Transposition Ciphers

Up to this point, the ciphers that we have used have been substitution ciphers – plaintext letters were replaced by other letters or numbers or symbols. Another type of cipher is the transposition cipher. Transposition ciphers use the letters of the plaintext message, but they permute the order of the letters.

It should be easy to spot a transposition cipher because the letter frequencies should mimic the usual frequencies for English – high frequencies for `a, e, i, n, o r, s, t`.

But, cryptanalysis of a transposition cipher might be difficult. The essential technique is anagramming – rearranging the ciphertext letters to "make sense."

The key to the cipher is the pattern of rearrangement.

Jumble

Another word game that appears in newspapers is Jumble. Each weekday Jumble consists of four words with scrambled letters – two five-letter words and two six-letter words – and a picture which has a clever caption that is determined by unscrambling a subset of the letters of the four words. The game is to unscramble the letters and determine the words and the caption. Jumble is solved by anagramming. Here are the four words from the May 31, 2001, *Cincinnati Enquirer* Jumble, unscramble them.

1a. `LUGAH`
1b. `YIXTS`
1c. `SLIZZE`
1d. `HIMSUL`

The first word LUGAH has five distinct letters. There are 5! = 120 ways to arrange five distinct letters, and exactly one of them should result in a word. A brute force attack would involve trying possible arrangements of the letters until the word were determined; it would take at most 120 trials. A better scheme is to use patterns in the language to put together pieces of the word and arrange the pieces to form the word. For example, a is a common initial letter; so, we might think of a _ _ _ _. It is unlikely that u would be the final letter; so, we might have u surrounded by consonants. That does not seem to work. It is unlikely that either a or u are the final letters; so, they might be surrounded by the consonants. Consonant-vowel-consonant-vowel-consonant seems unlikely for these letters. If consonants form a digraph; it seems most likely that those would be gl (probably at the beginning of the word) or gh (probably at the end of the word). In English, gh is much more common than gl. _ _ _ g h. l _ _ g h. If the vowels form a digraph, it seems likely that it would be au. laugh is the word.

The third word has repeated letters SLIZZE. There are 6! = 720 ways to arrange 6 letters. But, it is not possible to distinguish between the two zs. There are 2! = 2 ways to arrange 2 letters. If we could tell the two zs apart, there would be 720 ways to arrange the letters, but because we cannot distinguish between them and there are 2 ways to arrange them; the numbers of ways to arrange the 6 letters is 6!/2! = 360. e is likely as a final letter: _ _ _ _ _ e. Rarely used letters are often easier to place than commonly used ones. z combines most frequently with vowels – either vowel –z or z-vowel. z rarely combines with other consonants; if it combines with a consonant, it is likely to combine with another z. nz or zl are next most likely after zz. So, maybe zzl ending with e. _ zzl _ e or _ _ zzle. sizzle works.

Permutation of letters

Here is the key for a transposition cipher that rearranges blocks of 20 letters:

20 17 13 9 7 16 15 18 11 2 10 12 1 14 5 19 4 6 3 8

The key is a permutation of the numbers 1, 2, …, 20. We will use this key to encrypt the message Markworth attacked by two pursuit planes. First, we add some nulls at the end of the message (we could

have inserted them randomly in the plaintext) to make the length a multiple of 20.

```
Markworth attacked by two pursuit planes xnrpd
```

The ciphertext would be:

```
TDAHR  EKBTA  ATMCW  YKORT  DNNTU  XSRLO  PAWER
PUSPI
```

There are 20! = 2,452,902,008,176,640,000 ways to permute 20 (distinct) letters. There are $\frac{20!}{(2!)^8 \times 3! \times (4!)^2 \times 5!} = 22,915,517,625$ ways to permute the letters in this plaintext messages (including the nulls at the end).

We also could have encrypted `Markworth attacked by two pursuit planes` using the key with 16, 17, 18, 19, and 20 removed -- 13 9 7 15 11 2 10 12 1 14 5 4 6 3 8.

Here is a ciphertext message encrypted with another transposition that permutes a string of 20 letters:

```
EYAHO  ESALB  GINEL  PRPVI  ICRIT  CHPEE
```

Anagramming is easier (but still not easy) if we have two (or more) ciphertext messages. Because both messages are transposed with the same permutation, we can double anagram. Here's a second ciphertext message using the same transposition:

```
RABAN  SMLPE  EAASO  HIOCA  PCXCI  IEHTR
```

Good luck!

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.

