SECURITY CLASSIFICATION (If any)

CONFIDENTIAL

DISPOSITION FORM

FILE NO.

SUBJECT Basic Cryptologic Glossary

TO Chiefs, Offices and Staff Divisions

FROM TNG

DATE 25 Aug 54

COMMENT NO. 1

J. E. Carroll, 60317, ms

1. The attached glossary in draft form is submitted for your consideration and comment. It is requested that the glossary be given the widest practicable distribution, and that all interested parties be urged to make comments and suggestions as to possible revisions, additions and deletions. It will be appreciated if military members of NSA will study the glossary from the point of view of their particular Services, and make whatever suggestions they may deem appropriate. All such comments and suggestions will aid greatly in the preparation of a definitive edition which will be considered as prescriptive, and which should thus contribute toward the eventual standardization of cryptologic terminology within the Agency and the Services.

2. In order that the glossary may go to press as soon as possible, it is requested that the drafts with comments be returned to the Training Division by 10 October 1954.

SHELBY L. PATTERSON
Lt. Colonel, USAF
Chief, Training Division

Incl:
a/s

CONFIDENTIAL

NATIONAL SECURITY AGENCY
Washington 25, D. C.

BASIC CRYPTOLOGIC GLOSSARY

Training Division
7 July 1954

Explanatory Notes

1. This glossary is the first of a series of NSA prescriptive cryptologic glossaries. In its preparation, an effort has been made to bring together, for ready reference, the terms most frequently encountered in current cryptologic literature. Many of these terms, although frequently encountered, were found defined only in various specialized, very limited, or out-of-print glossaries and manuals. In the process of compilation, a further effort has been made to eliminate obsolete or obsolescent terms, to clarify or to complete those definitions which seemed obscure or incomplete, and in certain cases, to make a choice among various terms which referred to the same object, method, etc. Besides the limitation imposed by the selection of only the most common cryptologic terms, a further limitation has been imposed by the desire to keep the security classification as low as possible in order to permit the widest possible dissemination of the glossary, and thus increase its usefulness. Work has begun on the preparation of an unabridged glossary, of which the present glossary is to serve as a nucleus, and in which less common terms and terms of higher classification are to be included.

2. The terms in the present glossary are arranged in strictly alphabetical order, disregarding word spaces and hyphens. Single words and certain hyphenated words are followed directly by an abbreviation of the part of speech. Run-on entries, indicating a part of speech different from that of the main entry are shown simply by means of a series of dashes followed by the abbreviation of the part of speech, and the appropriate definition. Underlining of terms in the text of the definitions in a few cases indicates emphasis, but in most cases indicates that the term is defined elsewhere in the glossary. Abbreviations used for parts of speech, as well as those used to indicate examples, cross-references, etc., are those listed in Webster's New International Dictionary, Second Edition.

BASIC CRYPTOLOGIC GLOSSARY

A. Used as a symbol in various classification and evaluation systems, as follows: 1. In traffic analysis, to describe the validity of an identification or location as "confirmed" or "certain." 2. In intercept operations as a suffix to a frequency to denote "average". 3. In D/F bearing observation classification, to indicate that all bearings are within an arc of 4 degrees. 4. In D/F fix evaluation, to indicate a 90% probability that the true position of a given transmitter is within 25 miles of the fix.

accidental repetition. A repetition produced fortuitously, and not by the encipherment of identical plaintext letters by identical keying elements. Cf. causal repetition.

acknowledgment, n. A separate message from the addressee informing the originator that his message has been received and is understood.

action addressee. The activity or individual to whom a message is directed by the originator for action (in contrast to information addressee).

additive, n. A single digit, a numerical group, or a series of digits which, for the purpose of encipherment, is added to a numerical cipher, code group, or plain text.

additive book. A book comprising a group of additive tables.

additive position. The location within a long key of a particular additive (e.g., the page and line and column on that page where a specific additive appears).

additive system. A cryptosystem in which encipherment is accomplished through the application of additives.

additive table. A tabular arrangement of additives.

address, n. External or internal indication of message destination.

addressee, n. The office, headquarters, activity, or individual to whom a message is directed by the originator.

address group. A group of letters or numbers or both, assigned to represent one or more commands, authorities, activities, or units.

ADFGVX system. A German high-command cipher system used in World War I. Essentially, a biliteral substitution system employing a 6 x 6 square, to which a columnar transposition was subsequently applied.

agency of signal communication. The organization, teams, and personnel necessary to perform operational duties pertaining to signal communications.

allocation, n. The assignment or distribution of call signs, frequencies, code names, etc., (e.g., the allocation of call signs to radio stations in a net).

alternate group. See variant.

alternate vertical route transposition. Columnar transposition in which the route followed is alternately down and up, or up and down.

anagram, n. Plain language reconstructed from a transposition cipher by restoring the letters of the cipher text to their original order.---- v.t. To cryptanalyze a transposition cipher in whole or in part by combining one series of characters with another series from the same message to produce plain text, plaincode, or intermediate cipher text.

analogue, n. A machine which produces the same cryptography as another machine although the two machines may vary.

aperiodic system. A cryptographic system in which the method of keying results in the suppression of patent cyclical phenomena in the cryptographic text.

apparent period. The period usually ascertained first as a result of the study of the intervals between repetitions. This may be a secondary period, and may or may not be broken down into component primary periods. Cf. basic period.

apparent setting. In a cipher machine, the alignment of the rotors as represented by the particular letter on each which is aligned with the bench mark.

applique unit, teleprinter. A special cipher attachment used in connection with a teleprinter to provide cryptographic treatment for teleprinter messages.

arbitrary group. A group arbitrarily derived, as the decipherment of an enciphered-code group, a relative code group.

artificial word. A group of letters having no real meaning, constructed by the systematic arrangement of vowels and consonants so as to give the appearance and pronounceability of a bona fide word.

authentication, n. A security measure, usually involving a challenge and reply, designed to protect a communication system against fraudulent transmissions.

authentication element. A group of letters or numbers selected from a prearranged table serving as a test element in authentication procedure.

authenticator, n. A symbol or group of symbols selected in a prearranged manner and usually inserted at a predetermined point within a transmission for the purpose of attesting to the authenticity of the message or transmission.

autoencipherment, n. Encipherment by means of an autokey system, q.v.

autokey system. An aperiodic substitution system in which the key, following the application of a previously arranged initial key, is generated from elements of the plain or cipher text of the message.

auxiliary code. See supplementary code.

auxiliary table. In certain code books which have two meanings assigned to one group, that portion of the code which includes the second, or subsidiary, meaning only, the employment of which is normally indicated by a switch group. Cf. main table.

average frequency. The particular frequency derived by averaging several measured frequencies which are approximations of one basic frequency on which a target is observed working. (Appears with an "A" suffixed to the frequency.)

axis of signal communications. The line or route on which lie the starting position and probable future location of the command post of a unit during a troop movement. The main route along which messages are relayed or sent to and from combat units in the field.

B. Used as a symbol in various classification and evaluation systems, as follows: 1. In traffic analysis, to describe the validity of an identification or location as "highly probable". 2. In D/F bearing observation classification, to indicate that all bearings are within an arc of 10 degrees. 3. In D/F fix evaluation, to indicate a 90% probability that the true position of a given transmitter is within 50 miles of the fix.

Baconian cipher. A cipher system invented by Sir Francis Bacon (1561-1626). It is basically a monoalphabetic substitution system in which single plaintext letters are represented by five-letter cipher equivalents formed by permutations of two letters taken five at a time.

base, n. 1. A true code group or other substituted group or unit after the true key has been removed. 2. A value arbitrarily assigned to code groups when the true digits are not yet determined, such that the assigned value differs from the true by an amount which is constant for each group.

base letter. The character of the plain component against which the key element of the cipher component is juxtaposed.

base number. (Met.) A number, usually consisting of three digits, identifying a meteorological observation center and almost always transmitted as the first element in a meteorological report. Also called station indicator or IMC number.

basic book. The code book of an enciphered code system.

basic call sign. A constant group which is assigned to a particular radio station and used for the purpose of deriving the secret call sign of that station.

basic code. Plain code before encipherment, or resulting from the reduction of enciphered code groups to a common base by the removal of key.

basic period. A period, hidden or latent, which constitutes a basic element of a cryptographic system and which may act or be acted upon to produce a much longer external or apparent period. Cf. apparent period.

basket, n. A removable component of a cipher machine, made up of separators and endplates, in which rotors revolve.

baud, n. A mark or space impulse in the international (Baudot) teleprinter code.

Baudot alphabet. The 32-element alphabet employed in the Baudot code.

Baudot code. A five unit code applied to teleprinter systems by Jean Maurice Emile Baudot (1845-1903). It employs a 32-element alphabet composed of permutations of two elements taken five at a time. Also called the international teleprinter code.

BC. Broadcast, q.v.

bearing. In direction finding, the angle in degrees (reading clockwise) between true north and the line from the observer to the target.

Beaufort system. A polyalphabetic substitution system employing a key word in connection with a Vigenère square, but differing from the normal Vigenère method in its rules for application of the key.

begin spell. The plain equivalent of a code group indicating that the groups following represent elements taken from the syllabary.

Berne list. A listing of permanent radio call signs allocated to member nations and published by the International Telecommunications Union (formerly in Berne, now in Geneva, Switzerland).

Berne-type call. A semipermanent or permanent call sign in the correct nationality allocation block, but one not listed in the Berne publications.

biliteral, adj. Of or pertaining only to cryptosystems, cipher alphabets, and frequency distributions which involve cipher units of two letters or characters. See the more inclusive term digraphic; see also biliteral frequency distribution.

biliteral alphabet. A cipher alphabet involving a cipher component composed of two-character units.

biliteral frequency distribution. A frequency distribution of pairs formed by combining successive letters or characters. Thus, a biliteral distribution of ABCDEF would list the following pairs: AB, BC, CD, DE, EF. Cf. digraphic frequency distribution.

binary addition. Addition according to the modulus two.

binary counter. A device which counts to the base two.

binary net. A net consisting of two stations communicating with each other on the same frequency.

bipartite alphabet. A biliteral alphabet in which the cipher units may be divided into two separate parts whose functions are clearly defined, viz., row indicators and column indicators of a matrix.

bipartite system. A substitution system involving the use of a bipartite alphabet.

bisection, n. A process used in preparing plain text for encryption. It consists of dividing the plain text of a message into two segments or portions usually of unequal length, transposing the segments so that the actual beginning and ending of the message are buried, and in indicating the true beginning and ending in a distinctive manner.

blank, n. 1. A code group or cipher symbol to which no plain meaning has as yet been assigned. 2. Any symbol that does not appear in the cipher text, and hence does not appear in a frequency distribution. 3. A blacked-out cell in a matrix.

blank expectation test. See lambda test.

blind, adj. As applied to transmission, carried on without expectation of a reply. ---adv. blindly

blind sending. Transmission to a station without the knowledge that the transmission is being received by the station addressed.

block, n. 1. A matrix; a square, rectangle, or other geometrical design containing letters, figures, or other symbols. 2. A series of code groups and their plaintext values grouped according to alphabetical or numerical order to form a section of a blocked code.

blocked code. A form of modified one-part code in which the code groups and their corresponding plaintext values are arranged in alphabetical or numerical order within blocks. It differs from a normal one-part code in that the blocks are not in alphabetical or numerical order with relation to one another.

Boehme equipment. 1. Transmitting: Used for sending International Morse Code characters by passing Wheatstone tape through a keying head. 2. Receiving: Used for recording International Morse Code characters by ink syphon equipment on a moving paper tape.

book-breaker, n. A cryptanalyst who specializes in the recovery of plaintext values in code books.

book-breakers' index. A type of IBM code index in which the code group is replaced by its plaintext value when known, whether the code group is in control position or offset position.

book-breaking, n. Codebook reconstruction. The cryptanalytic recovery of the plaintext values in a code book.

book cipher. A cipher system, utilizing any agreed upon book, in which the cipher identifies a plain element present in the book.

book message. A message destined for two or more addressees, the content of which requires no coordination among addressees. Each addressee must be indicated as action or information.

break, n. 1. A pause between the heading and body of a message, between the body and signature, or elsewhere in the message. 2. An interruption in the transmission of a message by electrical means. 3. In solution, the initial entry into a system or element thereof.

brevity code. A code which has as its sole purpose the shortening of messages rather than the concealment of content. Also called condensation code.

broadcast, n. A transmission intended for general reception rather than directed to a particular addressee.

broadcast method. The method of transmitting a message by which the stations called do not answer the call, and do not receipt for the message or otherwise transmit in connection with its reception. The prosign "F" in the preamble or final instructions identifies a message sent by this method. Also known as "F" (FOX) method.

brute force method. An analytical machine method of comparing encrypted messages with each other with a view to discovery of coincidences which may aid in the proper alignment of the messages for overlapping. The resultant listing is known as a brute force run.

brute force run. An IBM listing of the data obtained by the brute force method.

BT. A prosign used as the last element of the heading and the first element of the message ending to separate the text from the other parts of the message.

bury, v.t. To place elements of a message, (e.g., call signs, addresses, signatures, etc.), in other than their usual place. To hide or conceal in the text of a message.

bust message. A message containing an error in encipherment which jeopardizes the cryptographic security of the message, and thus is potentially valuable to the cryptanalyst.

C. Used as a symbol in various classification and evaluation systems, as follows: 1. In traffic analysis, to describe the validity of an identification or location as "probable." 2. In intercept operations as a suffix to a frequency to denote "confirmed." 3. In D/F bearing observation classification, to indicate that all bearings are within an arc of 20 degrees. 4. In D/F fix evaluation, to indicate a 90% probability that the true position of a given transmitter is within 100 miles of the fix.

C/A. Cryptanalysis, q.v.

Caesar's cipher. An ancient form of simple substitution cipher in which each plaintext letter was replaced by the letter three places to the right of it in the normal alphabet; attributed to Julius Caesar.

call sign. A group of letters or numbers, or a combination of both, used as the identification for a telecommunication station (or stations), when stations are establishing contact with each other.

callsign, adj. Of or pertaining to a call sign or call signs; as callsign generation.

call-up. A set of signals used by a radio station to establish contact with another and to prepare for the transmission of traffic; also the part of a transmission containing such signals.

call word. (Radiotelephony) A bona fide word used in place of a call sign.

caption code. A code in which the phrases are listed under separate headings based upon the principal word or idea in the entire phrase.

case number. An arbitrary notation assigned by a communication intelligence agency to designate a target, link, group, net, etc., as identified by that agency.

causal repetition. A repetition produced by the encipherment of identical plaintext letters by identical keying elements. Cf. accidental repetition.

cell, n. An individual small square on cross-section paper, grilles, etc.

chadded tape. Perforated teleprinter tape; also known as "fully-chadded tape." Cf. chadless tape.

chadless tape. Partially-perforated teleprinter tape, overprinted. Cf. chadded tape.

chain, n. In its cryptologic application, a series, usually cyclic, of letters or other textual symbols following one another according to some rule or law. ---v.t. To form into chains.

chain of command. That part of Order of Battle indicating the organizational structure, usually reflected in the structure of administrative radio nets.

challenge and reply. A procedure for the exchange of authentication between two transmitters, the challenge being a transmission of test elements selected from a prearranged table; the reply, an appropriate response determined according to the prearranged system, establishes the authenticity of the answering station.

change-hour indicator. An enciphered indicator in a collective weather broadcast to show that the reported observations which follow were made at a different hour from those preceding it.

change-type indicator. An enciphered indicator inserted in a collective weather broadcast to make clear that the reported observations which follow are not of the same type as those which preceded it.

changing call sign. An assigned call sign which is changed periodically according to a prearranged system.

channel, 1. A band of frequencies. 2. A unit or subdivision of a link. 3. One of the grooves on a strip-board into which alphabet strips are inserted.

channel board. A base made of metal, paper, plastic, or similar material containing a series of channels into which alphabet strips may be inserted and slid.

characteristic, n. 1. Any distinguishing feature. 2. A property of a textual group expressed numerically and resulting from one of several possible arithmetical processes applied to digits of the group.

characteristic frequency. See normal frequency.

chat. See chatter.

chatter. Any transmission between operators on a communication link other than an actual message.

check decryption. 1. The process of insuring by decryption, prior to transmission of an encrypted message, that proper cryptoaids have been employed, and that the encryption of a message was properly accomplished.

check group. A transmitted group which, by giving the indicator or other information in a second form, serves as a check.

check symbol. A single character acting as a check. Cf. check group.

chiastic, adj. In general, arranged or shaped in the form of the Greek letter chi (χ). In its cryptologic application, pertaining to any transposition system involving an interchange of elements according to an X-shaped pattern.

chi square (χ^2) table. A mathematical table listing the probabilities of occurrence by chance of a chi-square value higher than those observed in a given case; an adjunct to the chi-square test.

chi-square (χ^2) test. A mathematical means for determining the relative likelihood that two distributions derive from the same source. For example, the test can be used to aid in the determination of whether a distribution is more likely to be random or not; in this usage, the observed distribution is compared with a theoretical distribution representing that which is expected for random. The end result of the test is a value representing the discrepancy between the two distributions which have been compared. This value, called a "chi-square value" may be interpreted as it is, or it may be interpreted through the use of a chi-square table.

chi (χ) test. A test applied to the distributions of the elements of two cipher texts either to determine whether the distributions are the result of encipherment by identical cipher alphabets, or to determine whether the underlying cipher alphabets are related. Also called the cross-product test.

cifax, n. Enciphered facsimile. The process of converting a plane image into an unintelligible image or series of electrical impulses and of reconverting it or them into intelligibility through the use of a key. ---adj. Using or pertaining to cifax.

