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.

BOUSTROPHEDON :

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 :

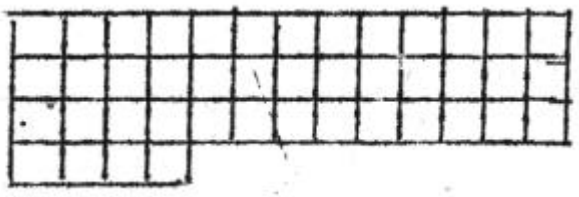
To place (call signs, addresses, signatures, etc.) in other than their natural places; to hide or conceal in the body of a message (so as to avoid giving cribs).

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 :

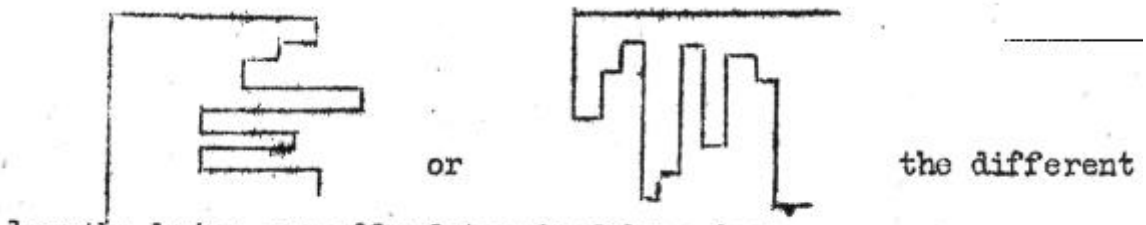
(in transposition ciphers). The letter or other symbol forming the top or head of a "column".

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 .

DOG CODE :

A code in which code-names or other letter-groups are substituted for units of the vocabulary before encodement; a code within a code.

DOMINANT :

Applied to a letter in a code or cipher group which receives special treatment or has a special function in the reciphering.

DORMANT :

(of a code or cipher system or any part thereof). Temporarily out of use; suspended.

DOTTERY, DOTTING :

Hand method of determining stecker of Enigma key when Wheel-order, Ring-stellung and message setting have been probably inferred. One stecker-pairing is assumed and the letters involved are deciphered throughout the message, producing (if the assumption is correct) a series of deciphered letters which are the steckers of the clear-text letters in these positions. A frequency count of these letters is made (by putting a dot for each occurrence opposite the letter on counting sheet). From this further steckers are inferred, and the process is continued.

DOUBLE CHI :

Double transposition.

DOUBLE-INPUT WARSPITE :

Type of Bombe in which current is put in at two points, designed to deal with a menu which consists of two dis-connected chains and to stop only when current gets round both simultaneously.

DOUBLE-LINER :

(in double Playfair with two squares). An encipherment of a bigram involving only one line in each of the two operations.

DOUBLE PLAYFAIR :

1. Playfair in which two distinct operations are involved in each bigram substitution.

2. Playfair using two letter-squares and two distinct operations in enciphering each bigram;

2. Playfair using two letter-squares and two distinct operations in enciphering each bigram;

	clear		intermediate		cipher
e.g.	AM	=	SW		
			SW	=	MG

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

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

DOUBLET :

A bigram, especially in Playfair, consisting of a repeated letter.

DOUBLE TRANSPOSITION :

A cipher system in which the letters of the plain language are successively transposed twice either on the same or on different keys. (see transposition).

D.R. :

Short for Decoding Room.

DRAG :

1. To try (a likely clear word or crib) in successive positions in a message in order to find: (a) in a polyalphabetic cipher a position that gives a likely key-sequence, and so reading the message; (b) in a machine cipher depth a position that yields good sense in the other message or messages, and so finding the key and setting the messages. See stencil-search table . (c) in Enigma, to stagger (a crib); see Stagger, v.2 .

2. To try (a good group) in successive positions in a reciphered code message with a view to finding a previously ascertained subtractor group which may enable the message to be set in depth with others; also to seek (a synthetic group) in successive positions.

DRAW INTO :

To include (dummies) in the columns of text taken out of a transposition cage.

DRUM :

(in Hagelin). That cylindrical part of the machine which carries, and is in part constituted by, the clip-bearing bars, and which is made to revolve once for the encipherment or decipherment of each letter, then imparting a varying kick to the printing wheel. (see Hagelin).

DUD :

(esp.). An Enigma message, on an already solved key, which fails to decipher (Usually owing to faulty indicators).

DUDDERY :

(in Enigma). The room to which duds are sent for further investigation.

DUENNA :

A machine specially designed for breaking Enigma keys on a crib when the wiring of the Umkehrwalze is unknown.

DUMMY :

1. A letter, figure, or other symbol, or group of such, included in a cipher or code message, usually for no other or no other known purpose than to perplex the cryptographer.

2. A cipher or code message sent merely as practice, or to produce an impression of activity where real traffic is rare or non-existent, or to complicate the work of the cryptographer.

3. A letter, figure, or other symbol used e.g. to fill blanks in a stencil cipher or transposition cage or to complete the final group, e.g. in four-figure or four-letter traffic transmitted in groups of five; a filler .

DUMMY GROUP :

A group of dummies (see dummy 1).

E BAR :

1. n. A barred E (Ebar), sent in Morse as ..-..

2. a. Characterised by having Ebar in the preamble.

E BAR v :

(in Enigma). To determine the stecker after wheel-order, ringstellung and message-setting have been found, by testing stecker assumptions on a cribbed message.

ECLECTIC :

(of a code-book) Using only a selection of the available numbers, especially for its pages; gapped.

EGGS :

(in Enigma) A catalogue giving the rod-pairings for every position of an Umkehrwalze and two wheels, used when nothing at all is known about the turn-overs.

EINS : v

1. To drag the word "eins" through a German cipher message or depth: also, to seek the word "eins" in a German cipher message or in any number of messages by any feasible method (cf. eins catalogue)

2. To drag any probable crib, 'good group', or synthetic, through a cipher or reciphered code message in any language.

EINS CATALOGUE :

(especially in Enigma) Alphabetic list of all the (17576) ways in which 'eins' can be enciphered with known wheel-order ringstellung and stecker, used to set further messages on the same day, especially when new sets of bigram substitution tables for indicators require to be solved.

EMENDER :

A person engaged in emending decoded or deciphered messages.

ENCIPHER, v :

1. To substitute cipher for (plain language), either by a hand or a machine process.

2. (misused for encode)

ENCIPHER, n :

1. An enciphered message.

2. (Misused for encode i.e. the first part of a two-part code).

3. (Used for recipher).

ENCIPHER(ING) TABLE :

Any kind of figure or letter-table used in enciphering (or deciphering) e.g. a short subtractor printed on one sheet of paper, a series of groups used for enciphering indicators, a set of Playfair keys, etc.

ENCIPHER KEY :

The natural numbers (i.e. from 1 upwards) of the letters forming the plain language of a message in transposition either arranged in the order in which these letters appear in the cipher version, thus showing by what rearrangement the encipherment is effected.

ENCIPHERMENT :

1. The process of enciphering or converting plain language, indicators, etc. into cipher.

2. The result of enciphering; the cipher version of a message, etc.

EN CLAIR :

1. In clear or plain language; not encoded or enciphered; (used especially of messages or parts of message, parts of preamble, indicator, date and time groups, etc., which are often or normally encoded or enciphered; also of single letters or groups which particular cipher systems leave unaltered).

2. (Misused for unreciphered).

ENCODE : v :

1. To substitute code-groups for the plain language units of (a text) according to a system embodied in a code-book.

2. (Misused for encipher).

ENCODE, n :

A code-book designed for encoding, i.e. substituting groups of figures or letters (usually of a fixed length) for any suitable units of plain language; the first part of a two-part code.

ENCODED :

Having plain language units represented by code-groups; converted into code.

END-ON :

Forming terminations; final.

ENIGMA :

1. A cipher machine using normally three of several twenty-six-circuit, stecker-wired, drums or wheels in any prescribed order-- each wheel having an alphabet-bearing tyre which is capable of being set (according to the ringstellung) in any of twenty-six positions in relation to the wiring --, an umkehrwalze or reflector wheel connecting the twenty-six circuits in fixed or variable pairs, and, in some models, an initial set (normally) of ten stecker-pairings. The right-hand wheel moves forward one position for each letter enciphered and each of the other wheels (except in some models the Umkehrwalze) moves forward one position for each complete revolution or in some models more than one position, according to the number and arrangement of the actuating teeth) of the wheel next to it on the right. See also Zusatzwalze .

2. A cipher system using the above machine, or any traffic enciphered by this.

E.P. v :

(short for en passant). To note possible cribs in Enigma messages as soon as they are deciphered and are, so it were on their way to Intelligence.

EQUATE :

1. (especially). To adjust the columns of a depth of reciphered code (e.g. by adding the same group to each group in a particular column) so that the same code group is represented by the same cipher group in whatever column it occurs.

2. To adjust similarly the columns of a periodic substitution cipher using various slides on one particular cipher alphabet or the like, written on the width corresponding to the period, so that the same clear letter, or other unit, is represented by the some cipher letter, or other unit, in all the columns.

EQUIDISTANCE :

(in Enigma). Recurrence of a pair of constatations which are less than twenty-six letters apart at the same interval at a distance which is a multiple of twenty-six, suggesting (if there is no turnover between the pair) that the same pair of rods is probably involved.

EQUIVALENT SEQUENCE :

An alphabetic sequence in which the interval between any two letters bears a constant relationship to the interval between the same two letters in another sequence.

ERSATZ :

(of cipher keys). Reserve; (usually forming the reserve key for one month and, if not required as such, the key for the next month).

EXPLOITATION :

The utilization of the results of development, including the deciphering of messages on ascertained keys known machine set-ups and solved indicators,
the stripping of reciphered-code messages on stretches of recovered key, their decoding by means of the reconstructed code-book, and (especially) the production of information from deciphered or decoded messages.

EXTERNAL :

Involving or occurring in a different text or message from the one under consideration.

EXTERNALS :

Those characteristics of a particular type of cipher traffic which can be discerned without breaking the cipher; e.g. characters used, whether letters or figures or both, size of telegraphic groups (if any), content of clear preamble (if any), presence and nature of indicators, etc.

FADING :

Temporary reduction in the strength of wireless signals.

F.A.G. :

Short for frequency allocation group.

FALSE :

1. Obtained by non-carrying addition or subtraction.

2. Provisional.

FALSELY :

Without carrying, i.e. in the normal cryptographic manner.

FAST WHEEL :

That wheel of a cipher machine which has the most movement, usually the wheel which moves forward for each letter that is enciphered; (in Enigma this is the right-hand wheel).

FEMALE :

The same constatation occurring at two different positions.

FID :

A line of subtractor key from a previous set of subtractor tables or the like used unchanged in a subsequent set, esp. when the latter are formed from the former merely by a typographical rearrangement of lines.

FILLER :

Any of one or more arbitrary letters, figures, or other symbols added or inserted to complete, e.g. a five-figure group, usually at the end of a cipher message when transmission is by five-figure groups.

FILL-UP :

A filler.

FILTER :

To reduce or narrow down (reports of aircraft) to definite information about hostile aircraft in the filter-room.

FILTER-ROOM :

A room in which reports of aircraft from a variety of sources are correlated, the tracks worked out, tracks of (known) friendly aircraft weeded out, and details of the remaining tracks (which are presumably of hostile aircraft) sent on to those who deal with such.

FINNERY :

Practice, first observed in Finnish Hagelin, of moving certain of the wheels forward one or more positions by hand at points (denoted e.g. by a letter of the indicator) in the encipherment of a message, designed to prevent or impede breaking.

FISH MACHINE :

esp. The Tunny machine

FIT :

(in Enigma).

1. A repeat or click involving two messages.

2. Two messages. set in depth on the evidence of the above.

FIVE CUPBOARDS :

A system of simple reciprocal substitution for which the key phrase is "five cupboards", used especially for sending intercepts or other 'raw material' over all British cable routes for security reasons.

