Examples of Solving *Cm* Cons*

Solving E-1 from Sample *Cm*

Route Transposition

* "*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 nudge@cryptogram.org

Solving a Route Transposition

Solving a Route Transposition is different from solving other cipher types. Patience is required. Lots of trials (and errors) when carefully checking different routes.

References

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

What is a Route Transposition cipher?

- A Route Transposition cipher uses a shape, like a rectanglular box, which will contain all the plaintext.

- Plaintext is entered into the box according to some rule (e.g., left to right, top to bottom).

- Ciphertext is formed by taking those same letters out of the box according to a separate rule (e.g., top to bottom, left to right).

What Types of Routes?

Some typical route types used:

- Horizontal, Alternating Horizontal

- Vertical, Alternating Horizontal

- Diagonal Up, Alternating Diagonal Up

- Diagonal Down, Alternating Diagonal Down

- Clockwise Spiral In, CW Spiral Out

- Counter Clockwise Spiral In, CCW Spiral Out

Examples of Types of Routes

6x5: TESTABCDEFGHIJKLMNOPQRSTUVWXYZ

Can you follow them all?

Horizontal

T	E	S	T	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

Alt Horizontal

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

Diagonal Up

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

Alt Diag. Up

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

CW Spiral In

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

CW Spiral Out

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

Vertical

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

Alt Vertical

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

Diagonal Down

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

Alt Diag. Down

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

CCW Spiral In

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

CCW Spiral Out

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

Route Transposition Example 1

PT: Solve a good crypt today.

```
S  O  L  V  E
A  G  O  O  D
C  R  Y  P  T
T  O  D  A  Y
```

CT: SACTO GROLO YDVOP AEDTY.

Route Transposition Example 1

PT: Solve a good crypt today. (pt in horiz.)

```
S  O  L  V  E
A  G  O  O  D
C  R  Y  P  T
T  O  D  A  Y
```

CT: SACTO GROLO YDVOP AEDTY. (CT out vert.)

Route Transposition Example 2

Spot the route to read the plaintext:

```
R E T E P
R E P I P
E K C I P
K C I P D
E P D E L
S R E P P
```

Route Transposition Example 2

Spot the route to read the plaintext:

```
R E T E P
R E P I P
E K C I P
K C I P D
E P D E L
S R E P P
```

Try left to right – nope.

Route Transposition Example 2

Spot the route to read the plaintext:

```
R  E  T  E  P
R  E  P  I  P
E  K  C  I  P
K  C  I  P  D
E  P  D  E  L
S  R  E  P  P
```

Try left to right – nope. Try right to left – better!

Route Transposition Example 2

Spot the route to read the plaintext:

```
R E T E P        ←──────────  1
R E P I P         ←──────────  2
E K C I P          ←─────────  3
K C I P D          ←──────────  4
E P D E L          ←──────────  5
S R E P P           ←─────────  6
```

PT: Peter Piper picked pickled peppers.

Route Transposition Example 3

Spot the route to read the plaintext:

```
E  E  B  S  L
R  S  S  A  E
O  E  L  E  S
H  H  L  S  E
S  T  E  S  H
A  Y  H  L  S
```

Route Transposition Example 3

Spot the route to read the plaintext:

```
E E B S L
R S S A E
O E L E S
H H L S E
S T E S H
A Y H L S
```

Note EHT in second column.

Route Transposition Example 3

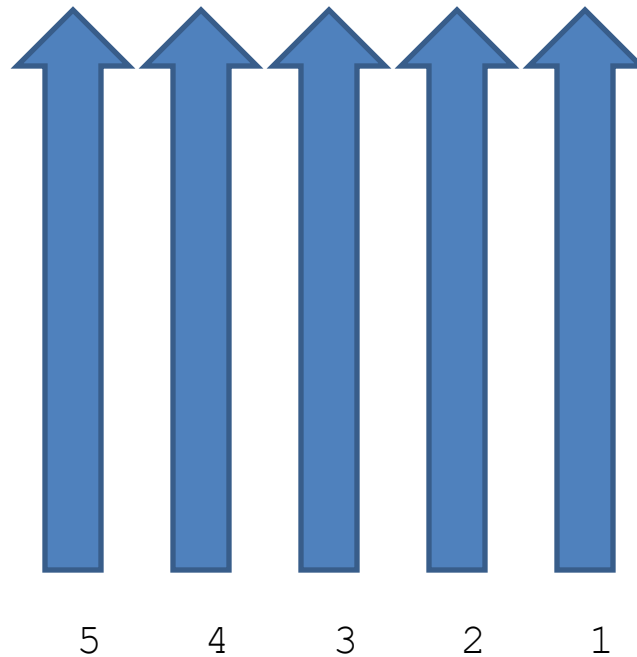Spot the route to read the plaintext:

```
E E B S L
R S S A E
O E L E S
H H L S E
S T E S H
A Y H L S
```

Note EHT in second column. EHS in last.

