The Bletchley Park 1944 Cryptographic Dictionary formatted by Tony Sale (c) 2001

EDITORIAL NOTE

It seems desirable to point out that this present edition of the Cryptographic Dictionary is not as complete or as useful, or even, perhaps, as accurate, as such a work of reference should be. It has been in course of preparation for a whole year, but for the greater part of that period the Editor has been engaged on other work.

The sources used for the vocabulary have been practical cryptography in the Research Section, various documents and reports in the Cryptographic Co-ordination and Records Section, and numerous supplementary contributions from different cryptographic sections to which the Editor had recourse for explanations of terms used in reports.

Words have been considered from the cryptographer's point of view rather than that of the cipher-maker or cipher-user. Various classes of words, e.g. key names, and cover names, have been deliberately omitted. American words and meanings have also been omitted, except when they appear to have been adopted in English cryptography.

Many cases of the misuse of technical terms have been brought to light,and some attempt has been made to indicate the most glaring of these misuses. With fuller information about present usage this could be extended with a view to regularising terminology at least to the extent of avoiding needless ambiguity; but some of the senses here designated as 'misuses' are too firmly established to be changed. There is no doubt but that the clear versions of cipher messages will continue to be called 'decodes' , and second encipherments of messages 're-encodements', however strongly the usage is condemned.

The dictionary, then, as now presented, is little more than an indication of what a cryptographic dictionary should be; but it is hoped that its limited circulation now will evoke criticisms and suggestions both on details, which are incorrect or absent, and on the scope and functions which a work of this kind should have. They will be gratefully received and, when circumstances permit, will be utilized to produce a mere complete and useful edition.

20th July, 1944

ADDER :

A series of figures or letters (or a group or single unit of such a series) which is added figure by figure or letter by letter, usually non-carrying, especially to the figures or letters of code-groups in the process of reciphering, and subtracted from cipher groups in the process of stripping a reciphered code message; a reciphering key or subtractor.

ADDER NUMBER :

A daily-changing number which is added to a basic number in the process of determining the page of the call-sign book, known as the Bird book, to be used on a particular day.

ADDER TABLE :

A reciphering table applied by addition.

ADDITION :

A process (used in enciphering, reciphering, deciphering, etc.) whereby two figures, two letters, or a letter and a figure are combined and the result denoted by a figure, a letter, and a letter respectively, on a conventional basis.

1. Addition of figures is usually non-carrying and in the scale of 10, the series 0 1 2 3 4 5 6 7 8 9 being treated as cyclic; so that 1 + 2 = 3, 5 + 9 = 4; but ordinary "carrying" addition is occasionally used, and non-carrying addition in other scales, e.g. 11, when 5 + 9 = 3.

2. In the addition of letters the letters A - Z may be treated as having the values 0 - 25 and as forming a cyclic series; addition is always non-carrying in the scale of 26, so that A + O = O, I + O = W, M + S = E. Or A - Z may be treated as having the values 1 - 26, i.e. 1 - 0, so that A + O = P I + O = X, M + S = F.

3. Addition of a letter and a figure is similarly non-carrying in the scale of 26, the figure indicating the number of places to move to the right in a cyclic alphabet, so that A + 4 = E Y + 5 = D, cf. Gronsfeld .

ADDITIVE. a :

(used especially of recipher keys). Applied by addition.

ADDITIVE. n :

= Adder .

ADMIT :

(of an Enigma message). To produce no crashes with (a particular version of a crib).

AITKENISMUS :

(in Enigma) A type of near-cilli, arising from the tendency to avoid repeated letters in outside indicators; the occurrence of this may (with luck) be detected by assuming a cilli and calculating back to the possible message-settings that follow from this assumption; if one of these agrees in two letters with a recognizable type (e.g., keyboard, pronounceable, etc.) but not in the third letter, and if the adjustment which the third letter requires would produce a final position having a repeated letter, the presence of "Aitkenismus" is indicated.

ALPHABET :

1. The letters and/or other signs or symbols employed in a particular code or cipher.

2. The order in which the letters and/or other signs or symbols employed in a particular cipher are arranged to represent the plain language letters (and other signs, if any) in their natural order for a particular key-letter or number. This order is often "hatted" and the "hatting" may be different for each different key-letter or the same alphabet may be "slid" cyclically according to the key-letter; (in Enigma) the thirteen substitution letter-pairings at any given position of the wheels. See also cipher alphabet .

3. (in Enigma key-breaking when the ringstellung is known or assumed) The complete series of possible stecker for a group of letters in a chain.

ALPHABETIC, ALPHABETICAL :

1. (of letters). occurring or arranged in their usual or natural order.

2. Employing letters or groups of letters

3. (spec. of code-books). Having the code-groups so assigned to the various items of the vocabulary that when the latter are arranged in alphabetical order the former are also in their natural order i.e. in numerical order in the case of figure-groups and alphabetical order in the case of letter-groups), and so permitting both encoding and decoding to be performed with one series of equivalents; unhatted; one-part, cf. Hatted . Two-part .

AMIR :

(in Enigma) A Crib sent from B.P. to Washington to be run on the naval bombes there.

ANAGRAM. n :

Plain language reconstructed from a transposition cipher by restoring the letters of the cipher text to their original order.

ANAGRAM. v :

1. To rearrange the letters of a transposition cipher (usually by trial and error) so as to restore the original plain language.

2. (misused for). To decipher any part of a Playfair cipher, either by utilizing bigram frequencies and a knowledge of the probable plain text, or by using a previously reconstructed Playfair square or squares.

3. (misused for). To break any part of a letter-subtractor, esp. machine-cipher, depth of two or more messages by differencing and stencil-search or virtual stencil-search.

ANAGRAM KEY :

The natural numbers (i.e. from 1 upwards) of the letters of a transposition cipher rearranged into the order which these letters have in the clear text, thus showing how the cipher letters are anagramed to restore the original plain language. cf. encipher key.

