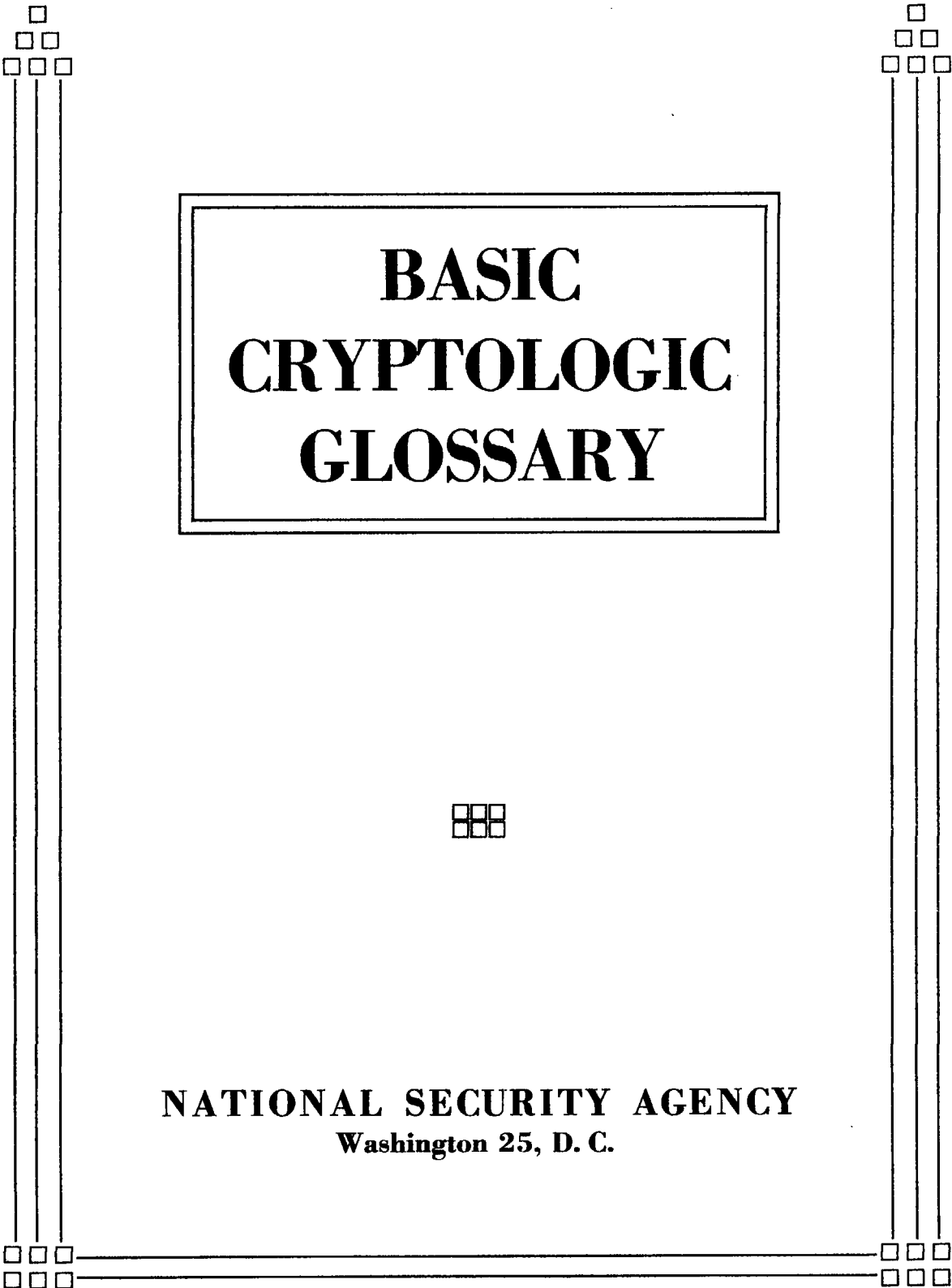


~~CONFIDENTIAL~~
~~Modified Handling Authorized~~



**BASIC
CRYPTOLOGIC
GLOSSARY**

NATIONAL SECURITY AGENCY
Washington 25, D. C.

~~CONFIDENTIAL~~
~~Modified Handling Authorized~~

MEMO ROUTING SLIP

REF ID: A64719
CONCURRENCE OF SENIOR OFFICERS

1	NAME OR TITLE <i>Mr. W. F. Friedman</i>	INITIALS	CIRCULATE
	ORGANIZATION AND LOCATION	DATE	COORDINATION
2			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

Here is the glossary you asked for. At the moment there is being multilithed a draft (for coordination) of a TOPSEC-you-know what glossary, which will eventually be printed as an Agency document.

Also enclosed is an unclassified cover in probability which I thought you might find interesting.

FROM NAME OR TITLE <i>W. Z. ...</i>	DATE <i>23 July 57</i>
ORGANIZATION AND LOCATION	TELEPHONE <i>663</i>

DD FORM 1 FEB 50 95

Replaces DA AGO Form 895, 1 Apr 48, and AFHQ Form 12, 10 Nov 47, which may be used.

16-48487-4 GPO ☆

~~CONFIDENTIAL~~

~~Modified Handling Authorized~~

NATIONAL SECURITY AGENCY

Washington 25, D. C.

Basic Cryptologic Glossary

~~CONFIDENTIAL~~

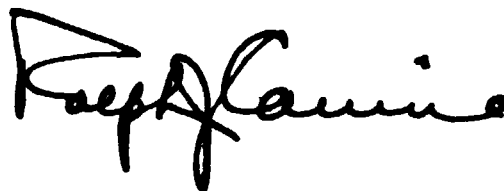
27 June 1955

LETTER OF PROMULGATION

The wide field of activity of modern cryptology, together with the unusual nature of its highly technical operations, has given rise to a diverse and uncoordinated terminology. Certain terms, through long usage, have become more or less standard and generally acceptable while other terms hold different meanings in different areas.

The lack of standardization has resulted, at times, in confusion and misunderstanding.

This is the first of a series of prescriptive cryptologic glossaries designed to help standardize cryptologic terminology. It is issued with a low classification so that it may be freely distributed in working areas and have the desk-top availability of a standard dictionary. Its frequent and wide-spread use is recommended.



RALPH J. CANINE
Lieutenant General, US Army
Director

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~**PREFACE**

1. In the preparation of this glossary 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, methods, 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.