CI message. Any message giving cryptologic instruction or information.

cipher, n. 1. A cipher system. 2. A cryptogram produced by means of a cipher system.---adj. Pertaining to that which enciphers or is enciphered. See also ciphertext.

cipher alphabet. An ordered arrangement of the letters (or other conventional signs, or both) of a written language and of the characters which replace them in a cryptographic process of substitution.

cipher clerk. A clerk who enciphers and deciphers messages.

cipher component. The sequence of a cipher alphabet containing the symbols which replace the plain symbols in the process of substitution.

cipher device. A nonmechanical and nonelectrical apparatus used for enciphering and deciphering.

cipher disk. A cipher device consisting of two or more concentric disks, each bearing on its periphery one component of a cipher alphabet.

cipher machine. A mechanical or electrical apparatus for enciphering and deciphering.

cipher square. An orderly arrangement or collection of sequences set forth in a rectangular form, commonly a square (e.g., a Vigenère square).

cipher system. Any cryptosystem in which cryptographic treatment is applied to textual units of regular length, usually monographic or digraphic Cf. code system.

cipher text. The text of a cryptogram which has been produced by means of a cipher system.

ciphertext, adj. Of or pertaining to the encrypted text produced by a cipher system or to the elements which comprise such text; as the ciphertext distribution. Often shortened to cipher.

ciphony, n. Enciphered telephony. The process of converting vocal communications into unintelligibility and of reconverting them into intelligibility through cryptographic treatment. ---adj. Using or pertaining to ciphony.

circuit, n. Generally speaking, a communications path between two or more points. Cf. channel, link, lane.

circular message. See book message.

citrol, n. The process of converting control and telemetering signals, such as those used in missile guidance, into unintelligibility and reconverting them into intelligibility through cryptographic treatment. ---adj. Using or pertaining to citrol.

civision, n. Enciphered television. A system of converting television signals into unintelligible signals and vice versa, in accordance with certain predetermined procedures. ---adj. Using or pertaining to civision.

clandestine traffic. 1. Traffic transmitted without the authority of the government of the country in which the transmitter is located. 2. Unauthorized traffic transmitted by an authorized transmitter. 3. Traffic transmitted in violation of the International Telecommunications Convention and Regulations.

classification, n. The security grading of a given message or other material.

classification group. A group, indicating the security classification of a message.

classify, v.t. 1. To assign a security classification. 2. In the early stages of code solution, before code groups are identified as to specific meaning, to segregate the code groups appearing in traffic into classes or sets of groups, based upon their distinctive behavior in the messages; for example, into those groups representing numbers, spelling groups, punctuation, nulls, or indicators.

clear. See plain.

clear text. Plain text, q.v.

code, n. 1. A code system. 2. A code book. ---adj. Pertaining to that which encodes or is encoded.

code book. A book or document used in a code system, arranged in systematic form, containing units of plain text of varying length (letters, syllables, words, phrases, or sentences) each accompanied by one or more arbitrary groups of symbols used as equivalents in messages.

codebook reconstruction. Book-breaking, q.v.

codebook recovery. See book-breaking.

code chart. A chart in the form of a matrix containing letters, syllables, numbers, words, and occasionally, phrases. The matrix has row and column coordinates for the purpose of designating the plaintext elements within.

code clerk. A clerk who encodes and decodes messages.

coded speech. The output of any device which changes in a nonsecret manner a signal derived from plain speech to another kind of signal preparatory to its encipherment in ciphony.

code group. A group of letters or numbers, or a combination of both, assigned (in a code system) to represent a plaintext element.

code index. A numerical or alphabetical listing of placode groups with preceding and succeeding groups, compiled from a number of messages.

code message. A cryptogram produced by encodement.

code system. A cryptosystem in which arbitrary groups of symbols represent plaintext units of irregular length, usually syllables, whole words, phrases and sentences.

code table. A short code in tabular form.

code text. The text of a cryptogram which has been produced by means of a code system.

code word. 1. A word which conveys an agreed upon meaning rather than its conventional meaning. 2. A cover name.

codress, n. A type of message in which the entire address is contained only in the encrypted text.

codress procedure. A procedure in which the full address (including the originator, the action addressee, and information addressee, if present) is buried and encrypted within the text.

coincidence test. The kappa test. A statistical test applied to two ciphertext messages to determine whether they both involve encipherment by the same sequence of cipher alphabets.

collateral information. In communication intelligence usage, information other than that derived from a study of intercepted communications.

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

collective call sign. A single call sign used for calling two or more stations simultaneously.

co-locate, v.t. To ascertain by analytic or other means that two transmitters, stations, or units are at the same place.

column, n. A vertical sequence of letters or numbers or groups thereof.

columnar transposition. A method of transposition in which the ciphertext equivalent of a message is obtained by transcribing the columns of a matrix into which the message was inscribed earlier according to some scheme other than this vertical one.

column coordinate. A symbol normally at the top of a matrix or cryptographic table, identifying a specific column of cells, used in conjunction with a row coordinate to specify an individual cell in the matrix or table. Also called column indicator.

column designator. See column coordinate.

column indicator. See column coordinate.

comb, n. A matrix with an irregular marginal blank pattern caused by variations in the length of the rows.

combined, adj. Between two or more forces or agencies of two or more Allies. (When all allies or Services are not involved, the participating nations and Services shall be identified: e.g., Combined NATO Navies.)

COMINT. Communication intelligence, q.v.

communication center. A communication agency charged with the responsibility for receipt, transmission, and delivery of messages. It normally includes a distribution center, a message center, a crypto-center, and transmitting and receiving facilities. Abbreviated as comm. cen. Also known as signal center.

communication concealment. All methods of hiding from the enemy the fact or method of communication.

communication intelligence. Evaluated and interpreted information derived from the study of intercepted communications.

communication intelligence analysis. Methods of deriving information from the communications of others. This term includes the interception of messages, location of transmitters, the solution of codes and ciphers, etc.

communication security. The protection resulting from all measures designed to deny to unauthorized persons information of value which might be derived from communications. Cryptosecurity, transmission security, and physical security are the components of communication security. Abbreviated as COMSEC.

commutative, adj. As applied to cipher matrices, so constructed as to permit coordinates to be read in either row-column or column-row order without cryptographic ambiguity.

complement, n. The difference between any integer and 10.

complex receiving. The system of radio frequency usage wherein two or more stations are assigned receiving frequencies; thus, a station when sending to another station will use the frequency assigned to the receiving station.

complex sending. The system of radio frequency usage wherein two or more stations are assigned transmitting frequencies, and each transmitter uses its assigned frequency to contact the other stations.

complex star. The system of radio frequency usage wherein the net control station transmits on one frequency to its outstations, the outstations transmitting to the control station on other frequencies.

component, n. One of the two sequences (plain and cipher) which compose a cipher alphabet.

composite code book. A list of the most common code groups in all available codes in a given language, arranged in decoding order and including plaintext values and frequencies where known. Its principal function is to serve as an aid in code identification.

composite difference book. A numerical listing of the minor differences between the most frequent code groups in all known codes in a given language. It is used to determine whether the plain code underlying an additive system is a known code.

compromise, n. The loss of security of a classified document, information, or material, which results from an unauthorized person or persons having knowledge thereof.

COMSEC. Communication security, q.v.

concealment system. A method of secret communication so designed as to convey a secret message without its presence being suspected by others than the addressee. In its most usual form, the plaintext elements are concealed by combining them with extraneous plaintext elements in such a way that the end result is an intelligible and apparently innocent message. Cf. open code.

condensation code. A code which has as its sole purpose the shortening of messages rather than the concealment of content. See brevity code.

condenser, n. A means of condensing code groups composed of digits into smaller groups composed of letters.

CONFIDENTIAL. A security classification pertaining to defense information or material, the unauthorized disclosure of which could be prejudicial to the defense interests of the nation.

confirmed frequency. The frequency on which a target is known to operate. Confirmation is obtained by compromise or by continued intercept.

continuity, n. Identity with respect to a series of changes. In cryptanalytic procedure, the maintenance of continuity involves keeping current a systematic record of changes in such variable elements as indicators, keys, conversion squares, discriminants, etc., on a given cryptochannel. In traffic analysis, the maintenance of continuity involves the tracing of changes in call signs, frequencies, schedules, or other variable elements assigned to a given radio station, link or net.

control, n. 1. A combination of letters or digits which determines the source of the keys by which the discriminant, indicator, address, or signature groups have been enciphered; because it depends upon some element of the message text, the control varies from message to message. 2. net control station, q.v.

control station. See net control station.

control traffic. Dummy traffic transmitted for the purpose of misleading enemy traffic analysts. Control traffic can be employed merely to hide an operation through maintaining a volume level on all nets, or it can be used deliberately to deceive by creating high volumes at points of slight military activity.

conversion square. A cipher square used in certain numerical cryptosystems to provide arbitrary cipher equivalents for the various key-plain combinations. It is normally a 10x10 Vigenère, non-Vigenère, or Latin square, in which each row contains all of the ten digits arranged in a mixed sequence; thus there is never a repeated digit within a single row.

converted code. A new edition of a code prepared by applying some form of encipherment to each of the individual code groups of the original codebook.

coordinate, n. See row coordinate and column coordinate.

copy, n. A written record of an intercepted radio transmission. Cf. recording and transcription (2). ---v.t. To prepare a written record of a radio transmission.

correction factor. The constant relation between a group of code or of key in relative form and a code or key in its original or primary form.

cover, n. 1. The provision for intercepting radio signals, especially those of a particular link, group, etc. 2. The concealment of undesirable traffic patterns, characteristics, address combinations, etc., as a communication security measure.

coverage, n. The degree to which intercept cover is applied or achieved.

coverage study. A study of the extent and nature of communications intercepted in order to ensure adequate interception.

cover call sign. A group used in place of an originator or addressee designation in a message heading for deception purposes, the actual originator or addressee identification appearing in the encrypted text.

crest, n. In its cryptologic application, a point of high relative frequency in a frequency distribution.

crib, n. 1. Plain text assumed or known to be present in a cryptogram. 2. Keys known or assumed to have been used in a cryptogram. ---v.t. To fit assumed or known plain text or keys into the proper position in an encrypted message.

crib dragging. A method of cryptanalytic attack in which a crib is assumed successively in every position throughout the text of a message.

cross cribbing. A process by which plain text from a message encrypted in one system is assumed to be present in a message encrypted in another system.

cross-product text. See chi test.

crown, n. In transposition solution, that part of a hat diagram containing textual units not definitely located as to column.

crypt-, crypto-. In general, a combining form meaning "hidden", covered", or "secret". Used as a prefix in compound words, crypt-, crypto-, pertains to cryptologic, cryptographic, or cryptanalytic, depending upon the use of the particular word as defined.

cryptanalysis, n. The steps and operations performed in applying the principles of cryptanalytics.

cryptanalyst, n. A person versed in the art of cryptanalysis.

cryptanalytic, adj. Of, pertaining to, or used in cryptanalytics.

cryptanalytics, n. That branch of cryptology which deals with the principles, methods, and means employed in the solution or analysis of cryptosystems.

cryptanalyze, v.t. To solve by cryptanalysis.

crypto-aid, n. Any table, mechanism, or device employed in the encryption or decryption of a message.

cryptoboard, n. In U.S. Navy usage, personnel assigned to encrypting and decrypting messages.

cryptocenter, n. An establishment maintained for the encrypting and decrypting of messages.

cryptochannel, n. A complete system of crypto-communication between two or more holders.

crypto-communication. Any communication that has been encrypted.

cryptodate, n. The date which determines the specific key to be employed.

cryptodevice, n. Any device employed in the encryption or decryption of a message.

cryptogram, n. A communication in visible writing which conveys no intelligible meaning in any known language, or which conveys some meaning other than the real meaning.

cryptographer, n. One who encrypts or decrypts messages or has a part in making a cryptographic system.

cryptographic, adj. Of, pertaining to, or concerned with cryptography.

cryptographic ambiguity. Uncertainty as to the method of decryption or as to the meaning intended after decryption; created by a fault in the structure of a cryptosystem.

cryptographic arithmetic. The method of modular arithmetic used in cryptographic procedures which involves no carrying in addition and no borrowing in subtraction.

cryptographic section. The component of a communication center whose function is to encrypt outgoing classified messages and decrypt incoming classified messages.

cryptographic security. See cryptosecurity.

cryptographic system. See cryptosystem.

cryptographic text. Encrypted text; the text of a cryptogram.

cryptography, n. That branch of cryptology which treats of the means, methods, and apparatus for converting or transforming plaintext messages into cryptograms, and for reconverting the cryptograms into their original plaintext form by a simple reversal of the steps used in their transformation.

cryptolinguistics, n. The study of those characteristics of languages which have some particular application in cryptology, (e.g., frequency data, word patterns, unusual or impossible letter combinations, etc.).

cryptologic, adj. Of, pertaining to, or concerned with cryptology.

cryptology, n. That branch of knowledge which treats of hidden, disguised, or encrypted communications. It embraces all the means and methods of producing communication intelligence and maintaining communication security; for example, cryptology includes cryptography, cryptanalytics, traffic analysis, intercept, specialized linguistic processing, secret inks, etc.

cryptomannerism, n. A habit of a message writer or cryptographer which results in a stereotype.

cryptomaterial, n. All documents, devices and machines employed in encrypting and decrypting messages.

cryptomathematician, n. One versed in cryptomathematics.

cryptomathematics, n. Those portions of mathematics and those mathematical methods which have cryptologic applications.

cryptonet, n. A group of stations using the same cryptosystems for intercommunication.

crypto-operating instructions. In cryptography, instructions describing the methods to be employed in the operation of a general cryptographic system. This includes a description of the general cryptographic system as well as the method of application of specific keys.

cryptoperiod, n. The specific length of time throughout which there is no change in cryptographic procedure (keys, codes, etc.).

cryptosecurity, n. That component of communication security which results from the provision of technically sound cryptographic systems and from their proper use.

cryptosystem, n. The associated items of cryptomaterial and the methods and rules by which these items are used as a unit to provide a single means of encryption and decryption. A cryptosystem embraces the general cryptosystem and the specific keys essential to the employment of the general cryptosystem.

cryptotext, n. See encrypted text.