ANALYSIS :

1. Systematic examination of cipher messages with a view to discovering e.g. indicators, limitations, or other characteristics of the system employed which may provide a point of attack or suggest a method of solution.

2. Systematic examination of a portion of key, esp. of a machine cipher, aimed at resolving it into its basic components.

3. (in Met.). A message containing a general description of the weather situation over a large area, e.g. Western Europe, at a particular time.

ANTI-CRIB, a :

(applied to regulations or methods). Designed to avoid giving cryptographic cribs.

APERIODIC :

(esp. of machine ciphers and keys). Showing no evidence of periodic repetition within the length of one message (owing usually to great length of key period).

ARBITRARY :

(of code-groups, indicators, etc.). Having had a provisional subtractor taken off; reduced to provisional, not true, figures or letters. cf. base

AUTOCLAVE :

A cipher system in which successive groups of one or more letters or figures are enciphered in a manner determined or partly determined by the key and/or plain language of the preceding group or a fixed combination of preceding groups; a cipher having a self-generating key.

AUXILIARY TABLE :

(in certain code-books which have two meanings assigned to one group). That portion of the code which includes the second, or subsidiary, meanings only; the employment of which is normally indicated by a switch-group; cf. main table.

BABY :

= Test-plate.

BABY BRUTE FORCE :

Brute force methods applied to a selected portion of traffic, especially to messages beginning on certain pages of a long subtractor, when the indicator system is partly solved and the page (but not the line and column) on which the messages begin is known.

BACKWARD CLICK :

(in Enigma). The occurrence of two different letters at the same position in two messeges in depth with each other, associated with the occurrence of the same two letters in the reverse order in the two cribs.

BAG :

(in Met.).

1. (short for Bag of Stations). A set or group of meteorological stations the observations from which are grouped together in a collective broadcast.

2. Such a group of observations in a collective broadcast; (e.g. the observations from stations in Holland form a "bag" in the W. European collective from Berlin).

BAN :

Fundamental scoring unit for the odds on, or probability factor of, one of a series of hypotheses which, in order that multiplication may be replaced by addition, are expressed in logarithms. One ban thus represents an odds of 10 to 1 in favour, and as this is too large a unit for most practical purposes decibans and centibans are normally employed instead.

BANBURISMUS :

1. The use of Banburies to set messages(especially Enigma messages) in depth with each other. When two Banburies are superposed identical letters in the same position are readily seen by (the light which comes through) the coincident holes; the number of clicks for any relative position of the two messages can thus be readily counted, and when this shows a proportion to the length involved which corresponds to clear language frequency, the two messages are probably placed in depth.

2. Action or process of identifying right-hand and middle wheels of an Enigma machine by relating distances or intervals between message settings (as found by placing in depth, e.g. pairs of messages having the first letter of that setting, as enciphered on the Grundstellung, the same and one or both of the other two letters different) to the possible intervals between the enciphered settings, noting and scoring all possible partial alphabets so obtained, eliminating contradictions, and so fixing position of turn-overs (which serve to identify the wheels).

BANBURISMUS MENU :

A menu prepared from alphabets found by the above process and used to determine the third wheel and the stecker.

BANBURY :

1. A sheet or strip of paper having vertical alphabets printed across its width at equal intervals on which a cipher message can be reproduced by punching out the consecutive letters of the text in consecutive columns, designed to facilitate the placing of messages in depth; (see Banburismus 1).

2. (of results). Produced or obtained by the use of Banburies.

BANBURY, v :

To reproduce (a cipher text) by punching on a Banbury.

BASE :

1. True code-group or other substituted group or unit before recipherment, or after true key has been stripped.

2. Values arbitrarily assigned to code-groups when the true figures are not yet determined, such that the assigned value differs from the true by an amount which is constant for each group, and therefore the differences between groups is a true difference. (Usually distinguished from sense 1 by the words arbitrary, common, or provisional).

BASIC :

(of a code-group in process of identification). Established as being a particular part of speech (e.g. noun, verb, adjective) but not more precisely determined.

BASIC BOOK :

The code-book underlying a cipher, the code-groups of which have been disguised by recipherment.

BASIC WHEEL ORDER :

(in Enigma). The wheel order prescribed in the month's keys for a particular day before the changes introduced by a Stichwort are made to it.

BEAUFORT :

Involving subtraction, not addition, in the process of enciphering or reciphering.

BEAUFORT SUBTRACTOR :

A subtractor which is applied to an encoded message by subtraction, not addition; (see the next).

BEAUFORT SYSTEM :

1. (codes). A system of reciphering code-groups with a subtractor or key in which, to produce the cipher, either (i) the code-group is subtracted from the key, or (2) the key is subtracted from the code-group; and hence, in deciphering to obtain the code-group (1) the cipher is subtracted from the key or (2) the cipher is added to the key.

2. (in the case of periodic or running key substitution on plain language by means of a Vigenere square). A system of enciphering in which either (i) the plain Language letter is found at the beginning of a line (or top of a column), the key-letter in the square, and the cipher letter at the top of the corresponding column (or end of corresponding line), or (2) the key-letter is found at the beginning of a line (or top of a column), the plain language letter in the square and the cipher letter at the top of the corresponding column (or end of corresponding line).

The processes involved in the two systems can be stated in equations as follows;

1. Reciphered Codes

(i) Reciphering
Key - Code group = Cipher

Stripping
Key - Cipher = Code group

(ii) Reciphering
Code group - key = Cipher

Stripping
Cipher + key = Code group

2. Substitution on P/L

(i) Enciphering
Key - Plain = Cipher

Deciphering
Key - Cipher = Plain

(ii) Enciphering
Plain - key = Cipher

Deciphering
Cipher + key = Plain

BEDSTEAD :

(in Tunny). That part of a Robinson which reads the tapes by photo-electric means, and combines and compares the results as required.

BEETLE :

1. The adjacent letters on a rod of an Enigma wheel, especially a clear bigram or any of its twenty-five possible encipherments when no turn-over intervenes.