2. The terms in the present glossary are arranged in 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 long dash followed by the abbreviation of the part of speech, and the appropriate definition. Italicizing of terms in the text of the definitions 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.

~~CONFIDENTIAL~~

BASIC CRYPTOLOGIC GLOSSARY

- A.** Used as a symbol in various classification and evaluation systems, as follows: 1. In cryptanalysis and 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 DF bearing observation classification, to indicate that all bearings are within an arc of 4 degrees. 4. In DF fix evaluation, to indicate a 90% probability that the true position of a given transmitter is within 25 miles of the fix. 5. Used followed by a number to indicate the location of a group from the beginning of a message, (i. e., the third group is called "A3").
- accidental repetition.** A repetition produced fortuitously, and not by the encipherment of identical plaintext characters by identical keying elements. Cf. CAUSAL REPETITION.
- acknowledgment, n.** A 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*).
- addee.** *Addressee*, q. v.
- 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 unit, code group, or plain text, usually by *cryptographic arithmetic*.
- additive book.** A book comprising a group of additive tables.
- additive position.** The location in a set or series of additives 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. Cf. ROUTING DESIGNATOR.
- 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, placed in the heading of a message, used to identify one or more commands, authorities, activities, units, or geographical locations; used primarily for the addressing of communications.
- address indicating group.** An address group which represents a specific set of action and/or information addressees. The identity of the originator may also be included. Abbr. AIG.
- ADFGVX system.** A German high-command cipher system used in World War I. Essentially, a bilateral substitution system employing a 6 x 6 square, to which a columnar transposition was subsequently applied.
- administrative link or net.** Links or nets used solely to pass administrative and command traffic via the organizational chain of command. Lateral working may also be noted.
- 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).
- alphabetical code.** See ONE-PART CODE.
- alternate callsign.** See VARIANT CALLSIGN.
- alternate control.** A radio station authorized to assume control of a net when the normal control station is unable to operate.
- alternate group.** See VARIANT.
- alternate horizontal route transposition.** Row transposition in which the route followed is alternately from left to right and from right to left in successive rows.
- alternate vertical route transposition.** Columnar transposition in which the route followed is alternately up and down in successive columns.
- alternative.** VARIANT, q. v.
- amplitude modulation.** In transmission, the process in which amplitude of a carrier wave is varied with time in accordance with the waveform of superimposed intelligence, e. g., speech.
- 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, plain code, or intermediate cipher text.
- analogue, n.** A machine which produces the same cryptography as another machine although the two machines may differ in construction. Generally applied to a cryptanalytic device or machine.
- aperiodic system.** A cryptographic system in which the method of keying results in the suppression of cyclical phenomena in the cryptographic text.
- apparent period.** The period usually ascertained first as a result of the study of the intervals between repetitions in a cryptogram. This may be a secondary period, and may or may not be broken down into component primary periods. Cf. BASIC PERIOD.

~~CONFIDENTIAL~~

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

applique unit, teleprinter. A special cipher attachment used in connection with a teleprinter to encrypt and decrypt teleprinter messages.

arbitrary group. A code group derived by applying *relative key* to the enciphered code text; a relative-code group, not on true base.

ARK traffic. That raw traffic which is forwarded by electrical means, and logs, daily coverage reports, and other communications intelligence technical reports in message form.

array, n. A number of elements arranged in rows and columns; as a square or rectangle.

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.

audio frequency. A frequency range which can be detected as sound by the human ear. The range of audio frequencies extends approximately from 20 to 20,000 cycles per second.

aural observation. In direction finding, a bearing observation obtained by the use of headphones or loud-speaker.

authentication, n. A security measure, usually involving a challenge and reply, designed to protect a communication system against fraudulent transmission. C. MESSAGE AUTHENTICATION, and STATION AUTHENTICATION.

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.

automatic Morse. A Morse system in which the sending and receiving instruments are automatic.

automatic relay. A type of relaying in which telegraphic impulses sent to the next destination are not only amplified, but also restored to original length and form. This method is used for long distance communication and is generally effected via one or two connecting relays. Cf. ORDINARY RELAY.

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 radio frequency derived by averaging several measured frequencies which are approximations of the 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 cryptanalysis and traffic analysis, to describe the validity of an identification or location as "almost certain." 2. In DF bearing observation classification, to indicate that all bearings are within an arc of 10 degrees. 3. In DF 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 multiliteral cipher system invented by Sir Francis Bacon (1561-1626) in which the cipher units are composed of arrangements of five elements, each of which may be chosen from one of two categories.

ban, n. A fundamental scoring unit for the odds on, or probability of, one of a series of hypotheses. In order that multiplication may be replaced by addition, the ban is expressed in logarithms.

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

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

base number. In meteorology, a group 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, indicative, or WMO number.

basic book. The code book used in an enciphered-code system.

basic callsign. A constant group, resembling a regular callsign, which is encrypted to derive the secret callsign of a particular radio 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.

basic station designator. A semi-permanent identification number or letter group assigned to a radio station for purposes of deriving its callsign by some process of selection from a master list, block, or book of callsigns. Cf. BASIC CALLSIGN.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

