

# MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

## DOUBLE COLUMN TRANSPOSITION – PART 4

Author: George Lasry

May 2014

# Introduction

The Double Column Transposition (DCT) cipher was one of the most popular hand ciphers in the 20th century. It was extensively used from World War I to the Cold War by all sides.

With long enough keys (longer than 20) and if different keys are used for the first and second transposition, it is very difficult to break this cipher – even with modern computing equipment and methods.

This series offers several mid-level DCT challenges with keys shorter than 20 or with other weaknesses, which should allow for their cracking using Hill Climbing or other computerized methods.

Good luck!

# Challenge

The DCT cipher was widely used by secret agents and spies in the 20th century. It is most secure if different keys are used for the two transpositions stages, and if the keys are at least longer than 20. This makes those keys difficult to remember. One of the techniques was to use expressions or sentences from a book.

In this challenge, a very difficult DCT encryption has already been solved, and you know the numeric keys (and their literal equivalents). You are now asked to find out the expressions from which the keys were derived. This was important in the past, for example, if numeric keys were always derived from keywords/sentences from a certain book. Knowing which words were used as a source for keys, could greatly help with identifying the book, and deciphering future ciphertexts.

A few details about how a numeric key is derived from a word or an expression:

Suppose the word is "suggest". You arrange the letters in alphabetical order and number them. For the same letter, the first occurrence will be assigned a lower number than the second occurrence, and so on.

E is the lowest, so its number will be 1.

G is the second lowest. So the first G will be given a number 2. For the second G, we can't use again 2, so we will assign it 3.

S is the next lowest letter. There are two occurrences of S, they will be assigned the numbers 4 and 5.

The next letter is T. It is assigned the number 6.

U is the highest letter. It is assigned 7.

So "suggest"  $\Rightarrow$  4,7,2,3,1,5,6, and its literal equivalent DGBCAEF

Unfortunately, there is no well defined process to convert a numeric/literal key back to its original phrase/expression/keyword. Also, there can be several words and expressions which map to the same key. For example, "runners", "ruppert" and "luciano" all produce the same "DGBCAEF" key (which was derived from "suggest").

It is advised to use the following link to check your conversion:  
<http://rumkin.com/tools/cipher/coltrans-double.php>  
Select the option "Key Word(s) - Duplicates numbered forwards" (instead of "Numeric Key - Spaced Numbers") and type in the word or sentence (no space), and the numeric equivalent is displayed below.

# Hints

Here are some details about the literal keys for which you are required to find the matching expression, for this challenge.

- ▶ The first key is: ODNUBIECAJFKPRGSVTHMLQ (22 letters)
- ▶ The second key is: AIEOFCEBJDMKPQGRTSHNL (20 letters)
- ▶ Both keys were derived from English expressions each containing two words.
- ▶ The answer consists of the two original expressions, in capital letters without punctuation or spaces, e.g., if the expressions were "niceguy" and "verymuch", then the answer would be NICEGUYVERYMUCH.