Columnar transposition

Columnar transposition is probably the most commonly studied transposition cipher. We will use that method to encrypt the following "pilot's saying:"

```
The nose is pointing down and the houses are getting bigger.
```

There are 49 letters in the message. We want to place the letters of the message in a rectangular array. In this case, because we would like the rectangular array to have 49 cells, a 7×7 array may be used. We also need a keyword having its length the same as the number of columns – we will use *analyst*.

A	N	A	L	Y	S	T
1	4	2	3	7	5	6
t	h	e	n	o	s	e
i	s	p	o	i	n	t
i	n	g	d	o	w	n
a	n	d	t	h	e	h
o	u	s	e	s	a	r
e	g	e	t	t	i	n
g	b	i	g	g	e	r

The ciphertext is obtained by reading down the columns in the order of the numbered columns (which are alphabetically ordered).

```
TIIAOEGEPGDSEINODTETGHSNNUGBSNWEAIEETNHRNROIOHSTG
```

Our message exactly fit the rectangular array. If the message does not completely fill the array, nulls may be added to fill it (this is the easier cipher to break) or not (this is harder to break because the columns do not all have the same length). In the latter case, the length of the keyword determines the number of columns, and the number of letters in the message determines the number of complete and partial rows.

The transposition should be applied several times if the plaintext message were longer than 49 letters.

Remember, for encrypting, "in by rows and out by columns."

Decrypting the columnar transposition

Here is a message that was encrypted using a rectangular array with keyword *analyst*.

```
TRLEELIGCIGEHALANTNCTECYENEN
```

Because the keyword has 7 letters, we know that the rectangular array has 7 columns. The message has 28 letters; therefore, the array must be 4×7. Each column must have 4 entries.

First, we place the letters of the keyword in alphabetical order: *aalnsty*. Then place the ciphertext letters in columns.

A	A	L	N	S	T	Y
t	e	c	h	n	t	e
r	l	i	a	t	e	n
l	i	g	l	n	c	e
e	g	e	a	c	y	n

Now rearrange the letters of the keyword to form *analyst*.

A	N	A	L	Y	S	T
t	h	e	c	e	n	t
r	a	l	i	n	t	e
l	l	i	g	e	n	c
e	a	g	e	n	c	y

The plaintext message is `the central intelligence agency.` (Notice that there could be some ambiguity about which "A" column comes first. We have used the convention that the first "A" column will correspond to the first *a* in *analyst*.)

Remember, for decrypting, “in by columns and out by rows.”

Cryptanalysis of the columnar transposition

We will do only "the easy case;" i.e., we will assume that the columnar transposition uses a rectangular array that was completely filled.

Here is the ciphertext:

```
ASAIR  ITFNM  IMTKL  SOIEE  M
```

The “key” to cryptanalyzing the ciphertext is to determine the number of columns; i.e., the length of the keyword. There are 21 letters in the ciphertext. Because we know that the message completely fills the rectangle, this suggests either a 3×7 or a 7×3 array.

We arrange the ciphertext in columns.

Either

A	I	T	M	T	S	E
S	R	F	I	K	O	E
A	I	N	M	L	I	M

or

A	F	L
S	N	S
A	M	O
I	I	I
R	M	E
I	T	E
T	K	M

.

The solution is by anagramming (making a word or portion(s) of word(s) by rearranging letters) a row.

The 7×3 arrangement seems unlikely because it has a string `TKM` with no vowels that is unlikely. Also, the `III` is unlikely. So, let us try the 3×7 arrangement. Notice that there are 7! = 5040 arrangements of the columns. We would like to not have to try all of them!

A	I	T	M	T	S	E
S	R	F	I	K	O	E
A	I	N	M	L	I	M

In the first row, `MATE` seems to leap out. This leaves `ITS`. Perhaps, a slightly wrong guess – `ESTIMAT-` seems to be a possibility.

Let us rearrange the columns.

E	S	T	I	M	A	T
E	O	K	R	I	S	F
M	I	L	I	M	A	N

Not quite, but there are two `T`s in the first row. Let us swap those columns.

E S T I M A T
E O F R I S K
M I N I M A L

This works. Notice that because we have multiple rows that are permuted the same way, we can use multiple anagramming for cryptanalysis.

It is often worthwhile to write the ciphertext in columns, cut out the columns, and rearrange the columns to do the anagramming.

Determining the dimension of the rectangle

Frequencies can help to determine the dimensions of the rectangle. In English approximately 40% of plaintext consists of vowels. Therefore, for the correct dimension, each row of the rectangle should be approximately 40% vowels. Consider our choice between 3×7 and 7×3.