- basket, n.** 1. A removable component of a cipher machine in which rotors revolve. 2. A removable component of a printing device used to hold the type bars or type wheels.
- baud, n.** The unit impulse of the code employed. Normally the impulse of shortest duration which can appear alone in a given telegraphic system, e. g., the dot in the Morse code, the impulse of teleprinter systems.
- Baudot alphabet.** A five-unit code applied to teleprinter systems by Jean Maurice Emile Baudot (1845-1903). It employs a 32-element alphabet designed particularly for telecommunications wherein each symbol intended for transmission is represented by a unique arrangement of five *mark* or *space impulses*, q. v.
- Baudot code.** *Baudot alphabet*, q. v.
- BC.** *Broadcast*, q. v.
- bearing, n.** In direction finding, the angle in degrees (reading clockwise) between true north and the line from the observer to the target.
- Beaufort system.** In cryptology, a polyalphabetic substitution system employing a key word in connection with a Vigenere square, but differing from the normal Vigenere method in its rules for application of the key.
- begin spell.** The plain equivalent of a code group indicating that the groups immediately following represent elements taken from the syllabary or other special list. Often called switch group.
- bench mark.** A mark on the casing of a cipher machine used as a reference point in the alignment of rotors.
- Berne lists.** Listings published by the International Telecommunications Union (formerly in Berne, now in Geneva, Switzerland), of call signs, frequencies, etc., allocated to member nations.
- Berne-type call sign.** An *International-type call sign*, q. v.
- bias, n.** 1. In teleprinter transmission, the lengthening of the *mark impulse* and a corresponding shortening of of the *space impulse*, or vice versa. 2. A permanent negative potential applied to the grid of a vacuum tube.
- 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 having 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 code.** In electronics, a code composed of a combination of entities, each of which can assume one of two possible states.
- 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 multiliteral alphabet in which the cipher units may be divided into two separate parts whose functions are clearly defined, e. g., 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 breaking 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 of indicating the true beginning and ending in a distinctive manner.
- bit, n.** In mathematics, a digit in the binary system, usually represented as 0 or 1. Similarly, in electronics, a quantity of intelligence which is carried by an identifiable entity, and which can exist in either of two states.
- 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.** A method of transmission in which the sending station sends traffic to a receiving station which does not respond, either because of temporary conditions or for security considerations. Receipt may be made at a later time by radio or other means. Cf. BROADCAST.
- 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, numerical, or other systematic order.
- blocked code.** A form of modified one-part code in which the code groups and their corresponding plaintext values are arranged in one-part order within blocks which themselves are scattered in two-part order within the code. When these reshuffled blocks are consistently of the same length as a page, the system is called a *repaginated code*.
- Boehme equipment.** A terminal equipment manufacturer's name loosely used to designate equipment for automatic Morse transmission and reception; originally applied to equipment used in transmitting International Morse Code by passing Wheatstone tape through a keying head, and in receiving for recording International Morse Code by ink syphon equipment on a moving paper tape.
- boil, v. t.** In the cryptanalysis of *noncrashing* systems, to line up a large number of encipherments of the same phrase and by elimination to arrive at plain text.
- bone traffic.** Logistical and administrative messages.
- bookbreaker, n.** A cryptanalyst who specializes in the recovery of plaintext values in code books.
- bookbreakers' index.** A type of IBM code index in which a code group is replaced by its plaintext value when known.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

bookbreaking, 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 which is destined for two or more addressees and is of such nature that the originator considers that no recipient needs to be informed as to the other addressees. All addressees are indicated as action. Book messages are prepared in the same manner as multiple-address messages with the exception that all addressees are indicated as action and the book message is sent to each addressee separately.

boustrophedon, n. In transposition, the method of taking each successive row or column in the direction opposite to that in which the previous row or column was taken. The terms *alternate horizontal route transposition* or *alternate vertical route transposition* are preferable.

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

brevery 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. 1. Generally, any method of exhaustive trials; e. g., an attack based on trial of all possible combinations of the cryptographic variable of a cipher machine in order to recover plain text from cipher text. 2. More specifically, a machine process which searches for multiple hits between messages by means of exhaustive trials.

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

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. Also see BREAK.

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 them in the text of the message by bisection or other procedure.

bust message. A message or set of related messages containing an error in encipherment or violating standard cryptographic security practices so as to jeopardize the security of the message or the system and thus be of potential value to the cryptanalyst.

C. Used as a symbol in various classification and evaluation systems, as follows: 1. In cryptanalysis and traffic analysis, to describe the validity of an identification or location as "fair." 2. In intercept operations as a suffix to a frequency to denote "confirmed." 3. In DF bearing observation classification, to indicate that all bearings are within an arc of 20 degrees. 4. In DF fix evaluation, to indicate a 90% probability that the true position of a given transmitter is within 100 miles of the fix. 5. In communications, a prosign meaning "correct" or "correction follows."

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.

Caesar slide. Offset of a normal alphabet by a given amount.

cake, n. 1. A component of a Hagelin key generator. 2. A matrix.

call, n. A transmission made for the purpose of identifying the transmitting station and the station for which the transmission is intended.

call number. A number which in itself is a complete callsign.

callsign, n. Any combination of letters, numbers, or a combination of both, used as the identification for a communications facility, command, authority, activity, or unit; used for establishing and maintaining communications. In U. S. military practice used also for the purpose of identifying message originators and addressees.—adj. Of or pertaining to a callsign or callsigns, as callsign generation.

call-up, n. 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 callsign.

canal, n. One of the high-speed communications "channels" that are transmitted simultaneously by employing frequency shift or comparable equipment. Each canal may carry either a voice link, a Morse link, a single-channel link, or a multi-channel link.

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, n. A target net, link, group, or other communications entity represented by a *case notation*, q. v.

case book. A listing of all known cases by callsign sequence or by frequency sequences.

case notation. An arbitrary group of letters and numbers assigned by a communication intelligence agency to designate a particular target, link, group, net, etc., as identified by the agency.

case number. A *case notation*, q. v.

categories, n. Classes of meanings grouped together by the *bookbreaker* in the reconstruction of a code book. Common categories are punctuation, grammatical indi-

~~CONFIDENTIAL~~

- cators, cardinal and ordinal numbers, dates, etc. Cf. CATEGORY NUMBER.
- category number.** A number assigned by the book-breaker to a code group whose meaning belongs to a certain category for the purpose of bringing all meanings of a given category together in a block in the encode section of a two-part or *hybrid code*.
- causal repetition.** A repetition produced by the encipherment of identical plaintext characters by identical keying elements. Cf. ACCIDENTAL REPETITION.
- CCR.** Communications control room.
- cell, n.** An individual small square on cross-section paper, grilles, etc.
- centiban, n.** A scoring unit for probability equal to one one-hundredth of a *ban*, q. v.
- chadded tape.** Perforated teleprinter tape; also known as fully-chadded tape, punched tape, and chad tape. Cf. CHADLESS TAPE.
- chadless tape.** A tape used in printing telegraphy/teleprinter operation. The perforations are not completely severed from the tape, thereby permitting the characters representing the perforations in the tape to be printed on the same 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.** The succession of commanding officers from a superior to a subordinate through which command is exercised. Also called Command Channel.
- challenge and reply.** 1. In authentication, a procedure by means of a prearranged system whereby one transmitter requests authentication of another transmitter (the challenge) and the latter by a proper reply establishes its authenticity (the reply). 2. In establishing identity, the challenge and reply is a prearranged method whereby one station identifies itself and requests the identity of another (the challenge) and the latter identifies itself (the reply).
- 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 callsign.** An assigned callsign which is changed periodically according to a prearranged system.
- channel, n.** 1. A frequency or narrow band of frequencies of sufficient width for a single radio communication. 2. Each of the separate parts of a transmission type capable of carrying simultaneously several different communications as in a two- or six-channel radioprinter. 3. Loosely, a lane. 4. One of the grooves on a *channel-board* into which alphabet strips are inserted.
- channel board.** A base made of metal, paper, plastic, or other material containing a series of channels into which alphabet strips may be inserted and slid. Also known as *strip board*.
- channel designator.** One or more letters assigned to a channel for its identification.
- channel number.** A number assigned sequentially to each transmission passing over a particular channel, to determine continuity and accountability of the transmission.
- 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, n.** Any unofficial communication between communication operators. Sometimes used to refer to all transmissions except messages between communication operators. Also called chat.
- check bearing.** In DF, a bearing observation made on a transmitter of known position in order to check the accuracy of DF equipment.
- check decryption.** The process of insuring by *decryption*, prior to transmission of an encrypted message, that the message was properly encrypted.
- chi, n.** The Greek letter χ , hence the chi test (cross product test).
- 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 than 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 sum 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 instructions or information on cryptographic or other communications subjects.