2. Two occurrences of a letter on (each of) the rods of an Enigma wheel, corresponding to two circuits in the wheel which have the same interval between their right-hand terminals as between their left-hand terminals measured in the same direction.

3. Two constatations involving the passage of current through the same loop in the unmoved wheels and in the same direction; cf. Starfish.

BEGINNER :

A crib or possible crib for the beginning of an enciphered message.

BERLINISMUS :

Practice, observed in a series of Enigma messages originating from Berlin, of assigning successive outside indicators such that each letter of any one of them was two places further down the alphabet than the corresponding letter in the previous outside indicator (e.g. CRM, ETO, GVQ, etc.), thereby suggesting that they had as message settings the letters next to each (i.e. in the above example, the letters DSN, FUP, HWR, etc.); as in fact proved to be the case.

BIFID :

(of a cipher system or cipher). Characterized by a dividing of each letter of the plain text into two elements (normally the co-ordinates of that letter in a key-square of 25 letters), a systematic rearrangement of these elements, and their substitution, in pairs, by the letters of which they are the co-ordinates in the same, or another, key-square,

BIGRAM :

A pair of adjacent (or otherwise associated) letters, figures, or other units in a text whether cipher or plain; vertical bigram, a pair of letters occurring one below the other when a text is written out in equal lines.

BIGRAM COUNT :

A tabulated record of the frequency of occurrence of different bigrams in one or more texts. (Also called bigram frequency count).

BIGRAMATIC :

Involving, or made on the basis of, pairs of adjacent letters, figures, or other units.

BITE :

Continuous series of blacked-out squares on any margin of a " pattern" used in transposition.

BLIST, n :

(short for Banister list). A register of Enigma messages showing especially indicators, call signs, intercepting station serial numbers, length of message, and time of origin, designed to facilitate detection of cillies, psillies, etc., and identification of crib messages.

BLIST, v :

To record particulars of on a Blist.

BLOCK :

A section of a book of trigram discriminants assigned to a particular Enigma key for a month, or to a group of such keys for a particular day; in which latter case the block is shared by the users in a regular (and hence predictable) manner.

BLOCK-SHARERS METHOD :

A method of identifying Enigma keys from a knowledge of how a block of discriminants is shared by the various users in a group.

BLOG, n :

A dummy code-group, especially one used as "padding" at the beginning or end of a message.

BLOG, v :

To insert blogs in encoded messages.

BLOGGER :

An encoder or encipherer who habitually uses blogs.

BOG WHEEL ORDER :

A wheel order considered unlikely to be used owing to its having been used on the key concerned fairly recently.

BOIL :

Method for determining the clear text of a large number of Enigma messages which begin or end in the same way, utilizing the fact that no letter can be enciphered by itself, i.e. by noting the missing letters in each column when the beginnings or ends are written below each other.

BOMBE :

Apparatus for breaking Enigma daily keys, i.e. ascertaining wheel-order, ringstellung, and stecker, by testing a crib and its implications in all possible settings and wheel-orders.

BONK :

1. (in Enigma). To bring (a hand machine) to any desired position by depressing a key or keys the requisite number of times.

2. Bonk out , to encipher or decipher on a hand machine.

BOOK :

Short for code-book.

BOOK, v :

To record occurrences of (cipher or code-groups, either true or provisional, indicators, etc.) in a book, e.g. in the process of book-breaking.

BOOK-BREAKER :

A cryptographer who specializes in determining the plain language represented by the code-groups of messages from which the reciphering key or subtractor (true or provisional), or other form of recipherment, if any, has been removed, with a view to reconstructing the original (decode) form of the code-book employed, or enough of this to make the traffic readable.

BOOK-BREAKING :

The work of a book-breaker; reconstruction of the decode form of a code-book.

BOOK FACTOR :

(of difference book). Proportion of total material in a particular type of traffic represented by the " good groups " from which the difference book has been made.

BOOK INDICATOR :

= DISCRIMINANT .

BOOK KRAC :

(in G.A.F. codes). A solution or identification of a group, especially in a three-figure alphabetical book.

BOOLEAN ADDITION :

A system of addition for units belonging to different, but not mutually exclusive, classes, which avoids counting more than once units which belong to more than one of these classes; e.g. Boolean addition is used to sum the kicks (i.e. activated bars) of individual wheels of a Hagelin machine using overlapping clips; any bar with two clips each opposite an active peg for the position in question is thus counted only once in the total.

B0USTROPHEDON :

Taking each successive line or column in the direction opposite to that in which the previous line or column was taken.

BOX, n :

1. A Playfair square, especially one used in double Playfair systems.

2. A cage in transposition systems.

3. (in Enigma). A cipher alphabet so arranged and if necessary so divided into compartments that when one of the components is slid on one position (cyclically in each compartment) a second cipher alphabet is produced.

BOX, v :

(of Enigma indicators). To show repeats in the second three letters corresponding to repeats in the first three, thereby suggesting that the message settings are being enciphered twice on a Grundstellung.

BREAK :

1. (required codes). To ascertain or "recover" (the key or subtractor) by placing a number of messages 'in depth' and identifying, usually from differences, already known 'good groups' in all the columns.

2. To establish the plain language equivalents of the groups of (a code-book).

3. (machine ciphers). To decipher simultaneously (two or more messages known to be in depth) by finding, usually by trial and error, key-letters which make reasonable sense of both or all the messages; to read (a depth).

4. To resolve (a length of key obtained by the above means) into its basic, short-period, components by analysis; to establish thus the essential structure and method of operation of (a cipher machine).

5. To reduce (any type of cipher) to plain language; to reconstruct (any cipher system).

BREAK-IN :

The first success in beginning to read or break a cipher or code.

BREAK-SIGN :

A letter or other symbol used to separate words.

BREAKABLE :

Capable of being read or solved.

BRUTE FORCE :

Involving detailed analysis of the whole of a large volume of reciphered code traffic.

BUILD-UP :

To construct or reconstruct, especially by a gradual process.

