



Young Tyros Newsletter

April 2008

Editor – Lionel@cryptogram.org

Staff – Fizzy

GGMA

Zanac

*COPS - Fleur de lis, Nuclear

Let Uncle Sam Figure Out This Ciphertext

*Contribution of Postage Stamps or Other Donations

February Errata (Thank you ANCHISES)

I notice that you entitled as ND E-1 and ND E-2 two ciphers that were actually in JF08. I guess this is part of necessary tuition for the Tyros: "Never trust anything that you haven't checked out for yourself". When I was young this was what we referred to as "a trap for young players" though of course old-timers can equally well fall into them. How many of our Young Tyros fell into the "trap"?

Cryptanalysis (ELCY) by Helen Fouche Gaines tells us quite a bit about vowel behavior. (ZANAC)

1. A, E, I, O, are normally high frequency, U is moderate and Y is low frequency.
2. Letters contacting low frequency letters are usually vowels.
3. Letters showing a wide variety of contact-letters are usually vowels.
4. In repeated digraphs, one letter is usually a vowel.
5. In reversed digraphs, one letter is usually a vowel.
6. Doubled consonants are usually flanked by vowels, and visa versa. (cvvc or vccv)
7. It is unusual to find more than 5 consonants in succession.
8. Vowels do not often contact each other.
9. If the CT letter with highest frequency is assumed E, any other high frequency letter which never touches E, can be assumed a vowel. A letter that contacts it very often cannot be a vowel.
10. E is the most frequent vowel and rarely touches O. Both double freely.
11. The vowel that follows and rarely precedes E is A.
12. The vowel that reverses with E is I.
13. Observations 11 and 12 apply to the vowel O. However, finding U it precedes E and follows O.
14. The only vowel-vowel digraphs of consequence are OU, EA and IO.
15. Three vowels in sequence may be IOU, EOU, UOU and EAU.

Patristocrat Solving Tip (TWEETY)

Look for ciphertext triplets (that's three identical letters in a row.) (Ex. 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 frequently used triplets are S and L. You can also find O, E and F.

JF Aristocrat Ciphers – "the" & "that" occurrences

A-1 (the-1), A-2 (the-3), A-3 (the-1, that-1), A5 (the-2), A-10 (high), A-12 (the-1), A-13 (the-2), A-16 (the-1), A-18 (the-1), A-19 (the-1),

JF Patristocrat Ciphers – “the” & “that” occurrences

P-1 (the-3, that-2), P-2 (that-2), P-3 (the-3, that-1), P-7 (the-1), P-8 (the-2), P-9 (the-1), P-11 (the-1, that-1)

JF A-24 Aristocrat – Look for one of the words in the title in the plaintext.

JF P-Sp-1 – Look for alliteration with the letter **K** (14 K’s)

JF P-Sp-2 – Look for alliteration with the letter **J** (13 J’s)

JF X-5 – Look for English key in the title. Crib (paratast) fits in one place. “T” is most frequently used Latin letter.

JF E-6 Amsco. Starting Point. (towels) TWEETY

Here’s a nice Period 7 “teeth cutting” Amsco for you to sink your bicuspid into. Check its construction process in the **ACA & You Handbook** and look for an opening plaintext of “Table...”

JF C-6 Multiplication Cryptarithm – Try a multiplier of 295.

Solving JF 2008 C-SP-2 Undecimal division by REAL NEO (Analysis by GGMA)

C-Sp-2 provides many clues that make it possible to solve this problem by paper and pencil methods:

1. $H*NO = NO$, so we know $H=1$.
2. $PPT - YMT = IW$. So $W=0$. Keep in mind that the H in IWH is a drop-down.
3. $EM-NO = HH$. Since M cannot be zero, there cannot be a carry, and $M=O+1$, and $E = N+1$
4. $YNA - YMT = PP$, or, if you will, $NA - MT = PP$. N is therefore greater than M, so the key must be of the form $WH..OM..NE$. The other letters in the key are $AIPTY$.
5. Lets return to clue 2 - we should note that $P > Y$ due to a carry, so $P=Y+1$.
6. From clue 4, $A = T + P$, and $N=M + P$, where $P = 3$ or more.
7. Next, $IWH = AIH + PW$ – since W is zero and H is 1, this gives us $AI+ P = IW$.
8. Therefore, $I = A+1$ (carry) , and $I+P = 10$ in base 11.

At this point, you can easily complete the solution by anagramming, or by trial and error.

MA D-1. Digital Checkerboard. From hell. (invented) BION

Solve this one as a Patristocrat. Crib placement at position 43 will lead you to two “the” trigraphs and multiple “te” and “th” digraphs.

MA A-20 Aristocrat. Two step. K3 (94) LIONEL

Look for “the” in the plaintext which will lead you to two “to’s.”

MA P-9 Patristocrat. Transparent thought. K2 (92/21) (QUFE) LIONEL

Plaintext begins with six letter pattern word. Look for trigraph “the” in the plaintext.

Sunny Ciphering,

LIONEL

cc: ACA Executive Board