~~CONFIDENTIAL~~

cipher, n. 1. A cipher system. 2. A cryptogram produced by a cipher system.—adj. Pertaining to that which enciphers or is enciphered. See also CIPHER TEXT.

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

cipher clerk. A clerk who enciphers and deciphers messages.

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

cipher device. A relatively simple mechanical contrivance for encipherment and decipherment, usually hand-operated or manipulated by the fingers, such as sliding strips or rotating disks.

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 relatively complex apparatus or mechanism for encipherment and decipherment, usually equipped with a keyboard and often requiring an external power source.

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

cipher system. Any cryptosystem in which cryptographic treatment is applied to plaintext 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.—adj. cipher-text. 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.

circulix, n. A square matrix each of whose rows is a slide by one position to the right of the preceding row. A *vigenère square* is a type of circulix.

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 cryptographic procedures.—adj. Using or pertaining to civision.

clandestine traffic. Secret or hidden traffic. Cf. ILLICIT TRAFFIC.

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

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.

click, n. Generally a pattern hit or coincidence. A coincidence of more than one element under specific conditions.

close garble. In digit codes a garble is called a "close garble" if the incorrect digit is one point higher or lower than it should be; e. g., a 3 for a 2 or 4, a 0 for a 9 or 1, etc.

code, n. 1. A *code system*, q. v. 2. A *code book*, q. v. 3. A system of signals used in electrical or electronic communication.—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.—adj. Codebook.

codebook reconstruction. *Bookbreaking*, q. v.

codebook recovery. *Bookbreaking*, q. v.

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. In machine processing, a numerical or alphabetical listing of plaincode groups with preceding and succeeding groups, compiled from a number of messages. Often called a code phrase index.

code message. A cryptogram produced by encodement.

code number. 1. Any number which conveys a meaning, prearranged by the correspondents, other than its conventional one. 2. Serves the same purpose as *codeword*, q. v.

coder, n. An initial-stage component of a ciphony or cifax machine which converts plain speech or plain facsimile into an on/off signal.

~~CONFIDENTIAL~~

code system. A cryptosystem in which arbitrary groups of symbols represent plaintext units of varying 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.

codeword, n. 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 within the text and encrypted.

coincidence, n. A recurrence of textual elements (single letters, digits, digraphs, etc.) occurring within a message or between messages.

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, n. In meteorology, a collection of weather reports from several stations for the same observation time, transmitted as a single message.

collective call sign. A call sign representing two or more communication facilities, commands, authorities, etc.

collocate, v. t. To ascertain by analytic or other means that two transmitters, stations, or units are active 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 is obtained by inscribing the plain text into a matrix in any way except vertically and then transcribing the columns of the matrix.

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.*

COMINT channels. A closed system of distribution through which is passed materials for the COMINT community only.

COMINT community. All those individuals, and organizations, or committees composed of such individuals, who have been indoctrinated and cleared and

have access to COMINT material and procedures for production, consumption, study, or other use.

COMINT element. Any component of the COMINT community, regardless of size or geographical location.

communication center. An organization charged with the responsibility for receipt, transmission, and delivery of messages. It normally includes a distribution center, a message center, a cryptocenter, transmitting facilities, and receiving facilities. Also known as signal center. Abbr. comm. cen.

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

communication intelligence. 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 a study of communications. *Cryptosecurity* and *transmission security* are the components of communication security. Abbr. COMSEC.

communications instructions. See SIGNAL OPERATION INSTRUCTIONS.

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.

commutator, n. 1. A device for reversing the direction of an electric current. 2. An attachment for the armature of a dynamo for commutating or rectifying the induced currents in the armature conductors, or in a motor for conveying the current to the conductors.

commutator wheel. See HALF-HEBERN WHEEL.

comparator, n. An analytic machine designed to make exhaustive trial comparisons between sets of text. The comparisons are scored and, when the score meets a predetermined criterion, the machine makes a record of the fact.

complement, n. The difference between any integer and the modulus used, ordinarily 10.

complex receiving. A system of radio frequency usage involving two or more stations in a net, wherein each station is allotted a different receiving frequency and all stations when sending to a particular station use the frequency allotted to that station.

complex sending. A system of radio frequency usage involving two or more stations in a net wherein each station is allotted a different frequency and uses that frequency to contact the other stations.

complex star. A star in which control uses one frequency and outstations use one or more different frequencies.

complex working. A system of radio frequency usage in which two or more stations communicate with each other on different frequencies. This general term includes *complex sending* and *complex receiving, q. v.*

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

component, n. 1. One of the two sequences (plain and cipher) which compose a cipher alphabet. 2. An independent or semi-independent part of a machine or device.

composite code book. A list of the most common code groups in all available codes of a given government arranged in specific order and including plaintext values and frequency of occurrences 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 of a given government. It is used to determine whether the plain code underlying an additive system is a known code.

compromise, n. The availability of classified material to unauthorized persons through loss, theft, capture, recovery by salvage, defections of individuals, unauthorized viewing, or any other physical means.

compromised code (key table, etc.). 1. One which has fallen into unauthorized hands. 2. In COMINT practice usually an enemy codebook (key table, etc.) which has become known, in whole or in part, by purchase, theft, photography, or other such means. Opposed to *recovered code*, q. v.

computer, n. A machine for executing prescribed programs, especially a high speed automatically sequenced machine.