BURY :

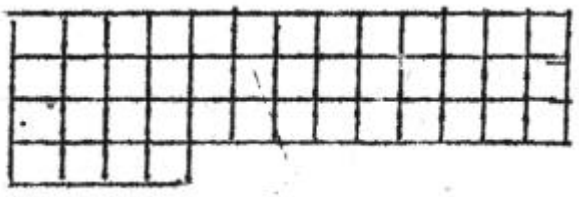
To place (call signs, addresses, signatures, etc.) in other than their natural places; to hide or conceal in the body of a message (so as to avoid giving cribs).

BUTTON-UP :

(in Enigma). To add a particular letter to each of the letters in both components of a cipher alphabet.

CAGE :

1. Rectilinear figure drawn round the text of a tranposition cipher written out on its key-length, or one of its key-lengths, on squared paper, and therefore consisting of a rectangle of small squares or, more usually, several complete and one incomplete line of small squares, e.g.



(continued)

As the shape is completely determined by the key-length and the number of letters in the message the recipient, knowing the key, can reconstruct the cage, and the cryptographer, knowing only the number of letters, can make tentative cages for different assumed key-lengths.

2. A Playfair square.

CALL SIGN :

A group usually of three or more letters and/or figures, sent either in clear or in cipher, either in the preamble or in the body of a message, and serving to identify the sender and/or the recipient; a code name.

CARRY :

1. To represent or convey.

2. (in addition, etc.: see carrying)

CARRYING :

Belonging to or obtained in conformity with the rules of normal adding and subtracting (whereby 9 + 7 = 16, 33 - 18 = 15), as opposed to normal cryptographic addition and subtracting (whereby 9 + 7 = 6, 33 - 18 = 25), which is non-carrying .

CATALOGUE :

(especially). A tabulated record of all the immediately relevant consequences or implications of each of a complete set of hypotheses in a consultable form.

CENTIBAN :

A scoring unit for probabilities equal to one-hundredth of the true scoring unit, enabling decimal fractions to be expressed more conveniently as whole numbers. The true score (i.e. the logarithm of the probability of a particular occurrence) multiplied by one hundred is the score expressed in centibans, cf. deciban .

CHAIN :

1. (in double Playfair). A series of non-reversible bigram equations such that the clear bigram of one equation is the reverse of the cipher bigram in the previous. From such a series it can be inferred that the letters forming every second bigram (either of the clear bigrams or of the cipher) occur in the same line in their respective squares, and are evenly spaced along that line.

2. (especially in Enigma). A connected series of constatations forming a menu or part of a menu; also, a set of consequences obtained from one stecker assumption.

(continued)

3. (in Met.). A series of reciphered trigrams related by having the same underlying trigram.

CHAIN, v :

1. To form or form into, chains or interlinked series.

2. (in Met.). To relate(several reciphered trigrams resulting from different enciphering tables) by the fact that the underlying trigram, though unknown, is the same in each case.

CHARACTERISTIC :

1. Any distinguishing feature.

2. (especially in Japanese codes). A relationship between the signs forming any group of a particular code, usually of the form wA + xB + yC + zD = a constant; where ABCD are the four signs of the code-group, and wxy are positive or negative integers. Such a relationship is primarily designed to check the correctness of the deciphered group, but it also makes the cryptographer's problem much easier.

CHECK-GROUP :

A figure or letter-group inserted in a cipher message at a prearranged point or at regular intervals as a check on the indicator or on the number of groups or the position of the message on the subtractor. It may, for example, give the number of groups in front of it, either in clear, in code or in cipher, or it may be an unaltered subtractor group.

CHECK-LETTER :

A single letter acting as a check; see check-group .

CHI (pron. tshi), n :

1. Transposition.

2. A transposition cipher.

CHI, v :

To transpose.

CHI (pron. ki), a :

Designation of (any of) the five regularly-moving wheels of the Tunny machine.

CHI-2 FUNCTION :

The addition (by a species of Boolean addition making two crosses add to a cross) of the pattern of the second chi wheel in the Tunny machine to the motor pattern produced by the two motor-wheels at the next (following) position; also, the addition (non-carrying) in the scale of 2 of the pattern of the second chi wheel to the fifth impulse of the preceding plain letter, followed by the addition of the reverse of this result by Boolean addition, to the pattern produced by the two motor-wheels one position later (cf. KTF), the final result being the motor at this later position.

CHIASMIC DIFFERENCES :

Two-column differences produced from two adjacent groups in any one message and any two groups in the same columns whether in one or two different messages (usually in a shallow depth), used in searching for cliches which have the same good groups opposite corresponding groups of them at different points of a depth but which, as these two groups are not in both cases (or in either case) in the same message, are not revealed by ordinary two-column differencing

For example, they would reveal the two groups cliche (denoted by CLI CHI) occurring in conjunction with two good groups (denoted GG1 and GG2) in such an arrangement as the following. (The maximum number of messages involved is six, though more would naturally be examined if available):

```
... ... GG1 ... ... ... ... ... ... ... ...
... ... ... ... ... ... ... ... CLI CHE ...
... ... ... GG2 ... ... ... ... ... ... ...
... ... ... ... ... ... ... ... GG1 ... ...
... ... CLI CHE ... ... ... ... ... ... ...
... ... ... ... ... ... ... ... ... GG2 ...
```

CILLI :

The employment or occurrence of the finishing position of one Enigma message as the setting for enciphering the message-setting of a second (i.e. as its outside-indicator), thus enabling the possible settings of the first message to be calculated for the various permissible wheel-orders and, (when this is a key-board sequence, pronounceable, or other recognisable type), the setting and probable wheel-order to be determined.

CILLI, v :

1. To use as the outside indicator of an Enigma message the letters appearing in the windows at the end of the enciphering of the previous message, thereby revealing the finished position for message and, in certain circumstances, facilitating the determination of its true setting and wheel-order.

CILLI. v. (continued)

2. (of an Enigma message). To have its true setting revealed (sc. as a keyboard, pronounceable, or the like) by back-calculation from a cilli.

