Spring 2015
Chris Christensen
CSC/MAT 483

Other Transposition Cipher

Railfence ciphers

A very simple form of [transposition cipher] is the rail fence, named for its fencelike appearance, which is the result of aligning rows of letters, then shifting them. The rail fence was a popular method in the early decades of cryptography. It faded with the rise of more complex systems such as nomenclators in the Middle Ages and codebooks in the 15th and 16th centuries. It regained some of its popularity during the American Civil War, when it was used for concealments of military messages as well as by Union and Confederate spies. *Code, Ciphers, & Other Cryptic & clandestine Communication*, Fred B. Wrixon.

Here is a message:

```
thisattackdependedonaweaknessintheprotocol
```

Here is the railfence with two rails:

```
t   i   a   t   c   d   p   n   e   o   a   e   k   e   s   n   h   p   o   o   o
  h   s   t   a   k   e   e   d   d   n   w   a   n   s   i   t   e   r   t   c   l
```

The rails may be taken off in either order for the ciphertext; here we take the first row first:

```
TIATCDPNEOAEKESNHPOOAHSTAKEEDDNWANSITERTCL
```

Breaking into five-letter blocks, we get:

```
TIATC  DPNEO  AEKES  NHPOO  AHSTA  KEEDD  NWANS  ITERT  CL
```

The key is the number of rails and the order in which they are taken off.

Here is another message:

```
thebritishsoldcapturedenigmamachinestoformercolonies
```

Here is the railfence with three rails:

```
t    r    s    l      p    e    i     m     i    t    r    c    n
 h  b  i i  h o  d  a  t r  d n  g  a  a  h  n  s  o o  m r  o o  i  s
   e    t    s     c    u    e     m     c     e    f    e    l     e
```

We will take off the rows from top to bottom:

```
TRSLPEIMITRCNHBIIHODATRDNGAGHNSOOMROOISETSCUEMCEFELE
```

Breaking into five-letter blocks, we get:

```
TRSLP  EIMIT  RCNHB  IIHOD  ATRDN  GAGHN  SOOMR  OOISE  TSCUE  MCEFE
LE
```

In addition to determining the number of rails and the order in which they are removed, an offset may occur. Here is the last message with three rails and an offset of one:

```
_    b    i    o    a    r    n    a    h    s    o    r    o      s
 t  e  r t  s s  l c  p u  e e  i m  m c  i e  t f  r e  c l  n  e
   h    i    h    d    t    d    g    a    n    o    m    o     i
```

Rails could be taken off in various orders.

Double columnar transposition

During World War I, Germany used a double columnar transposition cipher called übchi. The difference between what we will do below and übchi is that übchi padded the last row of each encipherment by nulls – the number of nulls being the same as the number of words in the keyphrase. In what follows, we will do only the double columnar transposition and not pad the last rows.

The plaintext is

```
In about three hours I shall send a telegram of great
importance to the President and Secretary of State.
```

The keyphrase is one word – *cryptology*. There are 86 letters in the message; so, we will need 8 complete rows and one partial row. We will not pad the last row.

Encrypt once; in by rows and out by columns.

c	r	y	p	t	o	l	o	g	y
i	n	a	b	o	u	t	t	h	r
e	e	h	o	u	r	s	i	s	h
a	l	l	s	e	n	d	a	t	e
l	e	g	r	a	m	o	f	g	r
e	a	t	i	m	p	o	r	t	a
n	c	e	t	o	t	h	e	p	r
e	s	i	d	e	n	t	a	n	d
s	e	c	r	e	t	a	r	y	o
f	s	t	a	t	e				

```
IEALE  NESFH  STGTP  NYTSD  OOHTA  URNMP  TNTET  IAFRG
ARBOS  RITDR  ANELE  ACSES  OUEAM  OEETA  HLGTE  ICTRH
ERARD  O
```

Then re-encrypt with the same key; in by rows and out by columns.

c	r	y	p	t	o	l	o	g	y
I	E	A	L	E	N	E	S	F	H
S	T	G	T	P	N	Y	T	S	D
O	O	H	T	A	U	R	N	M	P
T	N	T	E	T	I	A	F	R	G
A	R	B	O	S	R	I	I	D	R
A	N	E	L	E	A	C	S	E	S
O	U	E	A	M	O	E	E	T	A
H	L	G	T	E	I	C	T	R	H
E	R	A	R	D	O				

```
ISOTA  AOHEF  SMRDE  TREYR  AICEC  NNUIR  AOIOS  TNFIS
ETLTT  EOLAT  RETON  RNULR  EPATS  EMEDA  GHTBE  EGAHD
PGRSA  H
```

Route Transposition

We have chosen the simple “in by rows and out by columns” to place plaintext into the rectangular array and to remove it. That is easy for the sender and receiver to remember. It is one example of route transposition.

