ACA Guidelines

Keywords

Keywords may be used in Aristocrats, Patristocrats, Cryptarithms, Xenocrypts, and in many Cipher Exchange systems. Although a key may be optional, its use is recommended not only because it is a useful aid to solution but also because it reflects the historical use of keys in these ciphers.

Four basic schemes are referred to by number, K1 to K4. The alphabet is keyed by writing an arbitrary keyword or phrase followed by the rest of the alphabet in normal order. A letter occurring more than once is omitted after the first occurrence.

e.g. CONSTELLATION becomes CONSTELAI.

Either the plaintext or the ciphertext alphabet may be shifted ("wrapped round") to avoid a plaintext letter standing for itself in simple substitutions.

Regular Alphabetic Keywords

K1 Keyword Type: plain alphabet contains a key, CIPHER alphabet is 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 Keyword Type: plain alphabet is normal, CIPHER alphabet has the key.

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

K3 Keyword Type: Both alphabets are keyed with the same key.

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

K4 Keyword Type: Both alphabets are keyed, using different keywords.

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

5x5 Polybius Square

	1	2	3	4	5
1	E	O	Y	H	Q
2	X	R	B	K	S
3	T	D	C	L	U
4	R	I	F	M	W
5	A	N	G	P	Z

A Polybius Square is used to encipher plaintext in some ciphers. The use of row and column numbering may or may not be necessary. Since only a 25-letter alphabet can be used the I and J are combined in the same cell. In this example, the keyword EXTRAORDINARY is used in a vertical route. Other routes are possible.

For encryption, a plaintext or key letter J is replaced with I before encrypting. By convention, we use only I (not J) in ciphertext.

6x6 Polybius Square and 36-Letter Alphabets

	1	2	3	4	5	6
1	E	5	X	T	R	A
2	6	G	7	H	8	1
3	F	S	U	V	J	O
4	3	Q	Z	W	Ø	D
5	C	P	M	L	K	4
6	2	B	Y	N	9	I

When a 26-letter alphabet with 10 digits is used to encipher plaintext which includes numbers, then the digits MUST be placed immediately after their corresponding letters in the Polybius square or in the keyed/unkeyed alphabet: 1 after A, 2 after B, etc., whether they appear in the key or not.

The example at the left shows how to build a 6x6 square using a clockwise spiral with keyword = EXTRAORDINARY.

The following is an example of a 36-letter Ragbaby alphabet using the same keyword: E5XTRA1OD4I9NYB2C3F6G7H8J ØKLMPQSUVWZ.

Some ciphers which adapt to a 6x6 Polybius Square include:

6x6 Bifid
6x6 Twin bifid
6x6 Checkerboard
6x6 CM bifid
6x6 Foursquare
6x6 Nihilist substitution
6x6 Phillips
6x6 Playfair
6x6 Seriated playfair
6x6 Tri-square
6x6 Two square
36-letter alphabet Ragbaby

Length guidelines for 6x6 ciphers will be the same as their 5x5 counterparts.

Mixed Alphabetic Keyword Types

The keyed alphabets may be mixed rather than in normal sequence. The resulting keys are identified as K1M, K2M, etc. The mixing is done with a transposition block. The keyword alphabet is entered by rows, and the mixed alphabet is taken off by columns, either in left to right sequence or in alphabetical order of the top letters (a key):

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

By consecutive columns:
MA: RBKVODLWMFPXAGQYNHSZCITEJU

By order of top letters:
MA: AGQYCITEJUMFPXNHSZODLWRBKV

A transposition block may also be formed leaving spaces for letters used in the key. This will yield a different set of Mixed Alphabets (MA):

```
R O M A N C E         By consecutive columns:
- B - D - F G         MA: RHVOBIPWMJQXADKYNLSZCFTEGU
H I J K L - -
- P Q - S T U         By order of top letters:
V W X Y Z             MA: ADKYCFTEGUMJQXNLSZOBIPWRHV
```

Other arrangements submitted will ordinarily be returned to the author for re-encipherment, or will be discarded. With a proper choice of keyword, these systems have been found sufficient for a wide range of difficulty of keyword recovery. When keywords are used as an adjunct of plaintext recovery, these systems give enough play of possibilities. Rarely, an improperly keyed problem will be printed with a key designation, or it may be labeled "Variant", as in "K2V". This is used if the alphabet is split around the keyword, (for example, A B C <u>K E Y</u> D F G H I L ... Z)

Decimation

Given the recovered K3 alphabet:

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

decimation allows the solver to recover the keyword used to form the key alphabet. This process is used when trying to recover the keyword in the Headlines puzzles.

```
 1: XVOGMZFHQSTBARNDKYPWEIULJC
 3: XGFSADPIJVMHTRKWUCOZQBNYEL
 5: XZTDECMSNWJGQRPLOHAYUVFBKI
 7: XHNIOSKLMBPCFREVQDUGTYJZAW
 9: XSPVTWOBEGAIMRUZNLFDJHKCQY
11: XBUHPGNCTIFYORJSEZKVALQWMD
15: XDMWQLAVKZESJROYFITCNGPHUB
17: XYQCKHJDFLNZURMIAGEBOWTVPS
19: XWAZJYTGUDQVERFCPBMLKSOINH
21: XIKBFVUYAHOLPRQGJWNSMCEDTZ
23: XLEYNBQZOCUWKRTHMVJIPDASFG
25: XCJLUIEWPYKDNRABTSQHFZMGOV
```

That is, the first decimation at offset 1 is the original alphabet. The next is at offset 3, taking every third letter and wrapping when you get to the end: XvoGmzFhqStbA and so on. Only the offsets relatively prime to 26 are used, because otherwise the sequence repeats. Then you look carefully at each line to see which one might be composed of all vertical slices of the key table. It turns out to be offset 3:

```
X GFS ADP IJV MHT RKW UCOZ QBNY EL
```

The original mixed key alphabet is

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

Standard Features of Ciphers

Aristocrats, Patristocrats, and Xenocrypt Substitutions

1. Length: 75-100 letters. Pats should be 90-105, and in no case less than 85 or more than 140.
2. No more than 4 singletons (letters used only once).
3. At least 18 different letters should be used in each problem.
4. Repeated consecutive plaintext should be avoided.
5. No more than 3 proper nouns, each indicated by " * " at the left except in the case of Patristocrats.

Cryptarithms

1. Single or double keyed problems in division, multiplication, square roots and various equations are popular.
2. Additions should have no more than 3 terms plus the total.
3. Equations should have no more than 3 items.
4. Multiplications should have no more than 3 digits in the multiplier.
5. Divisions must not end in zero to be brought down as remainder unless a legitimate subtraction follows from it in the last step.
6. Problems must show all steps involved, not just components and answers.
7. Keywords MUST be complete (CRYPTAIHMS is not acceptable).
8. Several words may be used together (HOWISFRANK is acceptable).
9. Number-bases should be in the range 8-16.

Cipher Exchange

Acceptable lengths for Cipher Exchange ciphers are given with each cipher in Chapter 9.

Xenocrypts

Xenocrypts use Dutch, Esperanto, French, German, Latin, Italian, Portuguese, Spanish and Scandinavian languages. Other languages may be used, often as Specials.

Hyphens and Word Breaks

When a ciphertext contains word divisions and occupies more than one line when printed, there can be ambiguity as to whether a word at the end of a line is complete or not. To avoid confusion, use these conventions:

Use the single hyphen (-) to indicate that a ciphertext word is continued on the next line. This does not indicate proper syllabic hyphenation.

Use a double hyphen (=) to indicate that the original plaintext word is hyphenated.