Young Tyros Newsletter

February 2018

Editor – LIONEL@cryptogram.org

Staff – APEX DX ARDUINNA MSCREP

But I thought that an algorithm was an algebraic equation.

COPST - Contribution of Personal Solving Techniques

Algorithms

LIONEL

An algorithm (pronounced AL-go-rith-um) is a procedure or formula for solving a problem. The word derives from the name of the mathematician, Mohammed ibn-Musa al-Khwarizmi, who was part of the royal court in Baghdad and who lived from about 780 to 850. Al-Khwarizmi's work is the likely source for the word algebra as well.

Although our familiarity with the word “algorithm” may be one of a mathematical sense as an aid to solving ciphers, its use is far from simply mathematical. We use this procedure as a set of unambiguous steps in many of our everyday activities. It may be used for something as common as following a recipe for baking a blueberry pie.

An algorithm is characterized by the fact that certain distinct steps must be taken (find the largest number that can be divided into the first two numbers of the dividend) and that those steps may need to be repeated before a distinct answer is obtained. In modern cryptology, encipherment and decipherment are both mathematical operations that follow specific algorithms, differing from one ciphering system to another. An awareness of the algorithm system allows us to work at solving the cipher at hand. The algorithm stated above for long division is a simple one, easily followed. Algorithms used in cryptology can be simple or more complex. (Continued on page three.)

Practical Cryptanalysis – By B. NATURAL - Cryptographic ABC’s and Bifid Cipher by ZEMBIE – Free.

Tyro Tutorial Free E-Mail Offer. **LIONEL**

Tyro Tutorial (148 pages) by LIONEL, fundamental cipher solving processes of some thirty different cipher types.

Free Code and Cipher Books –Place an order. The mailing is also free.

Bi-literal Cypher of Francis Bacon – Gallup *Codes, Secret Writing* – Zim *Games to Go* – Gladstone
Glossary of Cryptography – Shulman *Invitation to Cryptograms* – Williams *Problem Solving* – **R. MASTERSON**
Secret Codes & Ciphers – Kohn *Top Secret* – Janeczko *Xenocrypt Handbook* - **PHOENIX**

ZANAC’s Gimme a Break – JF Aristocrats (may be digraphs / trigraphs) (1) unless otherwise stated

A-1, the (2), A-2, that, A-3, that, the, A-4, the, A-5, you (4) A-6, than (2), A-7, that, A-8, in (4), A-9, the, A-10, the, A-11, that, the (2), A-12, the, A-13, the, A-14, the, A-15, in (5), A-16, but, A-17, is (2), A-18, that, A-19, that, the, A-20, that, the, A-21, ess (2), A-22, colder, A-23, ow (13), A-24, ambush, A-25, hideous.

ZANAC’s Gimme a Break - JF Patristocrats (may be digraphs / trigraphs) (1) unless otherwise stated

P-1, in (4), P-2, you (3), P-3, in (4), P-4, the (3), P-5, that, the (2), P-6, you (2), P-7, that, the, P-8, on (4), P-9, the (3), P-10, that, the (2), P-11, BADH = mind, P-12, JLIV = know, P-Sp-1, ASNY = shop , P-Sp-2, HNUFY = while.

ND-1 Ornamental. Poetic. MSCREP **-** This ornamental is a simple Patristocrat. **BION**
See Cm page 11 to pry out the ciphertext symbols that represent the plaintext. Plaintext begins, “Thick”

ND-2. Foursquare. MSCREP offers crib extension to “fromanimalsanorphan” **BION**

ND-3. Quagmire II. MSCREP: Period Seven, extended crib “two or three percent of total” placed at pos. 38. **BION**

N**D-4. Bifid. (-nificantani-)** MSCREP: Period Seven, expanded crib “insignificant animal” position 58. **BION**

X-12. Spanish Grandpre. Mexican port. (No K or W in Key Square.) **EL CONDOR**
PARROT: Extend crib to “resalto que es la segunda vez que manzanillo”

ND. X-Sp-2. French Unknown. What are friends for? **PARROT**
Parrot identifies as Period Five Bifid, extended crib “cote quand vous etes dans” placed at position 34.

ND. E-7. Swagman. Christmas trees? (regarded) Period Five. Begins “Cons” **L. TWIN**

ND. E-8. Monome-Dinome. Too many disagree. (has said) Begins “Cen-” **EL CONDOR**

ND.E-9. Cadenus. Heavenly music. (movable) Horizontal ciphertext, begins “The tune” **FUNEREALLY**

ND. E-11. Tridigital. Happy New Year, happy birthday. (January) **THE DOC**
Crib fits in second seven letter location between separator digit “7.” First plaintext word “All”

ND. E-12. Homophonic. Working out frustrations. Parrot’s nudge: First letter of keyword “O.” **CILLBIPHER**

ND. E-17. Checkerboard. Nothing more than feelings. (opponents) Additional cribs (that, the) **MSREP**

ND. E-18. Grandpre. European origin. PARROT: Plaintext opens “Our Christmas tree” **LIFER**

ND. E-21. Bifid. Millennium of knowledge. Expanded crib “of the eleventh century” placed at position 69. **CRUX**

ND. E-23. Two-Square. Witchy women? (sitting on the sofa.) PARROT: Begins “Good witch staying” **AURION**

ND. E-24. Foursquare. Did he choose correctly? MANDRAKE advises on crib placement. **RIG R. MORTIS**
Drag crib “as an am ef or” across the first line of ciphertext to find three matches of pt and CT letters.

