Math 135 (Summer 2006)
Transposition Ciphers

A **transposition cipher** is one in which plaintext symbols are rearranged (i.e., transposed or permuted) to produce ciphertext. The method of transposition may be either mathematical or typographical in nature.

Rail Fence Cipher

Example: We encipher `NOTHING IS AS IT SEEMS` by first writing it on two lines in a zig-zag pattern (or *rail fence*). The ciphertext is produced by transcribing the first row followed by the second row.

```
N   T   I   G   S   S   T   E   M
  O   H   N   I   A   I   S   E   S
```

Ciphertext: `NTIGS STEMO HNIAI SES`.

To decrypt, we write half the letters on one line, half on the second. (Note that if there are an odd number of letters, we include the "middle" letter on the top line.)

Example: Decipher `MKHSE LWYAE ATSOL`.

Solution: Since there are 15 letters, we write 8 on the top line and 7 on the bottom line so that

```
M   K   H   S   E   L   W   Y
  A   E   A   T   S   O   L
```

Plaintext: `MAKE HASTE SLOWLY`.

Columnar Transposition

The number of columns is the key information.

To encipher: Plaintext is written horizontally in k columns, and is then transcribed vertically column-by-column,

To decipher: Suppose that the length of the ciphertext is n and the key is k. Then the letters will fill $n\,\mathrm{DIV}\,k$ full rows, and there will be one partial row at the end with $n\,\mathrm{MOD}\,k$ letters. Transcribing row-by-row will then yield the plaintext.

Example: Encrypt `NOTHING IN THE WORLD IS MORE DANGEROUS THAN SINCERE IGNORANCE AND CONSCIENTIOUS STUPIDITY` with a key of $k = 9$ columns.

Solution: We write the plaintext horizontally in 9 columns as follows:

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

The cipher text is therefore: `NTSES NDTIO HMRIO CIDTE OONRO OIHWR UCANU TIOES ENSSY NRDTR CCSGL AHEEI TIDNA IAEUN IGNGN NP`.

Example: Suppose the ciphertext is: `GPSDO AILTI VRVAA WETEC NITHM EDLHE TALEA ONME`. If it is known that the key is $k = 7$, find the plaintext.

Solution: There are 39 letters in the ciphertext which means that there are $39 \,\mathrm{DIV}\, 7 = 5$ full rows and one partial row with $39 \,\mathrm{MOD}\, 7 = 4$ letters.

				×	×	×

Plaintext: ____*
(*Archimedes)

Keyword Columnar Transposition

The order of transcription of the columns is determined by the alphabetical order of letters in the keyword. If there are repeated letters in the keyword, the columns corresponding to those letters are transcribed in order left-to-right.

Example: Encrypt `THE QUICK BROWN FOX JUMPED OVER THE LAZY DOG` if the keyword is `CORNELL`.

C	O	R	N	E	L	L
1	6	7	5	2	3	4
T	H	E	Q	U	I	C
K	B	R	O	W	N	F
O	X	J	U	M	P	E
D	O	V	E	R	T	H
E	L	A	Z	Y	D	O
G						

Ciphertext: `TKODE GUWMR YINPT DCFEH OQOUE ZHBXO LERJV A`

Cryptanalysis of a Columnar Transposition

For a simple columnar transposition, cryptanalysis is relatively direct. Attempt to decipher with various numbers of columns until intelligible plaintext appears.

Example: Cryptanalysis the following:

```
LAEST HWAOB ANHED MIEAO TLWOA ESUEN CAETU LDIVT
   IAUSE ILADE TMOCI OREHP SCSTC DROTS EOHVN
```

Note that there are $n = 75$ letters.

Solution: If $k = 2$ we have

$$\begin{array}{cc}
\mathtt{L} & \mathtt{V} \\
\mathtt{A} & \mathtt{T} \\
\mathtt{E} & \mathtt{I} \\
\mathtt{S} & \mathtt{A} \\
\mathtt{T} & \mathtt{U} \\
\vdots & \vdots
\end{array}$$

and so the plaintext is `LVATEISATU` ....

If $k = 3$ we have

$$\begin{array}{ccc}
\mathtt{L} & \mathtt{E} & \mathtt{T} \\
\mathtt{A} & \mathtt{S} & \mathtt{M} \\
\mathtt{E} & \mathtt{U} & \mathtt{O} \\
\mathtt{S} & \mathtt{E} & \mathtt{C} \\
\mathtt{T} & \mathtt{N} & \mathtt{I} \\
\vdots & \vdots & \vdots
\end{array}$$

and so the plaintext is `LETASMEUOSECTNI`....

If $k = 4$ we have

$$\begin{array}{cccc}
\mathtt{L} & \mathtt{O} & \mathtt{V} & \mathtt{E} \\
\mathtt{A} & \mathtt{T} & \mathtt{T} & \mathtt{H} \\
\mathtt{E} & \mathtt{L} & \mathtt{I} & \mathtt{P} \\
\mathtt{S} & \mathtt{W} & \mathtt{A} & \mathtt{S} \\
\mathtt{T} & \mathtt{O} & \mathtt{U} & \mathtt{C} \\
\vdots & \vdots & \vdots & \vdots
\end{array}$$

and so the plaintext is `LOVEATTHELIPSWASTOUC`....

If we continue the decryption, we find

```
⋮  ⋮  ⋮  ⋮
H  A  S  S
W  E  E  T
A  S  I  C
O  U  L  D
B  E  A  R
A  N  D  O
N  C  E  T
H  A  T  S
E  E  M  E
D  T  O  O
M  U  C  H
I  L  I  V
E  D  O  N
A  I  R
```

Love at the lips was touch
As sweet as I could bear;
And once that seemed too much;
I lived on air
    —Robert Frost (from *To Earthward*)