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. *Brevity code*, q. v.

condenser, n. In cryptology, 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. Cf. SECRET, TOP SECRET.

confirmed frequency. The radio frequency on which a target is known to operate. Confirmation is obtained by compromise or by continued intercept. May be indicated by the letter "C" following the frequency.

consolidated codebook. A code vocabulary derived from combining the complete vocabularies of codebooks of the same service of a given government or non-governmental group.

contact, n. The establishment of communication between two stations, usually involving exchanges of signal strength and readability, but no transmission of messages. Cf. CHATTER.

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, code books, etc., on a given cryptochannel. In traffic analysis, the maintenance of continuity involves the tracing of changes in callsigns, frequencies, schedules, or other variable elements assigned to a given radio station, link, or net.

continuous wave. A radio signal which maintains a constant frequency. In continuous wave radio emission, the transmission is interrupted to send letters, numbers, symbols, or other meanings, in Morse or other "codes." Abbr. CW.

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 encrypted; because it depends upon some element of the message text, the control varies from message to message. 2. *Net control station*, q. v.

control position. That position on an IBM card or in an IBM listing which contains the fundamental data on which the file is arranged for study. For example in an index the control position is the position on which the file has been sorted for tabulation.

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 10 x 10 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; also called HARD COPY.—v. t. To prepare a written record of a radio transmission.

copy number. See SERIAL NUMBER.

core, n. In cryptology, the wiring in a rotor.

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

correction factor. In cryptography, the constant difference between a group of code or of key in relative form and a code or key in its original or primary form. Also called corrector.

correspondent, n. One who communicates with another over a radio link or by other means.

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

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

- 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 determine the adequacy of interception.
- cover call sign.** In U. S. military usage 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.
- covername, n.** An arbitrary word used, for security reasons, to indicate a specific meaning such as a device, program, place, or unit and which specifically has no semantic connection with its meaning.
- cover number.** A general term for numerical code values used to designate a unit or place.
- CQ.** A general call, for all stations on a radio net.
- crest, n.** In its cryptologic application, a point of high relative frequency in a frequency distribution. Also called a peak.
- 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.* 1. To fit assumed or known plain text or keys into the proper position in an encrypted message. 2. In T/A to equate an unknown element, particularly call signs and addresses, to one that is already known, especially applicable in case of compromise.
- crib dragging.** A method of cryptanalytic attack in which a crib is assumed and tested 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 sum test.** 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 analysis of encrypted messages; the steps or processes involved in converting encrypted messages into plain text without initial knowledge of the key employed in the encryption.
- 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 encrypting and decrypting messages.
- cryptochannel, n.** A complete system of communication between two or more holders.
- crypto-communication, n.** Any communication that has been encrypted. Also the act of communication by means of cryptograms.
- 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 designated outgoing messages and decrypt incoming encrypted 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.
- cryptoguard, n.** The activity charged with the responsibility of encryption and decryption of messages for other organizations or activities which hold few or no cryptosystems.
- 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 means and methods of producing communication intelligence and maintaining communication security; for example, cryptology includes cryptography, cryptanalytics, traffic analysis, interception, specialized linguistic processing, secret inks, etc.
- cryptomannerism, n.** A habit of a message writer or cryptographer which results in a stereotype.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

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 cryptographic applications.

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

crypto-operating instructions. In cryptography, instructions prescribing 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.

C/S. *Call sign*, q. v.

CT. Control station. See NET CONTROL STATION.

C→P (read "C to P") sequence. In transposition cipher solution, a sequence, the successive terms of which indicate the positions that the successive letters of the cipher text occupy in the plain text. Also known as decipher sequence. Cf. P→C SEQUENCE.

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, n. 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 DF bearings. 3. That portion of a recording containing a continuous period of intercept on a given frequency, except where it is necessary to continue the recording on another disc, record, or tape.

cut-in, n. A message, the beginning of which was not intercepted. Also called an "In-here" message.

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 9 become the Morse equivalent of A, U, V, 4, 5, 6, B, D, N, and T, respectively. 2. A system of abbreviated Morse numbers, as letter-for-number substitution.

cut-out, n. A message, the last part of which was not intercepted.

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

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

cycle interruption. A cryptographic procedure applied in the operation of some cipher systems whereby the normal periodic 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 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 ciphertext repetitions in a cryptogram enciphered with a repeating key.

cyclometric, adj. Pertaining to the motion of rotors, so designed that a rotor turns once when and only when its *senior rotor* has completed one revolution. Cf. ENIGMA-TYPE MOTION.

D. Used as a symbol in various classification and evaluation systems as follows: 1. In cryptanalysis and traffic analysis, to describe the validity of an identification or location as "tentative." 2. In DF bearing observation classification, to indicate that one or more bearings are outside an arc of 20 degrees. 3. In DF 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, used when expressing dots and dashes vocally.

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-group check. A transmitted group of a message giving the day of the month and the number of groups transmitted, not including the date-check group. When this group is sent, it is usually the last group of the message.

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 at which the message was prepared for transmission, 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

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

- hour. A letter or letters may be added to indicate time zone. Generally this group is expressed in Z time (i. e., Greenwich Mean Time) for simplification, regardless of location. Abbr. DTG.
- decabit**, n. A binary expression composed of ten bits.
- deception**, n. Any practice carried on within a communications system for the purpose of confusing or misleading the enemy.
- deciban**, n. A scoring unit for probability factors equal to one-tenth of a *ban*, q. v.
- decimated alphabet**. An alphabet produced by *decimation*, q. v.
- decimation**, n. The process of selecting members of a series by counting off at an arbitrary 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.
- decipher sequence**. See C→P SEQUENCE.
- 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**. In machine processing, 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 encrypted communication into an intelligible one by a reversal of the cryptographic process used in encryption. (This does not include solution by cryptanalysis.)
- decryption**, n. The act of decrypting.
- decryptomt**, n. 1. The act of decrypting. 2. The text produced by decryption.
- dedupe**, v. t. To remove duplicate copies of messages from a quantity of intercepted traffic.
- deferred message**. A message bearing the precedence prosign *M*, q. v.
- degarble**, v. t. To make emendations in a garbled text.
- delta**, v. t. To *difference*.
- delta count**, n. A frequency count of differences.
- delta difference**. Lateral difference between two successive elements.
- delta I. C.** Index of coincidence applied to a small sample. See INDEX OF COINCIDENCE.
- 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.
- DF**. *Direction finding*, q. v., or direction finder, radio direction finding, radio 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 differences, usually minor, between frequent code groups.
- difference table**. A list which presents a sorted set of differences of code groups, each difference occurring only once. The code groups producing the difference are not given, but rather an indication of the likelihood of occurrence of that difference is given, all ways of arriving at that difference having been considered.
- 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. Abbr. "DF."
- direct signal**. See REVERSED POLARITY.
- direct standard cipher alphabet**. A cipher alphabet