FLAG. n :

Conventional triangular arrangement of all (minor) differences derivable from a series of code-groups, the groups concerned being written along the top and down the left hand side and each difference in the same column as one of the groups from which it is derived, and in the same line as the other.

FLAG v :

To write out all the minor differences arising from a series of code-groups or (more usually) the cipher groups forming a column in a depth of reciphered code, in the manner described above, esp. in a search for good or repeated differences in the process of key-breaking.

FORM :

(in Transposition). Apparently used for cage.

FORWARD CLICK

(in Enigma).The occurrence of the same letter at the same position in two messages in depth with each other, associated with the repetition of a different letter in two cribs.

FOSS SHEET :

A sheet of squared paper (having 26 small squares along each side distinguished by the letters of the alphabet in their natural order) designed for recording occurrences of bigrams or larger groups, or letters, bigrams, etc. associated with other bigrams.

FOSS SHEET v :

To enter or record on a Foss sheet.

FRACTIONATING :

(especially). Bifid or trifid.

FREEBORN, a :

Performed, produced, or obtained by means of the (hollerith) electrical calculating, sorting, collating, reproducing, and tabulating machines in Mr. Freeborn's department.

FREEBORN, v :

To list, arrange, analyse, or otherwise deal with cipher material by means of (Hollerith) electrical machines to aid cryptographic investigation.

FREEBORNERY :

1. Mr. Freeborn's department; Block C.

2. Any form of register, difference-book, stencil-search table, or other aid to cryptographic investigation produced in Mr. Freeborn's department.

3. The processes or operations involved in producing the above.

FREQUENCY COUNT :

1. A record of the frequency of occurrence of single letters (or figures), bigrams, or other groups, especially code-groups, in a given quantity of material.

2. A similar record of the frequency of occurrence of single letters, bigrams, trigrams, etc. in suitable plain texts (e.g. those provided by deciphers) of a particular language, usually arranged both alphabetically and according to the frequency, as an aid to cryptographic research.

FREQUENCY DISTRIBUTION :

Diagram or record showing relative frequencies, especially of individual letters of the alphabet in a representative text of a particular language, or of the individual letters or other symbols of a particular cipher.

FUER :

Used in front of a call-sign in the preamble of a German message to request retransmission by the receiving station to the authority indicated by the call-sign.

FUN and GAMES :

(in Enigma). The interacting process of simultaneously fitting two cribs (especially for the beginnings) to two messages on the same setting, often two messages having same text but different addresses, utilizing forward and backward clicks, avoiding stecker-contradictions, etc.

G.A.F. :

Abbreviation of German Air Force.

GAPPED :

(of an alphabetic or numerical series) Having gaps, not complete, selective.

GARBLE, v :

To arrange in hatted order.

GARBLE TABLE :

Table designed to facilitate the construction or checking of kana or other groups which have a characteristic sum.

GARBO :

An electrical tape-reading, tape-punching, and typing machine,designed to produce either a punched-tape or typed record of the result of any of a great variety of operations (e.g. differencing, substitution) which it is set to perform on one or more existing teleprinter tapes.

GENERAL :

(of Enigma keys.) Designed to be used for enciphering and deciphering by ratings or other ranks; (opposed to Offizier and Stab).

GENERALISED STECKER :

A system of stecker assumed, e.g. for purposes of stecker-knockout in which the assumed steckering of(say) A to B does not involve also assuming that B is steckered to A; i.e.assumed non-reciprocal stecker. Consequences derived from such an assumption can be readily tested by applying different slides to the second letters the correct slide being the one which produces self steckers and reciprocal steckers.

GO DOWN :

(of a menu or series of menus). To fail, esp. when run on the Bombe.

GOOD :

1. (of code-groups). Occurring or likely to occur a sufficient number of times to be of assistance to the cryptographer.

2. (of difference). Arising from good code-groups.

GOOD DIFFERENCE :

A difference which is equal to, and may be, the difference between two good groups.

GOOD GROUP :

1. A code-group of which the total occurrences amount to more than a given proportion of the material under consideration; a common group.

2. (in a code of which the groups have known limitations). A code group which has the proper limitation and is so known to be not corrupt.

GRAMMATICAL GROUP :

A code group indicating which of the alternative meanings or endings assigned to a particular code group is to be taken.

GREEN :

(of trigrams). Taken from the Heeressignaltafel.

GRID :

(in transposition). Used for cage.

GRILLE

(in Transposition).

1. A cage in which certain squares are blacked-out or otherwise marked as not to be used.
2. A perforated card or disc for determining which squares of a cage are to be used or have been used.

GRONSFELD CIPHER :

A letter-substitution cipher system using a numerical key, and therefore characterized by a limitation on the number of ways in which a particular letter can be enciphered, sc. a letter is enciphered either by itself or one of nine other letters.

GROUP :

1. Two or more letters, figures, or other symbols forming a unit in any code or cipher.

2. (especially). A series (usually 3, 4 or 5) of letters or figures or letters and figures used for a unit of plain language in a particular code; a code-group.

5. One of the series of letters, or figures, or letters and figures (usually 5 in number) separated by pauses in which a code or cipher message is normally transmitted or set out.

A number of wireless stations associated or working together.

GRUNDSTELLUNG :

(especially). The basic setting, changing daily, employed by all users of a particular Enigma key for enciphering (or rather, enciphering twice) their message settings.

G.T.O. :

Short for German time of origin.

HAGELIN :

1. A machine cipher in which the plain language is subtracted (by letter subtraction) from a key of great length produced from (five or) six short-period components embodied in the wheel-patterns and the arrangement of clips on the bars of a revolving drum. Each wheel has a number of pegs round its circumference corresponding to its period (the periods of all the wheels being prime to each other); and the same number of letters in alphabetical order round its outer edge for setting the wheels in any indicated, position. Each peg is set in the active or inactive position, according to the set-up in use at the time, the sequence of active and inactive positions constituting the pattern of the wheel. At a fixed point behind each wheel each active peg moves a lever which, in turn, activates as many (usually) of 27 bars on a revolving drum as have their clips set opposite it. The number of bars so activated constitutes the kick of the wheel.

   Some models have one clip, some two, on each bar, capable of being set opposite any of the wheels or in a neutral (non-operative) position. When the two clips on any one bar are both placed opposite wheels they are said to overlap and the total number of activated bars (when both such wheels have active pegs in contact with their respective levers) is one less than the total kicks of the wheels concerned for each such overlap. The wheel at the left side of the machine, by which the letter to be enciphered (or deciphered) is set, is normally lettered in the opposite direction to the printing-wheel alongside it, and capable of being set in any of 26 different positions relative to the latter, giving 26 different slides and 26 corresponding, self-reciprocal, substitutions.

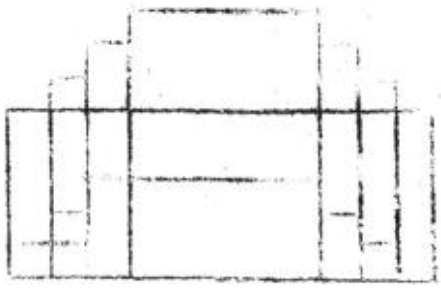
(continued)

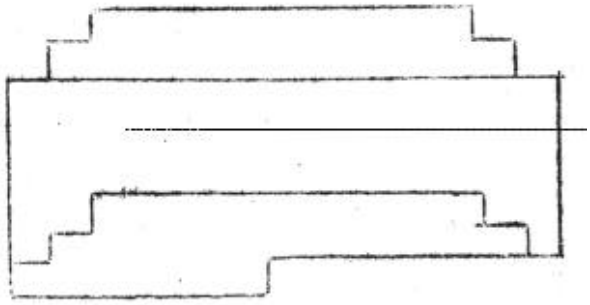
In operating the machine the requisite patterns are set on the wheels, the appropriate disposition of clips is made on the bars, the wheels are set at the positions corresponding to the indicator, the slide to be used is set between the outer left-hand wheel and the printing-wheel; the first letter to be enciphered (or deciphered) is set on the outer wheel (thereby subtracting it from the slide) and the drum is rotated e.g. by a handle on the right-side of the machine. Each of the activated bars on the drum (their number on each occasion being determined, as stated above, by the total number of clips opposite wheels which have an active peg for that position, less one for each overlap) advances the printing-wheel one letter, and the final letter reached is printed on the tape, the wheels all moving on one position as soon as one letter is thus enciphered, (if the slide is S, the kick of the bars K, the plain letter P, and the cipher letter C, the above operation can be expressed by the equation S - P + K = C; and as this can be re-arranged as S -C + K = P, it is clear that the operations for enciphering and deciphering are the same).

2. (any traffic). Enciphered on the above machine.

HAT, n :

1. (in Transposition). More or less hat-shaped figure into which the text of a message in simple transposition is written by the cryptographer when the key-length is known (or guessed) and the cage is not a complete rectangle.





2. Rearrangement of a series of letters or figures or groups of these in a new and other than alphabetic or numerical order.

HAT, v :

To rearrange in any non-alphabetical or non-numerical order.

HAT BOOK :

A code-book characterized by the fact that when the plain-language terms are arranged in alphabetical order the code groups are not in numerical (or alphabetical) order; a two-part code.

HATTED :

Arranged in other than numerical (or alphabetical) order.

HAT-DIAGRAM, HAT-FIGURE :

HATTED FIGURE :

= hat.

HEFT :

A set of 3-figure substitution tables used in the two main German meteorological ciphers according to a hatted time-table and changing every three hours.

HEXAGRAM :

Six consecutive letters or figures, especially when occurring as a repeat.

HIGH-ECHELON :

Used by or concerning Divisional H.Q. and higher authorities.

HIGH-GRADE :

1. (of code or cipher systems). Designed to provide security, i.e. resist breaking, for a comparatively long period or indefinitely.

2. (of Japanese Army Codes, etc.). Using enciphered indicators.

HOP OUT :

To break (an Enigma key) on a Hoppity menu.

HOPPITY :

Method of using a crib when Ringstellung of right hand wheel (and therefore the position of the turn-over) is known, consisting in preparing and running a single menu, instead of the usual set, e.g. of three alternative menus designed to provide for various possible positions of turn-over.

HORIZONTAL :

Proceeding from left to right as in ordinary reading and writing.

HST CODE :

A three-letter code, the trigrams of which are taken from the 500 spare trigrams at the end of the Heeressignaltafel.

IDENT :

Short for identification, esp. of a three-letter code-group.

IDENTIFICATION :

(in book-breaking, etc.). A solved or 'recovered' meaning for a code-group.

IDLE :

Having no necessary or significant function.

ILLEGAL :

Not in conformity with established practice.

INDEX :

(especially). To index by cipher groups; also, to record occurrences of (code-groups) as a process in book-breaking.

INDICATIVE :

(in Met.). A three figure number indicating the Meteorological Station concerned, and forming the first three figures of a synoptic report. (It may be either a Principal Indicative, i.e. one of 1000 three-figure groups assigned to 1000 different Met Stations in Europe by International agreement; or a subsidiary or National Indicative, i.e. a group, additional to the original 1000, assigned nationally to a station not on the original list).

INDICATOR :

One or more letter or figure or letter-and-figure groups (either sent in clear or enciphered on a separate system and placed at the beginning and/or end of a message, or in the body of it) indicating the key or subtractor used or, in the case of a long subtractor, the starting-point or starting-point and finishing-point.

INDICATOR GROUP :

A group forming the whole or part of an indicator, whether enciphered or not.

INDICATOR SYSTEM :

System by which key or starting-point indicators are enciphered or concealed.

INTERNAL :

1. (of repeats). Occurring within the same message.

2. Occurring in or derived from one particular type of traffic and applied to that traffic.

INTERVAL :

Distance between two symbols or groups, esp. in a cipher message expressed algebraically as the number of unit distances (i.e. distance between two consecutive symbols or groups), intervals from left to right being positive and from right to left negative.

INTERVAL KEY :

(in Transposition). Key giving intervals between the positions denoted by the consecutive terms of an encipher key.

