

Chapter 10

ACA Jargon and Familiar Terms

A - Aristocrat.

AC - Analyst Corner. A department of *Cm* containing more difficult messages with a "setting" but often no tip.

ACA - American Cryptogram Association

Anagram - Word or phrase constructed by the transposition of letters from another word, phrase or ciphertext. Anagrams may also be mixed, rather than forming another word.

Aristocrat - Simple substitution cipher with retained word divisions.

Asterisk (*) - (1) Indicates a proper noun in certain ciphers.
(2) Indicates success in solving every cipher in a section of *Cm*.
(3) Indicates unused letters in Xenocrypt tips.

C - Cryptarithm.

C/A - Used by the intelligence community to mean cryptanalysis.

Cm - Abbreviation for *The Cryptogram*.

CM - Conjugated Matrix. A type of bifid.

Caesar - (noun) Simple substitution cipher, each letter in a crypt being shifted the same amount. (verb) To run each letter in a crypt up or down an alphabet until a word is seen. Aka running down the alphabet.

Challenge - An unusual or difficult problem.

Cipher - A system of secret writing whereby plaintext letters or groups of letters are transformed to hide their meaning. (Not a code)

Cipher Exchange - A department of *Cm* containing a variety of cipher types.

Ciphertext - The text produced by applying an encryption method/system to a plaintext message – a cryptogram.

Cleartext - Plaintext.

Code - A special form of substitution cipher in which groups of letters, words, phrases or even whole sentences are replaced by groups of characters chosen arbitrarily.

Completer - A solver who has completed every problem (except specials) in all regular departments of the *Cm*; indicated by a * against the name or nom.

Con - A construction; a cipher problem.

Concealment Cipher - Message written in apparent plaintext used to cover hidden message within. See Steganography.

Consonant Line - A cryptanalysis aid in which tentatively identified consonants are graphically displayed.

Contact Count - A cryptanalysis aid, enumeration of different letters contacted by the letter in question.

COPS - Contribution of Postage Stamps. A voluntary donation of stamps or money to help defray costs.

Crib - A clue for entry into a cryptogram. (Also tip)

Cryptanalysis - The steps or processes involved in converting encrypted messages without initial knowledge of the key or the encryption process.

Cryptanalyst - One who solves codes or ciphers without knowledge of the system or keys.

Cryptanalyze - To solve by cryptanalysis.

Cryptarithm - An arithmetic problem in cipher.

Cryptogram - (Crypt); A communication in cipher.

Cryptography - The process of communication encipherment.

Cryptology - The science or study of encryption and decryption.

CS - The "Computer Supplement"; no longer published, but copies are still available.

CT - Ciphertext.

Decimation - The process of constructing a key alphabet from another one by taking letters at a fixed interval starting with the first. The interval must be relatively prime to the length of the alphabet – that is, for a 26-letter alphabet one cannot use an interval of 13 or any even interval, because the resulting alphabet will not include all letters.

Decipher - The specific process the cipher clerk uses to change ciphertext back into plaintext if a cipher is used. To convert ciphertext to plaintext knowing the keys and the system.

Decode - The process the cipher clerk uses to change ciphertext back into plaintext if a code is used.

Decrypt - To convert or transform a cryptogram into the original equivalent plaintext message by a direct reversal of the encrypting process.

E - The Cipher Exchange.

EB - The Executive Board of the ACA.

Elcy - *Elementary Cryptanalysis*; standard text now entitled *Cryptanalysis* (Dover Books).

Encipher - To convert or transform a plaintext message into a cryptogram by following certain rule, steps, etc. To convert plaintext to ciphertext using a system and a key.

Encrypt - See Encipher.

Encode - The process the cipher clerk uses to change plaintext to ciphertext if a code is used.

Fractionation - A process whereby a plaintext letter is spread across two or more ciphertext letters. See Bifid and Trifid.

Frequency Chart - Table of number of occurrences of each letter in a text.

Frequency Distribution - Occurrences of letters within the text of any language or ciphertext.

Gadsby - A novel of over 50,000 words written without the use of the letter "e" by Ernest Vincent Wright.

Index of Coincidence - Likelihood that any pair of letters in a message are equal to each other. Used to determine the key length in a periodic cipher. Also used to decide whether a cryptogram comes from a single alphabet.

K - Key.

K1, K2, K3M etc. - Keyword types. (See Chapter 8.)

Kasiski - A method for obtaining the period of a periodic cipher.
(See *Elcy* Chap XIV)

Key - A word, phrase, series of numbers or letters used to control the encipherment process.

Krewe - Members of the ACA.

Literal Key - An alphabetic key.

Naturals - An instance where the cipher letter and the plain letter are identical.

Nom - Code name (nom-de-plume) used by some members for anonymity and informality.

Null – (1) A letter, without meaning, added to pad out text, break up double letters or provide necessary amount of ciphertext to meet cipher requirements. (2) A type of cipher.

Ornamental - A cipher hidden in a graphic design. (See Steganography.)

P - Patristocrat.

Patristocrat - An Aristocrat cipher in 5-letter groups, i.e., word divisions are suppressed.

Pattern Word - A word in which one or more letters are repeated, providing a clue to identity.

Periodics - Ciphers in which substitutions occur in a periodic manner.

Plaintext - Original message before encipherment (Cleartext).

Polyalphabetic Substitution - A form of cryptography where more than one ciphertext alphabet is used.

Polybius Square - 5 x 5 square used to key substitution ciphers. I/J share one space. 6x6 squares which include 26 letters and 10 digits (See page 27) are used also.

pt - Plaintext.

Public Key Cryptography - System in which messages are encrypted and decrypted by using a combination of keys, one available to the general public and one private.

Quagmire - A mixed alphabet periodic cipher (named for its original keyword).

Scytale - Symbol of the ACA. Ancient Greek cipher device.

Simple Substitution - A cipher in which each letter of the Plaintext is replaced by one cipher letter, the replacements being unique and no letter standing for itself.

Slide - A mechanical device for aligning alphabets, used in manual cryptanalysis or encipherment of Periodics.

Sol - A solution.

Special - An unusual or difficult problem.

Steganography - A method of encrypting a message such that the presence of the message is not obvious to the casual observer (for example, Ornamentals, some Grilles, clever Baconians, etc.).

Tip - A clue for entry into a cryptogram. (crib).

Tramp - A transposition cipher.

Transposition - A cipher retaining the plaintext letters in a re-arranged form.

Unknown - A cipher using an unspecified system.

Vigenère - A class of periodic substitution ciphers.

Vowel Line - An analytic aid similar to a Consonant Line.

X - Xenocrypt.

Xenocrypt - A foreign language cipher.