CT Ciphers

CT (columnar transposition) ciphers are examples of *transposition ciphers:* The characters in the plaintext message are permuted to create the ciphertext. There are many types of transposition ciper; they differ in the method used to permute the characters, and consequently may differ somewhat in strength. For another example of a transposition cipher, see the article on the rail fence cipher.

The encryption key for a CT cipher consists of a word, formed with characters from the alphabet used for the plaintext. For reasons that will be apparent when the encryption is described, some convention must be adopted to treat the case when the keyword contains repeated characters. One possibility is that all but the first occurrence of each keyword character is deleted, (as one does for Playfair keys with repeated letters). For example, a keyword may be specified as *Massachusetts*, but one would use *Maschuet* as the key for the encryption and decryption. Another possibility is that when the columns are permuted, those that correspond to a repeated character of the keyword are kept in their original order. We shall adopt the latter convention, as illustrated in the second example below.

Suppose we want to encrypt the message "cranberries with orange peel" using a CT cipher with encryption key *feast.* Here is how we would proceed.

i. Tabulate the plaintext characters beneath the characters of the keyword as below.

f	e	a	s	t
c	r	a	n	b
e	r	r	i	e
s	w	i	t	h
o	r	a	n	g
e	p	e	e	l

ii. Now permute the columns so that the characters of the keyword are in alphabetical order.

a	e	f	s	t
a	r	c	n	b
r	r	e	i	e
i	w	s	t	h
a	r	o	n	g
e	p	e	e	l

iii. Finally, concatenate the columns of the table obtained in step *ii* (excluding the keyword row) to obtain the ciphertext: ARIAERRWRPCESOENITNEBEHGL.

Here is an example using a keyword with repeated characters. Suppose we want to encrypt the message "green beans and mushrooms in a casserole" using a CT cipher with encryption key *Pilgrim.* Here is how we would proceed.

i. Tabulate the plaintext characters beneath the characters of the keyword as before.

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

In this case, the keyword length does not divide the message length, so the last row of the table is shorter than the other rows. (A variant of the CT cipher does not do this – additional characters are added to the plaintext so that the table is completely filled. Leaving the last row shorter than the others actually makes the cipher a bit more resistant to cryptanalysis.)

ii. When we permute the columns so that the characters of the keyword are in alphabetical order, we keep the two columns labeled with "i" in their same order relative to each other.

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

iii. When we concatenate the columns from step *ii* we obtain the ciphertext:

EARAORNSIEBDOAEESHNREMMSGAUSSNNOCL

For practice, try encrypting the plaintext "harvest moon over Plymouth Rock" using a CT cipher with keyword *Squanto.* (This should result in the ciphertext VNYOEOMCTEUAOPHHMRTSVOKROLR.)

The following ciphertext was produced using a CT cipher with keyword *Mayflower.*

UPILAIAPCHAKACUPDWEINACNEMNPREMETS

See if you can decrypt it.

Since encryption with a transposition cipher is accomplished by scrambling the letters of the plaintext, frequency analysis on the ciphertext will produce a distribution identical to that of the plaintext message. Thus, for a sufficiently long message, the frequencies of its ciphertext characters should resemble the known overall frequencies of these characters in the language used for the plaintext.

When the frequency distribution of a ciphertext is similar to that of the plaintext language, this is a strong indication that a transposition cipher was used. Once a transposition cipher is suspected, anagramming and/or genetic algorithms can be applied to deduce probable keys. For these reasons, transposition ciphers are not very secure on their own. Typically they are combined with other encryption steps in order to enhance security (see the article on the trifid cipher for an example of how this can be done).