INVERSE ROD :

A rod showing the letters on the left side of a wheel of an Enigma machine that are consecutively connected to a fixed point in space at the right side for the twenty-six different positions which occur in one revolution of that wheel. There are twenty-six such rods for each wheel, corresponding to the twenty-six different points on the right side of the wheel, which, like the direct rods, form a rod-square, but have the diagonal running upwards from right to left. (The sequence of letters on an inverse rod is in fact an index of the sequence of direct rods on which the letter which denotes that inverse-rod is to be found for each of the twenty-six positions).

INVERT :

(in German Y Service traffic). A short message from a German ground station answering a request and giving the bearing desired.

JAM :

To make wireless signals incapable of satisfactory reception by transmitting interfering signals on the same frequency.

JARGON CODE :

A code using words (esp. nouns) instead of figure or letter-groups as the equivalent of plain language units.

JUMBO :

A type of bombe having the machine-gun attachment.

KANA :

Linguistic units consisting of single vowels or a consonant followed by a vowel used to transliterate Japanese characters into Roman letters, and in various Japanese codes and ciphers.

KENNUNG :

Indicator.

KENNBUCH :

Indicator Kenngruppenbuch .

KENNGRUPPE :

Indicator group or discriminant.

KEY

Series of figures, numbers or letters which are used in the encipherment and decipherment of messages in a given cipher system. The chief types of keys are separately defined.

1. (in reciphered codes). A series of figures usually in random order and, in the case of high-grade ciphers, of very great length, a portion of which (denoted by the indicator) is applied figure by figure, non-carrying, to the figures of the encoded message, either by addition or subtraction. Short keys and sometimes, in the case of long keys, single pages of key are treated cyclically when the end is reached; a subtractor . A vary short key is called a "recurring key".

   b. The group of key-figures used to recipher any one code-group of the message; also, a provisional evaluation of this, properly termed "provisional column subtractor", or "provisional subtractor group".

   c. (spec.) The key-group used to encipher an indicator.

2. (in Transposition). A series of natural numbers (i.e. from 1 onwards) arranged in non-numerical order (often obtained from a plain-language "key-phrase") which determine by their number the length of the cage used in transposition and by their order the sequence in which the columns are taken out of the cage in the process of encipherment and written in the process of decipher-ment.

3. (in Playfair systems). The order in which the letters of the alphabet are placed in the square or squares used.

4. (in Enigma). The wheel-order, ringstellung, stecker, and discriminants (if any) used by a particular group of stations on a particular day or other fixed period.

KEYBOARD :

(esp. of Enigma indicators). Obtained from or suggested by the order of the letters on the key-board of a cipher machine and hence having certain characteristics.

(n.) a keyboard indicator.

KEY-BOOK :

1. (in reciphered code systems). The book containing a long key or subtractor.
2. The novel or other book used as the running-key in Poly-alphabetic substitution ciphers.

KEYBREAKER :

Person occupied in solving the keys or subtractors used in any type of cipher, esp. reciphered codes.

KEY-BREAKING :

The action or process of discovering or "recovering" cipher keys or subtractors.

KEY-DIFFERENCING :

Method of key-breaking (esp. with machine keys) consisting in sub-tracting a length of key from itself at a particular interval with a view to eliminating the component whose period is equal to that interval.

KEY-GETTER :

= Key-breaker .

KEY-GROUP :

The series of key-figures used to recipher one particular group of a message or one particular column of a depth, or the value provisionally assigned to this; (spec.) the group of key-figures used to encipher an indicator.

KEY-INDICATOR :

An indicator.

KEYING FIGURE :

A figure constituting or denoting the recipher key used,esp. a short key.

KEY-LENGTH :

The length of the key used, esp. in Transposition systems.

KEY-LETTER :

(in poly-alphabetic ciphers). The letter which determines which of the available cipher alphabets is used to encipher a particular letter of plain-language.

KEY-SQUARE :

1. (in Playfair systems). The arrangement of 25 letters in a square which constitutes the key, or part of the key.

2. (in polyalphabetic ciphers). The table of substitution alphabets used, normally forming a square, 26 by 26, with the key-letters along the top, the plain letters down the side, and the cipher-letters in the square itself; but see Beaufort system .

KEY-WORD :

(In Transposition), Word determining by the number of its letters the length of cage used, and by the alphabetical order of its letters the order in which the columns of the cage are to be taken out or written in.

2. Word forming basis of order of letters in a Playfair square or in one or both components of a cipher alphabet.

KEY TABLE :

Table of key-groups, esp. one used for enciphering indicators.

KEY-TEXT :

Text constituting the running-key, e.g. in a poly-alphabetic substitution system.

KICK :

1. A movement of controlled but sometimes variable amount imparted to a rotating portion of a cipher machine either regularly, e.g. before or after the encipherment of each letter, or periodically.

2. (spec. in the Hagelin machine). The movement of the printing-wheel between cipher and plain-language letter at the encipherment of any given letter, or the portion of this total movement formed by the contribution of any particular wheel which has an active position for that letter, i.e. the number of bars activated by a particular wheel.

KISS, n :

Coincidence in time of origin of two messages, suggesting the possibility of a re-encodement.

KISS, v :

To examine (cipher messages) for kisses.

KRAC :

(in G.A.F. codes). The solution for a particular day of a three-figure code group in a code which is reciphered by daily substitution.

KREIS :

A form of W/T working in which each of several stations in a group has its own call-sign and communicates with any other station in the group direct (i.e. there is no Control).

KRYHA MACHINE :

Cipher machine consisting essentially of two circular alphabets, one rotating against the other, and a third wheel which imparts a variable kick to the rotating wheel after the encipherment of each letter.

KTF :

(short for Klartextfunktion). An autoclave element found in certain Tunny links consisting in the addition (non-carrying in the scale of two) of the fifth impulse of the preceding plain letter to the pattern of the second chi-wheel(cf. chi-2 function), followed by Boolean addition of the reverse of this result to the pattern produced by the two motor-wheels for the next position, the net result being the motor for that position, and designed to avoid giving depth even when the same message-setting is used more than once; also, a similar autoclave element applied to the key of the Sturgeon machine.

LAGE :

A list of Enigma keys showing the menus being run or waiting to be run on bombes at a particular time, with details of their structure and quality and the number of wheel-orders to be used; also the bombe situation revealed by such a list.

LANDLINE :

(esp.). Over-land telephone or telegraph (making use of wireless unnecessary).

LASH-UP :

A more or less improvised working model (of a machine or other ciphering device, etc.); = mock-up .

LATIN SQUARE

Square usually of 26 alphabets (or any number of series of different numbers) so arranged that each row and each column contains every letter or number.

LEFT. TO THE LEFT OF :

(in a series of figures, letters or other characters regarded as written from left to right and in successive lines under each other). In front of, earlier than.

LETTER-SUBTRACTOR . :

Employing letters which, having different numerical or positional values assigned to each, can be subtracted (non-carrying) from each other, as in Hagelin machines.

LEVEL, a :

(of message in depth). Beginning at the same point of the key or subtractor.

LEXICON :

(of a system of transposition of the letters in letter-groups). Preserving the order of the letters denoting the margin and those denoting the page respectively, while mixing the two sets together.

LIFE :

Period of currency of a code or cipher system or any part thereof.

LIFETIME :

= life.

LIMITATION :

Characteristic of certain code and cipher systems consisting in the fact that a particular letter or figure (or letters or figures) do not occur, or to not occur in certain positions or certain circumstances or occur less frequently or more frequently than others.

LINE :

A horizontal row of letters or figures, esp. in a Vigenere or similar square.

LINE UP, v :

To set (messages) in depth, especially messages which start level.

LINE-UP, n :

A placing of messages in depth.

LINER :

(in Playfair systems). A bigram both letters of which occur in the same line or row of the square or squares.

LINK :

Regular communication, esp. wireless communication, between two specified points, or facilities for this.

LOBSTER :

(in certain types of Enigma machines). A simultaneous turn-over of all four wheels (i.e. all wheels, including the Umkehrwalze), producing a cipher alphabet which is equal to the previous cipher alphabet unbuttoned one.

LOBSTER OUT :

(in certain types of Enigma machine). To break or recover (a key) by utilizing the characteristics of lobsters and the fact that message-settings have been enciphered twice on the basic Grundstellung.

LOG-READER :

Person engaged in reading W/T interception logs and obtaining W/T and other intelligence therefrom.

LONG SUBTRACTOR :

A subtractor which is longer, usually much longer, than any text to which it is likely to be applied.

LOW ECHELON :

Used by or concerning Divisional H.Q. and lower authorities.

LOW-GRADE :

(of a code or code system). Not expected to resist attempts to break it for long, esp. if used to any great extent; usually employing only one encoding or enciphering process, and that a fairly simple one. e.g. simple substitution, periodic substitution within a short period, simple transposition, unreciphered code.

MACHINE CIPHER :

A cipher system in which the enciphering and deciphering are performed by means of a machine.

MACHINE GUN :

A special attachment, characteristic of the Jumbo type of bombe, for dealing with stops involving legal contradictions, i.e. contradictions of the type A steckered to X and B steckered to X, where A and B are in the Menu, and making a noise suggestive of a machine-gun when so doing.

MAIN TABLE :

(in certain code-books which have two meanings assigned to one group). That portion of the code which includes the first, or principal meanings only. cf. auxiliary table .

MAJOR DIFFERENCE :

The larger of the two differences obtained when two code or cipher groups are subtracted the one from the other and the other from the one; it is normally numerically greater than a series of 5's.

MAJOR GROUP :

That one of two code or cipher groups which gives the minor difference when the other group is subtracted from it.

MAKE :

To transmit (a message) by W/T.

MAKE UP :

(of a crib). To provide a series of constatations of a specified (favourable or unfavourable) character, depending on the number and length of the chains and closures present.

MAP FIX :

A determination of the position on a map, usually of a W/T transmitter, from D/F bearings.

MARGIN :

Those figures (or letters) of a code-group which determine the position of the group on the page (in two-part codes, in the second part or decode only) as distinct from those which determine the page on which it occurs.

MASK :

(in the breaking of Enigma keys when the stecker is known). A form of search-stencil having desteckered constatations punched on it, used on an inverse-rod square (or having steckered constatations punched on it and used on a Wylie-box) to determine rod-pairings and so leading to the breaking of the other elements of the key.

MASTER :

Short for master-card.

MASTER-CARD :

(in Freebornery). A Hollerith card on which a maximum amount of information is hand-punched from originals (esp. cipher messages), and from which such excerpts as are required for any particular analysis can be a electro-mechanically reproduced.

MATE :

To match or fit (a crib).

MEDIUM GRADE :

1. (of code or cipher systems). Designed to provide security, i.e. resist breaking, for a comparatively short period, but for longer than low-grade systems, and used especially in circumstances where the apparatus and processes required by high-grade systems would be unsuitable and long-term security is not essential.

2. (of Japanese cipher systems). Using unenciphered, i.e. plain, indicators.

MENU :

(in Enigma). A series of more or less interconnected constatations of which the relative positions are known, esp. such a series prepared for key-breaking on the Bombe.

MESHING-POSITION :

Position where the two wheels of a Wheatstone cipher machine are in mesh, i.e. where one plain language letter is exactly opposite a cipher letter.

MESSAGE-TO-MESSAGE :

(of recurrences). Involving more than one message; external.

M.F., M/F :

Short for medium frequency.

MILK-RUN :

A series of two positional repeats of groups of reciphered code, suggesting a possibility of depth.

MINOR DIFFERENCE :

The smaller of the two differences obtained when two code or cipher groups are subtracted each from the other; it is not numerically greater than a series of 5's.

MINOR GROUP :

That one of two code or cipher groups which, when subtracted from the other group, produces the minor difference.

MINOR, v :

To express differences as minor differences only.

MINUEND :

A Beaufort Subtractor applied to code-groups by subtracting (non-carrying) the code groups from it.

