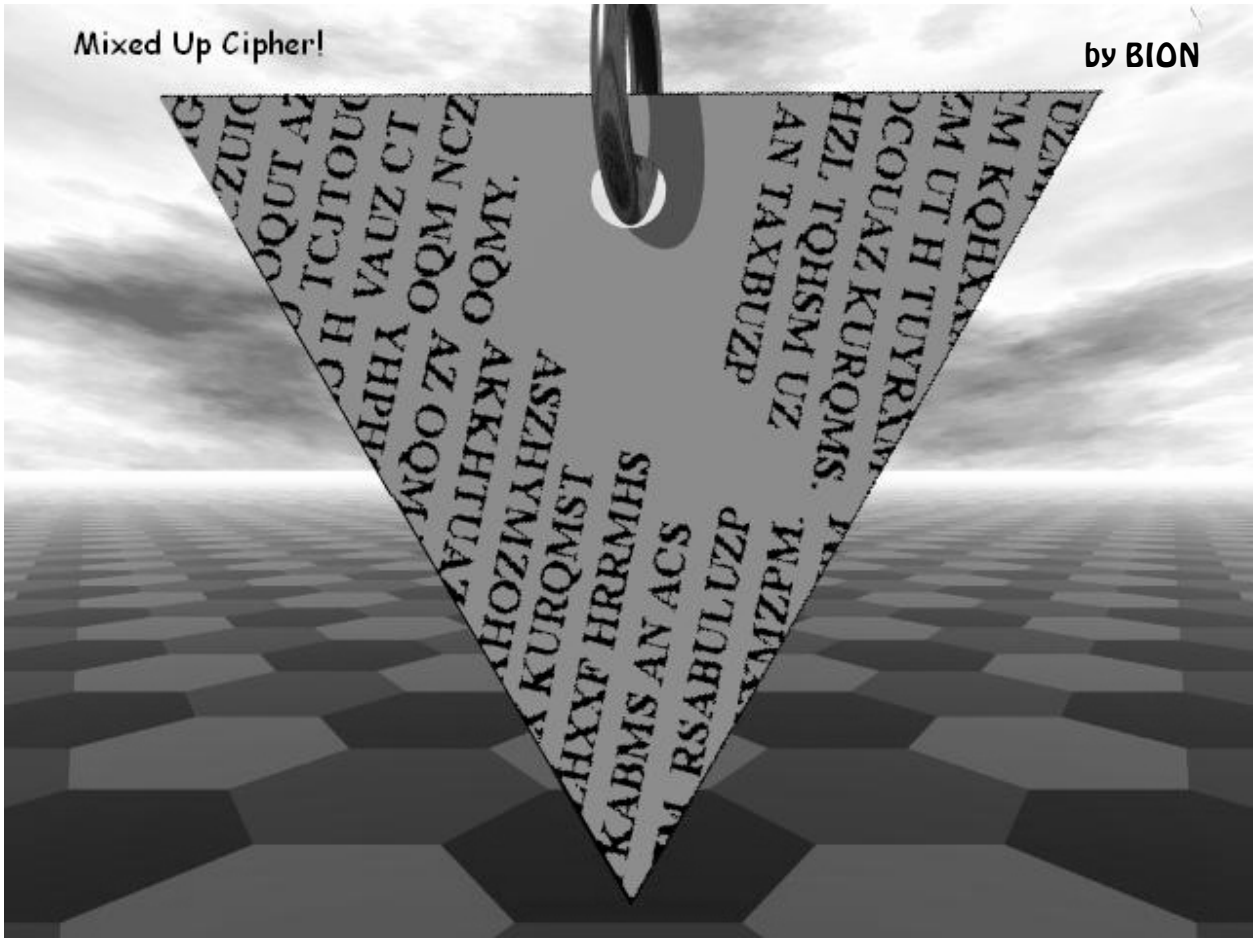
The Cryptogram

Journal of the
American Cryptogram Association
www.cryptogram.org



CONTENTS

Keyword Alphabets, Aristocrats	3
Patristocrats, Cryptarithms	4
Xenocrypts, Cipher Exchange	5
Analyst Corner, Ornamentals	8
Solutions, Membership Information	9
Membership Application	Appendix

This special issue of *The Cryptogram* will tell you about the American Cryptogram Association and explain our activities. It is your invitation to join us. Anyone with an interest in cryptography is welcome.