An article by THEANO in the November/December 2005 issue of *The Cryptogram* summarizes the classical transposition routes.

> *Classic route transposition* is the plain-vanilla form of *geometric transposition*, which uses a square or rectangular grid to disarrange a text. The text is written into the grid by one route, and taken out of the grid by another route.

There are six basic patterns.

> *Orthogonal* routes are straight. A simple orthogonal route runs in a uniform direction, while a *boustrophedon* alternates back and forth (pronounces ‘boo-struh-FEED-n’ from the Greek for “as the ox turns” while plowing). *Diagonal* routes are slanted and, like orthogonals, they can be simple or boustophedonic. A regular *spiral* coils from the corner to the center of the grid; a *crab spiral* reverses the route. Except for the crab spirals, which were added later, these routes were introduced in 1916 by Colonel Parker Hitt in his *Manual for the Solution of Military Ciphers*, a best-seller among soldiers and civilians alike.

Patterns for Classic Transposition Routes

Orthogonal

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

Diagonal

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

Spiral

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

Orthogonal Boustrophedon

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

Diagonal Boustrophedon

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

Crab Spiral

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

To each of these patterns is associated eight route transpositions; the other routes are obtained from the pattern by reflection or transposition (interchanging rows and columns). Consider the pattern for the orthogonal routes:

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

There are four reflections based upon this pattern: Top row -- no reflection and reflection in a vertical line. Bottom row – reflection in a horizontal line and reflection in a vertical line followed by reflection in a horizontal line.

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

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

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

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

And, there are the four transpositions of the arrays given above.

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

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

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

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

There are 48 ways to select a route to enter characters in an array, and there are 47 ways to select a route to remove characters from an array. So, there are $48\times 47 = 2256$ possible route transposition ciphers based upon these six patterns.

"In by rows and out by columns" corresponds to using the basic orthogonal route to enter characters into the array and using the transposition of the basic orthogonal route to remove characters from the array.

Turning grille

The Italian cryptographer (mathematician, physician, …) Cardano (1501 – 1576) used grilles to hide messages. For example, the ciphertext could (be arranged into) a meaningless square array of letters or words.

T	C	H	R	O	L
G	Y	P	K	K	T
U	F	R	O	M	D
L	X	G	C	Y	I
Z	S	Y	F	P	I
C	X	U	E	M	N

The grille was a square divided into cells. Some of the cells were cut out.

	X		X		
	X	X			X
			X		
X		X		X	X
	X		X		
		X			X

When the grille was placed over the ciphertext, the meaningless letters or words were covered up and the plaintext message appeared in the cut out cells of the grille.

	C		R		
	Y	P			T
			O		
L		G		Y	I
	S		F		
		U			N

The turning grille has little in common with that grille. The turning grille is often called the Fleissner grille after its inventor the Austrian cryptologist Eduard

Fleissner von Wostrowitz (1825 – 1888), who wrote *Handbuch der Kryptographie. Anleitung zum Chiffriren und Dechiffriren von Geheimschriften* (1881).

> The turning grille is usually a square … divided into cells. One quarter of these are punched out in a pattern such that when the grille is rotated to its four positions, all the cells on the paper beneath will be exposed and none will be exposed more than once. (The Codebreakers by David Kahn)

Here is a turning grille for a 6×6 square.

X			X		
	X	X			X
X			X		
		X			X

The Xs are the cells that are “punched out.”

We’ll take the first 36 letters of the plaintext message `the Enigma cipher machine had the confidence of German forces who depended on its security` and encipher them with the turning grille.

```
Theenigma  ciphermac  hinehadth  econfiden
```

We place the first nine letters in the punched out cells of the grille.

T			H		
	E	E			N
I			G		
		M			A

Now we rotate the grille 90° counterclockwise and place the next nine letters in the punched out cells of the grille.

	C			I	
P			H		
	E			R	
	M				
A			C		

Rotate again.

H			I		
		N			E
H			A	D	
		T			H

And, again.

