Young Tyros Newsletter

June 2009

Editor – LIONEL@cryptogram.org
Staff – FIZZY
GGMA
ZANAC
*COPST - ANCHISES, TWEETY

Cryptology Grads Diplomas in Ciphertext

*Contribution of Personal Solving Technique

New
***C**ontribution **O**f **P**ersonal **S**olving **T**echnique – Send us one of your personal pet methodologies.
Page Three – Classical Cryptology. Solving tips from past Cm and Newsletter articles.

ACA Web Site Resources Page at www.cryptogram.org
Current and past Newsletter issues are available at this site. Thank you, ACA Webmaster, **PARROT.**

Welcome New Solvers
We welcome new solvers, JABBERWOCK and TOMMY, to our Newsletter and Cm Solvers List.

***Contribution Of Personal Solving Technique**
Aristocrats - watch out for the apostrophes -- they can help you guess the word. **ANCHISES**

MA 09 A-1 BXSK'ES = they're, could also be they've or they'll;
MA 09 A-2 YDRXWG'H = ...'s, could also be wouldn't, couldn't;
MA 09 A-4 'QF = 'em;
MA 09 A-9 EJI'Q = don't, could also be won't, can't.
Others to look out for: I've, it's, he's, we've, you've, hadn't, that's, didn't, they've, there's.

Patristocrat ciphertext – Look for triplets (that's three identical letters in a row). **TWEETY**
(Example - miSS Some). They are easy to spot; after the second letter you can undoubtedly place a word divisor- they narrow the number of possible substitutions to two (or at most five). They can confirm or infirm other guesses (by elimination). The most frequent triplets are S and L. You can also find O, E and F.

Wordlist Web Site **ZANAC**
http://www.affixes.org/index.html Wordlists galore. http://www.quotationspage.com/ Frequent Authors

Gimme A Break – MA Aristocrats (the, that to, etc.) (1) Unless otherwise stated ZANAC
A-1 The, they're, there (2), to ,or, A-2The, he, when, A-3 that , a, I, of, for, and (2), A-4 A, and, that, hath, to, A-5 that, at the, A-6 A (2), that, there, nothing, iys, to, A-7 A, and, her they, A-8 that, the, to, two, how, are (2), A-9 a, and (2), all, don't, A-10 the (3) whether, A-11 the, they, and, bad, in, A-12, the (2), this, has, in, it, eight, A-13 a, the (2), underneath, A-14 I, the (2), to (3), don't, A-15 that, the, to, into, A-16 on, to, the, and, do, down A-17, fast, food, financier, A-18 Those, the, to, with, one's, of, or, A-19 a, and (2), with, what, A-20 queue, energy, empty, A-21 wood- (2), with, water, A-22, and, do, they, what, in (2), A-24 ou (11), to (2)

MA Patristocrat Ciphers – "to" "the" "that" & "you" (pattern occurrences)) (the, you- may be trigraphs)P-1 (the-3), P-2 (the-2, to-2), P-3 (derived) P-4 (the-5), P-5 (the, to-2), P-6 (to-2, you-2), P-7(the, that, to), P-8(the-3), P-9 (always), P-10 (cackles), P-11 (the, you, moment), P-Sp-1(Letter "V" alliteration, CFI = for), P-Sp-2 (polydactyl).

MA Cover Ornamental **TWEETY** **Analyst GGMA**
Solve the lower Sudoku first. Fill-in the lower-right 3x3 of the top sudoku with solution for the upper left 3x3 from the lower sudoku. Trying to solve the upper sudoku first generates too many possible solutions and would have you working with only eight letters as "D" does not appear in upper grid. (QUIPOGAM)

MA A-21. Nature Walk. K3 (92) **QSSV- - - - - - = wood- - - - - -** **OOBO**

MA P-10. Sound Off. K4 (84/18) (MBY) **APEX DX**
Look for pattern word/author at beginning or ending of cipher. See http://www.quotationspage.com/
Shakespeare, Einstein, Aristotle, Churchill, Mark Twain, Confucius, Nietzsche, Roosevelt, Benjamin Franklin, etc.