MIXED UNIT :

(of codes or code books). Having groups of more than one length, e.g. some 4-figure and some 5-figure groups.

MOCK-UP :

Reconstructed model or copy (of a machine, etc.).

MODULUS :

Scale or basis of arithmetic; that number which, or any multiple of which, is represented by 0, in any arithmetical system, (the number corresponding to the multiple being "carried" in ordinary, and ignored in cryptographic or "non-carrying" arithmetic); operations with figures are normally done with 10 as modulus, and operations with letters with 26.

MOTOR :

(in Tunny). The combined motor-wheel patterns together with any additional function (e.g. chi-2 or KTF) which regulate the movement of the psi wheels.

MOTOR-WHEELS :

(in Tunny). Those wheels, esp. the two wheels in the simplest model of the machine, whose patterns are combined to form the series of active and inactive contacts which determine the movement of the five psi wheels, and which therefore enter into the composition of all five of the single-impulse enciphering keys. The larger of the two (period 61) advances one position for each letter that is enciphered; and communicate this motion to the smaller (period 37) or not, according to whether an active or an inactive contact is being made at the time. The smaller wheel, either directly or after Boolean addition of one or more other components (see chi-2 function and KTF), moves the Psi wheels on one position when it has an active contact (represented by 1 for addition purposes) in the operative position, and does not move them when it has an inactive contact (represented by 0 for addition purposes) in the operative position, with the result that the last signs of the psi wheels are used again and the psi patterns characteristically extended.

MRS. MILES :

An electric tape-reading and tape-punching machine designed to read and add together up to four teleprinter tapes and punch the result on a single tape.

MONO-ALPHABETIC :

Involving or using only one alphabet.

MULTIPLE ANAGRAMMING :

Process of anagramming simultaneously several transposition messages of the same length that have been enciphered on the same key.

NEAR-CILLI :

The employment or occurrence of, not the finishing positions of one Enigma message, but of positions near these, as the outside indicator of the next message; (cf. Cilli and Aitkenismus).

NEAR DEPTH :

(in machine ciphers). Two or more messages or parts of messages that have been enciphered with all the wheels except one (or two) in the same positions.

NEARNESS :

The occurrence of choice of a message setting near the outside indicator of an Enigma message, so that after the former is enciphered the wheels are in or near the positions required for enciphering the text, thereby saving the operator the trouble of much further adjustment.

NETZ, n :

1. A form of W/T working in which two or more stations, each with a call-sign and a corresponding frequency, work to each other, each station using its call-sign and frequency for receiving purposes only.

2. (in former Enigma-breaking). Any of 60 sets each of 26 differently lettered double Foss sheets having holes punched in them corresponding to females at distances of three (i.e. one set for each possible wheel-order, and one sheet for each position of the left-hand wheel - the positions of the other wheels being represented by the co-ordinates of the holes). When the sheets of one set are super-posed, staggered according to differences in the outside indicator, the correct wheel-order and ringstellung are shown by the coincidence of holes in several sheets.

NETZ, v :

(of W/T stations). To use the netz system of working.

NIGELIAN WHEEL ORDERS :

A series of wheel-orders used in certain G.A.F. Enigma keys, characterised by the fact that it comprises only 30 out of the 60 possible wheel-orders.

NO-COLOUR :

(of Enigma messages). Not assignable to a particular key or colour; unidentified.

NON-CARRYING :

(of addition, subtraction, etc.). Performed without transferring multiples of 10, or any other modulus used, to the next figure on the left as units as in ordinary arithmetic; cyclical or cyclically; cryptographic.

NON-CLASHING RULE :

(in Enigma). Rule or principle not permitting, or tending to avoid, the same position for the same wheel on consecutive days.

NON-CRASHING :

misused for Non-clashing .

NON-CYCLIC :

Not treated as cyclic; using "carrying" addition.

NON-INDICATOR :

(esp. of German Army P/F) Having no indicator.

NON-MORSE :

1. Employing signals other than the morse code for the transmission of messages spec. transmitted (or transmitting) in the teleprinter alphabet .

2. (of ciphers) especially, belonging to the Tunny or Sturgeon type (which use the teleprinter a1phabet).

NON-REVERSIBLE :

(of bigrams in double Playfair with two squares). Characterized by having an equivalent cipher bigram which is not its equivalent plain-language bigram when it (i.e. the original bigram) is cipher;)a bigram in which at least one of the substitutions used in enciphering it is linear.

NON-TEXTUAL :

(of groups in cipher texts). Forming no part of the actual text as e.g. indicating and check-groups.

NULL :

A dummy figure or letter; a filler.

OFFIZIER :

1. (of German cipher keys). Designed to be used by Officers only; (opposed to General).

2. (of a message or part of a message). Enciphered on such a key by an officer and subsequently re-enciphered on a general key.

OFFSET :

(of messages in depth or recurrences in these). Beginning or occurring at different points of the subtractor key.

ONE-PART :

(of code-books). Alphabetic, and so not requiring a separate decode section.

ONE-TIME :

(of subtractor, esp. pad-subtractor). Designed to be used only once.

OPEN-SPELL :

A code-group used to introduce spelling groups.

ORIGINATOR :

The (official) writer or sender of a message.

OUT :

(of a code-book). Solved or reconstructed.

OUT-STATION :

Any station in a star other than the control station.

OVERLOAD :

To use (a subtractor or any part of a subtractor) so often that it is possible to set a sufficient number of messages in depth to strip off the subtractor and solve the code; to impair the security of by over-use.

P5 FUNCTION :

= KTF.

PAD :

A set of different subtractors each occupying one page of a pad, from which successive pages can be removed and destroyed, usually as soon as they have been used once.

PAGE :

The page-number of a code-book (in the case of two-part codes, the page number in the second part or decode section) forming usually either two or three figures of the code-group, the remaining figures of the group being those of the margin.

PAIR DAY :

(in certain Enigma keys). Either of two consecutive days so related that the letters which are steckered on the one are unsteckered on the other.

PAIRED DAY :

(in Naval Enigma). Either of two consecutive days on which stecker and grundstellung change but the wheel-order and ringstellung remain the same on any particular key.

PARITY :

(esp). Oddness or evenness of a figure or number, of a letter as determined by its position in an alphabetic or other series, of a tele-printer letter as determined by the number, e.g. of crosses used to represent it, or of any other symbol having a position or character to which a number corresponds.

PARKERISMUS :

(in Enigma). A system of registration designed to show up repeats of keys or any parts of keys (i.e. wheel-orders, ringstellung, and stecker).

PASS :

To transmit (cipher or other messages).

PASS-ON :

(of call-signs). Indicating retransmission, i.e. either that a message is to be retransmitted (in which case, e.g. fuer precedes it) or that it is being retransmitted (in which case de, rarely von, is used).

PATTERN :

1. Appearance or shape of tabulated record of occurrences of single letters, bigrams, or other units or symbols resulting from relative frequency or rarity, especially as shedding light on the nature of a particular cipher, or on the relationship between different messages or parts of messages in it.

2. Scheme of blank (usable) and black (non-usable) squares used in transposition system and distinguishable from a stencil in not being reveribl.

3. (in machine ciphers, esp. Hagelin, Tuuny and Sturgeon). The sequence of active and inactive, or operative and non-operative, positions round a wheel.

PATTERNED :

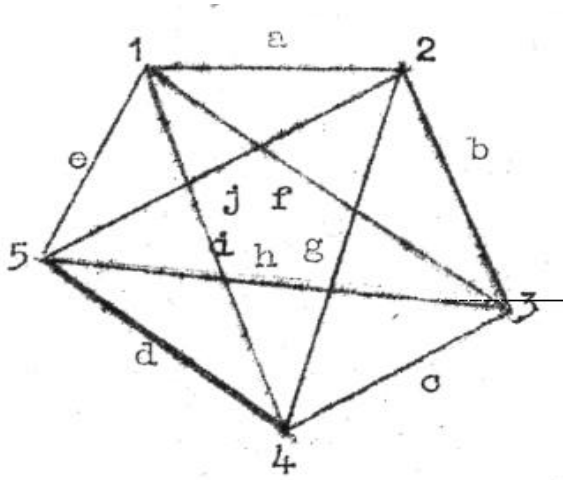
Having a recognizable or characteristic pattern.

PEG :

(esp.). One of the metal pins on the rim of a Haglin wheel capable of being moved at right-angles to the plane of the wheel to an active or inactive position, and so forming one unit in the wheel-pattern.

PENTAGON :

That part of the mechanism of the Sturgeon machine (e.g. T.52C) which effected the combination of the patterns of the individual wheels into seven sums each of four patterns in a manner capable of being diagrammatically represented by a pentagon and its five diagonals, the sides being lettered a, b, c, d, e, starting from apex No. 1. and preceding clockwise and the diagonals f, g, h, i, j, similarly, and the sixth and seventh sum being obtained from the diagonals alone by omitting the second and the fourth respectively.



PERIOD :

Interval at which any cyclic series repeats; e.g. the length of a recurring key, or of any component part (i.e. wheel) of a machine-key; the width on which transposition is applied; the width on which an analysis of a cipher or key is made.

PERIODIC :

Characterized by periods; recurring cyclically.

P/F :

Short for Playfair.

PHONETIC :

(of groups, esp, call-sign groups). Pronounceable.

PICTURE FRAME :

Type of transposition pattern having large rectangular block of black squares in centre.

PILOT :

(short for Pilot-balloon observation). A message containing observations of wind-speed and direction at successive levels in the upper atmosphere above a particular Met. station at a particular time.

PINCH, n

1. Action of obtaining by covert or any available methods secret official documents, esp. cryptographic documents, of another state or of any organisation.

2. Any secret document or collection of secret documents so obtained, esp. when of cryptographic value.

PLAIN :

(of language).

1. Uncoded or unenciphered.

2. Decoded or deciphered.

3. (erren. for unreciphered).

PLAYFAIR

Bigram substitution system in which a key-word; or other type of mixed alphabet of 25 letters written in a square (or two such alphabets in different squares) with simple rules for substitution, takes the place of bigram substitution tables.

PLAYFAIR, v :

To encipher or substitute in the Playfair manner.

PLOTTING CENTRE :

= filter-room.

POINT-TO-POINT :

(of W/T working, esp. in G.A.F.). Occurring between two ground , stations as opposed to between ground and air or air and ground.

POLY-ALPHABETIC

(cf. substitution systems). Employing more than one cipher alphabet.

POSITION INDICATOR :

= Indicator .

POSITIONAL :

(of external repeats). Occurring at the same distance either from the beginning of the messages or from another repeat and so suggesting that the messages are in depth with each other.

POWERFUL :

(of Enigma cribs,cillies, etc.) Likely to yield solutions; (cf. use of Good).

PREAMBLE :

1. Introductory part of cipher or code including e.g. call-sign date, time, serial number, number of groups, address, indicator, etc. either sent in clear before the cipher text, or partly in clear end partly in cipher, or wholly in cipher either at beginning of text or at some later point.

2. That part of the above, whether in clear or in cipher, which precedes the beginning of the text of the message.

PREDICATE :

The second portion of a short message having two portions; (1) a grid reference in one cipher, and (2) a very short message in another cipher.

PRE-ENCIPHER :

To encipher on one cipher system prior to re-enciphering on another.

PREFIX :

A discriminant or indicator put in front of a message.

PRESTART :

(in Enigma) Applied to the indicators or the position of the wheels before enciphering the first letter of a message as the machine in fact moves on one position before enciphering the first letter.

PRIMARY CIPHER ALPHABET :

Any one of a series of cipher alphabets produced by sliding a basic alphabet against a natural alphabet, two basic alphabets against each other, or any alphabet against itself.

PROGRESSION-KEY :

Key showing in what order the different alphabets of a polyalphabetic substitution cipher are used.

PRONOUNCEABLE, n :

An indicator-group (esp. in Enigma) forming, in its plain version, a pronounceable sequence of letters.

PROVISIONIAL :

(of code-groups or keys) See Base.

