MysteryTwister C3

DOUBLE COLUMN TRANSPOSITION – PART 3

Author: George Lasry

April 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!

MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Author: George Lasry

Challenge

The DCT was most of the times used in its secure form, with different keys for the first and second transposition. In some cases, it was used with the same key, for example by the US in WWII. This happened also sometimes by operator mistake. Needless to say that the version using the same key twice is less secure.

The following ciphertext has been encrypted using a single key – and both transpositions were performed using the same key. The answer to the challenge is the literal key, in capital letters.

For example, if the key was of length 5 and if the numerical key was 4,2,1,3,5, then the literal keys would be DBACE.

Challenge – Ciphertext

```
OHEALDYELHSAFWBCNTSENVBNNOTDIPECSUEBTHPESMTIYIHINBTSETNT
ANSVEASNBEFCYIYSAEENHUOSPHTKPOENHUVOTCDOILIWCTRPEOESSLTR
BOSANTWOUIGYEQGYWUTEEIHRLWWNOEOOORDRNISHNOAECTSDEHAEAHEY
SWRTREPMYOOLYDRDOOEYCSONNOSEEEUFUSYEOATTLAEOLSMEETYNPEVH
EACIIDYUTLFSOTNLEYFEUNCREEECENTSHDTINIUOJESUAEHUEEMDTWOO
IODBEHEAEILNOPAEKTURINHEXEWENONUHTTSTNFNTURIYUIAHESSAATC
ATTAIYEINDNOHORUAIOPGECEAMOAOVECISXTNOIOANRTINTLSATRHHOR
TTOUEOUAAWGDISOTEMSTLTHTSOEATQDHQMENSLLDAFTDHOTNBENNULOH
IENSXOAPNHCAYAEIERWTMTALORAIVLEHAASEEEITNEYTLEEREVCEWEEA
CARLIHOLIHIRNONLGWECLTNEUEGAASEWTWIUEWRDSMHSUATECYETMDRI
ISAHOTGTDWFNTTYOTQLIHUIGTNMYDEOHSIRGGUDUYSYEROMIENTONMEO
AORLRTUETEDTEIEMAPDIDCREUHVBBENEYQSGCEVRVITEARRPFILEEPOA
RAHITLTSSIABHINHHAYEPUEIPSSBOOEONOUEOSANHRCWKPEIOOSIKYOP
HAGHETELVURTANCEELSFEATLROENTTMEETRAAEOOANAEYETSVHNRNEKR
ODDERRTRTAIODIEONSTELBNIUIEDFSUSRTTYRTDEEETESNIUFESIEEAR
NHENETTTTTOOSAROHRWYTHNOHNGNBMGFNSTMHERDOYOOTOEIUIAEOFNR
AHSEHDRNMHD
```

Hints

- ▶ The plaintext is in English.
- ▶ The length of the transposition key is 15.
- ▶ The key is a random numerical key, not derived from any sentence or expression.