For a 3×7 rectangle, each row should contain approximately 2.8 vowels. Let us note the difference between this estimate and the actual count:

							Number of vowels	Difference
A	I	T	M	T	S	E	3	0.2
S	R	F	I	K	O	E	3	0.2
A	I	N	M	L	I	M	3	0.2

The sum of the differences is 0.6.

For a 7×3 rectangle:

			Number of vowels	Difference
A	F	L	1	0.2
S	N	S	0	1.2
A	M	O	2	0.8
I	I	I	3	1.8
R	M	E	1	0.2
I	T	E	2	0.8
T	K	M	0	1.2

The sum of the differences is 6.2. It appears that the 3×7 rectangle is more likely.

Using digraph frequencies to arrange the columns

Digraph frequencies can be used to help in the cryptanalysis in place of just looking for reasonable pairings of the columns. For example, consider our ciphertext above ASAIR ITFNM IMTKL SOIEE M. Again, we'll assume that a 3×7 rectangle is appropriate.

A	I	T	M	T	S	E
S	R	F	I	K	O	E
A	I	N	M	L	I	M

We will pair the first column with each of the other columns on the right and consider how likely it is that such digraphs will occur in English. The frequencies we will use come from Sinkov. Recall that there are $26 \times 26 = 676$ digraph frequencies.

AI	311	AT	1019	AM	182	AT	1019	AS	648	AE	13
SR	9	SF	8	SI	390	SK	30	SO	234	SE	595
AI	311	AN	1216	AM	182	AL	681	AI	311	AM	182
	631		2243		754		1730		1193		790

The most likely pairing is

AT
SF
AN

Oops! We know that this is not the correct pairing, but the second most likely pairing is correct. (During cryptanalysis, we don't always get the correct result on the first try.)

Once we have a pairing, we could then continue using digraph frequencies to select columns to add on the left and on the right. Etc.

More columnar transposition

It would be harder to do the cryptanalysis if the rectangle were not completely filled. For example, let's use a columnar transposition with keyword *norse* to encrypt the message `Germany seeks an alliance`. The message contains 22 letters; so, we need 4 complete rows and one partial row.

In by rows:

n	o	r	s	e
g	e	r	m	a
n	y	s	e	e
k	s	a	n	a
l	l	i	a	n
c	e			

Out by columns:

AEANG NKLCE YSLER SAIME NA

Because the columns do not have the same length, this would not be as easy to cryptanalyze. It would not be obvious how many columns were used. (The size of the rectangle would be either 2×11 or 11×2 if we knew that a full rectangle had been used; i.e., the keyword would have length either 11 or 2.)

However, if we know the keyword, decrypting is no problem. Try decrypting the ciphertext

```
IMYRA  CBILM  AANIE  NSBNR  ESE
```

which was encrypted with columnar transposition with keyword *norse*.

Double columnar transposition

Re-encrypting a columnar transposition cipher with another columnar transposition cipher – using the same key or another key – can result in more scrambling of the letters.

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 $5 + 6 = 11^{th}$ spot. The next at the $11 + 7 = 18^{th}$ 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 8^{th}, 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."

Exercises

1. Here is the Jumble from June 10, 2003:

IMNEC

ADEHA

GETURT

PHANEP

How many rearrangements of the letters are possible for each string of letters? For each string, what is "the" word?

2. How many rearrangements of the letters HACING are possible? What is "the" word?

3. How many rearrangements of the letters YOPPP are possible? What is "the" word?

4. How many rearrangements of the letters BREMME are possible? What is "the" word?

5. Consider the string QUIROL. Discuss its rearrangement into a meaningful word.

6. Create a Jumble. There should be four strings of letters – two of length five and two of length six. Each string of letters should anagram into only one word. If you wish, you might also construct a phrase from selected letters of the words.

7. Assume that you are to cryptanalyze a ciphertext that you know was encrypted with a columnar transposition cipher using a full rectangular array. For each of the following message lengths, determine what row × column dimensions for the array are possible.

7a. 25
7b. 22
7c. 45
7d. 12
7e. 24

8. Use a columnar transposition cipher with a rectangular array and keyword *mathematician* to encrypt the following message:

```
Sample the electronic environment of the east
coast of North Korea.  Emphasis is intercepting
coastal radars.
```

9. The following message was encrypted with a columnar transposition cipher using a full rectangular array and keyword *mathematics*. Decrypt it.

```
RIUGS   IPNCT   MSPAL   AUNCY   SOOCH   UEYSA
RTE
```

10. Cryptanalyze the following message. It was encrypted with a columnar transposition cipher using a full rectangular array.

```
NTDVC   ILRDT   LFNIT   AUEEE   UEOUA   OVSEN
CIOTN   CCSLS   ATIPN   RNVA
```

11. Explain the difference between a substitution cipher and a transposition cipher.

12. A message is encrypted with a transposition cipher. What should we see if we do a frequency analysis of the message?

13. Design a transposition cipher. Remember that the cipher should have a memorable key and not be prone to encrypting and decrypting errors. It should not be too complicated. After you have designed your cipher, discuss its strengths and weaknesses.