ACA is a nonprofit volunteer organization devoted to disseminating cryptographic knowledge. Our interest in cryptography is amateur, not professional. We date back to the 1920s, and are quite unique. There is not another organization like us in the world.

Our members construct problems in classical cipher systems for other members to solve without knowing the secret key. We do not get involved in secret messages of companies or governments. Members make up and solve their own creations strictly for the fun of it. The ornamental cipher shown on the cover page was created for this sample by the member whose nom is **BION**.

Every two months our ciphers are published in the ACA journal, *The Cryptogram*. Each issue contains about 100 ciphers They range from very easy to the formidable, in some sixty different systems. Some you probably have seen already, like those found on newspaper puzzle pages. Others you probably won't know unless you are experienced in the field. Even so, some of these can be worked out logically if you have an eye for patterns. You will probably need to do some studying before you can tackle still others. On the next pages, you'll find some examples.

Although they might be called puzzle ciphers today, it was not so many years ago that some of these ciphers were used in earnest. All the ciphers we work with are constructed and edited to be suitable for solving with pencil and paper. Machine ciphers and advanced computer cryptography are beyond our scope.

Many members send in their solutions, and the journal publishes those records. Of course, sending in solutions is voluntary. We are not in competition; each solver competes only against himself. The enjoyment of solving is the important thing.

The Cryptogram also publishes articles on practical cryptanalysis, history of the ACA and book reviews. Additionally, we offer a number of books and inexpensive monographs, difficult to find otherwise, which deal with various cipher systems and how to solve them.

Among the pleasures of membership are corresponding with other members, here and abroad – there are members in over twenty countries – and coming together at our annual convention each August or September. Though not obligatory, you are encouraged to adopt a nom de plume, a code name. It's partly for fun (be as imaginative as you want) but it also puts everybody on an equal footing. Our membership ranges in age from nine to ninety in a wide variety of jobs and professions, with an even wider variety of interests.

The ACA and You: *The Handbook for the Members of The American Cryptogram Association* contains an introduction to the ACA, a list of jargon and terms used in our publications, and the standards used for constructing cryptograms for publication. The handbook contains descriptions of all the cipher systems appearing in *The Cryptogram*. An online version of *The ACA and You* is available under the MEMBERS tab of our website, www.cryptogram.org. Members also receive the annual directory, listing names, addresses and noms.

What do we get out of it? Lots of fun! We have the pleasure of learning the various cipher systems that have been used throughout history. There is a little of everything: history, language, math, and they all come together in cryptography. Then, there is a thrill in making sense of what appears to be a meaningless jumble. It's a form of puzzle solving a bit like crosswords, but more challenging and engrossing. Cryptography is an ideal way to keep mentally alert.

If you enjoy tackling the problems on the following pages, we hope you'll join us. Find out how on page 9.

Keyword alphabets are used to encipher practically all simple substitution ciphers. Recovery can be a valuable aid in solving. Here are two of the most commonly used of the available eight types.

K1: Plaintext alphabet contains keyword; Ciphertext alphabet normal.

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

K2: Pt alphabet normal; CT alphabet contains keyword.

```
Pt: 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
CT: V W X Z K E Y B O A R D C F G H I J L M N P Q S T U
```

Caesar Alphabet: Tips are always given in this form, and appear in capital letters, usually within parentheses. Tips are enciphered to provide extra help for solvers if needed.

