
E	V	E	R	N	O	
T	I	C	E	T	H	
A	T	T	H	E	P	
E	O	P	L	E	W	
H	O	S	A	Y	T	
H	A	T	S	T	H	
E	W	A	Y	T	H	
E	B	A	L	L	B	
O	U	N	C	E	S	
A	R	E	U	S	U	
A	L	L	Y	T	H	
E	O	N	E	S	T	
H	A	T	D	R	O	
P	P	E	D	I	T	

# Solving E-7 from Sample Cm

In E-7, we quickly ruled out one size of rectangular block. Once the block size is known, strips of paper with the column ciphertext can be made and anagrammed. Alternatively, if you can visualize the rows vertically, horizontal strips are easy to print (or use lines in a text file).

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/](http://www.cryptogram.org/resource-area/sample-issue-cryptogram/)