CILLIER :

1. An Enigma encipherer who tends to use cillies.

2. An Enigma key on which cillies tend to occur.

CIPHER :

1. Any system whereby the individual letters, figures, punctuation marks, etc., of plain language, or the individual letters, figures or other symbols of an encoded message are rearranged among themselves (transposition) or with an admixture of other figures or letters (dummies) or replaced by different letters, figures, etc. (substitution), with a view to making the message unintelligible to anyone not in authorised possession of the knowledge or apparatus necessary to reverse the systematic process and so restore the order or letters, figures, etc. of the original plain language or encoded message.

2. A series of unintelligible letters, figures, and/or other symbols etc. produced from plain language or code by the above means; an enciphered message; a cryptogram.

3. (misused for). An encoded message.

CIPHER ALPHABET :

The letters of the alphabet and/or other symbols used, if any, arranged in the order in which they are substituted for the letters of the clear alphabet (a, b, c, etc.) for a particular key-letter, usually with the clear alphabet written alongside.

CIPHER-BOX :

A Playfair square.

CIPHER-DISC :

A ciphering device consisting of two concentric discs of unequal size (the smaller rotating on the larger) each being divided usually into 26 equal sectors in which the letters of the alphabet are inscribed. The smaller disc has the clear alphabet, usually in alphabetical order, on it, and the larger disc the cipher alphabet, usually in hatted order; but the orders may be alphabetical on both or hatted on both. Each of the 26 different relative positions of the discs gives a different cipher alphabet.

CIPHER-GROUP :

1. A letter-and/or figure-group in a cipher message.

2. (misused for code-group)

CIPHER-SLIDE :

A ciphering device consisting essentially of two rods, one sliding along the other, each bearing an equispaced alphabet, which is usually in alphabetical order on one, and hatted on the other. For convenience in use one of the alphabets is usually repeated. It is used in much the same way as the cipher-disc.

CIPHER-WHEEL :

The outer wheel of a Wheatstone or similar cipher machine containing the cipher alphabet.

CLASH, v :

1. (of wheel-orders in Enigma). To have the same wheel in the same position on two consecutive days on the same key.

2. (misused for crash).

CLASH, n :

An instance of the above (see Clash, v.), i.e. an infringement of the non-crashing rule.

CLEAR TEXT :

Plain language; usually, the text of a message before encoding or enciphering or after decoding or deciphering; a plain-language message.

CLEAR-WHEEL :

The inner wheel of a Wheatstone or similar cipher machine containing the clear alphabet.

CLICHE :

A set of two or more plain language words or code-groups that are known or expected to occur together in the same order in different cipher messages. See also split cliche.

CLICK :

A repeat or repetition of one or more cipher units usually in two or more messages, especially a repeat which, by its position in the messages or from the fact that it is one of a significant series, suggests that the messages are in depth, See also forward click, backward click, positional.

CLICK BOOK :

A catalogue giving under every constatation the constatations for the next position on the same pair of rods in each case as the constatation concerned, together with an indication of the position on the rods where the consequent constatation occurs.

CLICK MACHINE :

A machine designed to test short Enigma cribs at any desired number of positions in a message (assuming no turn-over of second wheel within the length of the crib), and distinguishing possible positions from positions which involve contradictions.

CLONK, v :

1. To turn over by hand the wheels of two Enigma machines simultaneously (the machines being coupled to the same lamp board and set at the requisite interval) in the process of testing for ringstellung on a limited range on two constatations; also, to turn over the wheels of a single machine in searching for the position that gives a particular constatation in a similar investigation of ringstellung or message-setting, esp. in the case of duds.

2. To test for or solve ringstellung by the above method.

CLONK :

A search for ringstellung by the method of clonking.

CLOSE SPELL :

A code-group marking the end of spelling.

CLOSURE :

(in Enigma). A constatation linking together directly two letters otherwise connected by (a part of) a chain, esp. in a menu.

COASTAL CODE :

A code used mainly by harbour defence vessels and Naval coastal-batteries.

CODE :

1. A substitution system having groups (usually of a fixed number, e.g. 3, 4 or 5, of letters, figures, or letters and figures) as the equivalents of words, syllables, letters, numbers, punctuation marks, etc., common phrases and even whole sentences of plain language. These words, syllables, letters, phrases, etc. are arranged in a consultable (i.e. alphabetic or other logical) order in a code-book with the equivalent code-group or groups

opposite each. If the code-groups are so assigned that when the plain language elements are in the above order they too are in alphabetical or numerical order (or nearly so), the same book can be used both for encoding and for decoding messages, and it is known as an alphabetic or one-part code; if these conditions are not present a second version of the code having the code-groups in alphabetic or numerical order and their plain language equivalents opposite them is required for decoding, and this is known as a "hatted" or two-part code.

2. A series of groups of the above character, esp. an encoded message.

3. A code-book.

CODE, v :

1. To substitute the equivalent code-groups in a code for corresponding units of plain language; to convert into code; to encode.

2. (misused for to cipher).

CODE-BOOK :

A book containing in a consultable order the words, phrases, sentences, endings, punctuation marks, letters, numbers, etc. used in a particular code with the equivalent code-group opposite each, and if necessary the code-groups also in a consultable form with their plain language equivalent opposite each, used for encoding and decoding messages; (see also code).

CODE-NAME :

A word or letter-group of pronounceable form, indicating a unit, station, department or the like.

CODEWORD :

A word which, when sent as a message, serves to convey a previously arranged meaning, e.g. that an expected situation has arisen or that a particular procedure is to be put into operation.

CODE-TABLE :

A short code in tabular form devised for a special limited purpose.

CODED :

1. Having plain language units replaced by code-groups; encoded.

2. (misused for ciphered).

COLLECTIVE :

A general broadcast to all meteorological centres in a large area, (e.g. Europe) of all the synoptic weather observations made in that area at a particular (synoptic) hour.