A Caesar tip is enciphered by moving forward or backward in the alphabet a certain number of positions. To recover, run down the alphabet until a word that makes sense appears. For the tip LQNLKOA, the sequence would be MROMLPB, NSPNMQC, OTQONRD, PURPOSE.

Now, for some examples and fun. Check your answers on page 9.

Aristocrats, most popular of the cipher types, are simple substitutions using normal word divisions. Each plaintext letter is replaced by a different ciphertext letter not equal to itself.

Each cipher has a number like (A-1), title, keyword indicator, letter count in parentheses, and constructor's nom de plume. There may also be a tip given in parentheses. An asterisk designates a proper noun.

A-1. City living. K1 [90] PRIME

```
OB ISZDPH *GQG EFBE KZE NZUZPJ SQQO ZE EQ EOFNN AKFA BQT YFP'A EKQTA

FA AKD YFA VZAKQTA JDAAZPJ F OQTAKITN QI KFZS.
```

A-2. Identity crisis? K2 [96] (XVEWL) WABBIT

```
JAVGX GZJTAT *HZPRBZJ, QAABJI RPZQC EZJ RKNNGA KLL IZPMZIA RPSEF,

NBEFQ BR SN, QCKSRBJI, "CAX GZTX! XKS TPKNNAT XKSP NSPQA!"
```

Patristocrats are similar in construction to Aristocrats, except that they do not use normal word divisions. They are presented in 5-letter groups. These ciphers are identified with numbers like (P-1), key type, letter count/number of different letters, title, clue in Caesar.

P-1. K1 [81/19] Inherited wisdom. (KFYMJW) ALCHEMYST

J A H O F H P T F D T D G E F D S P B F I H O D H T D A J F O P I M D

H O F E Y D I E P N O H O F W I W D S S A O D I D I U G Y O U H O P G

R I O F P I Y E U G N.

P-2. K2 [86/19]An eternal game (NSAJSYJI) BOATTAIL

S V U V W V R T N B X M U E I U Y I H C T F L B O R I X H B O O V N M

U U M U I Y I I U Y L M O Y T Y L O I I I M K L Y T S M R R M V U F V

W M I X L B E I C I I U X V R H.

Cryptarithms are mathematical problems in cipher, where the letters represent numbers. The number of words given with each puzzle refers to the keyword or words used to develop the original number/letter equivalence. A statement such as 0-9 indicates the range of numbers in use, in this case the decimal set (note that 0 may come first or last).

C-1. Division. (Two words, 9-0) ZIP

SPOILED ÷ SOLE = DYO; - SPMII = IDNED; - IESPO = MPIL

C-2. Multiplication.(Two words, 9-0) VERMONSTER

SUNNY * DAY = ADOONY; + NAMTSY; + SRMRNU = SAOMRASY

A more graphic representation would be written

```
      S U N N Y
          D A Y
---------------
    A D O O N Y
  N A M T S Y
S R M R N Y
---------------
S A O M R A S Y
```

Xenocrypts are various cipher types in different foreign languages. One does not necessarily have to be fluent in the language of the cipher in order to solve the problems.

X-1. Spanish. A Naked Foot! K1 (dejada) HUMBUG

FD NJE, MOHME NO SEW NKMO, TO WKHUHODNJK OAXHEKHNJDEHJETODXO YOH OD

SE EHODE NO SE USEBE SE JTUHOWJKD NOQENE UKH FD UJO NOWDFNK.

X-2. French. Big is Beautiful? K2 (qui; EYB) OOBOO

ERQ QFNIQOOWAR GQGAIKLZQ: "MQEF DEW O'KNNZWDEQRS SIAN KEF NQSWSQO

MVAOQO PQBWQRRQRS AIPWRKWIQGQRS WRMKNKLZQO PQO UIKRPQO."

Cipher Exchange includes problems in various systems of substitution and transposition. Tips are often given to aid in solution since space limits the length of the ciphertext. Several types are outlined here.