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

- in which both the plain and cipher components are the normal sequence, the two components being juxtaposed in any of the noncrashing placements. Cf. REVERSED STANDARD CIPHER ALPHABET.
- 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, used when expressing dots and dashes vocally. 2. A mark, usually a period, comma, or hyphen, used to denote a missing symbol. In all machine produced material, a dit is represented by a hyphen.—v. t. To denote missing symbols with dits.
- double banking.** Having more than one intercept position listening to a target in order to assure complete coverage.
- double-channel operation.** Simultaneous transmission on two frequencies by a single station. Cf. DUAL OPERATION.
- double frequency shift.** A system of transmission in which a four-position frequency shift signal is used to transmit simultaneously two independent channels of Morse, or any baud-based or bit-based keyed system. Abbr. DFS.
- double garble.** A garble of two elements of a code group. Cf. ONE-PLACE GARBLE.
- 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. Also called two-point hit.
- double position.** Two receiving terminals mounted together and manned by one operator.
- double side band.** A method of transmission in which the frequencies produced by the process of modulation are symmetrically spaced both above and below the carrier frequency and are all transmitted. Abbr. DSB.
- double single side band.** Two unrelated single side-band signals transmitted with one suppressed or reduced carrier. Abbr. DSSB.
- 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.** 1. A digraph or dinome in which a letter or a digit is repeated (e. g., LL, EE, 22, 66, etc.). 2. A code group representing two unrelated plaintext meanings.
- 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 material.
- drafter, n.** A person who actually composes a message for release by the originator or the releasing officer.
- drill message.** *Practice message.* q. v.
- drill traffic.** See PRACTICE TRAFFIC.
- drum, n.** 1. A cylinder whose surface is capable of storing a large number of magnetized spots which represent coded information. Information on the surface can be stored indefinitely and read off at high speeds as the drum rotates. 2. In a Hagelin machine, a cage of bars, each of which carries a lug or lugs.
- 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 or lacking indicator or discriminant.
- dummy group.** A null group
- dummy letter.** A *null,* q. v.
- dummy message.** A message sent for some purpose other than its content which may consist of dummy groups, or may have a meaningless text.
- dummy traffic.** A series of dummy messages.
- dupe, n.** A duplicate; especially a duplicate intercept, either of the same transmission or of a second transmission of the same message.
- duplex adj.** Applied to a circuit on which simultaneous transmission of two messages in opposite directions is possible. Cf. MULTIPLEX, SIMPLEX LINK.
- duplex operation.** Simultaneous transmitting and receiving of messages in both directions between two stations.
- duplex recording.** The recording on one tape, or other medium, of both terminal points of a given link, each transmitting to the other on different frequencies.
- E.** A symbol used in intercept operations as a suffix to a frequency to denote "estimated."
- ECM.** See ELECTRONIC COUNTERMEASURES.
- ECM 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.)
- ECM intelligence.** All intelligence derived from the study of electronic countermeasures.
- ECM reconnaissance.** See ECM SEARCH.
- ECM search.** The search for enemy-generated electromagnetic waves to determine existence, source, and pertinent characteristics.
- 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. Cf. APPARENT SETTING.
- EHF.** *Extremely-high frequency,* q. v.
- electromechanagrammer, n.** A cryptanalytic machine using IBM equipment to test statistically all the possibilities of juxtaposition of a sequence of cipher text with the remaining text of a transposition cipher. Also known as GEE WHIZZER.
- electronic countermeasures.** All measures taken to reduce the military effectiveness of enemy equipment employing or affected by electromagnetic radiations.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

- Electronic countermeasures (ECM) may include jamming, ECM deception, ECM search, or reconnaissance, or the collection, analysis, and evaluation of information pertinent to ECM, and dissemination of the resulting ECM intelligence.
- electronic deception.** The radiation or reradiation of electromagnetic waves in a manner intended to mislead the enemy in the interpretation of data received by his electronic equipment. See ELECTRONIC COUNTERMEASURES; JAMMING.
- ELINT, n.** Intelligence derived from the analysis of the electrical or electronic characteristics of a transmission.
- emergency message.** A message bearing the precedence prosign Y, q. v
- emergency system.** A stand-by encryption system for use in case of compromise of a regular system.
- emission analysis.** The processes employed in radio-fingerprinting.
- encipher, v. t.** To convert a plaintext message into unintelligible language or signals 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.
- enciphering table.** A cipher table so constructed as to facilitate encipherment.
- encipherment, n.** 1. The process of enciphering. 2. Text which has been enciphered.
- encipher sequence.** See P→C SEQUENCE.
- encode, 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.
- encodement, n.** 1. The act or process of encrypting plain text with a code system. 2. The text produced by encoding plain text.
- encrypt, v. t.** To convert a plaintext message into unintelligible language or signals by means of a cryptosystem.
- encrypted message.** A cryptogram.
- encrypted text.** The text produced by the application of a cryptosystem to a plaintext message.
- encryption, n.** 1. The act of encrypting. 2. Encrypted text.
- encryptment, n.** 1. *Encryption*, q. v. 2. An encrypted communication.
- endplate, n.** In a cipher machine, the stationary set of contacts at the beginning or end, or both, of the maze. A type of *stator*.
- end spell.** The plain equivalent of a code group indicating that a spelling has been completed and that the groups following represent words and phrases.
- Enigma, n.** A commercially made German cipher machine, involving wired rotors and a reflector.
- engima-type motion.** Pertaining to the motion of rotors so designed that a rotor turns one or more times as its *senior rotor* completes one revolution. Cf. CYCLOMETRIC.
- 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 plain code groups. Also called zeroizing.
- 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 base.** *Relative base*, q. v.
- equivalent key.** A specific key that produces the same cryptographic results as a different specific key.
- 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 radio frequency on which a target is observed operating. (Appearing with an "E" suffixed to the frequency.)
- executive method.** The method by which a transmitting station directs the addressees of a message to execute (take action on) its purport at an indicated moment.
- executive signal.** The transmission which indicates the instant at which action is to be taken on a given executive method message.
- exempted addressee.** In U. S. military usage, 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 are known, and which can be read by applying established procedures to recover the 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, the solution of specific controls such as indicators, specific keys, and traffic analysis.
- 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 fre-

