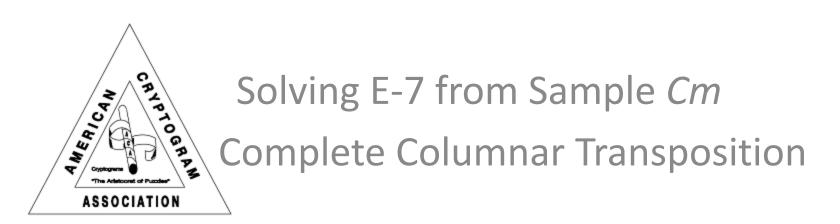
### Examples of Solving Cm Cons\*



<sup>\* &</sup>quot;Cm Cons" means "cipher constructions in The Cryptogram" -- the bi-monthly publication for members of the American Cryptogram Association (ACA) -- 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 <a href="mailto:nudge@cryptogram.org">nudge@cryptogram.org</a>

#### 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.

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

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
```

Plaintext: Come at once and bring your brotherX

S	t	a	g	е
4	5	1	3	2
С	0	M	Е	Α
Т	Ο	N	С	Е
Α	N	D	В	R
ı	Ν	G	Υ	0
U	R	В	R	0
Т	Н	E	R	Х

Reorder the columns

1	2	3	4	5
М	Α	Е	С	0
N	Ε	С	Т	0
D	R	В	Α	N
G	0	Υ	1	N
В	0	R	U	R
E	Χ	R	Т	Н

Plaintext: Come at once and bring your brotherX

S	t	a	g	е
4	5	1	3	2
С	0	M	Е	Α
Т	0	N	С	Е
Α	N	D	В	R
I	Ν	G	Υ	0
U	R	В	R	0
Т	Н	Ε	R	Х

Reorder the columns

_1	2	3	4	5
М	Α	Ε	С	0
N	Ε	С	Т	0
D	R	В	Α	N
G	0	Υ	I	N
В	0	R	U	R
Ε	Χ	R	Т	Н

Take off
Ciphertext by
columns

Ciphertext: MNDGB EAERO OXECB YRRCT AIUTO ONNRH

E-7. Complete Columnar Transpostion. (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

E-7. Complete Columnar Transpostion. (ball) WALRUS ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT 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?

E-7. Complete Columnar Transpostion. (ball) WALRUS ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT 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 x 2 x 3 x 7.

E-7. Complete Columnar Transpostion. (ball) WALRUS ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT 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 x 2 x 3 x 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).

E-7. Complete Columnar Transpostion. (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. (Strips of paper with the column letters also work well.)

```
S U L
```

E-7. Complete Columnar Transpostion. (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.

```
P S U L
```

E-7. Complete Columnar Transpostion. (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. Neither B has the letters ALL on the same line or the subsequent line. This must be the wrong size.

```
S
```

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

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

```
P
```

E-7. Complete Columnar Transpostion. (ball) WALRUS ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHF 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.

```
F
            Н
W T H Y
            Ε
            Н
            P
```

E-7. Complete Columnar Transpostion. (ball) WALRUS ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHF 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
Ε	V	Ν	0	R	Ε
С	I	Т	Н	Ε	Т
T	Т	Ε	Р	Н	Α
Р	0	Ε	W	L	Ε
S	0	Υ	Τ	Α	Н
Т	Α	Т	Н	S	Н
Α	W	Т	Н	Υ	Ε
Α	В	L	В	L	Ε
N	U	Ε	S	C	0

E-7. Complete Columnar Transpostion. (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
Ε	V	N	0	R	Ε
С	I	Т	Н	Ε	Т
Т	Т	Ε	Р	Н	Α
Р	0	Ε	W	L	Ε
S	0	Υ	Τ	Α	Н
Т	Α	Т	Н	S	Н
Α	W	Т	Н	Υ	Ε
Α	В	L	В	L	Ε
N	U	Ε	S	С	0

E-7. Complete Columnar Transpostion. (ball) WALRUS ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHF 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
Ε	V	N	0	R	Ε
С	I	Т	Н	Ε	Т
T	Т	Ε	Р	Н	Α
Р	0	Ε	W	L	Ε
S	0	Υ	Т	Α	Н
T	Α	Т	Н	S	Н
Α	W	Т	Н	Υ	Ε
Α	В	L	В	L	Ε
N	U	Ε	S	С	Ο

E-7. Complete Columnar Transpostion. (ball) WALRUS ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT 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
Ε	N	R	Ε	R	N
С	Т	Ε	С	Ε	Τ
Т	Ε	Н	Т	Н	Ε
Р	Ε	L	Р	L	Ε
S	Υ	Α	S	Α	Υ
Т	Т	S	Т	S	Т
Α	Т	Υ	Α	Υ	Τ
Α	L	L	Α	L	L
N	Ε	С	N	С	Ε

E-7. Complete Columnar Transpostion. (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
Ε	N	R	*	Ε	R	N
С	Т	Ε		С	Ε	Т
Т	Ε	Н	*	Т	Н	Ε
Р	Ε	L		Р	L	Ε
S	Υ	Α	*	S	Α	Υ
Т	Т	S	*	Т	S	Т
Α	Т	Υ		Α	Υ	Т
Α	L	L		Α	L	L
N	Ε	С		N	С	Ε

E-7. Complete Columnar Transpostion. (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	0	Ε	R	N
I	Н	С	Ε	Т
Т	Р	Т	Н	Ε
0	W	Р	L	Ε
0	Т	S	Α	Υ
Α	Н	Т	S	Τ
W	Н	Α	Υ	Τ
В	В	Α	L	L
U	S	N	С	Ε

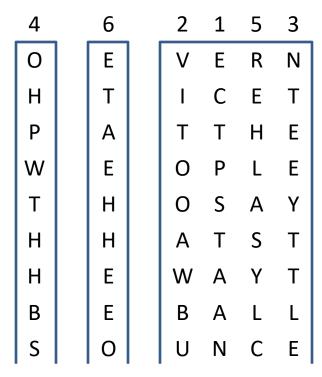
E-7. Complete Columnar Transpostion. (ball) WALRUS ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

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	*	0	Ε	R	N
ı	*	Н	С	Ε	Т
Т		Р	Т	Н	Ε
0		W	Р	L	Ε
0		Т	S	Α	Υ
Α	*	Н	Т	S	Т
W		Н	Α	Υ	Т
В		В	Α	L	L
U	*	S	N	С	Ε

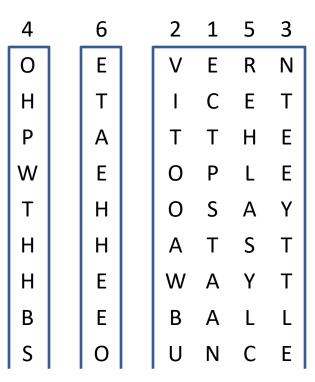
E-7. Complete Columnar Transpostion. (ball) WALRUS ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

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



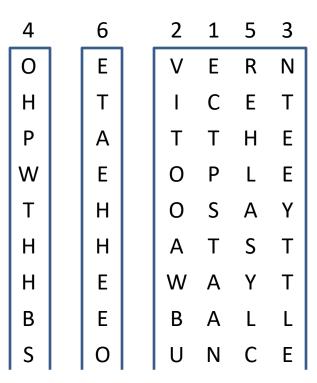
E-7. Complete Columnar Transpostion. (ball) WALRUS ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP WTHHB SUHTO TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

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



E-7. Complete Columnar Transpostion. (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.



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

Put the columns together with order 621534 for a last check to see if it still looks good.

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

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

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/