C/S. Call sign.

CT. Control station. See net control station.

custodian, n. The individual designated by proper authority to be responsible for the custody, handling and safeguarding of registered matter or other classified matter which is subject to special handling and accounting procedures.

cut. 1. The position of a point of division relative to the beginning of the text of an encrypted message. See on the cut and off the cut. 2. The point of intersection of two D/F bearings.

cut-in. A message, the first part of which was not intercepted.

cut numbers. 1. Numbers transmitted in Morse according to a scheme of abbreviation in which all dashes except one are omitted. Thus the numbers 1 to ∅ are represented by A, U, V, 4, 5, 6, B, D, N, and T, respectively. 2. Any system of abbreviated Morse numbers, as letter-for-number substitution.

cycle, n. Any series which recurs or is expected to recur in the same order. See period.

cycle interrupter. An element within the message which signifies the point at which, and also possibly the extent to which, cycle interruption occurs.

cycle interruption. A cryptographic procedure applied in the operation of some cipher systems whereby the normal cyclic progression is modified.

cyclic, adj. Periodic; continuing or repeating so that the first term of a series follows the last; characterized by a ring or closed-chain formation.

cyclic permutation. Any rearrangement of a sequence of elements which rearrangement merely involves shifting all the elements a common distance to the right or left of their initial positions in the sequence, the relative order remaining undisturbed; such a rearrangement requires that one consider the basic sequence as being circular in nature so that, for example, shifting that element which occupies the left-most position in the sequence one place to the left places this element in the right-most position.

cyclic phenomena. Periodic recurrences of repetitions in a system which uses a repeating key.

cyclometric, adj. Pertaining to any motion which is of a meter-like character.

D. Used as a symbol in various classification and evaluation systems as follows: 1. In traffic analysis, to describe the validity of an identification or location as "tentative". 2. In D/F bearing observation classification, to indicate that one or more bearings are outside an arc of 20 degrees. 3. In D/F fix evaluation, to indicate a 90% probability that the true position of a given transmitter is within 200 miles of the fix.

dah, n. A dash in Morse code.

daily keying element. That part of the specific key that changes at predetermined intervals, usually daily.

date break. The date on which a change in cryptographic procedure, keys, code, etc. takes place.

date period. The inclusive dates during which a certain cryptosystem or procedure is in effect.

date rota. A system in which a limited number of elements, such as call signs or frequencies, is repeated in a regular pattern, as on certain dates of each month.

date-time group. A transmitted group of a message giving the day of the month and the time, usually according to the twenty-four-hour clock. In U.S. practice a group usually composed of six digits, the first pair representing the day of the month, the second pair the hour of the day, and the final pair the minutes after the hour. A letter or letters may be added to indicate the time zone.

deception, n. Any practice carried on within a communications system for the purpose of confusing or misleading the enemy.

decimated alphabet. An alphabet produced by decimation, q.v.

decimation, n. The process of selecting members of a series by counting off at a chosen interval, the original series being treated as cyclic; or the result of the foregoing process.

decimation-mixed sequence. A mixed sequence produced by decimation, q.v.

decipher, v.t. To convert an enciphered message into its equivalent plain text by a reversal of the cryptographic process used in the encipherment. (This does not include solution by cryptanalysis.)

deciphering alphabet. A cipher alphabet in which the sequence of symbols in the cipher component is arranged in normal order for convenience in decipherment.

decipherment, n. 1. The process of deciphering. 2. The plain text of a deciphered cryptogram. 3. In an enciphered code system, the code text resulting from the removal of the encipherment.

decode, n. 1. That section of a code book in which the code groups are in alphabetical, numerical, or other systematic order. 2. The decoded, but not translated, version of a code message. ---v.t. To convert an encoded message into its plain text by means of a code book. (This does not include solution by cryptanalysis.)

decoded index. A type of code index in which the plaintext value (when known) of the code group in control position is inserted before the control block.

decodement, n. 1. The process of decoding. 2. The decoded, but not translated, version of a cryptogram.

decrypt, n. A decrypted, but not translated, message. ---v.t. To transform an unintelligible or cryptic communication into an intelligible one by a reversal of the cryptographic process used in encryptment. (This does not include solution by cryptanalysis.)

decryption, n. The act of decrypting.

decryptment, n. 1. The act of decrypting. 2. The text produced by decryption.

deferred message. A message bearing the precedence prosign M, q.v.

degarble, v.t. To make emendations in a garbled text.

depth, n. 1. The condition which results when two or more sequences of encrypted text have been correctly superimposed with reference to the keying thereof. Sequences so superimposed are said to be in depth. 2. The number of such superimposed sequences, as a depth of three.

derived cipher alphabet. An alphabet produced by the interaction of two primary components; a secondary alphabet.

derived numerical key. A key produced by assigning numerical values to a selected literal key.

D/F. Direction finding, q.v., or direction finder.

DFS. Double frequency-shift, q.v.

diagnosis, n. In cryptanalysis, a systematic examination of cryptograms with a view to discovering the general system underlying these cryptograms.

difference, n. The result of subtracting one element (a group, a letter, etc.) from another using a given modulus. --v.t. To obtain a difference. To obtain every possible difference of code groups, of cipher groups, of key, of cipher texts, of each letter from the next, etc.

difference book. A numerical listing of the minor differences between frequent code groups.

digraph, n. A pair of letters.

digraphic, adj. Of or pertaining to any combination of two characters.

digraphic frequency distribution. A frequency distribution of successive pairs of letters or characters. A digraphic distribution of ABCDEF would list the pairs: AB, CD, EF. Cf. biliteral frequency distribution.

digraphic idiomorph. A plaintext or cipher sequence which contains or shows a pattern in its construction as regards the number and position of repeated digraphs.

digraphic substitution. Encipherment by substitution methods in which the plaintext units are pairs of characters and their cipher equivalents usually consist of two characters.

dinome, n. A pair of digits.

directed net. A net in which no station except the net control station can communicate with any other station, except for the transmission of urgent messages, without first obtaining the permission of the net control station.

direction finding. Radiogoniometry. The process of locating a radio transmitter by employing special receiving equipment including directional antennas which can determine the direction from which a signal emanates. Abbreviated "D/F."

direct standard cipher alphabet. A cipher alphabet in which both the plain and cipher components are the normal sequence, the two components being juxtaposed in any of the noncrashing placements.

direct symmetry. A property of a cipher square in which the sequence of characters in the rows or the columns is the same throughout and is visibly identical with that of one of the primary components (i.e., patent symmetry as opposed to the latent symmetry of a cipher square exhibiting indirect symmetry).

discriminant, n. A group of symbols indicating the specific cryptosystem used in encrypting a given message. Also called system indicator.

distribution, n. See frequency distribution.

dit, n. 1. A dot in the Morse code. 2. A mark, usually a period or comma, used to denote a missing symbol. ---v.t. To denote missing symbols with dits.

double-channel operation. Simultaneous transmission of different traffic on two frequencies by a single station. Cf. dual operation.

double frequency-shift. A system of transmission whereby two different signals are combined into a single transmission signal by employing four frequencies one kilocycle (or less) apart. Abbreviated DFS.

double hit. The occurrence in two different messages of the same pair of cipher letters or groups, the intervals separating the members of each pair being identical.

double position. Two terminals mounted together and manned by one operator.

double station call. A call-up wherein both the sending station's call sign and the receiving station's call sign are used by the calling station.

doublet, n. A digraph or dinome in which a letter or a digit is repeated (e.g., LL, EE, 22, 66, etc.).

double transposition. A cryptosystem in which the characters of a first or primary transposition are subjected to a second transposition.

downgrade, v.t. To reduce the security classification of a classified document or an item of classified matter or material.

drafter, n. A person who actually composes the message for release by the originator or the releasing officer.

drum, n. 1. In a Hagelin machine, a cage of bars each of which carries a lug or lugs. 2. An electrical commutator or switching device.

DTG. Date-time group, q.v.

dual operation. Simultaneous transmission of identical traffic on two frequencies by a single station. Cf. double-channel operation.

dud, n. A cryptogram which cannot be decrypted promptly because of a faulty indicator or discriminant.

dummy group. A group of nulls.

dummy letter. A null, q.v.

dummy message. A message sent for some purpose other than its content.

dummy traffic. A series of dummy messages.

duplex, adj. Applied to a link on which simultaneous transmission of two messages in opposite directions is possible.

duplex operation. Simultaneous transmitting and receiving of messages in both directions between two stations. Each station uses two operators, one transmitter, and one receiver. (Two different frequencies must be employed.)

E. A symbol used in intercept operations as a suffix to a frequency to denote "estimated".

effective setting. In a cipher machine, the particular position on each rotor which at a given moment is directly contributing to the production of an element of key.

EHF. Extremely-high frequency, q.v.

electrical interception. Gaining possession by electrical means of communications intended for others.

emergency message. A message bearing the precedence prosign Y, q.v.

emission analysis. The processes employed in radiofingerprinting.

encicode, n. A portmanteau word for enciphered code.

encipher, v.t. To convert a plaintext message into unintelligible language by means of a cipher system.

enciphered code. A cryptographic system in which a cipher system is applied to encoded text.

enciphered-code message. A cryptogram produced by enciphering encoded text.

enciphered facsimile. See cifax.

enciphered speech. See ciphony.

enciphering alphabet. A cipher alphabet in which the sequence of letters in the plain component is arranged in normal order for convenience in encipherment.

<u>enciphering table</u>. A table so constructed as to facilitate encipherment.

<u>encipherment</u>, n. 1. The process of enciphering. 2. Text which has been enciphered.

<u>encipher sequence</u>. A sequence of numbers giving the order of the plain text letters as they occur in a transposition cryptogram. Noted as "P → C sequence", which is read as "P to C sequence".

<u>encode</u>, n. That section of a code book in which the plaintext equivalents of the code groups are in alphabetical, numerical, or other systematic order.---v.t. To convert a plaintext message into unintelligible language by means of a code book.

<u>encoded cipher</u>. The final text produced by enciphering the plain text and then encoding the enciphered text.

<u>encodement</u>, n. 1. The act or process of encrypting plain text with a code system. 2. The text produced by encoding plain text.

<u>encrypt</u>, v.t. To convert a plaintext message into unintelligible language by means of a cryptosystem.

<u>encrypted message</u>. A cryptogram.

<u>encrypted text</u>. The text produced by the application of a cryptosystem to a plaintext message.

<u>encryption</u>, n. 1. The act of encrypting. 2. Encrypted text.

<u>encryptment</u>, n. 1. <u>Encryption</u>, q.v. 2. An encrypted communication.

<u>endplate</u>, n. In a cipher machine, the stationary set of contacts at the beginning or end, or both, of the maze. Also called a <u>stator</u>.

<u>end spell</u>. The plain equivalent of a code group indicating that a spelling has been completed and that the groups following represent words and phrases.

equate columns. To adjust one column of an overlap to another by the application of an arbitrary key so that those enciphered code groups occurring in both columns, which are assumed to represent identical plain text, are made identical, and thus may be treated as placode groups.

equation, n. As used in traffic analysis, the process by which two frequencies, two routings, etc., or any combination of two such elements, are demonstrated to be equivalent; also, the condition resulting from this process. Equations may be continuities in which the elements are used successively, or they may involve elements used simultaneously.

equivalent primary component. A sequence which has been or can be developed from the original sequence, or basic primary component, by applying a decimation process to the latter.

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. See decimated alphabet.

estimated frequency. The approximate frequency on which a target is observed operating. (Appearing with an "E" prefixed to the frequency.)

executive method. The method by which the transmitting station directs the addressees of a message to execute (take action on) its purport at a given moment.

executive signal. The transmission which indicates the instant at which action is to be taken on a given message.

exempted addressee. An addressee included in the collective address designation of a message but for whom the message is not intended for either action or information.

exploitable system. A system whose basic elements have been solved, but which cannot be read without the solution of specific controls for individual messages or groups of messages.

exploitation, n. The production of information from messages which are encrypted in systems whose basic elements have been solved. Exploitation includes decryption, translation, and the solution of specific controls such as indicators, specific keys, etc.

external repetitions. Patent repetitions in encrypted text.

external text. In concealment systems, the apparently innocent enveloping text within which a secret message is hidden.

extremely-high frequency. The range of radio frequencies from 30,000 to 300,000 megacycles. Abbreviated as EHF.

facsimile, n. A system of telecommunication for the transmission of fixed plane images with a view to their reception in a permanent form.

factoring, n. An arithmetical process of determining the period of a polyalphabetic cipher of the periodic type by a study of the intervals between repetitions.

FDT. File-date/time, q.v.

field code. Primarily, a tactical code containing a limited vocabulary for low-echelon ground use.

file date/time. The date and time at which a message was filed in the communication center serving the originator. Abbreviated as FDT.

final period. In a periodic cipher system, the period determined by the cryptanalyst to be the true period.

fist, n. The characteristic swing of the dots and dashes of hand-sent Morse as sent by a given radio operator.

fix, n. In D/F, an area indicated as the location of a transmitter by the intersections of three or more bearings. Cf. cut.

fixed additive. An additive sequence which is repeated to make up the entire additive key.

fixed call. An assigned call sign which remains constant for an extended period of time.

flag, n. A graphic representation (triangular or square) of all comparisons possible among a set of elements. ---v.t. To make a flag.

flash message. A message bearing the precedence prosign Z, q.v.

flush depth. 1. The condition which results when two or more encrypted messages have been correctly superimposed, all starting at the same point in the key. 2. The number of such superimposed sequences, as a flush depth of three

"F" (FOX) method. See broadcast method.

four-level dinome cipher. A biliteral substitution cipher system employing four cipher sequences composed of two-digit numbers, by means of which all or nearly all of the plaintext letters are provided with four two-digit variant equivalents.

four-square matrix system. A partially digraphic substitution system employing a matrix which usually consists of four 5 x 5 squares in which the letters of 25-element alphabets (usually combining I and J) are inserted according to any prearranged order.

fractionating system. A cipher system in which plaintext units are represented by two or more cipher symbols which in turn are dissociated and subjected to further encipherment by substitution or transposition or both.

fractionation, n. A cryptographic process wherein the cipher symbols, which combined represent a plaintext unit, are dissociated and subjected to further encipherment.

free net. A radio net in which any station can communicate with any other station in the same net without first obtaining the permission of the net control station.

free routing. The type of routing wherein the destination of a message is designated by the originator but routes which the message will follow are left to the discretion of the relaying station.

free star. The system of radio frequency usage wherein one frequency is assigned to an entire net, and any station in the net may contact any other on that frequency.

frequency, n. 1. In its cryptologic application, the number of actual occurrences of a textual element within a given text. Cf. relative frequency. 2. In its electrical application, the number of complete cycles per second produced in an alternating current system.

frequency band. The range of frequencies between two definite limits.

frequency count. A frequency distribution.

frequency distribution. A tabulation of the frequency of occurrence of plaintext or ciphertext units in a message or a group of messages. A frequency count.

frequency table. A frequency distribution in tabular form, with frequencies indicated by numbers.

frequential matrix. A type of cipher matrix providing variants. A matrix in which the number of different cipher values available to represent any given plaintext letter closely approximates its relative plaintext frequency.

full-time coverage. The assignment of the intercept operators necessary to intercept all transmissions on a given frequency or associated group of frequencies.

gapped, adj. As applied to a sequence, having gaps, selective, not complete.

garble, n. An error in transmission, reception, encryption, or decryption which renders incorrect or undecryptable a message or transmission or a portion thereof. ---v.t. To make an error in transmission, reception, encryption, or decryption of a message.

garble table. Any table, chart, or other aid which may be used to correct garbles (e.g., a permutation table).