PSI, a :

Epithet of (any of) the five wheels of the Tunny machine characterized by having the same intermittent movement.

PSILLI :

(short for psychological or psychic Cilli). An Enigma message setting which is so related to the outside indicator (e.g. by completing a word which the outside indicator begins, or continuing the same sequence or series of letters, as in the series - the message settings are underlined WIR BRA : UCH ENZ : IGA RET : TEN ...) that its clear form can be inferred from the latter; also, any setting which can be guessed from a knowledge of the idiosyncrasies of the operator concerned.

PSYCHIC, PSYCHOLOGICAL :

See Psilli .

Q-CODE :

International three-letter code, the first letter of each group being Q, or any national adaptation of this, used mainly for signal-service communications by operators.

QUALIFIER :

A grammatical group.

RADICAL :

One of the 214 basic characters under which Chinese ideographs are grouped for dictionary purposes.

RADIO FINGER PRINT :

Enlarged or elongated film-record of morse transmission by means of which the type of transmitter used and the peculiarities of the individual sets of any type can be distinguished, serving to identify stations.

RADAR :

New name for Radiolocation or Radio-direction-finding.

RAILWAY CATALOGUE :

(in Enigma). A special form of catalogue (see Eins catalogue) designed for a machine with a rotating Umkehrwalze (first used on Railway traffic).

RANDOM :

Produced by chance or accident, or such as may have been so produced; (esp. of a series of letters, figures or other symbols) such that any one of the total number of different symbols used is equally likely to occur at any point; alternatively, having no discernible patterns or limitations nor any symbol the number of whose occurrences differs from the average number of occurrences by more than a definable and relatively small number, e.g. N(n-1) where N is the total number of symbols in the series and n the number of different symbols used, or a small multiple of this suitable to the size N.

R.D.F. :

Short for Radio-Direction-Finding.

R.E., R/E :

Short for Re-encodement (used for Re-encipherment).

READ :

To decipher or decode (messages) especially as the result of successful cryptographic investigation.

READABLE :

(of code and cipher systems, especially of reciphered codes). That can be read more or less currently.

READABILITY :

Extent to which cipher or code messages of a particular system can be read.

R.E.B. :

Coded form of the letters R.F.P.

RECIPHER, v :

1. To conceal the true character and figures or letters of an encoded message by applying a key or subtractor (usually by non-carrying addition or subtraction) or by any system of transposition or substitution.

2. To apply a further enciphering process to a text which is already enciphered.

3. (Misused for 'encipher').

RECIPHER n :

A series of figures or letters used for reciphering; a subtractor.

RECIPHERING TABLE :

Any table used for reciphering code messages, e.g. a substitution or subtractor table.

RECIPHERMENT :

1. Process of disguising the code-groups of an encoded message by applying a key or subtractor, etc.

2. (Misused for encipherment).

RECIPROCAL a :

1. Producing zero or a series of zeros when added non-carrying to a given figure or series of figures.

2. (of substitution systems). Consisting of or involving pairs of letters or groups so related that when one is the cipher equivalent of the other, the other is also the cipher equivalent of the one.

RECIPROCAL n :

1. That figure (or letter) which when added non-carrying to a given figure (or letter) gives zero as the sum e.g. in the scale of 10, 9, is the reciprocal of 1, 8 of 2, etc.

2. (in two-box Playfair). A bigram having as its enciphered form the same two letters in the opposite order.

3. (in Enigma) A backward click .

RECIPROCAL IDENT :

An identification obtained from another by utilizing the fact that the trigram substitution tables concerned are reciprocal.

RECOGNITION GROUP :

(used for discriminant).

RECOVER :

To solve or reconstruct (a key or part of a key).

RECOVERY :

1. Action or process of solving or reconstructing subtractor or other keys.

2. A subtractor or other key or any part thereof obtained by solving or reconstruction.

3. A code-group identification.

REDUCE :

(in full 'reduce to the same basis'). To equate (columns of a depth of reciphered code messages).

REDUCTION :

Action or process of equating columns e.g. of a depth of reciphered code messages.

RE-ENCIPHER :

1. To encipher on a different cipher or with a different setting or key on the same cipher (a message which has previously been enciphered, transmitted, and deciphered).

2. Used or misused for recipher)

RE-ENCIPHEREMENT :

A fresh encipherment of a message either on another setting or in a different cipher.

RE-ENCODE :

1. To encode (the same clear message) a second time, especially with a different code or system.

2. (Misused for re-encipher).

RE-ENCODEMENT :

i. A second encodement or encodement and recipherment of a message, especially one using a different code.

2. (Misused for re-encipherment), Especially a recipherment recognised as such by having e.g. the same time of origin, approximately the same length, contents calling for or worthy of retransmission, call-signs or other W/T features known to be associated with re-encipherments, and (when one of the two messages concerned has been read) utilized as a crib for the other message.

REFLECT :

To reproduce symmetrically as by a reflecting surface.

REFLECTOR (WHEEL) :

Umkehrwalze .

REGIONAL :

A general broadcast, similar to a Collective , to the Meteorological stations in a region (i.e. a subdivision of an area).

REGISTER n :

A tabulated record of cipher or code messages(usually of a particular system or type of traffic) including such particulars as call signs, frequency, originator, addressee, date and time of origin, indicators serial number, and beginnings and ends of the texts, etc., or as much of this as is available or known to be relevant.

REGISTER, v :

To enter particulars of (messages) on a register (q.v.)

REHASH, v :

(especially). To rearrange lines or columns of (a subtractor) so as to produce a new subtractor.

RE-HAT v :

To hat afresh, i.e. in a different order.

REHATTED :

Having the same numbers, letters, or groups in a different hatted arrangement.

REINCODING :

(Misused for re-encipherment).

REJECT, v :

(of an Enigma message). To crash with one or more of the possible variants of a crib. (To reject well is to crash with many or all but one of the possible crib-variants; to reject bad1y is to crash with few or none of them.

REJECTOR :

An Enigma message considered with regard to the extent to which it crashes with the alternative versions of a crib.

RELINEATION :

Rearrangement of line or margin numbers; (app. = remargination).

REMARGINED :

(of a code-book). Having two figures of the code-groups altered, especially by a rehatting of the margin numbers.

REMARGINATION :

Action or process of renumbering the margins, i.e. altering two figures of the groups in the code.

REPAGED :

(of a code-book). Having the page-numbers altered, and consequently all figures except two (normally the last two) of the code groups changed.

REPAGINATION :

Renumbering of the pages of a code book, normally affecting all except two of the figures of each code-group.

REPEAT :

1. (especially) A second or subsequent occurrence of a code or cipher passage or set of characteristics either in the same or in other messages.

2. A cipher passage or series of characteristics that occurs elsewhere, either in the same or in other messages.

3. A second or subsequent transmission of a message or any part thereof.

4. Re-use of subtractor tables or keys; a subtractor table or other key thus re-used.

REPEATER :

1. One that repeats or recurs.

2. A re-encipherment.

REQUEST :

(in German Y service Traffic) A short message from an aircraft giving the frequency and call sign of an enemy station which it has picked up, and asking for an immediate bearing to be taken on that station.

RE-RECIPHER :

A second reciphering key or process applied to an already reciphered code message.

RE-REGISTER :

A register of decoded messages designed to assist book-breaking especially on the introduction of a new code-book for the same traffic. See next.

RE-REGISTRATION :

A second registration of cipher or code messages; especially a egistration of decoded messages, made on the basis of originating unit or station, and including such particulars as date and time of origin, call-sign, address, signature, originator's serial number, transmitting station's serial number, nature of subject matter, and index number of decode, designed to facilitate book-breaking especially when a new book is introduced.

RESEARCH :

Systematic study or investigation of any (esp. of a new) type of cipher traffic aimed at (a) establishing its essential character, e.g. whether transposition or substitution and, if the latter, whether machine or hand cipher or code (b) determining the essential character of the processes and appliances or mechanisms, if any, involved in its production; and (c) devising methods of attack, and esp. methods of solution, appropriate to the ascertained nature of the problem; (cf. Development). Also, the production of general treatises on cryptography, e.g. this dictionary.

RESUBSTITUTION :

A second or subsequent substitution carried out on the top of a previous one.

RETROFLECTION :

Process whereby each of a series of numbers in numerical order is associated with one of another series in the reverse order (i.e. the smallest in the first series with the largest in the second), the second series being a continuation of the first, but written in the opposite direction.

REVERSE v :

(used for interchange)

REVERSED :

(of standard cipher alphabets) In which the clear and cipher components run in opposite directions.

REVERSIBLE :

(in Playfair systems) An equation of a clear bigram with a (different) cipher bigram which is still true when the bigrams are interchanged.

REVOLVING STENCIL :

A square stencil designed to disclose a different set of squares at each of three successive turnings through 90 degrees.

R.F.P. :

Short for Radio Finger Print.

RHYTHM :

(in transposition) A recurring series of differences between sets of adjacent or similarly spaced terms of an anagram key.

RIMA :

(in Enigma) A crib suggested to B.P. by the Naval Section at Washington (reverse of amir).

RINGSTELLUNG :

Position of alphabet-bearing tyre on wheel of Enigma machine, defined by number or letter at which a clip is set.

RINGSTELLUNG CUT OUT :

A running of a bombe with a restriction on the range of possible Ringstellungen.

ROBINSON :

(in Tunny). One of the high-speed machines (primarily designed to make counts and comparisons on any desired period) used to apply Tutte's method for the determination of unknown chi-wheel patterns and for the setting of chi-wheels whose patterns are known, by reading simultaneously two consecutive letters on each of two teleprinter tapes (one being that of a cipher message the other that of the two selected chi-wheels) by photo-electric means, combining and comparing the readings by suitable electric apparatus, and recording the counts for different settings by means of a printing attachment. Cf. Bedstead .

ROD :

Strip of wood or other suitable material ruled off in equal compartments, used e.g. in solving simple transposition ciphers; a similar device bearing a wheel-pattern or a cipher-machine or other key component of a cipher used for setting messages (see also direct rod , inverse rod).

ROD OUT :

To set (a message) and so, in Enigma, break (a key) by using rods or a rod square.

ROD-PAIRING :

(in Enigma). An association of two direct rods or of two letters at the same position on a pair of inverse rods, determined or suggested by an unsteckered constatation, especially in the process of setting a message.

ROD-POSITION :

(in Enigma). Position of the wheels of an Enigma machine corresponding to the rods of the wheels concerned and indicated by the letters (or figures) which would appear in the windows if the ringstellung were set at Z (i.e. zero) for each wheel.

ROD-SQUARE :

Square of 26 letters by 26 (or rectangle 26 by 52) formed by the Direct or Inverse Rods of a particular Enigma wheel arranged in order.

ROD-UPRIGHT :

A vertical column of a Rod-square,(representing the wiring of the wheel).

ROUTE :

Scheme of order or direction in which characters are written, read, or otherwise dealt with, especially order in which characters are written into, or taken out of, the cage in transposition.

ROUTING :

(especially). Pattern of sequence in which a text is written into or taken out of the cage in transposition.

ROUTINE, n :

A routine message.

ROW :

(especially). Series of 200 call-signs in Bird Book, constituting a Single row when the book is regarded as a single table having 200 rows and 200 columns.

R.R. :

Short for Registration Room,

R.S. R/S :

Short for Ringstellung.

R.T. R/T :

Abbreviation of Radiotelephony.

RUN, n :

1. A continuous stretch, especially of a subtractor or key.

2. (in Enigma). A consecutive test of all settings or of all settings and all or all likely wheel-orders, made by a bombe for a particular menu or set of menus.

RUN, v :

To test (a menu or set of menus) on the bombe in all possible or all likely settings and wheel-orders.

RUNNING KEY :

(in polyalphabetic ciphers). A non-periodic alphabetic key obtained from a book or any continuous passage of writing.

SALTATION :

Process of selecting units from a natural series so as to leave, usually irregular, gaps in the series.

SANDWICH, n :

One or more repeated characters enclosing one or more other characters.

