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.

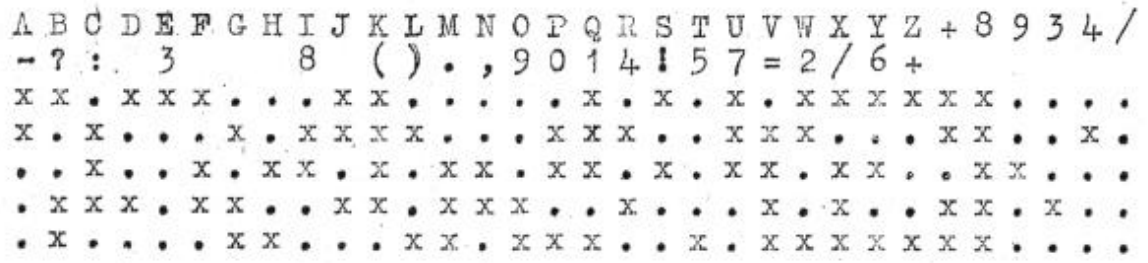
TELEPRINTER ALPHABET :

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.