Route Transposition Example 3

Spot the route to read the plaintext:

```
E  E  B  S  L
R  S  S  A  E
O  E  L  E  S
H  H  L  S  E
S  T  E  S  H
A  Y  H  L  S
```

5   4   3   2   1

PT: She sells sea shells by the sea shore.

Route Transposition Example 4

Spot the route to read the plaintext:

```
E Y L E X
R N A S S
O E U Y R
C V Q T A
S E E H E
R S S G Y
U D R I N
O N A E E
F A E S V
```

Route Transposition Example 4

Spot the route to read the plaintext:

```
E Y L E X
R N A S S        There is one Q.
O E U Y R
C V Q T A
S E E H E
R S S G Y
U D R I N
O N A E E
F A E S V
```

Route Transposition Example 4

Spot the route to read the plaintext:

```
E  Y  L  E  X
R  N  A  S  S
O  E  U  Y  R
C  V  Q  T  A
S  E  E  H  E
R  S  S  G  Y
U  D  R  I  N
O  N  A  E  E
F  A  E  S  V
```

There is one Q, and a U above it.

Route Transposition Example 4

Spot the route to read the plaintext:

```
E  Y  L  E  X
R  N  A  S  S
O  E  U  Y  R
C  V  Q  T  A
S  E  E  H  E
R  S  S  G  Y
U  D  R  I  N
O  N  A  E  E
F  A  E  S  V
```

There is one Q, and a U above it.

Try reading up the columns.

Route Transposition Example 4

Spot the route to read the plaintext:

```
E  Y  L  E  X
R  N  A  S  S
O  E  U  Y  R
C  V  Q  T  A
S  E  E  H  E
R  S  S  G  Y
U  D  R  I  N
O  N  A  E  E
F  A  E  S  V
```

There is one Q, and a U above it.

Try reading up the columns.

"Fourscore and seven years
equals eighty seven years."

Route Transposition Example 4

Spot the route to read the plaintext:

```
E  Y  L  E  X
R  N  A  S  S
O  E  U  Y  R
C  V  Q  T  A
S  E  E  H  E
R  S  S  G  Y
U  D  R  I  N
O  N  A  E  E
F  A  E  S  V
```

There is one Q, and a U above it.

Try reading up the columns.

"Fourscore and seven years
equals eighty seven years."

Hindsight: X null at the end.

Route Transposition Example 5

Spot the route to read the plaintext:

```
G  O  D  Y  Z
A  L  E  H  T
R  E  V  O  S
P  M  U  J  X
O  F  N  W  O
R  B  K  C  I
U  Q  E  H  T
```

Route Transposition Example 5

Spot the route to read the plaintext:

```
G  O  D  Y  Z
A  L  E  H  T      EHT in two rows.
R  E  V  O  S
P  M  U  J  X
O  F  N  W  O
R  B  K  C  I
U  Q  E  H  T
```

Route Transposition Example 5

Spot the route to read the plaintext:

```
G  O  D  Y  Z
A  L  E  H  T      EHT in two rows.
R  E  V  O  S      UQ in last row.
P  M  U  J  X      Try reading R-L from bottom.
O  F  N  W  O
R  B  K  C  I
U  Q  E  H  T
```

Route Transposition Example 5

Spot the route to read the plaintext:

```
G O D Y Z
A L E H T    EHT in two rows.
R E V O S    UQ in last row.
P M U J X    Try reading R-L from bottom.
O F N W O
R B K C I    "The quick brown fox jumps
U Q E H T      over the lazy dog."
```

Ready for E-1 from Sample *Cm?*

We have listed a variety of routes.

The variations help cover different orientations. Testing Horizontal 6x5 is basically the same as testing Vertical 5x6. This simplifies the task.

Now let's attempt to solve E-1 from Sample *Cm*.

Getting started: General Tips

Compute the length of ciphertext. Any unusual letters to spot/watch? What are the factors of the size? What size rectangle do they suggest? Choose a size to try.

Try writing ciphertext into a rectangle by some route. Look carefully to see if, by following some other route, plaintext can be found. If not, try writing-in with a different route. Be patient.

Solving E-1 from Sample *Cm*

```
E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.
```

What does the first line tell us?

Cipher ID: E-1

Type: Route Transposition

Title: Oversimplification.

Created by ACA member D'PLUME

Solving E-1 from Sample *Cm*

```
E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.
```

Cipher ID: E-1

Type: Route Transposition

Title: Oversimplification.

Created by ACA member D'PLUME

Length is 56 (Factors: 2 * 2 * 2 * 7)

Solving E-1 from Sample *Cm*

```
E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.
```

Cipher ID: E-1

Type: Route Transposition

Title: Oversimplification.