SANDWICH v :

To be repeated so as to enclose one or more characters.

SCALE :

Basis on which figures (or letters) above an agreed limit are represented by an extra digit; that number which is represented by 0 and a 1 which is either carried to the left (or dropped) in any arithmetical system; arithmetical modulus, (The common scale is the scale of ten).

SCORE :

The odds in favour of a particular hypothesis, esp. when stated as a logarithm, so that total can be obtained by adding instead of multiplying.

SCRAMBLE, n :

(especially). A re-arrangement of three-figure reciphering tables in an other than the normal day-of-the-month order.

SCRAMBLE, v :

1. To rearrange, especially in non-alphabetical or non-numerical order; to hat.

2. To render (telephonic conversation) unintelligible over a part of a system by interposing frequency-changing mechanisms.

SCREED :

A write-up.

SCRITCH, v :

(especially in Enigma). To test (a hypothesis or possible solution) by examining its implications in conjunction with each of a set of (usually 26) further assumptions in turn, eliminating those cases which yield contradictions and scoring the others.

SEARCH, a :

1. (of intercepting sets). Engaged in searching for transmissions from new stations or on new frequencies or any type of transmission not otherwise covered.

2. Derived from or connected with the intercepts or records of search sets.

SEARCH-STENCIL :

See stencil 2.

SECONDARY CIPHER ALPHABET :

The alphabet produced when a primary cipher alphabet is rearranged with its plain component in alphabetical order.

SECTOR CODE :

A German code associated with a particular coastal defence sector rather than with any particular formation.

SELF-EVIDENT :

SELF-STECKERED :

1. (of a letter). Steckered to itself, i.e. unsteckered.

2. (of a menu). Containing or consisting of unsteckered letters.

SELF-STECKERED SELECTION :

Method of setting menus on bombes so that stops only occur when at least one letter on the main chain is self-steckered.

SELF-SUMMING :

(of code-groups). Of which the characters sum to zero.

SEMI-HATTED :

(of code-books). Hatted within definite, and usually small, sections.

SEPARATOR :

A letter or other symbol used to separate words.

SEQUENCE :

(especially). Order of letters in the plain or cipher component of a cipher alphabet, or on wheels of the Wheatstone and Kryha machines.

SPECIAL NUMBER :

One of a series of natural numbers attached to a message as its reference number by its originator, (or by its interceptor, or by any other person who may subsequently deal with it).

SET, v :

1. To find the starting position of (a reciphered code message) on the subtractor.

2. To find the indicators or starting positions of the wheels for deciphering a machine-cipher message.

SET IN DEPTH :

(of messages). Written below each other in such a way that letters or figures enciphered or reciphered by the same letter or figure of the key lie in the same vertical column.

SETTING :

1. Initial position of moving parts, especially wheels, of a cipher machine, for enciphered a particular message, determining part of key used for the enciphering.

2. Position (usually denoted by page, line, and column numbers) on a reciphering key or subtractor, especially a long subtractor, where the reciphering of an encoded message begins. Cf. Indicator .

SET-UP :

1. Arrangement or character of those parts of a cipher machine (e.g. wheel-patterns, wiring-systems) which normally remain unaltered for comparatively long periods of time (e.g. a day or month) or for the encipherment of a large number of messages.

2. (misused for Setting 1)

SHIFT :

1. Difference in position of clear language etc. in staggered messages.

2. Adder number or slide.

SHORT SUBTRACTOR :

A subtractor which is shorter than the texts it is normally employed to recipher.

SHOT :

An attempt to break an Enigma key on a crib, especially one involving the running of one or more menus on the bombe.

SHUFFLE :

(used for transpose).

SHUFFLED :

(of alphabets). Hatted or rehatted.

SHUTTLE :

Characterized by motion to and fro.

SIGNAL :

(especially). A code or cipher message, usually one sent by wireless.

SIGNAL INTELLIGENCE :

The organization responsible for the interception of all enemy and neutral communications and radio transmissions (cf. Y Service, which is one part of this), their deciphering and decoding and the preparation of the Intelligence resulting therefrom in a useful form.

SIGNATURE :

Name of originator, usually occurring at end of cipher message; code-group for name of originator.

SIGNIFICANCE :

(especially). Quality whereby any feature of code or cipher message differs from what may be reasonably attributed to accident.

SIGNIFICANT :

1. Having meaning or significance.

2. Exhibiting some feature or limitation which cannot reasonably be attributed to chance.

SIGN-OFF :

A signal (usually VA) denoting the termination of a morse transmission.

SIMPLE TRANSPOSITION :

Transposition in which only one rearranging process is involved.

SINGLE CHI (pron. tshi) :

Simple transposition.

SINGLE-MENU :

Using or involving only a single menu (cf. Hoppity)

SLANT :

Oblique stroke, e.g. as used between shillings and pence.

SLIDE, n :

1. Movement of two alphabets or numerical series written or printed with equal spacing on two rods or other suitable mediums, against each other, or of one alphabet or series against itself, giving for (each different position a different substitution alphabet, etc. (For convenience one of the alphabets is normally repeated.).

2. Instrument consisting of one rod capable of being moved along a groove in another rod, both being divided into equal spaces for the reception of alphabets.

3. Amount which one alphabet (or other series) is slid against another or against itself, measured by the number of spaces a particular letter has moved across from a fixed starting-point, for enciphering a particular letter; normally determined by a letter or figure of the key.

4. (in Tunny). Incorrect relative position of part of a cipher text, occasioned by one or more missing or extra letters, and tending to add to the normal difficulties of chi-setting and/or deciphering.

5. (in Tunny). Similarity, specially of a chi-wheel pattern to itself, usually about four places farther on, giving similarities in the counts obtained from different settings.

SLIDE :

1. To move one alphabet or series of numbers against another or against itself, especially alphabets, etc. written for convenience on rods or a cipher-slide.

2. To compare two different frequency distributions or the like in different successive horizontal positions with a view to fitting one to the other.

SLIDE CODE :

A three letter code which is varied from time to time by sliding the code groups against the clear equivalents.

SLIDE-RULE :

1. A cipher-slide.

2. A log-scale.

SLIDING ALPHABET :

An alphabet which is slid against another or against itself in the process of enciphering or deciphering.

SLIP, n :

(especially). Sheet of paper containing short description of a particular code or cipher system with details of its external characteristics (e.g. call-signs, preamble, etc.), users, and period of currency.

SLIP, v :

To apply a subtractor or code-group at successive positions of a reciphered code message with a view to finding out where it may be located.

SOLID :

Written or recurring in one continuous run, i.e. without spaces or gaps.

SOLVE :

1. To read or break (a cipher or any part thereof).

2. To identify (a code-group).

SORT, n :

Process of arranging in any particular order.

SORT, v :

To arrange on any particular basis.

SPACED :

Characterized by spaces, especially equal spaces, between successive members of a natural or other series.

SPELLER :

Code-group for one or more letters used in spelling words; (= next).

SPELLS :

Code-groups for single letter, bigrams, or other units, used for spelling words, especially proper names, not otherwise provided for in the code.

SPIDER-WEB :

(in Enigma). Obsolete for a chain in a menu.

SPLIT CLICHE :

A set of two or more code-groups which tend to recur, not consecutively but at a more or less regular distance from each other.

SPOTTY :

(of a cipher text). Faulty or corrupt.

SQUARE :

1. The arrangement of 25 letters in a square, or one of several such arrangements, constituting the key or part of the key of a Playfair cipher system.

2. Any one of the compartments of a transposition cage into which a single letter is written.

3. A short key or piece of key or a table of key-groups for reciphering indicators printed, or regarded as printed, in a square or rectangular form.

SQUARE, v :

To reconstruct the square or squares used in Playfair cipher system.

SQUARE COUNT :

A count made on a square of squared paper each line of which corresponds to a different first letter or number of a bigram and each column to a different second letter or number; each entry has thus two co-ordinates. cf. Foss sheet .

S.S. :

Short for Self-steckered.

S.S.S. :

Short for Self-stecker Selection .

STAB :

(of German cipher keys). Used for "staff" messages. cf. Offizier .

STAGGER, n :

Occurrence of the same clear passage or the same code groups at almost but not exactly the same point in each of two cipher, or messages which are in depth with each other.

STAGGER, v :

1. To encipher the same clear text in a second message in depth with the first but in a position differing by one or more letters.

2. (in Enigma). To try a crib (especially a stagger stretch) at a number of consecutive positions of the message.

STAGGER STRETCH :

Portion of re-encodement or crib which is considered unlikely to vary, and which is tentatively fitted at a series of points in the message to find those positions where it does not crash.

STANDARD CIPHER ALPHABET :

A cipher alphabet in which the normal alphabet sequence is preserved in both plain and cipher components, or reversed in one of them, one being slid against the other.

STAR :

A group, usually of several W/T stations using a common frequency, having one controlling station to which all the others work, and through which all traffic must pass.

STARFISH :

1. The occurrence of two letters and the same two letters in the reverse order in the same position on two rods of an Enigma wheel, corresponding to two sets each of four terminals (sc. two on the right and two on the left side of the wheel in each set) those of each set having the same relative positions on the wheel and being connected in pairs by the wiring in such a way that the two circuits cross over in the one set but do not cross over in the other; cf. Beetle, 2 .

2. Two constatations involving the passage of current through the same loop in the unmoved wheels but in the opposite direction. cf. Beetle, 3 .

START :

(in Enigma). Position of wheels at which the first letter of a message is enciphered; cf. Prestart .

STARTING-POINT :

(especially). Point in a key or subtractor where reciphering of a code message is begun.

STATION GRUNDSTELLUNG :

The special setting, usually remaining unchanged for three weeks, on which a particular Enigma station re-enciphers a message-setting which has already been enciphered twice on the Basic Grundstellung.

ST. CYR SLIDE :

A cipher slide.

STECKER :

1. Scheme or system of cross-connecting circuits esp. on some types of Enigma machine (capable of variation as required, and normally changed daily or oftener), having the effect of a simple reciprocal substitution at the entry points on the right side of the right-hand wheel, affecting usually twenty of the twenty-six letters.

2. That part of an Enigma machine where the stecker or cross-connecting of circuits is effected.

STECKER KNOCK-OUT :

A method of determining the stecker of an Enigma key, especially when the circuits of the Umkehrwalze are unknown, by following out the consequences of a series of stecker-assumptions in terms of rod-pairings and further stecker-deductions until contradictions are produced or a consistent solution reached; (for each series of assumptions the right-hand wheel, or the two right-hand wheels, have also to be assumed).

STECKER-PAIRING :

1. System used in Enigma machines whereby when one letter is cross-connected to another that other is, by the same action cross connected to the one, thus giving a reciprocal substitution of the one for the other.

2. A pair of letters steckered as above, or assumed to be so steckered.

STENCIL :

1. A piece of cardboard or similar material having holes cut in it through which messages are written on to paper underneath in the processes of enciphering and deciphering (usually in transposition systems).

2. A piece of squared paper having holes cut at levels corresponding to the letters of a "probable" word or crib, and in successive columns from left to right, which is slid along a stencil-search table at the proper level with a view to locating the word in question.

   (This should perhaps be distinguished from 1 by the name "search-stencil").

STENCIL LENGTH :

Number of letters which can be enciphered (or deciphered) with a particular stencil at one operation.

STENCIL-SEARCH METHOD :

Method of breaking poly-alphabetic ciphers of which the key-sequence is determined by plain language, and depths of letter-subtractor (e.g. machine) ciphers, by seeking a probable word in a stencil-search table by means of a search-stencil.

STENCIL-SEARCH TABLE :

Table formed by writing the text of a poly-alphabetic cipher (or the difference of two letter-subtractor cipher messages in depth with each other) along the top, the letters in their normal alphabetic order down the side, and filling in the columns with the letters that are the sum (or difference, according to the ciphering system that is being used) of the letters at the top and at the side for each different position. (In practice this simply means writing the cipher component of the cipher alphabet used into each column, starting from the letter at the top). A "probable" word can be sought on such a table by cutting a search-stencil in the appropriate manner (see Stencil 2) and sliding it along the table at the proper level.