GCT. Greenwich Civil Time, q.v.

general call sign. A call sign representing all stations, units, commands, etc., in an area, in a major command, or in any combination thereof.

general cryptosystem. The basic invariable method of encryption included in a cryptosystem, excluding the specific keys essential to its employment.

general message. A type of message having a wide standard distribution, originated by the Navy Dept., or by a fleet commander. A general message is assigned an identifying title and usually a serial number. (e.g., ALNAV 5.)

general solution. A solution dependent on exploiting the inherent weaknesses of the cryptographic system arising from its own mechanics, without the presence of any specialized circumstances.

general system. See general cryptosystem.

generation. The production, either systematic or random, of call signs, keys, code groups, etc. In the case of call signs, generation is distinguished from allocation, which is the assignment of call signs or blocks of call signs to stations after generation. (Cf. allocation.)

generatrix, n. 1. One decipherment (or encipherment) out of a set of decipherments (or encipherments) of the same text, the set being exhaustive on a given hypothesis or given cryptographic principle. The elements of a generatrix are at a constant alphabetic (normal or cipher) interval from those of another generatrix of the set, (e.g., as in a strip system). 2. In connection with the method of completing the plain component sequence, any one of the rows, each of which represents a trial "decipherment" of the original cryptogram.

generatrix interval. The interval between a plaintext generatrix and a cipher generatrix.

GMT. Greenwich Mean Time, q.v.

goniometer, n. An electrical device used in direction finding to determine the azimuth of arrival of signals picked up by a direction-finder antenna.

good difference. In enciphered code solution, a possible difference or one likely to occur which is equal to, or may be, the difference between two high frequency groups.

good group. 1. A code group which occurs with a relatively high frequency; a common group. 2. A code group which has the proper limitation and thus is known to be not garbled.

grammatical group. A code group indicating which of the alternative grammatical inflections assigned to a particular code group is to be taken.

grammatically identified group. A code group in process of identification which has been established as being a particular part of speech, (e.g., noun, verb, adjective); but not more precisely determined.

grammatical table. A section in a code book containing grammatical groups.

Grandpré cipher. A type of substitution system providing variants. This system employs a cipher square in which are inscribed ten 10-letter words containing all the letters of the alphabet in their approximate plaintext frequencies. These ten words are further linked together by a 10-letter word which appears vertically in the first column as a mnemonic feature for the inscription of the words in the rows.

Greenwich Civil Time. Formerly, the mean solar time at the meridian of Greenwich. Abbreviated as GCT. Now superseded by Greenwich Mean Time, q.v.

Greenwich Mean Time. The mean solar time at the meridian of Greenwich. Abbreviated as GMT. Also known as universal time and Z (Zebra) time.

grid, n. In a transposition system, a form or matrix over which a grille is placed for the purpose of enciphering or deciphering.

grille, n. 1. A sheet of paper, cardboard, thin metal, plastic, or like material in which perforations have been made for the uncovering of spaces in which textual units may be written or read on the grid. 2. A matrix in which certain squares are blocked out or otherwise marked so as not to be used. Also called a stencil.

Gronsfeld system. A polyalphabetic substitution system employing the first 10 alphabets of a direct standard Vigenère table in conjunction with a numerical key. The cipher equivalent of a given plaintext letter is found by counting down the normal sequence the number of positions indicated by the numerical key; thus A_p with key of 4 is E_c.

ground wave. The portion of a transmitted radio wave which travels along the surface of the earth. Cf. sky wave.

group, n. 1. A number of digits, letters or characters forming a unit for transmission or for cryptographic treatment. 2. In radio, two or more links whose stations work together as a communication entity under a common operating control.

group count. A number, usually present in the preamble, which indicates the number of groups or words in a designated portion of a message, usually the text.

half-tone, adj. In facsimile, composed of a large number of shades of gray.

hard copy. A copy of a message in the conventional form on a page or printed tape, as opposed to a phonographic recording, perforated tape, etc.

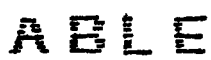
harmonic, n. A multiple of a fundamental frequency.

hat, n. The upper part of a hat diagram; a crown.

hat diagram. A figure formed by writing the text of a cryptogram enciphered by columnar transposition so that each column contains the textual units which, for an assumed matrix width, must have occurred in a single column of the original matrix, as well as others which may have occurred in that column.

heading, n. In communication intelligence usage, the information on an intercepted message preceding the message text; this information is in two parts, the intercept data (supplied by the intercept operator) and the preamble (transmitted by the target station).

Hellschreiber, n. A system of automatic telegraphy which is uniquely characterized by reception-printing on a paper tape in a facsimile-like manner, in that the printing is accomplished through the use of a helix and stylus rather than through the use of conventional type bars; thus, each printed character is made up of several closely spaced horizontal lines, as shown below:



HF. High frequency, q.v.

high-echelon, adj. Pertaining to organizational units at the army divisional level or higher, or their equivalents.

high frequency. The range of radio frequencies from 3 to 30 megacycles.

high-grade, adj. Pertaining to a cryptosystem which offers a maximum of resistance to cryptanalysis, for example: (1) complex cipher machines, (2) one-time systems, (3) two-part codes enciphered with an additive book. Cf. low-grade and medium-grade.

high-level cryptochannel. A cryptochannel composed of high commands, employing a cryptosystem which has limited distribution and relatively permanent physical and cryptographic security.

Hill's algebraic encipherment. A true polygraphic system for the encipherment of polygraphs of any order, involving algebraic treatment by means of coefficients for the transformation of a plaintext polygraph into its ciphertext polygraphic equivalent, and vice versa. Invented by Professor Lester S. Hill of Hunter College.

hit, n. A coincidence of textual elements (single letters, digraphs, trigraphs, etc.) occurring between messages.

holder, n. A command or activity authorized to draw and hold publications according to established distribution lists. In cryptologic application, an authorized possessor of cryptographic materials.

holocryptic, adj. Incapable of being deciphered without a key. For example, a one-time system might be termed holocryptic.

horizontal two-square matrix system. A digraphic substitution system employing a matrix which normally consists of two 5 x 5 squares placed side by side.

hypothetical code. Code obtained by deciphering selected groups from enciphered code messages by trial keys assumed to have been used.

hypothetical key. Key obtained by assuming plaincode groups to underlie selected cipher groups.

IBM. International Business Machines, q.v.

IBM method. A form of statistical analysis employing International Business Machines, q.v.

IBM run. A listing which is the result of (1) arranging data, through the use of IBM sorting machines and associated equipment, into a particular order and form for ease of study, and (2) subsequently printing these data by means of IBM tabulating equipment.

ICR. International commercial radiotelegraphy.

identification, n. 1. In cryptanalysis, determination of the plaintext value of a cipher element or code group. 2. In traffic analysis, determination of the specific unit, aircraft, ship, or Order of Battle involved in a given instance, but not its location.

Identification Friend or Foe. Radar recognition and identification. A system using radar transmissions to which equipment carried by friendly forces automatically responds, for example, by emitting pulses, thereby distinguishing themselves from enemy forces. Abbreviated as IFF.

identifier, n. A voice intercept operator who identifies the language and subject matter of voice transmissions.

identify, v.t. 1. In cryptanalysis, to determine the plaintext value of a cipher element or code group. 2. In traffic analysis, to determine the specific unit, aircraft, ship, or Order of Battle involved in a given instance, but not its location.

idiomorph, n. A plaintext or cipher sequence which contains or shows a pattern in its construction as regards the number and positions of repeated letters.

idiomorphic, adj. Exhibiting the phenomenon of idiomorphism.

idiomorphism, n. In a plain-text or cipher sequence, the phenomenon of showing a pattern as regards the number and positions of repeated letters.

IFF. Identification Friend or Foe, q.v.

IMC number. International Meteorological Code number. See base number.

"I" (Item) method. See intercept method.

immediate message. A message bearing the precedence prosign O, q.v.

index, n. An ordered listing of such data as cipher or code groups, traffic, etc. ---v.t. to prepare such an index.

index letter. That letter of a component of a cipher alphabet against which the key letter in the other component is juxtaposed.

index of coincidence. The ratio of the observed number of coincidences in a given cryptogram to the number of coincidences expected in a sample of random text of the same size as the cryptogram.

indicative, n. (Met.) A three-figure number indicating the meteorological station concerned, and forming the first three figures of a synoptic report.

indicative information. In connection with IBM listings, that data which serves to identify a given control group or a given line of textual material; indicative information usually appears at the left of any given line on a listing and includes such data as worksheet number, date, lane, etc.

indicator, n. In cryptography, an element inserted within the text or heading of a message which serves as a guide to the selection or derivation and application of the correct system and key for the prompt decryption of the message. See also the more precise terms discriminant and message indicator.

indicator group. A group forming the whole or part of an indicator.

indicator pattern. The meaningful order of elements of an indicator.

indicator system. 1. The total of conventions agreed upon to convey cryptographic data by means of indicators within a cryptographic system. 2. A system used to encrypt an indicator.

indirect symmetry. A property of a cipher square in which a pair of rows or pair of columns may be united to give a decimation of one of the primary components; i.e., latent symmetry as opposed to the patent symmetry of a cipher square exhibiting direct symmetry.

information addressee. The activity or individual to whom a message is directed by the originator for information only.

initial key. The key used in starting an encipherment; especially, the short key used to begin an autokey encipherment. Also called preliminary key or priming key.

inked tape. Paper tape on which code signals (usually dots and dashes) are recorded in the form of visible ink patterns. Also known as inked recording tape and undulator tape.

inscription, n. In a transposition system, the process of writing a message into a matrix.

integer, n. A whole number.

integrated diagram. A composite traffic analysis diagram of a given net, showing significant facts established about the net or network from various separate daily diagrams and other sources over a period of time.

intercept, n. A copy of a message obtained by interception. ---v.t. To engage in interception.

intercept control. The assignment of missions to intercept stations, and the furnishing of such stations with technical data to aid them in carrying out these missions.

intercept data. The information supplied by the intercept operator and appearing as the first part of the message heading. Intercept data generally include frequency, call signs, signal strength, signal readability, intercept date/time, intercept station number, and case number. According to some intercept formats now in use, some intercept data, such as time when transmission of message was completed and intercept operator's initials may be found just below the message.

intercept date/time. The actual date and time a message or chatter is heard by an intercept operator. Usually recorded in Greenwich ("Z") time.

interception, n. The process of gaining possession of communications intended for others without obtaining the consent of the addressees and without preventing or ordinarily delaying the transmission of the communications to those addressees.

intercept method. The method of transmitting by prearrangement a message from one station to another so that other stations for which it is intended may receive it without giving a receipt. The station called is responsible for the correct reception of the message at that station. Also called "I" (Item) method.

intercept position. The necessary equipment and facilities required to intercept one radio signal. (1) manned intercept position - The necessary personnel and equipment to intercept one radio signal, 24 hours per day if necessary. (2) installed intercept position - An intercept position in either an operational or a standby state. (3) double position - Two receiving terminals mounted together, manned by one operator, used for intercepting the signals from both ends of a radio link.

intercept station. An installation which collects communications for COMINT purposes.

interference, n. The impairment of reception by atmospherics, unwanted signals (not known to be deliberate) or the effects of electrical apparatus or machinery.

intermediate cipher text. Text in cryptographic form which has undergone part but not all of the deciphering or enciphering process.

internal indicator. A message indicator, q.v.

internal repetitions. Repetitions occurring within the same message.

internal text. In concealment systems, the secret text which is enveloped by open or apparently innocent text.

International Business Machines. Machinery using punched cards which are electrically read for accounting and statistical purposes.

international call sign. A call sign assigned in accordance with the provisions of the International Telecommunications Union to identify a radio station, and appearing in up to date lists published by the I.T.U. The first letter or first two letters of the call sign indicate the nationality of the station.

international Morse code. A widely-used code in which letters and numbers are represented by specific groupings of dots, dashes, or combinations of both. The international Morse code is used especially in radio telegraphy.

International Service Code. See service code.

International Telecommunication Union. A civil international organization established to provide standardized communication procedures and practices including frequency allocation and radio regulations on a world-wide basis. Abbreviated as ITU.

international teleprinter code. See Baudot code.

interpreter, n. A listener who translates (or summarizes) foreign language voice transmissions directly from actual transmission.

interrelated cipher alphabets. Cipher alphabets most commonly produced by the interaction of two primary components which, when juxtaposed at various points of coincidence, can be made to yield secondary alphabets.

interrupted key cipher. An aperiodic polyalphabetic cipher of which the key may be broken off and resumed at any point by prearrangement.

interrupted-key columnar transposition. A columnar transposition system in which the plaintext elements are inscribed in a matrix in rows of irregular length as determined by a numerical key.

interrupter, n. A specified character of the plain text or of the cipher text which by its occurrence determines an interruption in the basic keying operation or sequence.

interval, n. The number of units between two units of encrypted text (letters, digraphs, code groups, etc.) counting either the first or second of the two units but not both.

interval key. A transposition key expressed as the intervals between positions of symbols forming the plain text of a transposition cipher.

intrusive, adj. In a one-part code, pertaining to a code group whose meaning is out of normal alphabetical order with respect to the code group order, i.e., interrupting its normal alphabetical or numerical order.

intuitive method. A method of solution making use of probable words, probable keys, the supposed psychology of the encipherer, the reports of espionage services, and all other factors derivable from a given situation.

invariable digraph. A digraph composed of letters invariably associated with each other in the orthography of a given language (e.g., the English digraph QU).

inverse four-square matrix system. A four-square matrix system in which the cipher sections contain normal alphabets while the plain component sections contain mixed alphabets.

invisible ink. Any of several chemicals used for writing or printing which writing has the property either of being initially invisible to the naked eye or of becoming so after a short time.

invisible writing. Writing not visible to the naked eye. The characters composing such writing may be microscopic or inscribed with invisible ink.

isolog, n. A cryptogram of which the plain text is identical with that of another message encrypted in another system, key, code, etc.

isologous, adj. Pertaining to or having the nature of an isolog.

isomorph, n. A sequence exhibiting isomorphism.

isomorphism, n. The term applied to the phenomena arising whenever two or more sequences although different in composition nevertheless possess identical patterns as regards constituent repetitions.

jam, v.t. To make the satisfactory reception of electrical signals difficult or impossible by transmitting interfering signals.

jamming, v.t. The deliberate impairment of reception of electrical signals by transmission of interfering signals.

jargon code. A code using bona fide words, instead of the arbitrary groups of symbols usually associated with code systems.