ND. AC-1178. ??? Conversation needed. (prettier) MSCREP identifies as Frac Morse, crib pos. 52. **MANDRAKE**

ND. AC-1181. Grandpre. Tomorrow. PARROT: Ext crib to “writhing to begin with then the different” **APEX DX**

JF-10. Key Phrase. While living in Vermont. Begins “Writer” **CONFUOCO**

JF. A-23. Slapstick routine. Look for two appearances of circus humorists in plaintext. **OZ**

JF. P-10. Poetic Valentines Day. Plaintext start prompts search of Shakespeare’s Hamlet, Act 2, Scene 2. **G-MAN**

JF. X-2 and X-3. K1. Each of these Xenocrypt Aristocrats uses a K1 keyword alphabet. **BARK**

JF. X-7. ???? Source of evil. K2. (English key) Crib “een” **G-MAN**

JF. X-9, Latin /railfence. Fair play. (nos) Four rails, one offset, begins “Lex” **THE DOC**

JF. X-10. Italian Incomplete Columnar. L’importante. (devozione) Period 7. “Gandhi” in pt.” **MICROPOD**

JF. E-1. Complete Columnar Transposition. Reach for the sky. Period Seven, begins “the” **DLUX**

JF. E-2. Route Transposition. Save some for me. (garlic) Zig Zag column in, Zig Zag row out. **RIG R. MORTIS**

JF. E-3. Playfair. Larry L. King. Google, Larry L. King quotes for plaintext. **HONEYBEE**

JF. E-5. Railfence. Coupon message. Good railfence solving starter – 1, 2, 3 rails, no offsets. **ALCIBIADES**

JF. E-7. Morbit. Change places? (earth) Crib placement 83, second position. **G4EGG**

JF. E-11. Homophonic. Underwater groaner. First letter of keyword equal “C.” **CILLBIPHER**

JF. E-14. Null. Dorothy Parker quote. (the) **THE RAT**
Note position of crib letters in successive words appearing only in one part of ciphertext. Googling, Dorothy Parker quotes will turn up quotation length equal to the number of ciphertext words.

JF. E-18. Checkerboard. Value for money. (work more) Clockwise spiral key begin upper left corner. **THE DOC**

JF. E-22. Vigenere. Getting answers. Period Eight. Begins “We” **DANEEL**

JF. E-25. Foursquare. Contiguity. Start of extended crib “generally no man appears” placed at digraph 2. **LIONEL**

JF. C-14. Equations. (Three words, 1-0) Three, two and five letter words beginning with F, O and B. **APEX DX**

JF. C-Sp-1. Ninth Root. (Three words, 1-0) **FOMALHAUT**
Determine what single digit to the ninth power creates the digit pattern for the ciphertext subtrahend “ROTATION.

Sunny Ciphering, LIONEL

(Continued from page one.)

The complexity of an algorithm is defined by the number of arithmetical operations it performs and represented by the length of the input, ie, the number of bits required to store.
Fermat’s Theorem or Einstein’s Theory of Relativity are examples of complex algorithm procedures requiring a vast accumulation of mathematical computations.

Cryptographic Algorithm Applications
We practice algorithm procedures every time we make use of letter frequency and digraph / trigraph counts, study a Columnar Cipher or Route Transportation path, utilize keyword alphabets, follow ACA and You encryption procedures, use the 26 x 26 Vigenère Square or even execute the solution of a Caesar Cipher. The Caesar Cipher encryption can be depicted
by (N + X) letter shift in the alphabet where N is a fixed integer and X equals a numbered letter shift.

Deep-dish Blueberry Pie LIONEL
Serves 8 to 10 people
Six cups of fresh blueberries
1/2 cup flour
2/3 cup sugar
1/2 teaspoon cinnamon
One teaspoon lemon juice
Mix ingredients together and place in a deep, 8 by 11 inch rectangular pan which has previously been sprayed with Pam. Cover with rolled out pastry for a one crust pie.
Bake it in oven at 425 degrees for 40 to 45 minutes, or until the crust is brown.
Enjoy.

A far better algorithm encryption technique is to use a keyword alphabet table to define the letter substitutions to be made for each letter of the plaintext. We will use a twenty-six letter pangram to do this:

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
CIPHERTXT	N	E	W	J	O	B	F	I	X	M	R	G	L	U	C	K	S	H	A	Z	Y	T	V	P	D	Q

Algorithms need not be simply mathematic equations. They are a part of our everyday life.
We use them when we take the shortest route to the grocery store, cut the grass, water the flowers, instruct our young ones in the “do’s” and “don’ts” and choose our words carefully in debates with our significant other. Algorithms need not be complicated algebraic equations used to attempt to insure coverage of plaintext such as in Affine and Hill cipher types, but simply a way to plot a logical procedure to arrive at the cipher solution of the day or the baking of that delicious deep-dish Blueberry Pie**.**

(See Algorithm article ND 2013 Cm.)