14. For columnar transposition, would it be easier to break a ciphertext of 65 letters if a 5×13 or a 13×5 rectangle were used for the encrypting? Explain.

15. Use a railfence cipher with 3 rails – removing the rails from top to bottom – to encrypt the message

```
alan turing the enigma
```

16. Try decrypting this message that was encrypted by using a railfence cipher with two rails.

```
TEETN  WRTRA  HNWSE  EOEBA  TUSHR  ISHBS  KONOO
MCIEA  DVLPD  YRHRC  EBU
```

17. Try decrypting this message that was encrypted with a railfence cipher with four rails:

```
TTTPT  QDSYP  RSHII  XEDOH  EIUNS  ESLDY  TEMES
SERSE  NELSC  NEAUC  FLERE  GAMAE  BHDIH  SCUCD
NG
```

18. Decrypt the following message that was encrypted with a columnar transposition with keyword *welchman*.

```
LAOAE  CEDOS  EEOHN  NAHRE  FESSV  EGEGA  SCJMS
WDPSD  OTIAS
```

19. What problems would we encounter if we tried to cryptanalyze a message that had been encrypted with columnar transposition with a rectangular array that was not "full;" i.e., the message did not completely fill the rectangle?

20. Sometimes, to "fill out" a rectangle, meaningless letters – nulls – are inserted into the message. Discuss how inserting nulls would affect cryptanalysis of the ciphertext. Would it matter where the nulls appeared? Sometimes they are placed at the end of the message to fill out the rectangle, sometimes they are placed at the beginning, and sometimes they are scattered throughout the message.

21. Cryptanalyze the following message that was encrypted using columnar transposition.

```
RTAEQ  DEHLR  CEERQ  SVMOT  HDDMQ  EIEFI
```

22. Encrypt the message

```
If we have war with the United States, we will
have no hope of winning unless the United
States fleet in Hawaiian waters can be
destroyed.
```

using the following transposition technique.

Fill in the grid below -- row by row from left to right. Do not place a letter in a cell containing a *.

10	2	8	1	5	3	7	4	6	9
			*						
	*	*						*	
					*	*	*		
				*				*	

Encrypt the message by reading down column one, then down column two, etc.

What problems would we face if we tried to cryptanalyze a message encrypted with this method?

23. Upon searching a room, the following were found on scraps of paper. Use the first to cryptanalyze the second.

On the first scrap

10	2	8	1	5	3	7	4	6	9
t	h	e	t	r	a	n	s	p	o
s	i	t	i	o	n	w	a	s	t
h	e	r	e	a	l	s	t	u	m
b	l	i	n	g	b	l	o	c	k

```
THASR PNEOT IINAO SWTTS EELTA USRMH NLBOG CLIKB
```

On the second scrap

```
ERMND LAIEF ETATW HYHRD HUHPT UEGRO SLAOH WDELP
NAD
```

24. Transposition ciphers are often used to re-encrypt other ciphers. Here is a ciphertext that was first encrypted by a Caesar cipher and then encrypted again by a columnar transposition cipher using a full rectangle. Cryptanalyze it.

```
AMXTX  HXXVH  HBXYA  BTGXT  TXTMM  KMVMF  UKKGX
YFARX  MGAXD  FWKKL  KTTTZ  WUGBL  MEMRL
```

25a. Determine the eight routes that are obtained from the diagonal route transposition pattern.
25b. From the spiral route transposition pattern,
25c. From the orthogonal boustrophedon pattern.
25d. From the diagonal boustrophedon pattern.
25e. From the crab spiral pattern.

26. Enter the characters `ABCDEFGHIKLMNOPQRSTUVWXYZ` into a 5×5 array using the basic orthogonal boustophedon pattern, and remove the characters using the basic spiral pattern.

27. Construct a 6×6 turning grille that is different from the one given in the text. Describe a procedure for constructing a 6×6 turning grille. How many 6×6 turning grilles are possible?

28. Construct a 8×8 turning grille. Describe a procedure for constructing a 8×8 turning grille. How many 8×8 turning grilles are possible?