Young Tyros Newsletter

December 2008

Circulation – 100

Editor – LIONEL@cryptogram.org
Staff – FIZZY
GGMA
ZANAC
*COPS - GGMA, MICROPOD, SUGARPLUM

New President's Top Secret To Do List

*Contribution of Postage Stamps or Other Donations

Welcome A New Solver to Our Mailing List
We welcome new solver, RAMBELL, to our Cm Solvers List and Newsletter Mailing List.

WSJ.Com Making Every Word Count (12/08) FLEUR DE LIS
Check this site for word frequencies and a list of the one hundred most used English words.

Gimmie A Break – SO Aristocrats (Word frequency = 1 unless shown otherwise.) ZANAC
Entry points and thought processes applicable to all cryptanalysis work.

A1: The (3), I'm (2), to. A-2: The (3), that (3), to, he's, doesn't. A-3: The, to, on, one, who. A-4: Are, area, you (2), and. A-5: Of (2), For, to, F-Four. A-6: Of, for, on in. A-7: *Marshall *----, backward. A-8: Will, its. A-9: Title suggests "moon," "sun, earth" good bets. A-10: -illion, *China. A-11: to, other, the—A-12: TH (5 – earth, the, other, without, them), to. A-13: Of, for, off, you, to. A-14: Don't (2), do (2), it, to, you (2), the (2) A-15: I'm, to, out. A-16: The, I, am, *Van A-17: Title = age, to (4), be, best. A-18. Title "Tasty Concoction" needs recipe, bing cherry. A-19: ? nimbus, which, of, to. A-20: Digraphs IN, NI, AN work for ingenious, any, and, can. A-21: Of, from, frog, to. A-22: Check three and four letter word lists for "You, your, last, list," so, to. A-23: Nautical title, look for sailor, in, tiny, bay. A-25: Attack 122 pattern words not "too" frequent in number, title suggests "zoo" possibility via "bus," you (3)

SO Patristocrat Ciphers – "the" & "that" & "you" occurrences. (the, you- may be trigraphs)
P-1 (the-1), P-2 (the-1, you-2), P-3 (the-4, that-1,you-2), P-4 (the-1), P-5 (the-1, that-1, you-1), P-6 (the-2, you-2), P-7(you-2) P-9 (the-2,), P-10 (the-3).

SO. X-9. Italian Incomplete Columnar. MICROPOD (Analyst GGMA)
Period 8. Here is a slightly longer crib: "un grande"

SO. X-11. Spanish Myszkowski. On the road. EL CONDOR (Analyst GGMA)
Period 12.

SO. E-15. Unknown. Restrained nutritional strategy. WALRUS (Analyst GGMA)
IC=58, vowels = 39%, JQKZ = 0% - looks like a transposition cipher. The length of the con is 64 characters or 8x8 – could be a grille, nihilist transposition, or a route transposition. Guess which one?

SO. C-9. Base 13 Division. MORDASHKA (Analyst GGMA)
P*PUN = IUIU is a unique pattern. Only one value of PUN will create this pattern.

ND. A-18. Abecedarian. K2. (88) **ANGO-KA**
Opens up with a common English word and a pangram (use of every letter in the alphabet).

ND. P-11. Whew! (86/21) (VON) **KOSHKA**
Second word beginning with second letter of the ciphertext is a pattern word with a pattern of 12324567.

ND. E-2. Railfence. Useful equipment? **G-MAN**
Lengthy Railfence Period can be solved with no offsets.

ND. E-7. Route Transposition. Sea Scene. (six) **RIG R MORTIS**
Ninety-six letter cipher translates into twelve rows, eight column plaintext. Great use of alliteration by constructor. Diagonal input, row output.

ND. E-8. Incomplete Columnar Transposition. (engage) **DYETI**
Short ciphertext lends itself to a short period. (Try 5.) Plaintext begins with a very common diagraph.

ND. E-10. Unknown. Eliminating trouble. **EL CONDOR** **(Analyst GGMA)**
A letter frequency count for this con is A=11, B=20, C=23, H=21, N=8, O=19,S=17, T=22, U=14, and W=21 – Only 10 characters are used! This is highly unusual. A frequency count of the first and last letters of each digraph, reveals that the same 10 letters are used by both. This very strongly suggests the con is a double checkerboard. To find all the possible keywords, use the internet anagramming web site http://wordsmith.org/anagram/index.html. The advanced option allows you to specify you are looking for combinations of two 5 letter words, reducing the list considerably.

ND. C-9. Sudoku. (Two words) **MARSHEN**
Look for the solution in the top middle of 3 x 3 grids. First keyword begins with “H.”

The Value of Pencil and Paper Solving For Future Computer Solvers. (GGMA)
While I now have a good understanding of how stochastic solvers work (Hill Climbing), it is not something that lends itself to paper and pencil. It involves randomly making changes to the keyed alphabet, and determining which changes give us the best decrypt. Without a computer doing a relatively massive amount of work, this approach is impractical. This is why I am trying hard to learn the paper and pencil methods, in the hope that I can use whatever I learn to make my computer solving applications take advantages of some of these weaknesses.

Miscellany
Should any of our Newsletter verbiage be foreign to you (digraphs, offsets, pattern words, etc.) do not hesitate to contact LIONEL for definition or clarification. **The ACA and You Handbook** glossary, P. 87, may also be helpful.

Cipher Solving Lesson Plans **LIONEL**
Cipher Solving lesson plans are available for the following Cipher Types: Affine & Hill Elementary School Mathematical Ciphers, Aristocrat, Baconian, Bazeries, Checkerboard, Foursquare, Fractionated Morse, Kasiski Period Determination, Monome-Dinome, Morbit, Null, Patristocrat, Railfence, Sudoku and Swagman. Send $1.00 for postage and handling for each Cipher Type requested to Lee Melair, 1828 Howe Lane, Maple Glen, PA 19002-2915.

Thanks and a tip of the hat to GGMA & MICROPOD for completely funding our Nov & Dec Newsletters.

Sunny Ciphering, LIONEL cc: ACA Executive Board