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

quencies from 30,000 to 300,000 megacycles. Abbr. EHF.

facsimile, n. A system of radio or wire communication by which illustrations or printed pages are transmitted and received.

factoring, n. 1. An arithmetical process of determining the period of a periodic polyalphabetic cipher by a study of the intervals between repetitions. 2. In transposition, the process of determining column lengths by studying intervals between elements.

fading, n. Variations in the strength of a radio signal at the point of reception.

false addition. The method of modular arithmetic used in cryptographic procedures which involves no carrying. Cf. CRYPTOGRAPHIC ARITHMETIC.

false difference. The difference obtained by *non-borrowing subtraction*, q. v.

false subtraction. The method of modular arithmetic used in cryptographic procedures which involves no borrowing. C. CRYPTOGRAPHIC ARITHMETIC.

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

"F" (FOX) method. See BROADCAST METHOD.

Fibonacci series. A stream of digits produced by the successive addition of two adjacent digits, starting with an arbitrary unit of digits. Cf. AUTOKEY SYSTEM.

field, n. One or more columns of an IBM card which contain a unit of information.

field activity. Any active subordinate effort, operation, or instrumentality which is controlled by a superior headquarters.

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. Abbr. 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 DF, an area indicated as the location of a transmitter by the intersections of three or more bearings. Cf. CUT.

fixed additive. An additive which is repetitively applied throughout an enciphering process.

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

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

flag group. In meteorology, a group consisting of a significant combination of digits used to call attention to the particular portion of text following. (e. g., 1122, 55999, etc.) Cf. STUTTER GROUP.

flash. In DF, a message sent from a net control station to alert other stations in the net.

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

flat, adj. 1. As a characteristic of a frequency distribu-

tion, implies statistically not rough. 2. May be used more restrictively to mean statistically like a square distribution. Cf. SMOOTHNESS.

flexible multiplex. A multiplex system which can switch from one given number of channels to another; for example, two-channel to three- or six-channel.

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

four-level dinome cipher. A bilateral 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 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.

fox test, n. In cifax, a transmission of a test pattern to determine circuit operating conditions.

fractionation. A cryptographic 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.

free operation. A method of network operation in which a number of stations work on the same frequency, any station being permitted to contact any other station on the assigned frequency. In free operation, there is no control station, but there may be a "senior station" which can exercise control if needed.

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.

frequency, n. 1. The number of cycles completed each second by an electric current, a sound wave, or vibrating object. 2. In cryptology, the number of actual occurrences of a textual element within a given text. Cf. RELATIVE FREQUENCY.

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

frequency count. A frequency distribution.

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

frequency modulation. The process of varying the frequency of a carrier wave in accordance with the amplitude and frequency of an audio signal.

frequency multiplex. A technique for the transmission of two or more signals over a common path, each signal being characterized by a distinctive reference frequency or frequency band.

frequency shift keying. A method of keying a transmitter whereby the transmitter frequency alternates between two frequencies in response to the keying. Abbr. FSK.

~~CONFIDENTIAL~~

- frequency table.** A frequency distribution in tabular form, with frequencies indicated by numbers.
- fractional 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.
- Friedman square.** A cipher square in which all the diagonals reading in one direction contain the same sequence; in machine cipher solution, the square represents the substitution effected by rotating a single rotor through all possible positions. Also known as a rod square.
- FSK.** *Frequency-shift keying*, q. v.
- full-time coverage.** The assignment of enough operators to intercept all transmissions on a given frequency or associated group of frequencies.
- fusion, n.** That phase of communication intelligence operation in which the results of traffic analysis, cryptanalysis, and related collateral material are integrated and a combined end-product is produced.
- gamma I. C.** Index of coincidence applied to a universe, i. e., a very large sample. See INDEX OF COINCIDENCE.
- 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 check.** A procedure designed to reveal garbles in code or cipher text and to assist in their correction.
- garble table.** Any table, chart, or other similar aid which may be used to correct garbles.
- GCT.** *Greenwich Civil Time*, q. v.
- GEE WHIZZER.** See ELECTROMECHANAGRAMMER.
- general callsign.** A callsign 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 of a cryptosystem, excluding the specific keys essential to its employment.
- general purpose system.** A specific cryptosystem intended for any type of message. Cf. SPECIAL PURPOSE SYSTEM.
- 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, n.** The production, either systematic or random, of callsigns, keys, code groups, etc. In the case of callsigns, generation is distinguished from allocation, which is the assignment of callsigns or blocks of callsigns 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 the plaintext generatrix and a cipher generatrix.
- GMT.** *Greenwich Mean Time*, q. v.
- gnomonic chart.** In DF, a map on which great circles appear as straight lines.
- 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 difference which is equal to, or may be, the difference between two high frequency groups.
- good garble.** A garble which falls into the category of ordinary encrypting, transmission, or transcription error. Usually a one-place garble.
- good group.** 1. A code group which occurs with a relatively high frequency; a common group. 2. A code group which has no garbles; a valid group.
- grammatical group.** A code group indicating which of the alternative grammatical inflections assigned to a particular code group is to be taken.
- grammatical table.** A section in a code book containing *grammatical groups*.
- 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.
- Grandprè cipher.** A type of substitution system providing dinome 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. Abbr. GCT. Now superseded by *Greenwich Mean Time*, q. v.
- Greenwich Mean Time.** The mean solar time at the meridian of Greenwich. Abbr. GMT. Also known as universal time and Z (Zebra) time.
- grid, n.** 1. In a transposition system, a form or matrix over which a grille is placed for the purpose of enciphering or deciphering. 2. A system of numbers or other designations used to represent geographic areas.
- 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 or key may be written or read on a grid. 2. A matrix in which certain squares are blocked out or otherwise marked so as not to be used. Also called a stencil.

~~CONFIDENTIAL~~

Gronsfeld system. A polyalphabetic substitution system employing the first 10 alphabets of a direct standard Vigenere 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 Ap with key of 4 is Ec.

ground station. In air/ground communication, used to designate the ground station as opposed to aircraft.

