

Chapter 7

How to Encipher a Problem for *The Cryptogram*

The Cryptogram depends on you for problems published for the pleasure of all. Make a note of interesting plaintext as you read. Polish your language skills and gain new insights by enciphering. Then send the results to the Department Editors so others may pit their skills against your challenge!

No game is entertaining unless players are assured a square deal. Thus, to ensure justice and to maintain high standards, guidelines have been worked out over the years. All are subject to editorial judgment in individual cases. A contribution which meets the standards will always be more welcome than one which does not.

The departments give varied fare for experts and beginners. Your contribution will be tested by the Department Editor and graded for difficulty. You are encouraged to add a title and tip to your contribution. Editors may override these suggestions. However, if you have not suggested a title or tip, a suitable tip and title may or may not be added by the editor.

Please use a separate sheet of paper for each encipherment, write on one side of the paper only, and use the format employed for that cipher in *The Cryptogram*. You should show your working of the solution on a separate page. If submitted by email, please use a separate message for each con and include the type of cipher in the subject line.

We hope all members will contribute generously and regularly so the Editor's "bins" (files) will be kept full. Remember that a published "con" can be counted as a "sol".

Enciphering Guides

1. Text must make sense. Check word meanings to avoid impossibilities and contradictions. Telegraphic text, incomplete sentences without verbs, or mere lists of words are not acceptable.
2. Definite and indefinite articles may be omitted, but punctuation must be correct for Aristocrats. Numerals are to be written out in full (except for those cipher using 6x6 Polybius squares and other ciphers using digits in their alphabets, such as a 36 letter Ragbaby).
3. Misspelling, mixed cases, wrong tenses, or other grammatical errors must be avoided. Check and recheck before submitting.
4. Text worth reading should be the solver's reward. Unfair tactics reduce the value of the challenge; cleverness is the essence of a tough problem. Find what features of the cipher aid in its decipherment, and see if you can obscure these features suitably.

5. Double-check quotations to make sure they are accurate. If they are being paraphrased brutally for an Aristocrat that's one thing, but if they are intended to be literal quotes they should be quoted correctly.
6. Follow the guidelines in this book for proper lengths for ciphers. Good problems may have to be discarded because of excessive length, but don't spoil a poem or a quotation for the sake of a few letters!
7. Unfair text contains words not listed in standard dictionaries with the exception of proper nouns and popular slang. Obsolete words, reformed spellings, and foreign words are unacceptable.
8. In Xenocrypts, simple language is preferred to technical quotations. Accents are always omitted. In simple substitutions, use a keyword to aid in deciphering irregular verbs, singletons, etc. (K2s are preferred; K3s, K4s, and random alphabets must not be used). (See Chapter 8 for the types of keys.)

Keys may be in English or in the foreign language, but should be chosen to assist the decipherment. Study what other encipherers do.
9. In Simple Substitutions, use only capital letters. No letter may stand for itself. Add an asterisk to the left of any proper noun in an Aristocrat, Keyphrase, or Ragbaby, and any Xenocrypts of these types. (In Xenos an asterisk is also used in the tip to denote a letter or group of letters that do not actually appear. That is, it may be used to denote one or more letters missing in the alphabet, the square, or in the text.)
10. In Periodics, the ciphertext should be submitted in blocks of five letters.
11. In Cryptarithms, use no base under 8 or over 16. Bases 10, 11, 12, and 16 are preferred. Root extractions are limited to square and cube roots. There must be only one possible solution to a Cryptarithm. Check, for instance, that any letters occurring once only are not in the same column.
12. Editors may choose to use the American spelling of a British word in a quotation by a British author.

The Question of Original Systems

One-time pads were used by spies and were unbreakable. Rudolf Abel's cipher was probably also unbreakable. His messages were not read until he explained the cipher, and even knowing the general system, it may still confound many people. More recently, Bruce Schneier invented a playing-card-based system called Solitaire which has so far resisted attacks.

So you have the perfect indecipherable system? Perhaps you have heard that the ACA is a proving ground for such things? Stop! While we all like a challenge, the purpose of the ACA is not to test for indecipherable systems.

For over 400 years, cryptographers have been writing seriously on the subject. Systems once thought to be unbreakable have succumbed to analysis. Without a thorough knowledge of what has been done, and of what makes a good system, the chances of inventing a useful new one are slim. Variations are endless and too often worthless.

Below is a list of guidelines for a successful military cipher. Variations for diplomatic and commercial use are minor, but in any case the ciphers are intended for heavy traffic use with difficulty of solution appropriate to the timeliness of the enciphered message. Few cryptographers are able to judge the weak spots of a system, even one that seems to meet the requirements. If you do invent a new one, let it sit for a while and "digest" in your mind while you try to find a similar system already in use, or used in the past.

Note that we already use some 60 ciphers in *The Cryptogram*. To be considered seriously, you would first have to describe your new cipher in an explanatory article. Based on this, and your own record of ability in cryptography, the system might be considered for acceptance for regular use if the reaction of the membership were favorable.

Auguste Kerckhoffs (1835-1903), was a Flemish linguist and cryptographer. The most famous dictum on his list is #9, which is commonly called "Kerckhoffs' Law". His criteria for a suitable military cipher are:

1. The cipher must be suitable for telegraphic transmission, with no special symbols.
2. Ciphertext should not be much longer than the plaintext for rapidity in encipherment, transmission, and legitimate decipherment.
3. Security must not depend on any limitations of plaintext.
4. Decipherment must yield unambiguous plaintext; one possible message. A few ACA ciphers do not obey this rule.
5. Necessary apparatus must be small enough to be easily carried.
6. Methods of encipherment and decipherment must be simple, requiring few operations and putting little mental strain on the operator.
7. Errors being inevitable, omission or error in a letter or group should not affect the rest of the text. Rapid and easy correction must be possible.
8. Text comparisons of several cipher messages with a fragment of plaintext, or with the text of another cipher, should not lead to a "break".
9. Kerckhoffs' Law: The interceptor is assumed to possess all details of the system but the keyword. An unalterable system, or one with few variations, is poor. The key must be easily altered, easily remembered, easily applied, and vastly variable.

During World War II the ACA was the proud reservoir of cryptographic talent for our country. Today, paper and pencil work is still vital to our national well-being. The FBI has professional codebreakers solving ciphers much like ours, so our skills are still useful. In considering new systems for presentation to the ACA, we give more weight to the cryptanalytic interest, subjectively judged, than to adherence to any specific requirements. Experience must still back any invention, for only through solving can you come to judge the degree of interest your own invention might generate among fellow members.