



Young Tyros Newsletter

August 2009

Editor – LIONEL@cryptogram.org

Staff – FIZZY

GGMA

ZANAC

*COPST - BION

Krewe contracting for Niagara Falls barrel ride.

*Contribution of Personal Solving Technique

ACA Web Site Resources Page at www.cryptogram.org

Current and past Newsletter issues are available at this site. Thank you, ACA Webmaster, **PARROT**.

*Contribution Of Personal Solving Technique – Send us one of your personal pet methodologies.

See page three for BION methodology in determining a Slidefair Period.

A To Z Young Tyro Supporters

Thank you ARTEMIS and ZANAC for your book additions to our Young Tyros Library.

Welcome New Solvers

We welcome new solvers, RAVENNA and CODE PENGUIN, to our Newsletter and Cm Solvers List.

Web Site Interesting Links

<http://home.earthlink.net/~fpcorr/AcaTools.html>

<http://home.comcast.net/~acabion/>

GGMA

Gimme A Break – MJ Aristocrats (may be trigraphs) (1) Unless otherwise stated ZANAC

A-1 the, that, A-2 the (3), A-3 the, (2), A-4 the, A-5 the, A-6 A (2), the (2), A-7 in (2), the, A-8 the, A-9 into, A-10 the, A-11 the, A-12, I'm, A-13 No, A-14 fish (2), A-15 men, A-16 and, A-17, was, A-18 of, by, A-19 has, A-20 after, A-21 one-, A-22, with, A-23 qu (4), A-24 st (2), A-25 with (2)

MJ Patristocrat Ciphers – (may be digraphs, trigraphs) (1) unless otherwise stated

P-1 is (3), P-2 (the (5), P-3 the (2) P-4 the, that, P-5 an (2), P-6 it (3), that, P-7 the (2), you (3), P-8 that, the, P-9 the (2), P-10 ist (2), the, P-11 th (3), P-12 people, P-Sp-1 in (8), P-Sp-2 er (4), CT “Q” alliteration.

MJ A-25. Delicious meal. K4 (77) Dumpster Analyst GGMA

This is a difficult con. There are several words with the pattern “1231” – one of which is often done when playing ball. Look for the restaurant culinary preparer in the plaintext.

MJ X-5. Swedish Xenocrypt. Sleep theory. (oss-3) OOBOO

This one looks difficult with the sparse crib given, but the K-2 Alphabet along with frequently used Swedish short words (vad, vi, att, ett, det, men, inte) gleaned from the **ACA Xenocrypt Handbook**, make it duck soup.

MJ E-5 Null. Take flight. (away) REAL NEO

You will find letter repetitions of two, four, six and ten entwined in the ciphertext surrounding this crib but a one through six letter repetition (not in that order) will lead you to the promised land (solution).

MJ E-8. Autokey. Always look on the bright side of life. REAL NEO Analyst GGMA

The crib “senile” is placed at MXOMTR. Key between six to eight letters long, title related to key.

MJ E-18. Playfair. Human nature. (ends: Truman) ANCHISES Analyst GGM
When the crib is placed at the end, the plaintext may end TR UM AN or T RU MA N? Extend the crib to one of these: PRESIDENT TRUMAN, HARRY S. TRUMAN or HARRY TRUMAN.

JA A-14. Some old words. K2 (85) CONFUOCO
Quotation of great Irish playwright involving the Golden Rule.

JA A-20. Escape artists. K2 (101) OZ
Eight plaintext “z’s.”

TG-1. Q Power. K2 (97/18) (KOCN) LIONEL
Cm crib in error. “Q” alliteration and key start.

JA P-8. No place like it. K4 (96/19) (BIGY) MICROPOD
Four “the” occurrences.

JA P-Sp-1. Worst nightmare. K2 (105/18) DYETI
Letter “C” alliteration appears eight times.

JA E-1. Homophonic. In the public eye. (KHYR) DABASAP
Celebrity fame plays a role in this cipher.

JA E-7. Incomplete Columnar Transposition. Apt advice. (ACPY) DANEEL
Period six cipher with advice recommendation.

JA E-8 Amsco. Sure investment. (double) CRAW
Title and crib suggests money advice.

JA E-11 Nihilist Substitution. This one wasn’t Quayle. GIZMO Analyst GGMA
Period Seven

JA C-Sp-2. Addition. (Three words, 0-9) LIONEL
M = 0. N = 9.

JA AC-926. ??? NASCARitis. (104) Homophonic Cipher Type LIONEL

Cipher Solving Lesson Plans LIONEL

Cipher solving lesson plans are available for: Affine & Hill Elementary School Mathematical Ciphers, Aristocrat, Baconian, Bazerics, 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 Cipheryng, LIONEL cc: ACA Executive Board

(Slidefair Period Determination follows on page three.)

SLIDEFAIR PERIOD DETERMINATION

By BION

(1) Separate the cipher into two parts: the even letters and the odd letters.

For MA08, E-11, the cipher is:

CS MJ AL PU NE XQ FS EG KF SO IW KC VZ YM AM WP IT BP PW ST TG OW IT SI BU AJ SD EL DE
LK TO BK LV CQ NN SE MY KR KD PH ST GP OF CT LC NL AY CE RD OE JR WE LK RV HA QC EN
LC TO BK WV SD QD MR BG.

So the even letters are:

CMAPNXFEKSIKVYAWIBPSTOISBASEDLTBL CNSMKKPSGOCLNACROJWLRHQELTBWSQMB

The odd letters are:

SJLUEQSGFOWCZMMPTPWGTIUDLEKOKVQNEYRDHTPFTCLYEDEREKVACNCOKVDDRG

(2) Treat the even letters as an ordinary periodic cipher – a Vigenere or something like that. Try to find the period in the same way you do for an ordinary Vigenere. If you use the index of coincidence the results are:

Index of coincidence for even letters:

Index of coincidence for odd letters:

<u>Period</u>	<u>IC</u>		<u>Period</u>	<u>IC</u>
2	0.038337		2	0.037207
3	0.043434		3	0.043001
4	0.040686		4	0.036520
5	0.048718		5	0.015385
6	0.037710		6	0.044444
7	0.090476	<== maximum	7	0.068254 <= maximum
8	0.016865		8	0.034722
9	0.035714		9	0.025132

In this case, the maximum occurs at period 7 for both evens and odds, so it's a good bet the cipher is a period 7.

The evens and odds don't always form perfect periodic ciphers because in Slidefair encryption you have the special case of plaintext pairs in the same column -- they are encrypted by moving one letter to the right. However, the special case pairs should be rare enough that they don't throw the index of coincidence calculations off.

O'PSHAW wrote a good article about this in the JA98 Cryptogram.

BION