Worksheet 18 (Cryptography 2): Transposition Ciphers

Group Names: Solutions

1. The easiest transposition cipher takes a plaintext message, arranges it into an array using rows of equal length, padding if necessary, and then uses the columns of the array to form the ciphertext, but it doesn't change the order of the columns.

   Consider the following plaintext:

   THE RIGHT OF THE PEOPLE PEACEABLY TO ASSEMBLE

   (a) Fill in the following grid with the letters of the plaintext (ignore spaces) working across the rows, and then down. The first four letters have been filled in for you. You will need to fill in any extra spaces in the grid with "dummy" or "nonsense" characters (say, X or Q or J).

T	H	E	R	I	G	H	T
O	F	T	H	E	P	E	O
P	L	E	P	E	A	C	E
A	B	L	Y	T	O	A	S
S	E	M	B	L	E	X	Z

   (b) Now construct the ciphertext by writing down the letters in the columns, in a row. (You can choose to divide up the ciphertext into arbitrary shorter units—groups of 5 is traditional—if you like.)

TOPAS HFLBE ETELM RH PYB IEETL GPAOE HECAX TOESZ

   (c) Decrypt the phrase

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

   assuming it was encrypted using a grid with 5 columns (spaces added only to help keep track).

   i. There are 30 letters in the phrase. Since we are using 5 columns, how many rows must there be? 30/5 = 6

   ii. Fill in the array down the **columns** with the ciphertext.

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

   iii. Now decrypt the message by reading across the **rows**.

OR ABRIDGING THE FREEDOM OF SPEECH X

2. Next, we will encrypt a phrase using a **keyword** which tells us how to mix up the columns.

   Consider the following plaintext:

   O R P R O H I B I T I N G T H E F R E E E X E R C I S E T H E R E O F

   (a) The plaintext has 35 letters (excluding spaces). How many rows are necessary if there are 6 columns? 35/6 = 6 How many extra letters will be needed? 1

   (b) Write the plaintext in the **rows** under the key word in the left-hand grid. Add some extra letters to complete the final row.

   (c) Rewrite the letters in the keyword RIGHTS so that the letters are in order from earliest alphabetically to latest: G H I R S T

   (d) Rewrite those letters in the new order on the top **row** of the right-hand grid, and fill in the corresponding **columns** from the left-hand grid.

R	I	G	H	T	S
O	R	P	R	O	H
I	B	I	T	I	N
G	T	H	E	F	R
E	E	E	X	E	R
C	I	S	E	T	N
E	R	E	O	F	X

G	H	I	R	S	T
P	R	R	O	H	O
I	T	B	I	N	I
H	E	T	G	R	F
E	X	E	E	R	E
S	E	I	C	N	T
E	O	R	E	X	F

   (e) Now produce your ciphertext by reading down the **columns** from left to right using the right-hand grid.

PIHES ERTEX EORBT EIROI GECEH NRRHX OIFET F

3. Using the same keyword RIGHTS, undo the previous process to decrypt the following message, which is 24 characters long. It has been separated into groups of 5 to make it easier to see, not because those are the word lengths.

   E O L Y R F B X H T A R T H I U G R J X I T Y X

   (a) How many rows will you need? 24/6 = 4 Fill in your sorted keyword on the top row of the **left** grid and then fill in your ciphertext down the columns.

   (b) Then transfer the columns to your **right-hand** grid and read off the plaintext in the rows.

G	H	I	R	S	T
E	R	H	T	G	I
O	F	T	H	R	T
L	B	A	I	J	Y
Y	X	R	U	X	X

R	I	G	H	T	S
T	H	E	R	I	G
H	T	O	F	T	R
I	A	L	B	Y	J
U	R	Y	X	X	X

   (c) What is the plaintext?

The right of trial by jury x