Route Transposition: A message is written into a rectangular block in one direction (horizontally, vertically, diagonally, spirally) and taken out in another direction. E.g., "Solve a good crypt today" written in horizontally and taken out vertically (in 5-letter blocks for ease of transcription):

```
Pt: S O L V E
    A G O O D  CT: SACTO GROLO YDVOP AEDTY.
    C R Y P T
    T O D A Y
```

These are Route Transposition Ciphers. Recover each message by finding the correct route.

Route 1)

```
R E T E P
R E P I P
E K C I P
K C I P D
E P D E L
S R E P P
```

2)

```
E E B S L
R S S A E
O E L E S
H H L S E
S T E S H
A Y H L S
```

3)

```
E Y L E X
R N A S S
O E U Y R
C V Q T A
S E E H E
R S S G Y
U D R I N
O N A E E
F A E S V
```

4) LIONEL

```
G O D Y Z
A L E H T
R E V O S
P M U J X
O F N W O
R B K C I
U Q E H T
```

Now try finding the path used to read and write a route transposition.

E-1. Route transposition. Oversimplification. D'PLUME

IPSXE TRRAI EERUI OYOSO SFVLE LTNRC BINWG EPHOI OOLMA RMTSD EPNME L.

Null Cipher: This is a concealment cipher. First letters, last letters, the second letter of each word, a sequence of letters such as first-second-third, first..., letters following each vowel, etc., are some of the great variety of ways a null cipher may be constructed.

Pt: HELP! CT: THE GREAT OLD PUMPERS.In this example, the middle letter of each word is used to encipher the plaintext message.

E-2. Null. Self-reliance (his) BOATTAIL
ELVES EARN YAMS. AGNOSTIC PRAGMATIST DIDN'T LIE. SCHOOL INSTRUCTS "ONWARD!" NECESSARY ANNOTATION OVERLOOKED.

E-3. Null. LIONEL
Patio furniture may stain ornately sculptured tiled mall.

E-4. Null. LIONEL
Leave early route, hue truly entitles rd.

E-5. Null. LIONEL
Feds see pirate bunch go blow safe via borings by deli layout . FBI apprehends.

E-6. Null. LIONEL
Aware, I tie, add aisle. Tea nets appeal.

Complete Columnar Transposition: The message is written horizontally into any size block which is factorable. Nulls can be used to fill spaces at the end if the plaintext needs padding to make the block size factorable. Each column is numbered and the message rewritten into a block according to the number of the column. The ciphertext is then taken off by columns.

```
4 5 1 3 2   1 2 3 4 5
C O M E A   M A E C O
T O N C E   N E C T O
A N D B R   D R B A N
I N G Y O   G O Y I N
U R B R O   B O R U R
T H E R X   E X R T H          becomes  MNDGBE AEROOX ECBYRR CTAIUT OONNRH.
```

E-7. Complete Columnar Transpostion. (ball) WALRUS
ECTPS TAANE LNTEV ITOOA WBURL OAPNT EEYTT LESTS RIOHP WTHHB SUHTO

TREHL ASYLC UYEDD ETAEH HEEOA AEHP.

Checkerboard: The Checkerboard cipher uses a 5 x 5 Polybius square (I and J occupy the same space). Each plaintext letter is represented by two letters, that is, a digraph.

	W	H	I	T	E
B	K	N	I	G	H
L	P	Q	R	S	T
A	O	Y	Z	U	A
C	M	X	W	V	B
K	L	F	E	D	C

The plaintext letter o is represented by the ciphertext AW,
the letter r becomes LI,
and d becomes KT.

Pt: repeated letters cause repeated digraphs

CT: LI KI LW KI AE LE KI KT KW KI LE LE KI LI LT KE AE AT LT KI LI KI LW KI AE

LE KI KT KT BI BT LI AE LW BE LT.

Anagram the first letters of the following digraphs to find the word to place in the far left hand column. Anagram the second letters of the digraphs to find the word to place above the top row.

