

Crypto Glossary

(taken from: David Kahn, *The Codebreakers*, Scribner, 1996)

cipher A system of encryption.

cipher alphabet The list of equivalents used to transform the plaintext into the secret form in a substitution cipher. There may be more than one *cipher alphabet* in a substitution cipher.

ciphertext The encrypted message, as opposed to the plaintext.

code A list of words, phrases, letters and syllables with the *codewords* or *codenumbers* that replace these elements. A *code* need not be designed or used for cryptographic purposes, eg. the morse code.

codetext The encoded message, the result of passing a plaintext through a code.

cryptanalysis The process of cryptanalyzing. Sometimes called *codebreaking*.

cryptanalyze To break down or solve the ciphertext. This process is illegitimately done by a third party that do not possess the key.

cryptogram The final secret message, wrapped up and transmitted.

cryptography The science of rendering a message unintelligible to outsiders.

cryptology The science of secret. It encompasses cryptography, steganography, cryptanalysis, secure multiparty computation, secret sharing, etc.

decipher To reverse the transformation of a cipher, on a ciphertext, in order to bare the original message. This process is done by a legitimate owner of the key. Synonym: to *decrypt*.

decode To reverse the process of encoding, on a codetext, in order to get the plaintext.

encipher To pass a plaintext through the transformations specified by a cipher. Synonym: to *encrypt*.

encode To pass a plaintext through the transformations specified by a code.

homophones Alternate equivalents used for a single plaintext letter in a substitution cipher.

key Most ciphers employ a *key*, which specifies such things as the cipher alphabets in a substitution cipher or the pattern of shuffling in a transposition cipher.

monoalphabetic A substitution cipher is *monoalphabetic* if only one cipher alphabet is in use.

nulls A symbol in a cipher alphabet that means nothing and is intended to confuse the interceptor.

plaintext The message that will be encoded or put in secret form. Synonym: *cleartext*.

polyalphabetic A substitution cipher is *polyalphabetic* if only two or more cipher alphabets are employed.

steganography The science of concealing the very existence of the message.

substitution The letters of the plaintext are replaced by other letters.

transposition The letters of the plaintext are shuffled.