COLOSSUS :

(in Tunny). One of the high-speed machines designed to set known chi wheels but also utilized for the determination of unknown chi-wheel patterns by Tutte's method , incorporating the five chi-wheel periods in the form of double rings of thyratrons controlled by the sprocket-holes in the teleprinter tape, reading tapes of cipher messages by photo-electric means, combining and differencing as required, counting by valve-counters, and finally delivering the results in typed form.

COLOUR :

(in Enigma). A key (keys having originally been given the names of colours).

COLUMN :

1. (in transposition ciphers). Any one of the "vertical" series of letters (under a number of the key) according to which the text is "taken out" of the cage in the process of enciphering or "written in" in the process of deciphering.

2. (in a Vigenere or similar table). Any one of the "vertical" series of letters or other symbols representing the sums, or differences, of the clear letters in the margin and the key-letter at the top, or indicating how the clear letters in the margin are substituted for a particular key-letter.

3. (in reciphered codes). A series of cipher-groups, usually one from each of a number of messages, which have been reciphered with the same subtractor group and so form a vertical series when the messages are written out in depth; also, a vertical series of groups on a subtractor sheet, etc.

4. (in machine and other substitution ciphers). A series of cipher letters or other symbols from the same or different messages which have been enciphered with the same key-letter or the same cipher alphabet and so from a "vertical" series when the messages are written out in depth or (in the case of periodic substitution) when the message or messages are written out on the width corresponding to the period.

COLUMN HEAD :

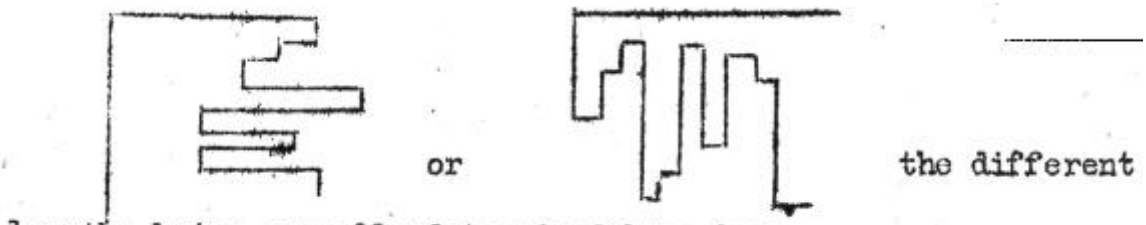
(in transposition ciphers). The letter or other symbol forming the top or head of a "column".

COLUMNAR :

(of transposition systems). Using "columns" as the basis of rearrangement.

COMB :

Irregular "toothed" pattern used as cage in transposition systems consisting of a series of lines or columns (of small squares) of unequal length, e.g.



or the different lengths being normally determined by a key.

COMB TRANSPOSITION :

Transposition using a "comb" in place of the normal cage.

COMPLEX :

(in W/T). General term for a group of stations working together.

COMPONENT :

Any one of the distinct or separable parts which together make up a whole, esp. either of the two series of letters and/or other symbols constituting a cipher alphabet and termed respectively the clear component and the cipher component.

COMPROMISE :

To diminish or impair the security of (a code or cipher system or any part thereof).

CONCEAL :

= bury.

CONDENSER :

A code or substitution system which has the effect of shortening a code or cipher message, e.g. by substituting letter-groups for longer figure-groups.

CONSTATATION :

(in Enigma). The association of a cipher letter and its assumed plain equivalent for a particular position.

CONTROL :

1. The central station with which a group of out-stations is associated. See star.

2. (esp. in Japanese ciphers). The group or groups which indicate with what key-group the indicator has been enciphered.

CO-ORDINATE :

The distance of anything from one of two or more lines of reference; esp. the figure, letter, number, or group of letters, either in the left-hand margin or at the top, e.g. of a square table, which together with the corresponding figure, letter, number or group of letters either at the top or in the left-hand margin, serves to denote the position of a particular unit or group in the table; the number (or letter) of the line or column in which a term occurs. When two co-ordinates are given, as is usual, the one in the left-hand margin, indicating the line, is normally given first.

CORRECTION :

The figures, letters, or other symbols which require to be added to or subtracted from a group or column to produce true figures, letters, etc.; the difference between corresponding groups of the true and provisional subtractor.

COUNT :

(short for frequency count). A record of the number of times the various letters, figures, and/or other symbols used in a particular cipher occur either singly, in pairs (bigram), threes (trigram), or larger groups in the whole, or any special part, of the messages concerned; the distribution thus ascertained sheds light on the nature of the cipher by departures or otherwise from normal or random, and counts of larger groups may reveal periodicities or the existence of depth. Also, a similar record of plain language, esp. for comparison with the above.

COUNTING-SHEET :

A sheet designed for recording occurrences of letters, figures, etc., but more usually bigrams, trigrams, etc. of these in cipher or code texts.

COVER, n :

Provision (sc. of sets and operators) for intercepting wireless signals, esp. signals of a particular traffic, link, or key.

COVER, v :

To make adequate provision for intercepting (a particular type of) wireless signals.

COVER NAME :

A code name.

COVER OFF :

To be in depth.

COVERAGE :

Adequacy of provision for intercepting wireless signals (of a particular type or link of traffic).

CRACK :

To make a beginning in the process of reading or solving a cipher or code.

CRASH :

(in any reciprocal substitution system, and esp. in Enigma). The occurrence of a plain letter opposite the same letter in the cipher text in one of the positions or versions in which a crib is tried, normally involving rejection of that position or version.

CRASH , v :

1. (of a crib or version of a crib). To involve the enciphering of a letter by itself at a particular position (which is impossible from the structure of the Enigma machine or in any substitution system having a reciprocal character).

2. Misused for clash.

CREAM-RUN :

A series of three or more positional repeats (of groups of reciphered code), suggesting a high probability of depth.

CREEPING SUBTRACTOR :

A subtractor having a fixed starting-point, e.g. for each day or other suitable period, the starting-point for each successive day or period being advanced a prescribed (and usually regular) number of units.