E-8. Checkerboard. A thought from Parker Hitt. (analysis) ARTEMIS

LC YC UP UP LT LC LC CC YC LY UT LT UP CP KY CY LT UC KC LT KR KT

KR LT LT UT LC KY LT UC LC LT LP LT UC UR KR UP LT UR KR UR LY YP

LC CP LC CP KR KT YC CP KT CP LR KR UR KR UT LY YC UP CT.

SWAGMAN: A transposition cipher. A keysquare is chosen of size 4-8 in which no digit is duplicated in any row or column. The message is written horizontally into a rectangle the same height as the square, adding nulls if necessary to fill out the last row. The enciphered message is taken out vertically by columns in the order of the corresponding key column.

```
Key: 4 3 2 1    Pt: Ciphertext length is a multiple of the square height.
     2 1 4 3
     3 2 1 4
     1 4 3 2

 Pt: C I P H   E R T E   X T L
     E N G T   H I S A   M U L
     T I P L   E O F T   H E S
     Q U A R   E H E I   G H T

Key: 4 3 2 1   4 3 2 1   4 3 2
     2 1 4 3   2 1 4 3   2 1 4
     3 2 1 4   3 2 1 4   3 2 1
     1 4 3 2   1 4 3 2   1 4 3

     Q I G H   E O S E   G E L
     E I A L   H R E T   M T T
     T N P R   E I T I   H U L
     C U P T   E H F A   X H S

CT: QETCI INUGA PPHLR TEHEE ORIHS ETFET IAGMH XETUH LTLS.
```

E-9. Swagman. [44] (swagman) BECASSE

```
UBARR ANGIM EWAED AAKNE IDVIR SNILN OGGAI PSEAK XEWB.
```

E-10. Swagman. [64] (resistance) BECASSE

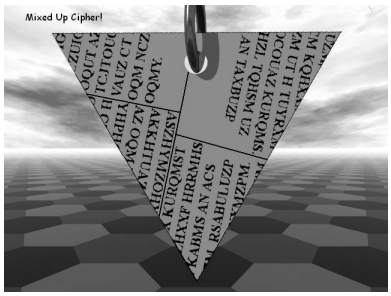
```
OOCNC FFOFU EFRTE EAAAO FRRGM EENIA OATRS RMAKR TEABS SSWEA ITENI

SNTRC AYEX.
```

Analyst Corner provides the challenge of real-world cryptographic problems with limited information and sparse clues. These more difficult ciphers may bend the normal rules. Longer cipher lengths prevail to allow statistical analysis and aid in solution.

Ornamentals appear on the cover of *The Cryptogram* several times a year. They are clever, artistic, and contain a message using one of the many ciphers used in the ACA. For the Ornamental shown on the cover of this sample, find where the edges of the pieces have to be, then cut them out and try it!