Jefferson cipher. A polyalphabetic substitution system invented by Thomas Jefferson and independently at a later date by the French cryptographer Bazeries. It provided for encipherment by means of a manually operated device involving a number of revolvable disks, each bearing a mixed alphabet on its periphery.

joint, adj. Between, two or more Services of the same nation. (Wher all Services are not involved the participating Services shall be identified, e.g., Joint Army-Navy).

joint communication. Common use of communication facilities by two or more Services of the same nation.

kappa plain constant. A constant employed in coincidence tests to denote the probability of coincidence of a given textual element or unit in plain text. It is the sum of the squares of the probabilities of occurrence of the different textual elements or units as they are employed in writing the text; for example, in English telegraphic plain text, the monographic and digraphic plain constants are .0667 and .0069 respectively.

kappa random constant. A constant employed in coincidence tests to denote the probability of coincidence of a given textual element in random text. It is merely the reciprocal of the total number of characters used in writing the text. If a 26-letter alphabet were employed, for instance, the constant denoting the probability of coincidence of various textual elements would be derived as follows:

a. single letters 1/26 = .0385

b. digraphs 1/676 = .00148

c. trigraphs 1/17576 = .000057

kappa test. See coincidence test.

kc, kcs. kilocycle, kilocycles.

key, n. 1. In cryptography, a symbol or sequence of symbols applied to successive textual elements of a message to accomplish their encryption or decryption. 2. A specific key.

key book. A book containing key text, or plain text forming specific keys.

keyed columnar transposition. A transposition system in which the columns of a matrix are taken off in the order determined by the specific key, which is often a derived numerical key.

key generator. A device for producing a key sequence.

key group. A group of key symbols.

key-in, v.t. To recover key by means of a crib.

key index. An ordered listing of keys showing preceding and following keys with proper designations of source.

key letter. A letter of key; especially in polyalphabetic ciphers, the letter determining which of the available cipher alphabets is used to encipher a particular letter.

key list. In cryptography, the publication containing the keys for a particular cryptosystem.

key phrase. An arbitrarily selected phrase from which a key is derived.

key recovery. The cryptanalytic reconstruction of a key.

key text. Text from which a key is derived.

key word. An arbitrarily selected word used as a key per se, or from which a key is derived.

keyword, adj. Of or pertaining to a key word or key words; as keyword recovery.

keyword mixed alphabet. An alphabet constructed by writing the prearranged key word or key phrase, (repeated letters, if present, usually being omitted after their first occurrence) and then completing the sequence from the unused letters of the alphabet in their normal sequence.

kick, n. A movement of controlled but usually variable amount imparted to a rotating element of a cipher machine either regularly or cyclically.

kilocycle. One thousand cycles per second.

lambda (Λ) test. A test for monoalphabeticity in a message, based on a comparison of the observed number of blanks in its frequency distribution with the theoretically expected number of blanks both in (a) a normal plaintext message of equal length and (b) a random assortment of an equal number of letters. Also called the blank-expectation test.

lane, n. A path, electrical, physical, or both, in one direction connecting two correspondents regardless of the route involved.

language specialist. One who has developed a specialized competence in one or more aspects of a foreign language.

latent repetition. A plaintext repetition not apparent in cipher text but susceptible of being made patent as a result of analysis.

latent symmetry. See indirect symmetry.

lateral communication. 1. Communication between outstations of a group or net. 2. Less frequently, communication between adjacent units along a front, or between units of the same echelon of command.

Latin square. A cipher square in which no row nor column contains a repeated symbol.

lexical, adj. Of, pertaining to, or connected with words. In its cryptologic sense, the word is used to characterize those cryptographic methods (chiefly codes) which deal with plaintext elements comprising complete words, phrases and sentences.

LF. Low frequency, q.v.

limitation, n. A restriction imposed upon a system or on some part of a system, such that certain elements or characters either do not occur at all, or occur only under certain conditions. (e.g., a 5-figure code using only groups beginning with the digits 0-5; a 5-figure code using only groups whose digits sum to an even number.)

line. See row.

linguist, n. One who has expert knowledge of a foreign language.

link, n. Any single direct system of telecommunication between two points using one communication means. Cf. circuit.

link call. A common call sign used by two stations for intercommunications.

listener, n. A language specialist who deals with a foreign language in its spoken form.

listing, n. A tabulation of data (e.g., the printed result from a deck of IBM cards.). Also called a run.

literal key. A key composed of a sequence of letters.

literal system. Any cryptosystem designed for off-line literal communication in which the plaintext and ciphertext symbols produced or accepted are the normal alphabetical characters and the digits.

local stereotype. A stereotype which is characteristic of a particular originator.

log, n. 1. An orderly record of observed events. 2. In intercept operations, a record kept by an operator of everything heard on a circuit. ---v.t. To keep a log.

logarithmic weights. Numerical weights assigned to units of plain text, which weights are actually logarithms of the probabilities of the plaintext units, and which are used to evaluate the results of certain cryptanalytic operations.

log reader. A person engaged in reading the logs of intercept operators for communication intelligence purposes.

long title. The full descriptive name assigned to a document or device by the preparing agency.

loran, n. A long range radionavigation position fixing system using the time difference of reception of pulse type transmissions from two or more fixed stations.

low-echelon, adj. Pertaining to organizational units below the level of the army division or its equivalent.

low frequency. The range of radio frequencies from 30 to 300 kilocycles. Abbreviated LF.

low-grade, adj. Pertaining to a cryptosystem which offers only slight resistance to cryptanalysis; for example: (1) Playfair ciphers, (2) single transposition, (3) unenciphered one-part codes. Cf. medium-grade and high-grade.

low-level cryptochannel. A cryptochannel composed of commands in low echelons, employing a cryptosystem which has wide distribution, fair physical security, and temporary cryptographic security.

M. 1. United States Military precedence prosign for DEFERRED. Usually transmitted as "MM" to ensure accuracy. Assigned to messages whose delivery to the addressees is not required until the beginning of the office hours following the day on which filed. 2. Used in intercept operations as a suffix to a frequency to denote "measured".

machine cipher. A cipher system in which the enciphering and deciphering are performed by a machine; or a message produced by such a system.

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 meaning only. Cf. auxiliary table.

major difference. The larger of the two differences obtained when two code or cipher groups are subtracted each from the other by modular arithmetic.

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

marking impulse. One of the two types of impulses used in teleprinter transmission; normally, that impulse during which current flows through the teleprinter receiving magnet. The other type of impulse is the spacing impulse, q.v.

master card. An IBM card which contains data common to a particular series of cards.

master decode. The principal and authoritative decoding section of a code book, maintained during its reconstruction. The master decode contains all possible code groups in the system under study, and all partial or complete identifications with their appropriate validity indicators.

matrix, n. A geometric form or pattern. In transposition systems, the figure or diagram in which the various steps of the transposition are effected; in substitution systems, the figure or diagram containing the sequence or sequences of plaintext or cipher symbols.

matrix-reconstruction diagram. In transposition solution, a diagram of the C → P sequence from which the size and shape of the original transposition matrix may be deduced.

maze, n. The more or less intricate network of paths along which an electrical current may flow in a cipher machine; specifically, the unit of a cipher machine which intervenes between the input or generating impulse leading into the apparatus and the output or resulting impulse.

mc, mcs. megacycle, megacycles.

meaconing, n. A system of receiving beacon signals and rebroadcasting them on the same frequency to confuse navigation. The meaconing stations cause inaccurate bearings to be obtained by aircraft or ground stations.

means of signal communication. A medium, including equipment, used by an agency for transmitting messages.

measured frequency. The exact frequency on which a target was observed operating, as measured by the intercept operator. (Appearing with an "M" suffixed to the frequency.)

medium-grade, adj. Pertaining to a cryptosystem which offers considerable resistance to cryptanalysis; for example: (1) strip ciphers, (2)double transposition, (3) unenciphered two-part codes. Cf. low-grade and high grade.

megacycle. One million cycles per second.

message, n. Any thought or idea expressed in plain or secret language, prepared in a form suitable for transmission by any means of communication.

message alignment. See message placement.

message authentication. A security measure designed to establish the authenticity of a message by means of an authenticator within the transmission derived from certain predetermined elements of the message itself.

message center. An agency charged with the responsibility for acceptance, preparation for transmission, receipt and delivery of messages.

message center number. A message reference number assigned by the message center in order to facilitate internal administrative handling.

message externals. Those components of a transmitted message which are not encrypted as a part of the message text. Specifically, the entire preamble, the indicators and discriminants, and the postamble if present.

message format. The agreed upon arrangement of the various parts of a message.

message indicator. That part of the specific key which changes with every message.

message keying element. See message indicator.

message placement. The determination of the correct relative position of key and message.

message print. An IBM machine reproduction of messages to facilitate solution. These message prints may vary in form or in the type of data included, depending upon the nature of the problem involved.

message serial number. A reference number assigned by the originator to each out-going message to facilitate checking, handling, and filing.

meteorological message. A message giving data about atmospheric conditions; usually in synoptic form.

MF. Medium frequency, q.v.

minor difference. The smaller of the two differences obtained when two code or cipher groups are subtracted each from the other by mod-10 arithmetic.

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

minuend, n. The key used in the minuend method, q.v.

minuend method. A method of enciphering code in which the placode text is subtracted from the key. In the process of decipherment, the enciphered code text is subtracted from the key.

mission,radio intercept. A definite task, duty, or assignment given to an intercept activity or unit. Cf. target.

mixed cipher alphabet. A cipher alphabet in which the sequence of letters or characters in one or both of the components is not the normal sequence.

mixed-length system. A cryptosystem in which the units of cipher text or code text are of irregular or nonconstant length, as for example, a monome-dinome system, or a code system employing both 4-letter and 5-letter groups.

mixed-unit, adj. Applied to codes having groups of different length, (e.g., some 4-character and some 5-character groups.

mnemonic key. A key so constructed as to be easily remembered.

MNR. Message center number, q.v.

MOA. Morse operator analysis, q.v.

model encode. As used in codebook reconstruction, the encoding section of a previous code book in the same language and of approximately the same type and size as the code under study. Its function is to serve as a guide in the selection and limitation of the vocabulary to be used in solution.

modular, adj. Pertaining to a modulus, q.v.

modulo, adv. With respect to a modulus, q.v. (Abbreviated as mod; e.g. mod-10, mod-26, etc.)

modulus, n. Scale or basis of arithmetic; the number n is called the modulus when all numbers which differ from each other by n or a multiple of n are considered equivalent.

monitor, v.t. To intercept and copy one's own or friendly radio and wire transmissions for the purpose of detecting and correcting violations of regulations.

monitoring position. The necessary equipment and facilities required to monitor one radio or wire signal.

monoalphabeticity, n. A characteristic of encrypted text which indicates that it has been produced by methods involving a single cipher alphabet or single code book, unenciphered. It is normally disclosed by frequency distributions which display "roughness", or pronounced variation in relative frequencies.

monoalphabetic substitution. A type of substitution employing a single cipher alphabet by means of which each cipher equivalent, composed of one or more elements, invariably represents one particular plaintext unit, wherever it occurs throughout any given message.

monographic, adj. Of or pertaining to any units comprising single characters.

monographic substitution. Encipherment by substitution methods in which the plaintext units are single characters and their cipher equivalents usually consist of single characters.

monoliteral system. A substitution system in which the elements of the cipher component are single characters.

monome, n. A single digit.

monome-dinome system. A substitution system in which certain plaintext elements have single-digit cipher equivalents, while others are represented by pairs of digits.

Morse codes. Various communication codes, of special and limited usage, in which letters and numbers are represented by specific groupings of dots, dashes, or combinations of both.

Morse operator analysis. Any system of cataloguing and identifying the manual keying characteristics of a Morse operator. Abbreviated as MOA.

multiliteral, adj. Of or pertaining only to cryptosystems, cipher alphabets, and frequency distributions which involve cipher units of two or more letters or characters. See the more inclusive term polygraphic.

multiliteral cipher alphabet. A cipher alphabet in which one plaintext letter is represented by cipher units of two or more elements.

multiliteral system. A substitution system involving one or more multiliteral cipher alphabets.

multiple-address message. A message transmitted to two or more addressees each of whom is informed of all the addressees. Each addressee must be indicated as Action or Information.

multiple-alphabet system. A type of substitution in which successive lengthy portions of a message are each monoalphabetically enciphered by a different alphabet; monoalphabetic encipherment by sections.

multiple anagramming. A process of anagramming simultaneously several transposition messages of the same length that have been enciphered with the same key.

multiple call. A call directed to two or more stations, in which the individual call signs of the stations called are used (in contrast to collective call).

multiple key. A key whose value has not been uniquely determined.

multiplex, adj. Pertaining to a communication system permitting the simultaneous use of a number of channels on a single link.

multiplex link. A link between one transmitter and one receiver whose characteristics are such as to permit simultaneous use of a number of channels with separate transmissions on each channel.

NCS. A net control station, q.v.

near depth. Depth which, but for some minor inconsistencies in the progression or identity of keying elements, would be true depth.

net, n. A group or a number of groups of stations and links assembled on the basis of common operating characteristics, presumably under the administrative direction of an immediate common superior headquarters station.

net authentication. Identification used on a communication net to establish the authenticity of the several stations.

net call sign. A collective call sign used to contact all stations in a net on the same frequency.

net control station. The station designated to direct transmission activities and enforce discipline within a net. It usually serves the senior unit of the net. Abbreviated as NCS. Also known as "control" or "control station."

network, n. The total apparent radio system of a military unit, military service of a nationality, or other organization, including all subordinate or related nets.

nonborrowing subtraction. Subtraction to the modulus ten; i.e., the tens digits are disregarded.

noncarrying arithmetic. Arithmetic to the modulus ten; i.e., the tens digits are disregarded.

noncarrying sum. A sum produced in cryptographic (mod 10) arithmetic.

noncommutative, adj. As applied to bipartite matrices, so constructed that row and column coordinates must be read in a certain prescribed order, for example, in a row-column order.

noncrashing, adj. A term used to describe that feature of the structure of certain cryptosystems which does not permit a plaintext unit to be self-enciphered.

nonliteral system. Any cryptosystem designed for the transmission of data in which the symbols or signals produced or accepted are other than the normal alphabetical characters and the digits (e.g. teleprinter, IFF, ciphony, cifax, civision, etc.).

non-Morse, adj. Pertaining to methods of transmission using symbols other than those of the Morse code, (e.g., those of the Baudot alphabet).

nonperforated grille. A matrix with numbered cells over which a transparent paper is placed to obtain a transposition square.

nonregistered publication. A publication which bears no register number and for which routine accounting is not required.

nonrepeating key. A key sequence which does not repeat within a given message.

nonsecret code. A code which has for its sole purpose the abbreviation, not the concealment, of messages, and therefore may be of any construction preferred by the issuing unit. A brevity code.

nontextual, adj. Forming no part of the actual text of the message; as for example, address and check groups.

nontransposability, n. A characteristic incorporated in certain codes in which the code groups are constructed in such a manner that the transposition of any two letters will not produce another bona fide code group in that code.

normal alphabet. The conventional sequence of letters which form the elements of written language and are used to represent approximately the sounds of the spoken language. The direct standard alphabet beginning with "A" and ending with "Z".

normal frequency. The standard frequency of a plaintext unit or letter relative to other such units or letters, as disclosed by the statistical study of a large volume of text.

normal sequence. The normal alphabetical sequence of those letters which are used in the written text of any particular language, or any cyclic permutation thereof.

normal uniliteral frequency distribution. A distribution showing the standard relative frequency of single plaintext symbols as disclosed by statistical study of a large volume of text.

NR. Station serial number, q.v.

null, n. In cryptography, a symbol or unit of encrypted text having no plaintext significance.

numerical key. A key composed of a sequence of numbers.

numerically-keyed columnar transposition. A transposition system in which the columns of a matrix are taken off in the order determined by a numerical key.

numerical table. In a code book, a list of code groups representing numbers, dates, and amounts.

O. United States Military precedence prosign for IMMEDIATE. Usually transmitted as "OO" to ensure accuracy. Assigned to important tactical messages pertaining directly to the operations in progress and, when necessary, those messages concerning the immediate movement of ships, aircraft, or ground forces.

