

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

- 31 -

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, Ringstellung 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;

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.

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

- 34 -

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.

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

- 35 -

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.

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

- 36 -

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 constations 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.

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

- 37 -

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 constation 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.

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

- 38 -

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.

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

- 39 -

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.

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

- 40 -

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.

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

- 41 -

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.

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

- 42 -

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.

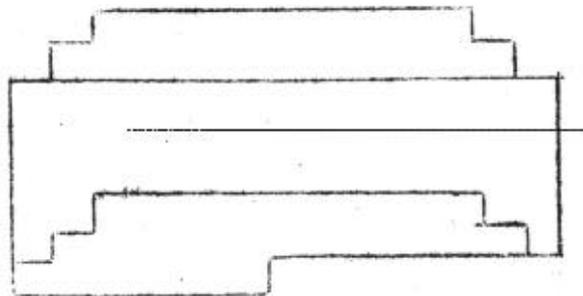
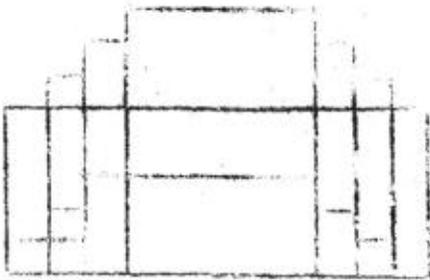
(continued)

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 :

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

- 44 -

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.

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

- 45 -

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.

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

- 46 -

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.

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

- 47 -

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 deciphered 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 very short key is called a "recurring key".

b. The group of key-figures used to decipher 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 decipherment.
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 deciphered 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.

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

- 48 -

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 subtracting 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 .

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

- 49 -

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 deciphered 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).

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

- 50 -

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.

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

- 51 -

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 Umkerwalze), producing a cipher alphabet which is equal to the previous cipher alphabet unbuttoned one.

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

- 52 -

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.

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

- 53 -

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 constataions 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 dsteckered constataions punched on it, used on an inverse-rod square (or having steckered constataions 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 electro-mechanically reproduced.

MATE :

To match or fit (a crib).

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

- 54 -

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 constations 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.

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

- 55 -

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.

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

- 56 -

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 superposed, 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.

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

- 57 -

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 alphabet).

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.

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

- 58 -

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.

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

- 59 -

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 teleprinter 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 reversible.
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 :

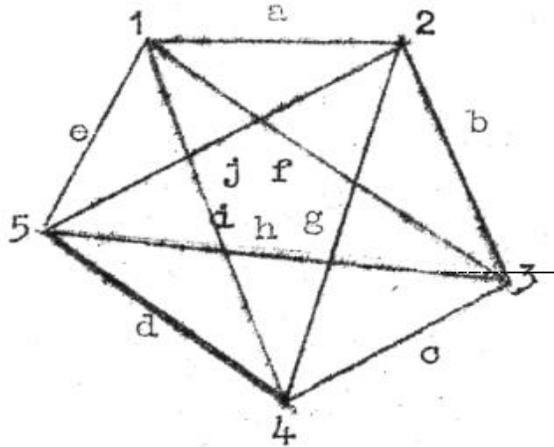
Having a recognizable or characteristic pattern.

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.