STICHWORT :

(in Enigma.)

1. A code-word directing the application of a key-word (see below) and hence the introduction of the altered set-up which that key-word indicates.

2. A key-word indicating by its letters alterations or slides to be applied to existing set-ups.

STOP :

A point in a run at which a bombe stops; especially one giving a solution of a particular menu which may contain stecker-contradictions of certain types, e.g. A steckered to X, and B steckered to X, where A and B occur in the menu. (Opposed to Story).

STORY :

A solution of particular menu especially by a bombe containing no stecker-contradictions of any kind. (A bombe-run normally produces more stops than stories). Also, a possible solution obtained by one cryptographic process, calling for further investigation by another.

STRAIGHT :

(of alphabets, etc.). Unhatted.

STRIP, v :

1. To remove the true or provisional key (from a depth of reciphered code), especially by identifying good groups from good differences; also, to reduce a reciphered code message to true or provisional code-groups, the true or provisional key and the starting-point of the message on it having been previously determined.

2. To remove (the true or provisional key) from a depth of reciphered code messages, from a column of such a depth, or from a single message as above.

STUMER :

A corrupt or incorrect letter, figure or other unit in a cipher or code message.

STURGEON :

1. A German electric teleprinter letter-subtracting and impulse-permuting machine having ten wheels whose periods are prime to each other and whose patterns (representable either by series of crosses and dots or by ones and noughts for arithmetical addition and subtraction, non-carrying, in the scale of 2, cf. Tunny) are utilized in any desired order and either singly or in combination (e.g. of fours and sixes) first to alter, by addition or subtraction, the impulses of the plain Language letter as in Tunny and then to permute the resulting five impulses by causing or not causing an interchange in each of five pairs of adjacent impulses in turn, according to whether the impulse controlling that part of the permuting mechanism is a dot or a cross. Combinations of wheel-patterns to form the subtracting and permuting series are effected, e.g. in the model known as T.52C, by a mechanism called the Pentagon (q.v.) The latest model, T.52D, has no Pentagon, single wheel patterns being used instead of combinations, the regular motion of all ten wheels has been replaced by intermittent motion, the movement or non-movement of any particular wheel between the encipherment of two consecutive letters being determined by the patterns of the other wheels one-third of a revolution distant from their active (enciphering) positions, and a KTF has been introduced whose nature is as yet unascertained. As in Tunny the plain language is enciphered by one machine, transmitted in cipher, received, deciphered, and printed in clear on a tape by the receiving machine, the wheels of both machines being set in the same initial positions and the same steckers and combinations (if any) being applied in both. Thus as in Tunny, the cipher version of the message has normally only a momentary existence as electrical impulses, except when otherwise intercepted.

2. Any traffic enciphered on a machine of the above type.

STUTTERING DUMMY :

A dummy which is a repetition of the preceding letter or other symbol.

SUBSCRIBER :

An official or authorised user of a particular cipher or code.

SUBSTITUTION :

Process or action of putting one letter, figure, or other symbol or group of such, in place of any other unit or group. Systematic substitution is the basis of all codes and all ciphers except transposition ciphers.

SUBTRACTOR

1. A series of figures or letters (or a group or single unit of such) which is added non-carrying figure by figure or letter by letter to the figures or letters of code groups in the process of reciphering or to the letters of plain language in the process of enciphering, and subtracted from the cipher in the processes of stripping and deciphering; an adder or additive.

2. A series of figures or letters (or a group or single unit of such) from which the figures or letters of code-groups are subtracted non-carrying figure by figure or letter by letter in the process of reciphering or from which the letters of plain language are similarly subtracted in the process of enciphering, and from which the figures or letters of the cipher text are subtracted in the processes of stripping and deciphering; properly a Beaufort subtractor, type one. cf. Minuend.

3. A series of figures or letters(or a group or single unit of such) which is subtracted non-carrying figure by figure or letter by letter from the figures or letters of code groups in the process of reciphering or from the letters of plain language in the process of enciphering, and added to the cipher in the processes of stripping and deciphering; properly a Beaufort subtractor, type two.

   Note: all three types are also variously termed, recipher, recipher key, key, etc., as well as adder, additive key, subtractor. This inconsistency in nomenclature is inevitable as reciphered codes can in fact be stripped and broken and made wholly readable without knowing which of the above types of recipher is used, unless some limitation, or other feature, or accident, reveals the true figures.

4. Short for "subtractor cipher", i.e. a reciphered code.

SUMBOOK :

A book containing in numerical order the sums of every pair of a convenient number of good groups in a code- book (including the sum of each group and itself) together with the two good groups which each sum represents, designed to assist key-breaking with subtractor tables having as the second half of each table the groups which are the reciprocals of the groups in the first half in the same order.

SUMMER :

A code or other group or part of a group which has a characteristic (non-carrying) sum.

SUPER(EN)CIPHERMENT :

The action or process of enciphering a second time a text which is already enciphered.

SWITCH :

Short for "switch group".

SWITCH GROUP :

Code group indicating from what section of a book have more than one section, or (occasionally) with which of two or more alternative meanings, a particular code-group or series of such has been taken or used.

SYLLABIC :

Consisting of or based on syllables.

SYNOPTIC :

A message containing a weather observation in the International Meteorological Code made at a synoptic hour .

SYNOPTIC HOUR :

A fixed hour at which meteorological observations are made at all meteorological stations in a particular area, e.g. Europe, and for which a separate weather chart is normally drawn. In Europe there are 8 such hours in the 24.

SYNOPTIC PERIOD :

The interval between one synoptic hour and the next.

SYNTHETIC, a :

Produced by combining known code-groups with known subtractor groups, known code-groups with cipher groups, or known subtractor groups with cipher groups.

SYNTHETIC, n :

A synthetic subtractor cipher or code group.

SYNTHETIC GROUP :

(esp.) A probable or possible cipher group produced by reciphering a known good code-group with an already solved subtractor group, with a view to locating other messages reciphered with this subtractor group.

SYSTEM INDICATOR :

Discriminant.

SYSTEMATIC :

(of code-books) Having a systematic arrangement which permits the same book to be used both for encoding and decoding, without being strictly alphabetical.

TABLE :

Short for enciphering (or reciphering) table.

TACK ON :

(of two originally disconnected parts or chains of a menu) To be connected by the steckering of a letter in one part to a letter in the other part at a stop in the run.

TAIL :

Figures or letters added at the end of an enciphered message usually to complete the last group of five.

TAILING :

Habit or practice (almost characteristic of Japanese reciphered codes) of beginning the reciphering of the next message at the point of the subtractor where the reciphering of the last one stopped.

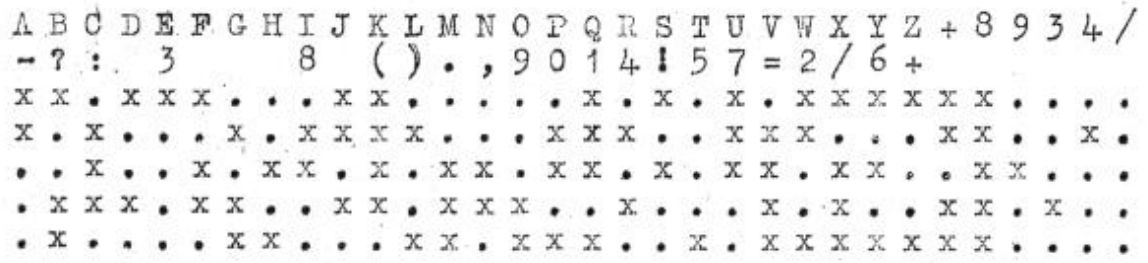
TELEPRINTER ALPHABET :

1. The thirty-two characters (including the 26 letters of the ordinary alphabet, the space, 9, letter-shift, 8, figure-shift, 4, carriage-return, 3, line-feed, 4, and oblique /) used to represent the five- (or seven-)unit signals in which teleprinted, esp. enciphered teleprinted, traffic is passed. (e.g. Tunny and Sturgeon).

2. The thirty-two five- (or seven-)unit signals corresponding to the above, which can be regarded as consisting each of a (positive) start impulse, a negative (stop) impulse, and five impulses between these, each of which is either positive or negative. A negative impulse is conventionally represented by a cross (x) and a positive by a dot (.) and the start and stop impulses ignored, so that each character has five impulses each of which can be either a dot or a cross. Impulses are combined by addition, non-carrying, in the scale of 2 (or subtraction, which in this scale gives the same result), a cross being treated as 1 and a dot as 0.

TELEPRINTER ALPHABET (contd) :

3. A list of the above thirty-two characters and their values (if any) on the figure-shift, with its cross-and-dot representation opposite each, viz.:



TEMP :

A message containing observations of pressure, humidity, and temperature at successive levels in the upper atmosphere above a particular meteorological station.

TEPHIGRAM :

A diagram showing the condition of the atmosphere at different levels in terms of its temperature, t and entropy, phi (i.e. extent to which the total energy of a system is randomly distributed in that system and therefore unavailable in that system).

TEST-PLATE :

A Hollerith machine, incorporating a form of the Enigma machine, designed to produce a complete record of the 17576 consecutive encipherments of a single letter, of a series of letters (e.g. the word eins), or of the whole alphabet, when the wheel-order, ringstellung,and stecker are known.

TETRA :

Short for Tetragram.

TETRAGRAM :

A set or group of four letters, figures, letters and figures, or other symbols, esp. when forming a repeat or click.

THRIPPLE :

1. (especially in Met. ciphers) To substitute two three-figure groups for a five-figure group such that the non-carrying sum of the third figure of the first group and the first figure of the second group is the middle figure of the original five-figure group, the other four figures being unaltered. (This splitting of five-figure groups is normally done before recipherment).

2. (of two three-figure groups arising from the above process) To be reduced (to a five-figure group) by the non-carrying addition of the third figure of the first group and the first figure of the second.

THROW-ON, n :

(in Enigma). A pair of letters representing two encipherments of the same (unknown) letter at two different positions, esp. at a distance of three or four in indicators that have been enciphered twice on a Grundstellung.

THROW-ON, v :

(of Enigma indicators). To Box.

TIE-UP :

Relationship between two or more code or cipher systems or keys arising from re-encodements from one to the other and offering possibilities of cribbing.

T/L :

Short for three-letter.

T/L I :

A list of identifications in a three-letter code.

TOP-AND-TAIL :

(of an Enigma crib). Involving the beginning and the end of a message; also (of a menu), made up from such a crib.

TRAFFIC :

Messages or signals, especially code and cipher messages passed by wireless or other means between any two or more particular stations or of a particular type.

TRAIL :

(of a reciphered code message or part-message). To have its starting-point on the subtractor a comparatively short distance after the finishing-point of the last message or part-message sent by the same encipherer; cf. Tailing.

TRANSPOSITION :

An enciphering or reciphering system or process whereby the plain language letters (or figures or letters, etc. of an encoded or enciphered version) of a message are rearranged among themselves according to a key before transmission.

In ordinary transposition the message is written into a cage under the key (q.v.2) from left to right, and copied out column by column according to the order of the figures in the key. One such operation is known as "simple transposition", When a second cage is used the

TRANSPOSITION , (cont'd)

rearranged letters are again written in horizontally from left to right and taken out in columns according to a numerical key which may be the same as that used in the first operation or a different one and the whole enciphering process is called "double transposition". Complications or refinements are often introduced by using irregular cages, e.g. combs or stencils or patterns or by variations in the routing, i.e. direction or order in which the message is written into the cage or taken out of it.

Transposition is also employed in conjunction with substitution, as indicated above.

TRANSPOSITION KEY :

See Key 2.

TRANSPOSITION CIPHER , TRANSPOSITION SYSTEM :

A cipher or cipher system using transposition.