O/B. The order of battle, q.v.

office of record. The agency charged with maintaining the ultimate accounting records for registered documents.

off-line operation. A method of operation in which the processes of encryption and transmission and/or reception and decryption are performed in separate steps, rather than automatically and simultaneously.

offset, adj. Applied to messages in depth or repetitions in these, beginning or occurring at different points of the key.

offset duplicate. A pair of messages in depth having identical or nearly identical plain text except that the plain text of one is displaced along the keying cycle in relation to the other.

off the cut. As applied to the division of cipher text into polygraphs, beginning elsewhere than with the initial character of a bona fide polygraph.

one-deep reading. The keying-in of assumed placode of a single message.

one-part code. A code in which the plain-text elements are arranged in alphabetical or numerical order accompanied by their code groups also arranged in alphabetical, or numerical order.

one-time pad. A form of key book used in a one-time system, so designed as to permit the destruction of each page of key as soon as it has been used.

one-time system. A cryptosystem in which the key, normally of a random nature, is used only once.

on-line operation. A method of operation in which the processes of encryption and transmission and/or reception and decryption are performed automatically and simultaneously.

on the cut. As applied to the division of text into polygraphs, beginning with the first textual character.

open code. A cryptosystem in which units of plain text are used as the code equivalents for letters, numbers, words, phrases or sentences. The code equivalents themselves, usually words or phrases, can be combined to form the intelligible text of apparently innocent messages. Cf. concealment system.

operating signal. In joint and combined usage, a trigraph beginning with "Q" (in international usage, "Q" and "Z") used to facilitate the handling of traffic, to direct net operation, or to convey certain originator's instructions in a message. Operating signals are also used by aircraft to convey certain operational information such as movements, reports during flight, and meteorological advice.

optimum traffic frequency. The most effective frequency at a specified time for ionospheric propagation of radio waves between two specified points (commonly taken as 85% of the monthly median value of maximum usable frequency for the specified time and path).

order of battle. Information concerning the details of a nation's military services; (e.g., the units composing them, their disposition and strength, personalities, etc.).

originator, n. The individual (a commander or his officially designated representative) by whose authority a message is sent.

outstation, n. Any station other than the control station on a link, group, or net.

overlap, n. 1. The encipherment of two or more encrypted texts by the same or portions of the same key. 2. A worksheet containing cryptographic text so written that the elements enciphered in the same key will fall in the same column. 3. In the Hagelin machine, the condition arising when there are two effective lugs on the same bar. ---v.t. To superimpose enciphered texts.

P. United States Military precedence prosign for PRIORITY. Usually transmitted as "PP" to ensure accuracy. Assigned to important matter which requires prompt delivery to the addressee. It is the highest precedence designation which may be assigned to nonoperational messages of an administrative nature.

padding, n. Extraneous text added to a message for the purpose of concealing its length and beginning or ending or both.

page copy. A copy of a message received by teleprinter on a page.

page symbol. 1. That part of the indicator in an enciphered code system, indicating page in key book. 2. That part of a code group indicating the page on which the plain equivalent is to be found.

pagination, n. 1. The act or process of assigning identifying symbols to the pages of a code book or a key book. 2. The sequence of symbols identifying the pages of a code book or key book.

panel code. A prearranged code designed for visual communications between ground units and friendly aircraft by means of specially colored or shaped strips of cloth or other material.

paraphrase, v.t. To change the phraseology of a message without changing its meaning.

partially periodic repetition. A repetition in the cipher text caused by two identical sections of plain text being enciphered by a repetition of part of the key.

partially-polygraphic system. Any polygraphic substitution system in which the encipherment of certain members of the polygraphs shows group relationships; small matrix systems, such as the four-square, two-square and Playfair systems involve such group relationships and are considered to be partially-digraphic systems.

partition, n. Resolution of an integer into a set of integers (e.g., representation of the integer 6 as 1 and 5, 2 and 4, 3 and 3).

part message. A message divided into two or more parts, each of which is sent as a separate transmission.

patent repetition. A repetition which is externally visible in the original cryptographic text.

patent symmetry. See direct symmetry.

pattern. See idiomorph.

pentagraph, n. A set of five letters.

pentanome, n. A set of five digits.

period, n. The number of elements (letters of a cryptogram, consecutive steps of a wheel, etc.) that must occur before cyclic properties become manifest.

periodic, adj. Characterized by cyclic usage, as of key in a periodic system, q.v.

periodicity, n. In its cryptologic application, the quality or state of exhibiting cyclic phenomena.

periodic substitution. Periodic polyalphabetic substitution. A method of encipherment involving the cyclic use of a plurality of alphabets. Also called repeating key method.

periodic system. A system in which the enciphering process involves a cryptographic treatment which is repetitive in character and which usually results in the production of cyclic phenomena in the cryptographic text.

permutation table. A table designed for the systematic construction of code groups. It may also be used to correct garbles in groups of code text.

personality file. A file containing the histories of all personalities appearing in intercepted communications, together with the circumstances in which they were mentioned.

phase, n. 1. A period or interval. 2. The relationship between two sequences (of text, of key, or of text and key), each having its own cycle. Such sequences are in phase with each other whenever the starting points and the successive elements of the periods coincide, and out of phase whenever the elements of the period do not. When a message is affected by two periods, e.g., code-group length and a transposition key length or additive key length, those portions of it written on the cycle of the product of the two periods are said to be in phase.

phi (ϕ) test. A test applied to a frequency distribution to determine its monoalphabeticity. See also kappa plain constant and kappa random constant.

physical security. That component of communication security which results from all physical measures necessary to safeguard classified communication equipment and material from access thereto by unauthorized persons.

pibal, n. A weather report based on pilot-balloon observations of upper winds. (From "pilot" and "balloon.")

pilot letter. A letter which is usually followed by a certain letter; the first of the members of an invariable digraph.

placode, n. A portmanteau word used to designate plain or unenciphered code.

plain, adj. Of or pertaining to that which is unencrypted. See also plaintext.

plain code. Unenciphered code.

plain component. That sequence of a cipher alphabet which comprises the sequence of plaintext symbols.

plain component equivalents. In connection with the method of completing the plain component sequence, the plaintext equivalents for cipher units derived from an arbitrary juxtaposition of the components of a cipher alphabet.

plaindress, n. A type of message in which the complete address is contained in the heading. Cf. codress.

plain language. Plain text, q.v.

plain text. 1. Text or language which conveys an intelligible meaning in the language in which it is written, with no hidden meaning. 2. The intelligible text underlying a cryptogram.

plaintext, adj. Of or pertaining to that which conveys an intelligible meaning in the language in which it is written with no hidden meaning; as the plaintext equivalents. Often shortened to plain.

Playfair system. A type of digraphic substitution using a single matrix normally of 25 cells.

Poisson table. Table of the Poisson distribution. A type of mathematical table containing probability data applicable to the phenomena of repetitions expected to obtain in samples of random text; used in cryptanalysis to determine whether or not the repetitions observed in a given sample of cryptographic text are causal repetitions or accidental (random) repetitions.

polyalphabetic substitution. A type of substitution in which the successive plaintext elements of a message, usually single letters, are enciphered by a succession of different alphabets which may be used more than once and which are used in a predetermined order.

polygraphic, adj. Of, pertaining to, or connected with any groupings comprising two or more letters or characters.

polygraphic substitution. Encipherment by substitution methods in which the plaintext units are regular length groupings of more than one element.

polypartite alphabet. A multiliteral alphabet in which each letter of plain text is represented by a cipher unit of two or more characters whose functions are clearly defined. See bipartite alphabet, tripartite alphabet.

Porta system. A forerunner of the Vigenère system of polyalphabetic substitution, this system employs 13 alphabets formed by sliding the second half of the normal alphabet against the first half. Each alphabet may be identified by either of two key letters.

position assignment. That number of intercept targets or monitor targets which can be adequately covered by one position manned 24 hours a day.

postamble, n. The information transmitted immediately following the actual text of a message. Date, group count, and cryptographic indicators are frequently transmitted in the postamble.

post-card grille. See rectangular grille.

practice traffic. Training traffic sent for the purpose of drilling communications personnel in handling traffic; distinguished from control or dummy traffic, in which there is intended deceit.

preamble, n. The information transmitted just before the text of a message. The preamble generally includes the station serial number, the group count, the file date/time, precedence indicator, and address. Cf. heading.

prearranged message code. A code adapted to the use of organizations which require special or technical vocabulary and composed almost exclusively of groups representing complete or nearly complete messages.

precedence designation. A designation assigned, usually by the originator, to each outgoing message, indicating its degree of urgency; thus, precedence designations indicate the order in which messages are to be handled.

preliminary check coverage. The assignment of intercept operators to cover all transmissions on a link, group, or net for a prearranged length of time for the purpose of compiling information as to the stations' operation, echelon, relative importance, and other data concerning the circuit.

preliminary key. See initial key.

primary frequency. A frequency assigned for normal use on a particular circuit.

primary period. See basic period.

primary sequence. The basic sequence from which other sequences may be derived or which may be slid against another basic sequence to produce secondary alphabets.

priming key. See initial key.

priority message. A message bearing the precedence prosign P, q.v.

private code. A code constructed for the exclusive use in correspondence of a group of individuals or a company.

probable word. Plain text assumed or known to be present in a cryptogram. A crib.

probable-word method. The method of solution involving the trial of plain text assumed to be present in a cryptogram.

procedure analysis. That component of transmission security which determines trends in security and procedure violations, maintains a continual check on such occurrences, and initiates remedial and corrective measures when and where necessary.

procedure message. A short, plaindress message used to expedite the handling of traffic.

procedure sign. Prosign. An abbreviated code signal used to convey the most frequently used orders, instructions, requests, and information related to communications. Procedure signs are supplemented by operating signals.

procedure word. A word or phrase limited to radiotelephone procedure and used in lieu of a prosign.

proforma message. A message in standardized form, designed to convey intelligence by conventions of arrangement and abbreviation.

progressive alphabet system. A periodic polyalphabetic substitution system in which the successively used cipher alphabets are produced by successively sliding a pair of sequences through all possible juxtapositions.

prosign, n. Procedure sign, q.v.

proword, n. See procedure word.

pseudo-code system. A cipher system which produces a cryptogram whose groups resemble those produced by a code system.

pseudo-polygraphic system. A polygraphic substitution system in which at least one of the letters in each polygraph is enciphered monoalphabetically.

publication correction. A joint or intra-service amendment which is issued as a message, letter or memorandum, to meet operational requirements.

publication status. Past, present or future state of effectiveness of a publication.

pyrotechnics code. A prearranged code in which meanings are assigned to the various colors and arrangements of pyrotechnics.

Q. A symbol used in D/F bearing observation classification to indicate, "insufficient time for accurate measurement or classification".

Q code. A code made up of Q signals adopted by the International Telecommunications Conference at Cairo, 1938.

Q signal. See operating signal.

quinqueliteral alphabet. A cipher alphabet in which each plaintext letter is represented by a 5-character equivalent.

R. United States Military precedence prosign for ROUTINE. Usually transmitted as "RR" to ensure accuracy. Assigned to messages which must be delivered to the addressee without delay, but are not of sufficient importance to justify a higher precedence.

radar, n. Radio equipment for the determination of a target's direction and range. Derived from the phrase, "radio detecting and ranging".

radar deception. The radiation or reradiation of radar emissions in a manner intended to deceive the enemy.

radio countermeasures. All measures taken to reduce the military effectiveness of enemy equipment employing or affected by electromagnetic radiations. Radio countermeasures (RCM) may include jamming, RCM deception, RCM search or reconnaissance, or the collection, analysis, and evaluation of information pertinent to RCM, and dissemination of the resulting RCM intelligence.

radio deception. The radiation or reradiation of radio waves in a manner intended to deceive the enemy.

radio discipline. Enforcement of the rules and regulations for the use of radio.

radio fingerprinting. The process of identifying a radio station by a study of the characteristics of the emissions of its transmitter. Abbreviated RFP.

radiogoniometry. See direction finding.

radioprinter. A radio teleprinter. See teleprinter. Abbreviated R/P.

radio procedure. Standardized methods of transmission used by radio operators to save time and prevent confusion. By ensuring uniformity; radio procedure increases security.

radio silence. The shut-down of radio transmission within a command as ordered by the commander.

radio spectrum. The entire range of radio frequencies.

radio station. One, or a number of co-located transmitters and receivers operating in any number of radio links, but serving the same organization.

radiotelegraphy, n. Transmission of telegraphic signals by radio. Abbreviated W/T.

radiotelephony, n. Transmission of voice signals by radio. Abbreviated R/T.

rail-fence transposition. A transposition system in which the plain text is written alternately in two lines, one above the other and the cipher text is taken off as the two rows of the resulting diagram.

RAM. Rapid analytical machinery, q.v.

random, adj. 1. In mathematics, pertaining to unsystematic or chance variations from an expected norm. 2. In cryptanalysis, pertaining to any situation in which a statistical analysis will show variations from a calculated expected norm indistinguishable from those due to chance, provided that this analysis is not correlated with the cryptographic system involved. Thus, in a search for characteristics of the cryptographic system, statistical analyses are made, and those which show variations not likely to have been produced by chance may suggest the nature of some element of the system. The statistical analysis to be successful must be designed to provide for the possibility that variations not likely to be those produced by chance will appear and thus, by inference, must be correlated with the cryptography. The norm is calculated on the assumption that chance variation is present, and it is from this standard that variations are measured.

randomize, v.t. 1. To give random characteristics to; to allow or cause events to occur or to appear according to no order other than that determined by chance or accident; to select elements of a population at random. 2. Loosely, to re-arrange so as to exhibit no evident law of formation.

randomized code. A two-part code, q.v.

random text. Text which appears to have been produced by chance or accident, having no discernible patterns or limitations.

rapid analytical machinery. Any high-speed cryptanalytic machinery, usually electronic or photoelectric in nature. Abbreviated RAM.

raw traffic. Intercepted traffic showing no evidence of processing for communication intelligence purposes beyond sorting by clear address elements, elimination of unwanted messages, and the inclusion of a case number and/or an arbitrary traffic designator.

RCM. Radio countermeasures, q.v.

RCM deception. The radiation or reradiation of electromagnetic waves in a manner intended to deceive the enemy. (This does not include friendly traffic manipulation or communication security.)

RCM intelligence. All intelligence derived from the study of radio countermeasures.

RCM reconnaissance. See RCM search.

RCM search. The search for enemy-generated radio waves to determine existence, source, and pertinent characteristics.

read, v.t. 1. To decrypt, especially as the result of successful cryptanalytic investigation. ---v.i. To yield intelligible plain text when decrypted.

readability, n. 1. Capability of being understood, as, the readability of radio signals. 2. The extent to which cipher or code messages of a particular system can be read.

readable, adj. Pertaining to those code and cipher systems in which sufficient plaintext values or keys have been recovered to permit the reading of messages encrypted in these systems.

readable system. A system whose basic elements and specific controls have been solved to the extent that messages can be read without further cryptanalysis. Cf. exploitable system.

readdress, v.t. To direct a message to addressees not included in the original address without rewriting or re-enciphering the message.

reader, n. A language specialist who deals with a foreign language in its written form.

receipt, n. A communication sent by the receiving station indicating that a message or other transmission has been satisfactorily received.

receipt method. The method of transmission in which the transmitting station requires a receipt for each of its transmissions. Also known as "R" (Roger) method.

reciprocal, n. 1. An element which bears a reciprocal relation to another element. 2. The quotient of unity divided by any quantity. ---adj. Interchangeable as to plain-cipher relationships; (e.g., in a reciprocal alphabet, if $A_p = B_c$, then B_p must equal A_c).

reciprocal cipher alphabet. A cipher alphabet in which either of the two sequences may serve as plain or cipher since the equivalents exhibit reciprocity.

reciprocity, n. As used in cryptology, interchangeability of plain-cipher relationships (e.g., $A_p = B_c$ and $B_p = A_c$).

recognition signal. See authenticator.

reconstruction matrix. A skeleton matrix employed in the solution of cryptosystems involving a substitution matrix. It aids in the correct relative placement of plaintext or ciphertext values as recovered, and thus often affords clues as to the internal arrangement of the original matrix.

recording, n. A representation of an intercepted radio transmission by any means other than a written record, (e.g., magnetic, inked, or punched tapes; disks, wire, etc.).

recover, v.t. To solve; to reconstruct (e.g. cryptographic data or plain text).

recovery, n. 1. The process of making encrypted text intelligible through cryptanalysis. 2. Any cryptographic data or plain text obtained through cryptanalysis.

rectangular grille. A grille differing from the ordinary grille in that the apertures are greater in width than in height, and thus permit the inscription of several letters or a word in the space disclosed on the grid by each perforation of the grille. The grille itself admits of but two positions with its obverse side up and two with its reverse side up. Also called post card grille.

reduction square. A matrix employed in cryptanalysis to reduce cipher elements to a more usable form without altering their interrelationships, (e.g., to reduce a multiliteral cipher to uniliteral terms).