CRIB :

A plain language (or code) passage of any length, usually obtained by solving one or more cipher or code messages, and occurring or believed likely to occur in a different cipher or code message, which it may provide a means of solving.

CRIB, v :

1. To solve or read by means of a crib.

2. (of a message). To contain or provide a crib into another message.

CRIBBABLE :

Capable of being solved by means of a crib.

CROSS-CRIBBING :

1. (especially in Met.) Utilization for breaking purposes of two versions of the same message, either reciphered with the same tables but differently thrippled, or reciphered with different tables, whether differently thrippled or not.

2. The use of cribs, re-encodements, or re-encipherments in general.

CRUM'S SQUARE :

Square alphabetic table devised by Mr. Crum for obtaining Sturgeon keys (i.e. the teleprinter letters representing the subtractor and the permutation applied by the machine) directly from the ten wheel-patterns for any desired position of the starting-points on the wheels and the order in which the ten wheel-patterns entered the Pentagon, were known; used for the further decipherement by hand of set messages, and, in a simplified form, for the setting of further messages using the same starting-points, sc. by obtaining wheel-patterns from possible keys.

CRYPTOGRAM :

An encoded or enciphered or encoded and reciphered text.

CRYPTOGRAPHER :

A person engaged in investigating often irregularly-procured copies of cipher and code-messages passing esp. between officials and agents of other countries or the like, with a view to reconstructing the methods of encipherment and the codes used, and so making the contents of these messages available to his employers; whom to prevent reading such messages the codes and ciphers were originally designed.

CRYPTOGRAPHIC :

1. Of, belonging to, or employed in cryptography.

2. (spec. of addition, subtraction, and multiplication). Non-carrying.

3. Encoded, enciphered, or encoded and reciphered.

CRYPTOGRAPHICALLY :

In a manner characteristic of or peculiar to cryptography; without carrying.

CRYPTOGRAPHY :

The art or science of ascertaining, usually by a gradual process employing both analytical methods and imagination controlled by sagacity and/or experience, the essential natures of codes and ciphers and reconstructing the systems and operations used by the encoders and encipherers, or enough of these to enable the messages to be read. See research.

C/S. C.S. :

Abbreviation of call-sign.

CSKO :

(pron. "sisko"). (in Enigma short for "Consecutive stecker knock-Out"). A method of running a bombe so as to eliminate stops which involve consecutive stecker (sc. the steckering of a letter to the letter next to it), used in breaking certain G.A.F. keys which avoid consecutive stecker.

CUT :

Position of points of division when, e.g. a subtractor or a cipher or code message is divided into equal groups. On the cut: (of a reciphered message) using the same subtractor as one or more other messages and having the group-divisions falling at the same points. Off the cut: using the same subtractor but having the group-divisions falling at different points.

CUT-OUT :

See Ringstellung Cut-out.

CUT-UP :

A re-arrangement of the entries on a blist under frequencies or associated frequencies and in German-time-of-origin order, effected by cutting the original blist into strips and sorting these in the above manner.

CYCLE :

1. The number (in practice, a number between 1 and 150) indicating the line of the key-table used by a particular station for determining the page of the Bird Book on which its call-sign is to be found on each of the days of a particular month (the particular call-sign on that page being determined by the Row allotted to the station).

2. Any series which recurs or is expected to recur in the same order, either immediately after it ends or at some later time.

CYCLIC :

That behaves as if it formed a circle or circular series; continuing or repeating so that the first term of a series follows the last; characterised by regular repetition of a particular pattern; periodic.

CYCLICALLY :

In a cyclic or periodic manner.

CYCLOMETRIC :

(of the turn-over mechanism in Enigma). So assigned that no wheel can turn over except when all the wheels to the right of it turn over too; (of turn-overs) produced by a turn-over of the next wheel on the right.

CYPHER :

see cipher.

CYRIL, CYRILLIC :

Applied to the alphabet, variety of morse code, etc., used by Russians.

D/C :

Short for daily-changing.

DECADE :

A group or unit of ten figures or letters as forming part of a subtractor.

DE-CHI, v :

To remove from (a Tunny cipher message) that component of the key which is contributed by the chi wheels.

DE-CHI, n :

A Tunny cipher message from which the component of the key contributed by the chi wheels has been removed; (see Tutte's method)

DECIBAN, n :

A scoring unit for probability factors equal to one-tenth of the true scoring unit, enabling decimal fractions to be expressed (approximately and) more conveniently as whole numbers. The true score (i.e. the logarithms of the probability factor of a particular occurrence) multiplied by ten is the score expressed in decibans. cf. centiban.

DECIBAN, v :

To score in decibans.

DECIMATION :

The process of forming a new sequence of symbols (e.g. an alphabet) from an existing one by selecting symbols at a fixed interval, the original sequence being treated as cyclic.

DECIPHER, v :

1. To convert a cipher text into the original plain language by reversing the operations of enciphering.

2. To remove the key or subtractor from a reciphered code and thus obtain the code-groups; to strip.

3. (Misused for decode.

DECIPHER, n :

Plain language or a plain language message obtained by deciphering a cipher message.

DECIPHERABLE :

That can be deciphered.

DECIPHER-BOARD :

A board usually containing a series of alphabets and furnished with appliances to aid in the deciphering of any particular (especially a poly-alphabetic substitution) cipher.

DECIPHERER :

A person who deciphers cipher messages.

DECIPHERMENT :

1. The action or process of deciphering.

2. Plain language obtained by the above process.

DECODE, n :

1. Plain language or a plain language message obtained by decoding a code message.
2. (misused for). A plain language text obtained by deciphering a cipher message; a decipherment.

3. That section of a hatted code-book in which the groups are arranged in numerical order with the plain language equivalent opposite each; the second part of a two-part code.

DECODE, v :

1. To substitute their plain language equivalents for the code-groups of a coded message; to reduce to plain language thus.

2. (Misused for decipher). To convert a cipher text into plain language.