Solutions:
A-1 (citypets) My friend Bob says his living room is so small that you can't shout at the cat without getting a mouthful of hair.
A-2 (METALLIC) Newly landed Martian, seeing trash can topple off garbage truck, picks it up, shouting, "Hey lady! You dropped your purse!"
P-1 (parents) By the time a man realizes that maybe his father was right, he usually has a son who thinks he is wrong.
P-2 (OXYGENATED) Monopoly was invented by Charles Darrow in Nineteen Thirty-Three. Eighty million copies have been sold.
C-1 D O N E S I M P L Y
C-2 D U S T Y M A N O R
X-1 (naufragio) Un dia, cerca de las doce, me sorprendio extraordinariamente ver en la arena de la playa la impresion dejada por un pie desnudo.
X-2 (GRANDIOSE) Une expression memorable: "Ceux qui s'appliquent trop aux petites choses deviennent ordinairement incapables des grandes."
Route-1 Peter piper picked pickled peppers.
Route-2 She sells seashells by the seashore.
Route-3 Four score and seven years equals eighty seven years x.
Route-4 The quick brown fox jumps over the lazy dog.
E-1 Alt diag/diag. For every complex problem there is a simple solution, and it is wrong.
E-2 1st-3rd. Every man paddles his own canoe.
E-3 Try a null. (3rd letter each word)
E-4 Every other letter.
E-5 See how easy it is . (Last letter of each word.)
E-6 Write a distant pal. (Letter following each vowel.)
E-7 (RECOIL) Ever notice that the people who say that's the way the ball bounces are usually the ones that dropped it.
E-8 (LUCKY CRYPT SOLVER) Successful decipherment needs perseverance, analysis, intuition, and luck.
E-9 Breaking a Swagman is like unweaving a braided rope.
E-10 Courage is resistance to fear, mastery of fear - not absence of fear. Mark Twain
Ornamental [K2 Aristocrat] (ARISTOCRAT) Ornamental ciphers occasionally appear on the cover of our magazine, providing a unique challenge. This one is a simple substitution cipher. Join us and share in the fun of solving them.



(Keywords are in parentheses: K1 lc, K2 UC)

Dues/Subscriptions:

Regular dues for individual members are $18 in North America and $22 overseas. Individuals paying full dues may optionally reduce the multi-year total by $1 for a 2-year renewal, by $3 for 3 years, by $6 for 4 years or by $10 for a renewal of 5 or more years. Members 65+ with 10 years prior membership or full-time students may pay $10 in North America and $15 overseas. Student memberships must be renewed annually.

Send payment to

ACA Treasurer
56 Sanders Ranch Rd
Moraga CA 64556

Prepared by **ARACHNE** and **PHOENIX** with contributions by **SY S. ABEND** and other ACA members.

AMERICAN CRYPTOGRAM ASSOCIATION
MEMBERSHIP APPLICATION

Mail application and dues payment in US funds to:

Charles F. Schretzmann
ACA Treasurer
56 Sanders Ranch Rd
Moraga, CA 94556

Checks and money orders should be made payable to The American Cryptogram Association or ACA.

I am applying for membership in the American Cryptogram Association.

New Memberships	North America	Overseas
Regular	$23	$32
Full-Time Student*	$15	$25

One-Year Renewal	North America	Overseas
Regular	$18	$22
Full-Time Student*	$10	$15
Members 65 & over with 10 years prior membership	$10	$15

Multi-Year Discounts	North America	Overseas
Regular 2 year renewal (save $1)	$35	$43
Regular 3 year renewal (save $3)	$51	$63
Regular 4 year renewal (save $6)	$66	$82
Regular 5 year renewal (save $10)	$80	$100
More than 5 years	Subtract $10 from total.	

* See student application section on next page. Students must renew annually.

NAME _____

ADDRESS _____

_____

_____

Telephone number (optional) _____

Do you want your phone number published in our Directory? Yes _____No _____

My first choice of nom is _____

My second choice of nom is _____

No nom selected at this time _____

Amateur radio call sign, if any _____

e-mail, if any _____

How did you hear about the ACA? _____

Signature _____ Date _____

Student Membership Application

To be eligible for ACA Student status, you must meet the following requirements:

- You must be enrolled in an educational institution that grants academic diplomas or degrees (e.g., a high school, college, or university).
- You must be actively pursuing an academic diploma or degree.
- You must be attending as a full-time student.

Most full-time pre-college, undergraduate, and graduate students will satisfy these requirements. Part-time students and those engaged in independent study outside of a formal educational program do not qualify.

If you would like to apply for ACA Student Status, please complete and sign this section of the application and mail it to the ACA Treasurer. Student memberships must be renewed annually.

I am enrolled as a full-time student and am pursuing an academic degree or diploma.

EDUCATIONAL INSTITUTION _____

CITY and STATE _____

DIPLOMA/DEGREE _____ YEAR EXPECTED _____

Signature _____ Date _____