Created by ACA member D'PLUME

Length is 56 (Factors: 2 * 2 * 2 * 7)

Could be rectangle of 7x8, 8x7, 4x14, etc. Try 7x8.

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Horizontal

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

Write in by Horizontal?

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Horizontal

```
I  P  S  X  E  T  R
R  A  I  E  E  R  U
I  O  Y  O  S  O  S
F  V  L  E  L  T  N
R  C  B  I  N  W  G
E  P  H  O  I  O  O
L  M  A  R  M  T  S
D  E  P  N  M  E  L
```

Write in by Horizontal?

This cipher has only one H. Find and focus around the H to check for acceptable plaintext. Check all the various routes.

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Horizontal

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

Write in by Horizontal?

Nothing hopeful spotted.

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Vertical

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

Write in by Vertical?

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Vertical

```
I  A  Y  E  N  O  S
P  I  O  L  W  O  D
S  E  S  T  G  L  E
X  E  O  N  E  M  P
E  R  S  R  P  A  N
T  U  F  C  H  R  M
R  I  V  B  O  M  E
R  O  L  I  I  T  L
```

Write in by Vertical?

Nothing hopeful spotted.

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Clockwise from UL

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

Write in by Clockwise spiral?

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Clockwise from UL

```
I  P  S  X  E  T  R
L  T  N  R  C  B  R
E  M  A  R  M  I  A
L  L  M  E  T  N  I
V  O  N  L  S  W  E
F  O  P  E  D  G  E
S  I  O  H  P  E  R
O  S  O  Y  O  I  U
```

Write in by Clockwise spiral?

Nothing hopeful spotted.

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Anti-Clockwise from UL

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

Write in by Counter-clockwise spiral?

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Anti-Clockwise from UL

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

Write in by Counter-clockwise spiral?

Nothing hopeful spotted.

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Diagonal Up L-R

```
I  S  T  I  I  S  N
P  E  A  U  O  T  G
X  R  R  S  L  W  O
R  E  O  E  N  I  R
E  Y  L  I  O  A  D
O  V  B  H  M  S  N
F  C  P  L  T  P  E
R  E  O  M  E  M  L
```

Write in by Diagonals, sloping up?

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Diagonal Up L-R

```
I   S   T   I   I   S   N
P   E   A   U   O   T   G
X   R   R   S   L   W   O
R   E   O   E   N   I   R
E   Y   L   I   O   A   D
O   V   B   H   M   S   N
F   C   P   L   T   P   E
R   E   O   M   E   M   L
```

Write in by Diagonals, sloping up?

The H is next to T, but nothing more.

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Diagonal Down L-R

```
I P X R E O F
S E R E Y V R
T A R O L C E
I U S E B P O
I O L I H L M
S T N O M T E
N W I A S P M
G O R D N E L
```

Write in by Diagonals, sloping down?

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Diagonal Down L-R

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

Write in by Diagonals, sloping down?

Now the H is between T and E on the opposite diagonal. This looks hopeful!

I can see "THERE" on a diagonal reading from bottom to top, from right to left. Can you spot more plaintext?

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Diagonal Down L-R

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

Write in by Diagonals, sloping down.

"THERE" is on a diagonal reading from right to left, bottom to top.

Read along those diagonals?

We get "F" then "RO" then "EVE" then "OCYR". "Froeveocyr". Not so good.

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Diagonal Down L-R

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

Write in by Diagonals, sloping down.

What if we read those diagonals from top to bottom?

We get "F" then "OR" then "EVE" then "RYCO". "Foreveryco" – not bad, but it does not continue well.

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Diagonal Down L-R

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

Write in by Diagonals, sloping down.

THERE was going from bottom to top. Try Alternating Diagonals, R-L. Start in top right corner.

Read up (F), then down (OR), then up (EVE), then down (RYCO), etc.

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Diagonal Down L-R

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

Write in by Diagonals, sloping down.

Read plaintext on Alternating Diagonals, R-L. Start in top right corner.

Read up (F), then down (OR), then up (EVE), then down (RYCO), etc.

Solving E-1 from Sample *Cm*

E-1. Route transposition. Oversimplification. D'PLUME
IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA
RMTSD EPNME L.

Diagonal Down L-R

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

Write in by Diagonals, sloping down.

Read plaintext on Alternating Diagonals, R-L. Start in top right corner.

Record the solution so you could later submit it for credit.

E-1 For every complex problem there is a simple solution and it is wrong.

Solving E-1 from Sample *Cm*

Solving a Route Transposition can be frustrating, but it is very satisfying when you find the combination that solves it.
Try write-in routes one at a time, thoroughly checking for plaintext by other routes.

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/