3. (Misused for decipher). To admit of deciphering; be deciphered.

DECRYPT :

To decode or decipher (a code or cipher message) cryptographically.

DECRYPTION :

The action or process of decoding or deciphering.

DEDUPE :

To remove (normally the less reliable or less complete) duplicate copies of cipher texts from (a quantity of traffic), esp. before Freeborning.

DELIVERY GROUPS :

Code groups for route instructions and addresses of code and cipher messages.

DE-PSI, v :

(used for). To set the psi-wheels in a Tunny message with the help of machines after it has been de-chied.

DEPTH :

1. A series of code messages reciphered with the same, or the same part of a, reciphering key especially when written under one another so that all the groups (usually one in each message) that are reciphered with the same group of the subtractor lie under each other and form a 'column'.

   (b) two or more messages in a transposition cipher that are of the same length and have been enciphered on the same key;

   (c) two or more messages in a machine or similar cipher that have been enciphered on the same machine-setting or on the same key.

2. be in depth : (of messages). Stand to each other in any of the relationships described above.

DEPTH CHART :

A diagram showing the position of (reciphered code) messages on the key, and thus indicating the depth at any given point.

DEPTH-CRIBBING :

(in Enigma) = Fun and Games .

DERECIPHER :

To strip off the subtractor or other form of recipherment from a re-ciphered message.

DESTECKER, v :

(in Enigma). To replace (the letters of a text or of a crib, or of the constatations obtained from a text and its crib) with the letters to which they are steckered or assumed to be steckered.

DESTECKERED :

(of letters in Enigma). Replaced by the letters to which they are steckered or assumed to be steckered.

DETYPEX :

To restore typexed matter to its original form by deciphering on a Typex machine.

DEVELOPMENT :

1. The utilization of the results of Research (when successful) and the application of the methods it has evolved, to break further, especially current, keys and settings; or (in the case of reciphered codes) to find further strippable depths, recover the reciphering key and break or reconstruct the underlying code-book; (cf. exploitation).

2. The complete list of different cipher alphabets produced by a cipher machine.

DF:

Direction-finding; a bearing or location obtained by this means.

DIAGONAL :

(in Enigma). The order in which the letters of the alphabet appear on the diagonal of the rod-square, determined by the order in which the letters (i.e. the keys) of the key-board are wired to the consecutive entry-points on the right side of the machine.

DIE :

(of a code or cipher system or any part thereof). To cease to be used; to become obsolete.

DIFFERENCE, n :

1. The results obtained when two groups (usually of code, or reciphered code that are in depth) are subtracted, usually non-carrying, the one from the other; a minor difference is one which is numerically less than a group of 5's; a major difference one which is greater.

2. The result obtained when two lengths of letter-subtractor cipher that are in depth with each other are subtracted; as such subtraction eliminates the key, this result is the difference between the two plain-language texts.

DIFFERENCE, v :

1. To obtain the differences, usually only the minor differences, of every possible pair in a number of (good) code-groups or in a column of cipher-groups in a depth of reciphered code.

2. To subtract a length of subtractor key, esp. of letter-subtractor machine key, from itself at the interval of one of the basic components (or wheels) in order to eliminate the component whose period is that interval, as a step in key-analysis or key-breaking.

3. To subtract two cipher texts (produced by a letter-subtractor machine) which are in depth with each other, the one from the other, thereby eliminating the key and obtaining the difference of the two clear texts, as a step in reading a depth of two messages, by the stencil-search method.

4. To subtract a cipher text from itself, usually at an interval of one, as e.g. in Tutte's method .

DIFFERENCE BOOK :

A book containing in numerical (or alphabetical) order usually the minor (but sometimes the major or also the major) differences between every pair of a convenient number of 'good groups' in a code-book, together with the two good groups from which each such difference arises.

DIFFERENCE PAPER :

Paper ruled in columns of suitable width to contain a group of cipher, and in sets of three lines, so that the cipher groups, code-groups, and plain-language equivalents of messages can be written below each other.

DIGRAPHIC :

Consisting of, or having as unit, two figures (or letters).

DILLYISMUS :

(in Enigma). A method of determining stecker when wheel-order, ring-stellung, and message-setting have been found or probably inferred, consisting in deciphering the message on an unsteckered machine, assuming each letter self-steckered in turn, and making twenty-six counts or dotteries on the same counting sheet, one for each assumption. Self-steckered letters are usually discernible from the fact that they yield similar counts and the stecker of the commonest letter will normally be shown by the best group in these. cf. Dottery .

DINGY, a :

(of a crib). That has repeatedly proved, and is consequently considered likely to prove, unsuccessful.

DINGY n :

DIRECT :

(of a cipher alphabet). Having both plain and cipher components running in the same direction; (opp. to reversed).

DIRECTED :

(of investigations, analyses, etc.). Applied or operating within certain prescribed limits, or based upon definite assumptions.

DIRECTED BOIL :

(in Enigma). A boil made to determine the relative likelihood of particular cribs.

DIRECT ROD :

A rod showing the letters on the right side of a wheel of an Enigma machine that are consecutively connected to a fixed point in space at the left side, for the twenty-six different positions of that wheel which occur in one revolution. Twenty-six such rods can be constructed for each wheel, one for each of twenty-six fixed points on its left side (corresponding to the contacts on a non-turning second wheel), and when these are placed in a square in order the diagonals from bottom left to top right all have the same alphabetic or other (e.g. QWERTZU) sequence.

DISC :

Short for Discriminant .

DISC CIPHER :

A cipher employing a cipher disc.

DISCRIMINANT :

A group (or, rarely, two groups), placed normally in front of the text of a cipher message, indicating - in the case of reciphered codes - the particular code-book and reciphering key, and/or the cipher procedure, used, or - in the case of machine ciphers - the particular set-up used, and so serving to indicate the degree of secrecy of the message or to distinguish one type or section of traffic from another.

DISCRIMINATE :

To use a discriminant group (or groups).

D.I.W. :

Short for Double-input Warspite .