TRIFID :

(of a cipher system or cipher). Characterised by a dividing of each letter of the plain text into three elements (normally the co-ordinates of that letter in a key-cube of 26 (or 27), letters), a systematic rearrangement of these elements, and their substitution, in threes, by the letters of which they are the co-ordinates in the same, or another, key-cube.

TRIGRAM :

A set or group of three letters, figures, letters and figures, or other symbols.

TRIPLET :

(in Naval Enigma). Any one of three consecutive days on which wheel-order and ringstellung are the same, stecker and grundstellung being changed daily, on any particular key.

TRUE :

1. (of the figures or letters of subtractors, code-groups, etc.) (Requiring no further correction to make them) the same as those actually used by the encipherers; (opposed to provisional).

2. (of machine-cipher depths). That are completely in depth, i.e. as distinct from near-depth .

TUNER :

A tuning message.

TUNING MESSAGE :

A message sent normally by the control station, usually immediately after a change of frequency, for the purpose of ensuring that all the stations in the group are correctly tuned in (to the new frequency).

TUNNY :

1. A German electric letter-subtractor, or virtual letter-subtractor, cipher machine using the teleprinter alphabet, and enciphering each of the five impulses constituting a letter separately on a long key produced (in the simplest form of the machine) from four short period components, two of which are common to the five keys and two independent, i.e. from twelve short-period components in all, the periods being all prime to each other. The exact method of operation can only be probably inferred, but the essential character of it can be represented as a mechanical driving so far as the effect of the motor-wheels (q.v.) on the psi wheels is concerned, and as addition (non-carrying) in the scale of 2 so far as the chi and psi wheel patterns affect the plain language impulses.

   Each of the five chi wheels and each of the five psi wheels bears a pattern which can be considered as a succession of ones and noughts (in practice written as crosses and dots), the numbers of ones on any of these wheels being as a rule approximately equal to the number of noughts. In the chi wheels the distribution of ones and noughts is more or less random, i.e. any sign is as likely to be followed by the same sign as by a different sign; but in the psi wheels there are usually many more changes of sign than continuations, apparently in order that the psi-wheel patterns should have an approximately random sequence when extended by the motor.
   (cf. Turing's method and motor).

   Encipherment is effected by the addition (non-carrying) in the scale of two of each of the impulses of a letter to the signs of the appropriate chi and psi wheels which are at the operative position for that letter, the resulting five signs being transmitted as a teleprinter letter. This, on reception, operates, and is operated on by, an identical machine having its twelve wheels set in the same positions as the enciphering machine; and this by the same cycle of operations deciphers the letter and prints the clear equivalent on a tape.

2. Any traffic enciphered on the above machine.

TURING's METHOD :

A method, devised by Mr. Turing, for obtaining the wheel-patterns from a length of Tunny key, utilizing the fact that unextended psi patterns are characterised by many more changes of sign than continuations and the consequent fact that the five extended psi patterns are characterized by either remaining all the same from one position to the next or by all, or nearly all, changing. The key is first differenced at an interval of one, producing at each position, as a result of the above characteristics, either the true chi first differences at that point or the reverse, or almost the reverse, of these. One or two assumptions, usually of the former type (i.e. that the differences are the true differences), are

TURING's METHOD , (Cont'd)

made and repeated at the respective chi periods throughout the differenced key. From the agreement or disagreement of these assumptions with the differences at these periods inferences are made as to whether the true difference or its reverse occurs at that point, and by correlating the results of these inferences the chi first differences (and from these the chi patterns and from these the psi and motor wheel patterns) can be obtained. (in practice it does not matter much whether the original assumption is correct or not as the wrong assumption gives results for the chi first differences which only required to be reversed.)

TURN-OVER :

A usually periodic forward movement of a wheel or other cyclic component of a cipher machine; especially of any wheel other than the fast wheel.

TUTTE's METHOD :

A method, devised by Mr. Tutte, for obtaining the chi wheel-patterns (and hence the psi and motor wheel-patterns) of a tunny cipher message, or for setting chi wheels, of which the patterns are already known (and hence the psi and motor wheels and so deciphering the message), utilizing the psi wheel characteristics described under Turing's method (q.v.) and previously ascertained useful measures of agreement or disagreement between pairs of impulses of the teleprinter letters and other signs constituting the clear text of similar messages. Certain variations in the method can be introduced according to the capacity of the machinery used to apply it , but essentially it consists in adding the two selected impulses of the cipher letters together and differencing the result at an interval of one, (thus largely eliminating the psi wheel contribution, as well as the clear language contribution in so far as the two impulses concerned agree or disagree). The resulting difference, being, in consequence of these eliminations, in appreciably more than fifty per cent of its signs the sum of the first differences of the two chi wheel patterns concerned, is written diagonally into a rectangle combining the two chi periods and this rectangle is resolved into the two chi first difference patterns. Other suitable pairs of impulses are similarly treated until the five chi first differences are all determined. From these the five chi wheel patterns (and their settings for the message) are found, and the chi wheel contributions are subtracted from the cipher text. The resulting de-chi (q.v.) is then examined especially for repeated letters, which often correspond to repeated psi patterns combined with repeated plain letters or other symbols, or for consecutive letters having otherwise significant differences, and the characteristics of extended psi patterns are again utilized to confirm and then to extend 'cribs' located by this means until the complete psi patterns and finally the motor-wheel pattern are obtained.

TWIDDLE :

(in Enigma). To turn round the wheels of an Enigma machine in hand-testing for a particular constatation, esp. in the procedure for setting duds. Cf. Clonk .

TWO-PART :

(of a code-book). Having the code-groups so assigned to the plain language units that when the latter are in alphabetical order the code-groups are not in numerical order, and so involving a second or decode section in which the code-groups are in numerical order and the plain language units not in alphabetical order; non-alphabetical; hatted.

TYPEX :

A British cipher machine.

TYPEX, v :

1. To encipher on a typex.

2. To transmit after encipherment on a typex.

UMKEHRWALZE :

The wheel on the left side of an Enigma machine, fixed in position in some models and designed to turn over in others, serving to connect the twenty-six circuits constituted by the wiring of the other wheels in fixed (or, in some models, in variable) pairs; the returning or reflector wheel.

UNBUTTON :

(in Enigma). To subtract a particular letter or value from each of the letters in both components of a cipher alphabet.

UNDECODABLE :

(apparently misused for). Undecipherable.

UNDERLYING :

(of a code-book). Concealed or disguised in cipher messages by recipherment.

UNDUPED :

(of a cipher text). Of which no alternative (independently intercepted) version is available.

UNENCIPHERED :

(misused for). Unreciphered .

UNRECODED :

(misused for). Unreciphered .

UNRECIPHERED :

(of a code-book or code-groups) Used or sent without recipherment.

VALUATION SYSTEM :

System for evaluating or computing code-groups which have a characteristic limitation. Cf. garble-table .

VALUE LIMITATION :

Feature of code-books or code-groups where the individual units of each group when combined by a given formula have a constant sum or value. Cf. Characteristic .

VALUE SYSTEM :

Valuation system .

VERTICAL :

(of letters, figures, etc.). Written or lying under one another in columns and not side by side in lines.

V.H.F., V/H/F :

Abbreviation of Very High Frequency.

VIENNISMUS :

A practice, observed in a series of Enigma messages originating from Vienna, of assigning successive outside indicators which formed a sequence(e.g. ARN, BSO, CTP), and simultaneously using a different, but similar, sequence of message settings (e.g. KCV, LDY, MEX); (cf. Berlinismus).

VIGENERE ENCIPHERMENT :

Encipherment by means of an alphabetic key and a Vigenere table.

VIGENERE TABLE :

A square table consisting of twenty-six cyclic alphabets, each successive line or column being slid one back from the previous line or column, used for combining letters of plain language and letters of key in certain types of poly-alphabetic ciphers. Letters are added by finding the line with one of them at its left end and the column with the other at its top (or vice versa) and taking as the sum the letter common to such line and column. Letters are subtracted from each other by finding the line with the letter it is desired to subtract at its left, the letter it is desired to subtract this from on this line, and reading off the result at the top of the column in which this occurs, or vice versa i.e. proceeding down a column and then leftwards along a line.

WAHLWORT :

Any non-textual word or phrase used at the beginning or end of German cipher text to avoid stereotyped beginnings and endings; a "padding" word or phrase.

WHEATSTONE MACHINE :

A ciphering device consisting essentially of (1) a circular dial having an outer ring which is divided into 27, and an inner ring which is divided into 26 equal compartments, and (2) two hands pivoted at its centre - the larger serving the outer ring and the smaller the inner - so geared together that for each complete revolution of the larger the smaller turns through one revolution and a twenty-sixth (in other words, so that when the larger hand is advanced any number of compartments round the outer ring, the smaller hand moves forward the same number of compartments round the inner ring). The plain alphabet (with one additional sign) is written in the compartments of the outer ring and the cipher alphabet in those of the inner ring. Enciphering is done by pointing the larger hand at the letters of the plain language in turn, moving it always in the same (clockwise) direction, and writing down the cipher letters indicated by the smaller hand for each. The effect of the difference in the number of compartments in the two rings and the gearing is that the smaller hand is advanced one compartment in relation to the larger for each complete revolution of the larger, thus giving a new cipher alphabet for each of twenty six revolutions, or rather a simple slide of one on the original cipher sequence.

WHEEL :

Used for wheel-pattern; see Pattern.

WHEEL-ORDER :

Order in which the interchangeable wheels, especially of an Enigma Machine, are arranged on a particular day or other period.

WHEEL-SETTING :

Letter or number on rim of wheel of cipher machine serving (usually in conjunction with window or other mark) to indicate position of wheel at commencement of enciphering.

WHEEL TRACK :

(in Enigma machines; esp. machines with numerous turn-overs). Pattern showing position of turn-over-producing teeth or notches in relation to the letters of the alphabet-bearing tyre.

WILLI WILLI :

A short weather message in a special code sent normally by a U-boat reciphered on Enigma using special indicator tables and forming a tie-up with Met. ciphers.

WINDOW :

1. Aperture in cipher stencil through which one or more letters can be written or read.

2. Aperture in inner cover of wheels of a cipher machine through which one of the series of letters or numbers round a wheel can be read, serving as a reference point for setting the wheel.

3. Sequence of cipher or code-groups providing context of group in question (and usually, together with that group, forming 10 groups in all and constituting a unit (normally one line) in a list of cipher or code-groups; also, a list of cipher or code-groups of this character.

WINDOW POSITION :

Position of the wheels of an Enigma machine as shown by the letters or figures in the windows, the ringstellung being correctly set.

W.O. :

Short for Wheel-order.

WORD DIVIDER :

A separator .

WORD SUBTRACTOR :

A subtractor used with a number of different routines, characterized by a to-and-fro or up-and-down movement - the particular routing used being normally denoted by part of the indicator.

W/T :

Short for Wireless telegraphy or wireless telegraphic , esp. as opposed to R/T (radio-telephony, radio-telephonic, which implies speech).

WYLIE BOX :

Wooden frame in which inverse rods can be arranged according to any desired stecker, used to determine rod-pairings when steckered constatations have been punched on masks.

Y SERVICE :

"The organisation responsible for the interception of all enemy and neutral radio transmissions including the operation of D/F Services".

ZENIT :

1. A message containing the weather observations made by a German aircraft on a meteorological flight.

2. The cipher used by a German aircraft for transmitting such messages to its base.

ZIP :

A report originating in B.P.

ZODIAC :

The special form of zenit employed when zenit observations are rebroadcast in a German Naval collective.

ZONING :

1. Arrangement in zones or sections.

2. A limitation in a code book consisting in the restriction of particular classes of code-groups to particular classes of plain language units, e.g. the use of groups beginning with a particular figure or letter for words beginning with a particular letter or particular letters.

ZUSATZWALZE :

The fourth wheel (i.e. fourth from the right) of a four-wheel Enigma machine, not interchangeable with the other wheels and not turning over during the encipherment of a message, but capable of being set in any of twenty-six positions and so together with the Umkehrwalze providing in effect a set of twenty-six different Umkehrwalzen.