MA X-9 Latin Checkerboard. **Marital Not So Bliss. (English Keys) GUNG HO Analyst GGMA**
Crib extension: (cogitat aut)

MA E-10 Portax. New Microscopic Find. BION Analyst GGMA
Period ten.

MA E-2 Railfence. Brave words. (ZYUL) **THE DOC**
Short ciphertext suggests three rails. You determine the offsets.

MA E-11 Checkerboard. Heredity. (from) **LIONEL**
If Checkerboards are not your cup of tea, assign letters to the ciphertext digraphs and solve as a Patristocrat. CIPHERTEXT digraphs yielding senorita letters (Not in order) – CN, AI, KN, RI, RN, RT, TN, TR.

MA E-13 Amsco. Power and Happiness. (diamonds) EL CONDOR Analyst GGMA
Period seven. Begins "My……" Quotation by great playwright and poet.

MJ E-3 Vigenere. Bright Ideas. **ERNO**
Period nine. Think, Thomas Edison.

MJ E-6 Route Transposition. Not so Different. (construct) **HANO**
Diagonal in, spiral out.

MJ E-7 Amsco. Better with Age. (hundred – 2) **EL CONDOR**
Period seven.

MJ E-9 Redefence, Sign of respect. (themselves) **TWEETY**
Maximum rails, almost as many offsets.

Cipher Solving Lesson Plans **LIONEL**
Cipher solving lesson plans are available for: Affine & Hill Elementary School Mathematical Ciphers, Aristocrat, Baconian, Bazeries, Checkerboard, Foursquare, Fractionated Morse, Kasiski Period Determination, Monome-Dinome, Morbit, Null, Patristocrat, Pollux, 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.

Sunny Ciphering, LIONEL cc: ACA Executive Board

(Page three follows.)

MA/MJ 2001 ACA Cryptogram Journal Kiddee Korner Column

CLASSICAL CRYPTOLOGY

Cipher Types
1) Substitution – Letters (ciphertext) are substituted for real message (plaintext or cleartext).
2) Transposition – Plaintext message letters retained but scrambled or rearranged.
3) Concealment – Plaintext message letters are concealed beneath subterfuge message.

Substitution Cipher
The classical substitution type cipher which retains word breaks and is seen most often in your daily newspaper is referred to in our ACA as the Aristocrat Cipher. In real life cryptology, some knowledge of the subject exists as well as a lot of ciphertext to analyze. Limited space in newspapers and magazines such as the ACA Cm, limit the amount of ciphertext that can be provided. In place of large messages, subject titles and tips (cribs) are often given.

Useful Tools

Titles and tips. Do not overlook cipher titles as good leads to plaintext words. Each plaintext word correctly placed provides valuable letters to other words in the cipher. Also remember your Caesar Cipher alphabet training to convert any ciphertext tip to plaintext. Placing the tip in a message leads to many other words in the plaintext.

Frequency counts. The first step in solving by most cryptanalysts is a simple tally of how often each ciphertext letter appears in the message. This is called a frequency count and is used to compare each ciphertext letter of appearance with that of the normal frequency of letters in the English language. Such a comparison allows us an educated guess at what a ciphertext letter may be. SENORITA contains the most frequently used letters in the English language.

English Language Frequency Table (Percent occurrence) **ACA and You Handbook**

```
 e  t ao nir sh ld cupf mwy bgy   kqxjz - Less than one percent.
13  9  8  7   6  4   3    2   1
```

Short words. Look for these short words in a cipher: ‘a’ and ‘I’ (the only single letter words), an, in, is, it, on, of, the (often starts a sentence and often appears more than once in a cipher), and, was, when, why, you.

Pattern words. These are words with repeating letters. Pattern word “that” = 1-2-3-1. Pattern word lists are readily available on the Internet (Google Pattern Word Lists or wordpat). Look for these common pattern words: All, off, too, see, good, poor, that, there, where, these, little, people. Pattern word lists are also available in many cryptology books. A good beginner’s word list, with pattern and non-pattern word lists of the 1000 most commonly used English words, can be found in a Dover Publication, “Cryptograms and Spygrams by Norma Gleason.

Solving Lucidity. Your solving logistics, plaintext comprehension and ease of continuity will be helped by the use of upper case letters for ciphertext and lower case letter for plaintext with all letter certainties noted in red.