		E			C
				O	
	N			F	
		I			D
	E			N	

Removing the grille leaves the square

T	C	E	H	I	C
H	E	E	I	O	N
P	N	N	H	F	E
I	E	I	G	R	D
H	M	M	A	D	A
A	E	T	C	N	H

The ciphertext can be read off in any pattern to which the sender and receiver have agreed.

> At the end of 1916, transposition messages again appeared in German military communications.
>
> By January, 1917, the French cryptanalysts recognized these as turning grilles. … The Germans provided their signal troops with a variety of sizes for different length messages. Each grille had a codename: ANNA for 25 letters, BERTA for 36, CLARA, 49, DORA, 64, EMIL, 81, FRANZ, 100. These codes names were changed weekly.
>
> Grille systems are particularly susceptible to multiple anagramming – which is the general solution of transposition systems – because their sections are of necessity of equal length. But the system produces intriguing geometrical symmetries, and the French soon devised attacks exploiting this and other weaknesses. The grilles lasted four months. (The Codebreakers by David Kahn)

If the length of the sides of the grille is odd, there is a cell in the center. Sender and receiver should agree how to use (or not use) that cell.

Double Cross

The following is the scheme used by “Snow” the first Double Cross agent [In World War II, the Double Cross agents were German agents in England who had been captured by the British and turned on the Germans. They transmitted false information back to their German controllers.] This example is taken from Appendix I of *Action This Day* and is based upon material in the (British) Public Records Office.)

Snow used a transposition cipher to communicate with his German controller. The cipher used the keyword *congratulations* – so, 15 columns. The cipher array had 12 rows. Initially, some cells in the array were left blank. The blanks were determined as follows: The first blank is arbitrarily determined, say at the fifth cell of the first row. The next blank cell is at the 5 + 6 = 11th spot. The next at the 11 + 7 = 18th spot. Etc. The blanks are in cells 5, 11, 18, 26, 35, 45, 56, 68, and 81. This places blank cells in the array half way down. The array is then turned upside down and the same procedure is followed so that the blank cells are symmetrical.

C	O	N	G	R	A	T	U	L	A	T	I	O	N	S
3	9	7	4	11	1	13	15	6	2	14	5	10	8	12
				X						X				
		X								X				
				X										X
										X				
							X							
					X									
									X					
							X							
				X										
X										X				
				X								X		
				X						X				

The plaintext message was put “in by rows” skipping the blank cells. Then the blanks are filled in with nulls. Ciphertext is taken “out by columns,” but there is a twist. The columns are not always “taken out” in the same order; the order depends on the date on the message. If the date were the 8th, the first column taken out would be column 8. Then columns 9, 10, 11, 12, 13, 14, 15, 1, 2, 3, 4, 5, 6, and 7 are taken out.

Prior to the transmission of the ciphertext, the time, date, and number of letters in the message is transmitted, but this information is encoded. The keyword is used to encode the message information.

```
C O N G R A T U L A T I O N S
1 2 3 4 5 6 7 8 9     0     0
```

Repeated letters are not used and either I or S is used to represent 0.

The time of transmission is encoded using this letter/number correspondence. For example, 2230 would be OONI (or OONS) and 1245 would be COGR. The date (day and month only) and the total number of letters (including the nulls) are encoded in a similar way.

Skytale

Probably the most famous transposition cipher and the first cryptological device is the skytale (or scytale; rhymes with Italy).

> It was the Spartans, the most warlike of the Greeks, who established the first system of military cryptography. As early as the fifth century B.C., they employed a device called the “skytale,” the earliest apparatus used in cryptology and one of the few ever devised in the whole history of the science for transposition ciphers. The skytale consists of a staff of wood around which a strip of papyrus or leather or parchment is wrapped close-packed. The secret message is written on the parchment down the length of the staff; the parchment is then unwound and sent on its way. The disconnected letters make no sense unless the parchment is rewrapped around a baton of the same thickness as the first: then the words leap from loop to loop forming the message. David Kahn, *The Codebreakers*

wikipedia

Suppose that parchment is wrapped around the rod so that 4 letters can be placed around the rod. Consider the message `department of mathematics`. The plaintext message contains 23 letters. There will be 4 “columns” on the parchment around the rod.

d	m	m	a
e	e	a	t
p	n	t	i
a	t	h	c
r	o	e	s
t	f	m	

This would unroll to `DMMAEEATPNTIATHCROESTFM`. The key is the diameter of the rod, which determines the number of columns.

The method of using the skytale that we have described corresponds to using a columnar transposition “in by columns and out by rows.”