reflector, n. 1. An element of a cipher machine, usually with a single set of contacts wired together in pairs, each of which establishes a reciprocal circuit through the maze. 2. Specifically, in a wired rotor machine of the Enigma type, that particular rotor which bears on one side the usual 26 contact points and bears on the other side 13 wires which connect these 26 points into 13 sets of two points each; thereby effecting a reciprocal circuit. Sometimes called a reversing wheel.

regional call sign. A collective call sign used to contact a number of specific stations in a net or group, usually within a particular geographic area.

registered document. See registered matter.

registered matter. Any classified matter registered usually by number and periodically accounted for.

register number. A number assigned to registered matter for accounting purposes.

relate columns. See equate columns.

related alphabets. Any of the several secondary cipher alphabets which are produced by sliding any given pair of primary components against each other.

relative, adj. Pertaining to code groups, indicators, etc. from which a provisional encipherment has been removed; reduced to provisional, not true, figures or letters. Cf. base.

relative code. Code text from which an encipherment has been removed in relative terms, but not reduced to plain-code text, so that the groups differ from the actual, original plain code by an interval constant for every group; thus the difference between two relative code groups is the same as that between their plain-code equivalents.

relative frequency. In its cryptologic application, the ratio of the actual occurrences of a textual element to the number of possible occurrences within a given text.

relay message. A message which reaches its destination by passing through one or more intermediate stations.

releasing officer. A properly designated individual who may authorize the sending of a message for and in the name of the originator.

repaginate, v.t. To supply a new sequence of page symbols for a code book or key book.

repaginated code. A code in which the pages of the code book have been assigned a new sequence of identifying symbols.

repagination, n. The assignment of a new set of symbols identifying the pages of a code book, or key book.

repeating-key method. See periodic substitution.

repetetive encipherment. A type of encipherment in which the primary cipher text of a cryptogram is subjected to further encipherment with either the same or a different system. Double transposition is a frequently-encountered example of repetitive encipherment.

rephase, v.t. To put back in phase. See phase.

resultant period. See apparent period.

reversed standard cipher alphabet. A cipher alphabet in which both the plain and cipher components are the normal sequence, the cipher component being reversed in direction from the plain component.

reversibility, n. That characteristic of the relationship between a plain-text digraph and its cipher digraph equivalent which permits the elements of each to be reversed (e.g., $AB_p = CD_c$ and $BA_p = DC_c$).

revision, n. A complete publication, superseding all copies of the publication revised.

revolving grille. A type of grille in which the apertures are so distributed that when the grille is turned successively through four angles of 90 degrees and set in position on the grid, all the cells on the grid are disclosed only once. Also called rotating grille.

RFP. radio fingerprinting, q.v.

"R" (Roger) method. See receipt method.

room circuit. A circuit which has no connection with outside stations and which is used for encipherment and decipherment in off-line operation.

rota, n. A table of call signs, frequencies, or other communication items used in cyclic order.

rotating grille. See revolving grille.

rotation, n. The method of changing call signs or frequencies within a given initial allocation.

rotor, n. A disk which is designed to rotate within a cipher machine and which controls the action of some other machine component or produces a variation in some textual or keying element.

rotor alignment. The setting of rotors with reference to a bench mark.

rotor order. Order in which the interchangeable rotors of a cipher machine are arranged on a particular day or during a specified period.

rotor setting. A letter or number on the rim of a rotor serving to indicate its position at commencement of enciphering.

roughness, n. That characteristic of a frequency distribution where there is displayed in the distribution a pronounced variation in relative frequencies of the elements considered. Cf. smoothness.

route transposition. A method of transposition in which the ciphertext equivalent of a message is obtained by transcribing, according to any prearranged route, the cells of a matrix into which the message was inscribed earlier according to some other prearranged route.

routine message. A message bearing the precedence prosign R, q.v.

routing, n. The process of determining and prescribing the path or method to be used in forwarding messages.

routing designator. A symbol or group of symbols appearing in a message preamble, serving as a guide to radio stations in routing the message to the final recipient.

row, n. As applied to a matrix, a horizontal sequence of letters or numbers or groups thereof.

row break. In enciphered code solution, the determination of the beginning and end of the rows constituting an additive page.

row coordinate. A symbol normally at the side of a matrix, or cryptographic table, identifying a specific row of cells, used in conjunction with a column coordinate to specify an individual cell in the matrix or table. Also called row indicator.

row designator. See row coordinate.

row indicator. See row coordinate.

R/P. Radioprinter, q.v.

R/T. Radiotelephony, q.v.

run, n. See listing.

running key. In polyalphabetic ciphers, a non-periodic key arbitrarily prepared or obtained from a book or any continuous text.

running-key system. A substitution system employing a running key, q.v.

S. Strength (of radio signals). See signal strength.

sampling coverage. The assignment of intercept operators to take periodic samples of transmissions on a certain frequency.

scanner, n. A reader who examines foreign language texts to assess their intelligence content.

schedule, n. A time during which a link, group, or net is known to work.

scramble, v.t. 1. In telephony, to make telephony unintelligible to casual interception. 2. In cryptography, to mix in random or other fashion.

search, v.t. To sample transmissions on various frequency bands in an effort to find stations or other communications activities which are not already under regular coverage assignment.

search coverage. The assignment of intercept operators to listen continually on a given band of frequencies in order to discover new target frequencies in use.

secondary alphabet. An enciphering or deciphering alphabet resulting from the juxtaposition of two primary components, at least one of which is mixed. A secondary alphabet, though different in appearance from the primary alphabet, is cryptographically equivalent to the primary alphabet.

secondary frequency. A frequency assigned for use on a particular radio circuit when primary frequency becomes unusable for any reason.

SECRET. A security classification pertaining to defense information or material, the unauthorized disclosure of which could result in serious damage to the nation.

secret ink. Any of several chemicals used for writing or printing which have the property of being initially invisible to the naked eye or of becoming so after a short time. Also called invisible ink or sympathetic ink.

secret language. Text which conveys no intelligible meaning in any language or which conveys an intelligible meaning that is not the real, hidden meaning.

secret writing. 1. Visible writing in secret language. 2. Invisible writing.

sectional, adj. Pertaining to a code so constructed that a particular class of code groups represents a particular class of plaintext units; (e.g., all code groups beginning with a given symbol represent numbers, spelling groups, etc.).

self-evident code. A code whose meanings are self-evident owing to a visible connection between code groups and their meanings, (e.g., ADV means advance, ADR means address, etc.).

separator, n. 1. A word separator, q.v. 2. A stationary element between moving rotors in a wired-rotor cipher machine, which comprises a ring of contacts on which the contacts of the rotors impinge.

sequence, n. An ordered arrangement of symbols (letters, digits, etc.) having continuity. Specifically, the members of a component of a cipher alphabet in order; the symbols in a row, column, or diagonal of a cipher square in order; key letters or key figures in order.

serial number. 1. A number assigned to a document by the originating office for the purpose of counting the copies prepared and of controlling their distribution. It is not to be used for accounting purposes and therefore is not to be confused with a register number. Often called a "copy number". 2. The number of a message in a series.

seriation, n. A process of inscribing plain or cipher elements in two rows and subjecting the vertical pairs to further cryptographic treatment.

service message. A message between communications personnel pertaining to any phase of traffic handling, communication facilities or circuit conditions.

setting, n. The arrangement and alignment of the variable elements of a cryptographic device or machine at any moment during its operation.

set-up, n. 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 or for the encipherment of large numbers of messages.

SHF. Super-high frequency, q.v.

shift, n. 1. Difference in position of text in messages, offset as regards the key. 2. Slide. 3. In the operation of a teleprinter, the mechanical action which takes place when the platen is moved from the letters to the figures position, or vice versa.

shoran, n. An abbreviated name for a short range radio navigation system. It is a precision position fixing system using a pulse transmitter and receiver and two transponder beacons at fixed points.

short title. A short, identifying combination of letters and/or numbers assigned to a document or device for purposes of brevity and/or security.

sigmage, n. As used in cryptomathematics, a measure of the standard deviation from normal, expressed in terms of sigma (σ).

signal center. See communication center.

signal communication. The means of conveying information of any kind from one person or place to another except by direct unassisted conversation or correspondence.

signal intelligence. A term formerly applied to communication intelligence, with which it is synonymous.

Signal Intelligence Service. Formerly, an organization of the Army Signal Corps which was charged with the functions now performed by the Army Security Agency.

signal operation instructions. A series of orders issued periodically for technical control and coordination of the signal communication activities of a command. The SOI include related subjects such as instructions for the use of codes, ciphers, and authentication systems; and an index of the special signal communication instructions issued by an organization in the field. Abbreviated SOI.

signal security. Communication security, q.v.

signal strength. The relative audibility of a station's transmission, expressed on a numerical scale from least to greatest audibility.

significant, adj. 1. Having meaning or significance. 2. Exhibiting some feature or limitation which cannot reasonably be attributed to chance.

sign off. A signal denoting the termination of a transmission.

simple substitution. Monoalphabetic uniliteral substitution.

simple transposition. See single transposition.

simplex circuit. See simplex link.

simplex link. A radio link so constituted that communication between the two stations is possible in only one direction at a time. Within this definition, there are at least two distinct uses of the phrase: (1) To describe that system of frequency allocation, on a link of any transmission type, in which only one frequency is assigned for communication in either direction; and (2) to describe a link using single-channel teleprinter equipment.

simplex operation. A type of operation used on a simplex link, q.v.

single position. A receiving terminal manned by one operator.

single-station call. A station call-up wherein one call only (either the sending station's call or the receiving station's call) is used by the calling station.

single transposition. A transposition in which only one inscription and one transcription are effected.

S.I.T. Special identification techniques, q.v.

sked. Schedule, q.v.

skip zone. The space or region within the range of transmission wherein radio signals from a transmitter are not received. It lies between the farthest point reached by the ground wave and the nearest point at which sky waves come back to earth. Also known as dead space.

sky wave. The portion of a transmitted radio wave which is radiated outward into space. Cf. ground wave.

slid depth. The condition arising when messages are enciphered with the same key but offset with regard to that key.

slide, n. 1. In the Hagelin machine, the relative displacement between the alphabet wheel and the printing wheel. 2. The interval between two different juxtapositions of the same cipher and plain components. ---v.t. To match one sequence of text or a distribution against another sequence of text or a distribution.

slide code. A code which is varied from time to time by sliding the code groups against the plain equivalents.

slide run. An IBM listing of the results of sliding one text against another.

sliding, n. The process of testing possible placements of cipher on key by deciphering at all possible juxtapositions.

sliding components. Components which are slid against one another in the process of enciphering or deciphering.

sliding strip. A strip of cardboard or similar material which bears a sequence and which can be slid against other such strips to various juxtapositions.

smoothness, n. That characteristic of a frequency distribution where there is displayed in the distribution no pronounced variation in relative frequencies of the elements considered. Cf. roughness.

SOI. Signal operation instructions, q.v.

solution, n. In its cryptanalytic application, the process or result of solving a cryptogram or cryptosystem by cryptanalysis.

solve, v.t. To cryptanalyze. To find the plain text of encrypted communications by cryptanalytic processes, or to recover by analysis the keys and the principles of their application.

SOP. Standing operating procedure, q.v.

spacing impulse. One of the two types of impulses used in teleprinter transmission; normally, that impulse during which no current flows through the teleprinter receiving magnet. The other type of impulse is the marking impulse.

special check coverage. The complete cover of a case number for a limited period of time.

special identification techniques. A collective term including Morse operator analysis, radio fingerprinting, and direction finding. Abbreviated S.I.T.

special purpose system. Specific cryptographic aids intended only for certain types of messages. They include General and Auxiliary Signal Books and Signal Vocabulary, Authenticator Systems, Aircraft Codes, Fighter Director Vocabulary, etc.

special solution. A solution which depends on circumstances which are not peculiarly caused by the inherent principles of the particular cryptosystem. For example, solution of a periodic system by exploiting a pair of isologs which have been produced by identical sliding components but which involve two different repeating keys; solution of a double transposition system by simultaneously anagramming the corresponding elements of several cryptograms which are of identical length and which all involve use of the same specific key; etc.

specific key. An element which is used with a specific cryptosystem to determine the encipherment of a message and which includes both the message keying element and the daily keying element. It may consist of a letter, number, word, phrase, sentence, a special document, book, or table, etc., usually of a variable nature and easily changeable at the will of the correspondents, or prearranged for them or for their agents by higher authority.

speller, n. A spelling group, q.v.

spelling group. A code group of which the plain equivalent is a letter or combination of letters used for spelling words not included in the code vocabulary.

spelling table. Syllabary, q.v.

split calls. Two or more call signs which are used individually, in a specific prearranged manner to identify a particular radio station or link. For example, a particular call sign may be associated with a particular frequency, where several frequencies for a station are involved.

spotter, n. A reader who sorts traffic by means of key terms.

square, n. See matrix.

square table. A cipher square (e.g., A Vigenère table).

SSI. Standing signal instructions, q.v.

stagger, n. A pair of offset duplicates; staggered depth. ---v.t. To encipher the same plain text in a second message in depth with the first but in a position differing by one or more characters.

staggered depth. Depth in which identical plain texts are superimposed with reference to the keying elements but are offset (retarded or advanced) one or more steps with reference to each other. Were it not for this advance or retarding, the cipher texts would be identical.

standard cipher alphabet. A cipher alphabet in which the sequence of letters in the plain component is the normal, and in the cipher component is the same as the normal, but either reversed in direction or shifted from its normal point of coincidence with the plain component.

standard uniliteral frequency distribution. See normal uniliteral frequency distribution.

standing operating procedure. A set of uniform standardized procedures and techniques established by a commander as a guide for the performance of all contemplated operations capable of standardization without loss of efficiency. Abbreviated as SOP.

standing signal instructions. Signal instructions containing items of operational data not subject to change, and instructions for the use of the SOI.

star, n. The system of radio frequency usage wherein a group of stations operate on a common frequency and direct all their traffic through the net control station.

starting point. A point in a key where enciphering or deciphering begins.

star with lateral. The system of radio frequency usage wherein a number of stations operate on the same frequency with some degree of lateral communication. Cf. star.

station authentication. A security measure designed to establish the authenticity of a transmitting or receiving station.

station indicator. See base number.

station serial number. A message reference number assigned by the transmitting operator to each message transmitted in direct communication to another station. Abbreviated NR.

stator, n. An endplate, q.v.

stencil, n. See grille.

stereotype, n. A word, number, phrase, abbreviation, etc., which as a result of language habits, has a high probability of occurrence, especially at the beginning or ending of a message.

stereotyped messages. Related encrypted messages which are recognizable as such because of distinctive characteristics of the underlying plain text.

strip, n. Sliding strip, q.v. ---v.t. To remove key, especially from enciphered code.

strip-cipher device. A cipher device employing sliding alphabet strips.

stripper, n. One who recovers keys.

substitution alphabet. See cipher alphabet.

substitution cipher. 1. A cipher system in which the elements of the plain text are replaced by other elements. 2. A cryptogram produced by enciphering a plaintext message with a substitution system.

substitution system. A system in which the elements of the plain or code text are replaced by other elements.

subtractive method. See minuend method.

subtractor, n. A number or series of numbers from which numerical code, cipher, or plain text is subtracted in the process of encipherment.

suffix call sign. 1. A call sign normally associated with a unit move, in which the advanced headquarters is identified by the normal call for the unit (e.g., XYZ) with a suffix "1" (e.g., XYZ1). Since the physical separation of the two parts of the unit is temporary, no separate call sign allocation is normally made in such cases. 2. Berne-type calls in which various suffixes to a given letter call sign designate different transmitters at a single location.

sum check. 1. That digit of a textual group which by design represents the units digit of the sum of the other digits in the group. 2. To exhibit the property of a sum check.

sum-checking digit. A preselected digit (normally the final digit) in a code or cipher group which is the noncarrying sum of the other digits in the group.

summing group. A code or cipher group in which the sum of the digits is a preselected constant.

summing-trinome system. A substitution system in which each plaintext letter is assigned a unique numerical value of 0 to 27. This value is then expressed as a trinome, the digits of which sum to the designated value of the letter.

supercession date. The date on which cryptographic procedures, keys, codes, etc., are changed.

superencipher, v.t. To subject a cipher text to a further process of encipherment.

superencipherment, n. A form of superencryption in which the final step involves encipherment. ---v.t. Superencipher.

superencrypt, v.t. To subject an encrypted text to a further process of encryption.

superencryption, n. A further encryption of the text of a cryptogram for increased security. Enciphered code is a frequently encountered example of superencryption. ---v.t. Superencrypt.

super-high frequency. The range of radio frequencies from 3000 to 30000 megacycles. Abbreviated SHF.

superimpose, v.t. To write cryptographic text so that elements enciphered by the same keying elements will fall in the same column.

superimposition, n. See overlap (1).

supplement, n. A separate publication, related to a basic publication, and prepared for purposes of promulgating additional information or summaries, and may include extracts from the basic publication.

supplementary code. A code, used in conjunction with another code, containing second, or subsidiary, meanings, or special categories of meanings (e.g., geographical terms) the use of which is normally indicated by a special code group. Also called auxiliary code.

switch group. A group used within a message to indicate that the following textual elements are encrypted with a different key or code book.

syllabary, n. In a code book, a list of individual letters, combinations of letters, or syllables, accompanied by their equivalent code groups, usually provided for spelling out words or proper names not present in the vocabulary of a code; a spelling table.

syllabary square, A cipher matrix containing individual letters, digits, syllables, frequent digraphs, trigraphs, etc., which are encrypted by the row and column coordinates of the matrix.

syllabic, adj. Of, pertaining to, or denoting syllables.

symbolic form. The conventions of arrangement used by international agreement for transmitting weather information in order to conserve time and expense.

sympathetic ink. See invisible ink.

synoptic, n. (Met.) A proforma message giving complete meteorological data obtained from a single observation at a single station.

synoptic hour. (Met.) A fixed hour at which meteorological observations are made at all meteorological stations in a particular area (e.g. Europe).

synoptic period. (Met.) The interval between one synoptic hour and the next.

synthetic group. In an enciphered code system, a probable or possible cipher group produced by enciphering a known good group with an already solved key group with a view to locating other messages enciphered with this key group.

system, n. See cryptosystem.

systematically-mixed cipher alphabet. A cipher alphabet in which the component that is mixed has been disarranged by systematic procedure. Cf. random-mixed cipher alphabet.

system indicator. See discriminant.

T/A. Traffic analysis, q.v.

tactical call sign. A call sign which represents and identifies a tactical command or communications facility.

tail, vi. Of two messages, to exhibit tailing.

tailing, n. The practice of beginning the encipherment of one message with the element of key immediately following the element of key used to encipher the last textual group of the preceding message.

tandem, adj. Pertaining to a kind of cipher-machine operation in which the plain text is enciphered and the resultant cipher text simultaneously deciphered on another machine as a check on the encipherment.

tandem operation. In cryptography, electrically or mechanically coupling two cipher machines to produce automatic decipherment simultaneous with encipherment.

tape copy. A copy of a message received on tape, printed or punched, or both.

tape-to-card process. A process whereby an incoming message recorded on perforated tape is automatically punched on IBM cards therefrom.

target. Radio intercept. A specific point, area, station, group of stations, etc., toward which intercept activities are directed. Cf. mission.

task. An assignment to an intercept operator to cover the transmission of a link, group, or net.

TDS. Time division scrambling, q.v.

telecommunications. Any transmission, emission, or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, visual, or other electromagnetic system.

telecon. A teleconference, q.v.

teleconference, n. A conference between persons remote from one another but linked by a telecommunications system. Abbreviated as telecon.

telemetering, n. Automatic electrical communication, intended to indicate or record a measurable, variable quantity at a distance.

teleprinter, n. An electrically-operated instrument resembling a typewriter, used for the transmission and reception-printing of messages by electrical means. Also called teletypewriter.

teletypewriter, n. A teleprinter, q.v.

teletypewriter exchange service. Commercial service permitting teleprinter communication on the same basis as telephone service, operating through central switchboards, to stations within the same city or in other cities. This service is limited to subscribers as is telephone service. Abbreviated as TWX.

terminal, n. Equipment required to receive and reproduce in usable form one radio signal.

test element. One of the characters in a message from which the authenticator is derived.

tetragraph, n. A set of four letters.

tetranome, n. A set of four digits.

text, n. The part of a message containing the basic information which the originator desires to be communicated.

text key. Key used to encipher the text of a message.

textual element. An individual letter, a unit of encryption, or a complete word from the actual text of a message.

tfc. Traffic, q.v.

thripple, v.t. In meteorological ciphers, to substitute two three-figure groups for a five-figure group so that the sum (nonncarrying) 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.

time division scrambling. Transposition achieved by delaying elements of intelligence by varying amounts in accordance with a key. The term is normally applied to ciphony and cifax systems.

time of intercept. The time at which a message was received by an intercept operator. Abbreviated as TOI.

time of origin. The time at which a message was originated. Abbreviated as TOO.

time zone. One of the 24 longitudinal divisions of the earth's surface, each 15 degrees wide, having a standard time differing by one hour from the standard time in adjoining divisions.

TOI. Time of intercept, q.v.

TOO. Time-of-origin, q.v.

TOP SECRET. A security classification pertaining to information or material, the defense aspect of which is paramount, and the unauthorized disclosure of which could result in exceptionally grave damage to the nation.

traffic, n. All transmitted communications. Abbreviated as tfc.

traffic analysis. That branch of cryptology which, through a study of signal transmissions by all means short of cryptanalysis of message texts, assembles information concerning communication networks.

traffic-flow analysis. A statistical appraisal of the variations in the nature, volume, and direction of traffic from which certain inferences as to the causes thereof may be drawn.

traffic intercept. A copy of a communication obtained through interception.

trail, v.i. To exhibit trailing.

trailer card. An IBM card used as a supplementary card when the desired information requires more than eighty columns.

trailing, n. The practice of beginning the encipherment of one message with an element of key at a comparatively short interval after the element of key used to encipher the last textual group of the preceding message. Cf. tailing.

transcriber, n. A listener who converts foreign language voice transmissions into the written form of the foreign language.

transcription, n. 1. In a transposition system, the process of removing the text from a matrix or grid by a method or route different from that used in the inscription. 2. A written copy of a previously recorded radio transmission; also the process of preparing such copy from tapes or records.

translator, n. A reader who translates written materials from a foreign language into English.

transmission security. That component of communication security which results from all measures designed to protect transmissions from interception and traffic analysis.

transmitter call. The call sign of the radio station actually transmitting a message by radio.

transparency, direct. That characteristic of cipher text which indicates that certain plaintext elements may have been self-enciphered.

transparency, inverse. That characteristic of cipher text which indicates that certain cipher digraphs may be merely reversals of the corresponding plaintext digraphs.

transposition cipher. 1. A transposition system. 2. A cryptogram produced by enciphering a message with a transposition system.

transposition error. An error arising from the exchange of position of textual elements without a change in their identities.

transposition-mixed cipher alphabet. A cipher alphabet in which at least one component (plain or cipher) has been constructed by applying a form of transposition to either a standard or a mixed sequence.

transposition system. A cryptosystem in which the elements of plain text, whether individual letters, groups of letters, syllables, words, phrases, sentences, or code groups or their components undergo some change in their relative positions without a change in their identities.

trick, n. The usual period during which an operator is on duty. Also known as watch.

trigraph, n. A set of three letters.

trigraphic, adj. Of or pertaining to any three-character group.

trigraphic frequency distribution. A frequency distribution of successive trigraphs. A trigraphic frequency distribution of ABCDEF would consider only the trigraphs ABC and DEF. Cf. triliteral frequency distribution.

trigraphic substitution system. A substitution system in which the plaintext units are composed of three elements.

triliteral, adj. Of, or pertaining only to cryptosystems, cipher alphabets, and frequency distributions which involve cipher units of three letters or characters. See the more inclusive term trigraphic; see also triliteral frequency distribution.

triliteral frequency distribution. A distribution of the characters in the text of a message in sets of three, which will show: (a) each character with its two preceding characters or (b) each character with its two succeeding characters, or in its most usual form, (c) each character with one preceding and one succeeding character. A triliteral frequency distribution of ABCDEF would consider the groups ABC, BCD, CDE, DEF.

trinome, n. A set of three digits.

trinome-digraphic system. A substitution system in which plaintext digraphs are represented by 3-digit cipher elements.

tripartite alphabet. A triliteral alphabet in which the cipher units may be divided into three separate parts whose functions are clearly defined, viz, page, row, and column indicators of a dictionary system.

triplet, n. A group of three like symbols.

trough, n. In its cryptologic application, a point of low relative frequency in a frequency distribution.

true, adj. 1. As applied to figures or letters of key, code groups, etc., requiring no further correction to make them the same as those actually used by the encipherers. ---Ant. provisional. 2. As applied to machine-cipher depths, those that are completely in depth, i.e., as distinct from those in which there is some variation in rotors.

true periodic repetition. A repetition in the cipher text arising from a repetition of the keying cycle itself and caused by two identical sections of plain text being enciphered by the same sequences of key.

true polygraphic system. Any polygraphic substitution system in which the individual elements of the polygraphs display no evidence of monoalphabeticity, nor evidence of relationships within any group of polygraphs; that is, in a true polygraphic system, changing one letter in any plaintext polygraph affects the equivalent ciphertext polygraph in its entirety. Cf. partially-polygraphic system and pseudo-polygraphic system.

TT. Teletypewriter. See teleprinter.

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

two-element differential. The characteristic incorporated in certain codes in which the groups differ from one another by a minimum of two elements, either in identity or the positions occupied. When the elements are letters, the characteristic is called a two-letter differential; when the elements are digits, it is called a two-digit differential.

two-figure differential. A two-element differential in which the elements are digits.

two-letter differential. A two-element differential in which the elements are letters.

two-part code. A randomized code, consisting of an encoding section in which the plain-text groups are arranged in an alphabetical or other significant order accompanied by their code groups arranged in a non-alphabetical or random order; and a decoding section, in which the code groups are arranged in alphabetical or numerical order and are accompanied by their meanings as given in the encoding section.

two-square matrix system. A digraphic substitution system which normally employs a matrix consisting of two 5 x 5 squares arranged either horizontally or vertically.

TWX. Teletypewriter exchange service, q.v.

U. A symbol used in D/F fix evaluation to indicate the fix is outside the limit of accuracy of a "D" fix. See D.

UHF. Ultra-high frequency, q.v.

ultra-high frequency. The range of radio frequencies from 300 to 3000 megacycles. Abbreviated UHF.

undulator tape. Inked tape, q.v.

uniliteral, adj. Of, or pertaining only to cryptosystems, cipher alphabets and frequency distributions which involve cipher units of single letters or characters. See the more inclusive term monographic; see also uniliteral frequency distribution.

uniliteral frequency distribution. A simple tabulation showing the frequency of individual characters of a text.

uniliteral (simple) substitution. A cryptographic process in which the individual letters of a message text are replaced by the single-letter cipher equivalents.

universal stereotype. A stereotype commonly used by many originators. Cf. local stereotype.

unrelated cipher alphabets. Separate and distinct cipher alphabets having no relationship to one another in any way.

validity grading. Any method of indicating in a brief manner the degree of reliability of information derived from or used in various COMINT activities.

variable spacing. During encryption on cipher machines, the random use between words of two or more of the following throughout the message: (a) no space; (b) normal space; (c) more than one space.

variant, n. 1. One of two or more cipher or code symbols which have the same plain equivalent; also called variant value. 2. One of several plaintext meanings which may be represented by a single code group.

variant call signs. Two or more call signs which may be used interchangeably to identify a particular radio station. Also known as alternate calls.

variant system. A substitution system in which some or all plaintext letters may be represented by more than one cipher equivalent.

variant value. See variant

vertical digraph. A pair of letters written one over the other.

vertical two-square matrix system. A digraphic substitution system employing a matrix which normally consists of two 5 x 5 squares arranged vertically.

very high frequency. The range of radio frequencies from 30 to 300 megacycles. Abbreviated VHF.

very low frequency. The range of radio frequencies below 30 kilocycles. Abbreviated VLF.

VHF. Very high frequency, q.v.

Vigenère square. The cipher square commonly attributed in cryptographic literature to the French cryptographer Vigenère, having the normal sequence at the top (or bottom) and at the left (or right), with cyclic permutations of the normal sequence forming the successive rows (or columns) within the square.

visible writing. Writing in which the characters are inscribed with ordinary writing materials and can be seen with the naked eye. Cf. invisible writing.

visual analysis. A procedure involving inspection of superimposed punched IBM cards.

VLF. Very low frequency, q.v.

voice call sign. A word or combination of words used in voice transmission to identify a radio station.

voice translator. A listener who translates recorded foreign language voice transmissions to English.

war indicative. (Met.) Value substituted for a base number during war time to conceal the identity of the base number.

watch. The usual period for which an operator is on duty. Also known as trick.

wave propagation. The radiation, as from an antenna, of radio frequency energy into space.

weather code. A code used for the transmission of weather data.

weather collective. A general broadcast to all meteorological centers in a large area of all the synoptic weather observations made in that area at a particular (synoptic) hour.

weather synoptic. A proforma message giving complete meteorological data obtained from a single observation at a single station.

Wheatstone cipher device. A cipher device consisting essentially of two rings mounted concentrically in a single plane, the outer (and larger) ring being the plain component of the device and comprising 27 equi-sized divisions, the inner (and smaller) ring being the cipher component, comprising 26 smaller divisions. The device incorporates two hands (similar to those on a clock) pivoted at the center of the device--the larger hand serving the outer ring and the smaller hand the inner--so geared together that for each complete revolution of the larger, the smaller turns through one complete revolution plus one twenty-sixth.

Wheatstone tape. Paper tape on which code signals (dots and dashes) are recorded in the form of two-unit perforations; used for automatic transmission of Morse code.

wheel, n. Rotor, q.v.

window, n. 1. Aperture in a grille through which one or more letters can be written or read. 2. An aperture in the cover of a cipher machine through which one of a series of letters or numbers on the peripheries of the rotors of a cipher machine can be read, serving as a reference point for setting the rotors.

word pattern. The characteristic arrangement of repeated letters in a word which tends to make it readily identifiable when enciphered monoalphabetically.

word separator. A unit of one or more characters employed in certain cryptosystems to indicate the space between words. It may be enciphered or unenciphered. Also called a word spacer.

word transposition. A cryptosystem in which whole words are transposed according to a certain prearranged route or pattern.

writer, n. The person who actually prepares and signs the message blank. The writer may be the originator or his offically designated representative.

W/T. Wireless telegraphy; radiotelegraphy, q.v.

X test. See chi test.

Y. United States Military precedence prosign for EMERGENCY. Usually transmitted as "YY" to ensure accuracy. Assigned to messages amplifying reports of initial enemy contact and for messages required in situations of emergency which affect the current implementation of a tactical action.

Z. 1. United States Military precedence prosign for FLASH. Usually transmitted as "ZZ" to ensure accuracy. Assigned to messages reporting initial enemy contact, or special emergency operational combat traffic.

2. Used as a suffix on a date time group to indicate Z time, q.v.

zeroize, v.t. To restore cryptographic elements of a cipher machine to a fixed original position.

zoning, n. In enciphered code systems, the practice of limiting commands to the use of certain specified blocks of pages in an additive book.

Z time. The time according to the 24-hour clock within the time zone centered on the zero meridian of longitude. Formerly referred to as GCT (Greenwich Civil Time) and now known as GMT (Greenwich Mean Time.)

(BLANK)