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, one 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-duplex operation. The transmitting and receiving of messages in both directions alternately between two stations. Each station uses one operator and one machine for both transmitting and receiving. Cf. DUPLEX OPERATION.

half-Hebern wheel. A wired rotor with fixed slip ring contacts on one side and a rotatable set of contacts on the other. Sometimes called a commutator wheel. Cf. HEBERN ROTOR.

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

hand cipher. See MANUAL CIPHER.

hard copy. 1. The original, as opposed to a carbon copy. 2. 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.

Hebern rotor. A rotor, q. v., named for the American inventor, Edward Hebern, who independently developed the rotor for use in a cipher machine of his own design.

Hellschreiber, n. A system of automatic telegraphy which is 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 conventional type bars, thus, each printed character is made up of several closely spaced lines.

HF. *High frequency*, q. v.

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

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

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 held by high commands, employing a cryptosystem which has limited distribution and relatively permanent physical and cryptographic security.

Hill's algebraic encipherment. A polygraphic system for the encipherment of polygraphs of any order, involving algebraic treatment 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 slang expression meaning a *coincidence* of textual elements.

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 message print. A form of message print listing a number of textual elements, words, code value code groups, or other, to the line but without frequency or other information. Cf. VERTICAL MESSAGE PRINT.

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.

hybrid code. A code in which both one-part and two-part features appear. See MODIFIED ONE-PART CODE.

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 certain plain code groups to underlie selected cipher groups.

IBM. *International Business Machines*, q. v.

IBM method. A punched-card machine processing system for manipulative, statistical, and computational processes employing IBM equipment.

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 the data by means of IBM tabulating equipment.

IC. *Index of coincidence*, q. v.

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.

~~CONFIDENTIAL~~

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 in a prearranged manner, thereby distinguishing themselves from enemy forces. Abbr. IFF.

identifier, n. See LINGUISTIC PERSONNEL.

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 elements.

idiomorphic, adj. Exhibiting the phenomenon of idiomorphism

idiomorphism, n. In a plaintext 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.

"I" (Item) method. See INTERCEPT METHOD

illicit 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.

indefinite call sign. A call sign which does not represent a specific facility, command, authority, activity, or unit, but which may represent any one or any group of these.

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 body of text or key to the number of coincidences expected in a sample of random text of the same size. Commonly known as I. C. See also DELTA I.C. and GAMMA I.C.

indicative, n. See BASE NUMBER.

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 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 indi-

cators 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. Cf. DIRECT SYMMETRY.

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

"IN HERE." A phrase, inserted by an intercept operator, preceding the first portion of an intercepted message to indicate that part of the preamble or that the preamble and part of text has been missed.

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 Morse code signals or teleprinter signals are recorded in the form of visible ink patterns. Also known as inked recording tape and undulator tape.

inscription, n. 1. In a transposition system, the process of writing a message into a matrix. 2. The process of writing a series of numbers, letters, or coded meanings into a code chart or table.

insertions, n. Those code values inserted in approximate alphabetical order as additions to a one-part codebook.

installed intercept position. An intercept position in either an operational or a standby state.

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.

intelligence, n. The product resulting from the collecting and processing of information concerning actual and potential situations and conditions relating to foreign activities and to foreign or enemy-held areas. This processing includes the evaluation and collation of the information obtained from all available sources, and the analysis, synthesis and interpretation thereof for subsequent presentation and dissemination.

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 before the first part of the intercept message heading. Intercept data generally include frequency, call signs, signal strength, signal readability, intercept date/time, intercept station number, and case number. In some intercept formats, certain 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.

~~CONFIDENTIAL~~

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

intercept material. Raw intercepted traffic or intercept technical reports concerning intercept activities, or both.

intercept method. The method of transmitting a message by prearrangement 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 operator. A person responsible for operating a radio intercept position.

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.

intercept technical reports. Reports on intercept activities, such as coverage reports, T/A bearings, hearing reports, etc.

interference, n. The impairment of reception by atmospheric, 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. A line of commercial accounting and statistical machines utilizing punched cards to manipulate data.

international callsign. A callsign assigned in accordance with the provisions of the *International Telecommunications Union* to identify a radio station, and appearing in lists published by the I.T.U.

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 Telecommunications Union. A civil international organization established to provide standardized communication procedures and practices

including frequency allocation and radio regulations on a world-wide basis. Abbr. ITU.

international teleprinter code. See BAUDOT ALPHABET.

international-type callsign. A callsign in the correct ITU nationality allocation block, but one not listed by ITU, or one used in a manner which differs from its listed purpose.

interpreter. See LINGUISTIC PERSONNEL.

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 interrupts the basic keying operation or sequence.

interval, n. A distance between two points or occurrences, especially between recurrent conditions or states. The number of units between a letter, digraph, code group, etc., and the recurrence of the same letter, digraph, code group, etc., counting either the first or second occurrence but not both. Frequently called cryptanalyst's interval.

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, or other well defined pattern.

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.

inversion, n. *Transposal*, q. v.

invisible ink. Any of several chemicals used for writing or printing which 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.

ionosphere, n. That portion of the earth's atmosphere extending about 30 to 250 miles above the earth, important in radio transmission because of its effect on radio waves.

ionospheric wave. A radio wave that is propagated by

~~CONFIDENTIAL~~

- reflections from the ionosphere and sometimes known as the sky wave.
- isolog**, n. A cryptogram in which the plain text is identical or nearly identical with that of a message encrypted in another system, key, code, etc.
- isologous**, adj. Pertaining to or having the nature of an *isolog*.
- isomorph**, n. A plain or cipher sequence which exhibits an idiomorph identical with that of another plain or cipher sequence.
- isomorphism**, n. The existence of two or more identical idiomorphs.
- item**, n. That portion of a technical report dealing with one case number or target.
- ITU**. *International Telecommunications Union*, q. v.
- jamming, electronic**. The deliberate radiation or re-radiation of electromagnetic waves with the object of impairing the electrical communications of the enemy.
- 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 Bazerics. 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. Connotes activities, operations, organizations, etc., in which elements of more than one Service of the National Military Establishment participate.
- joint communication**. Common use of communication facilities by two or more Services of the same nation.
- junior rotor**. Of two sequential rotors, the rotor whose motion is controlled by the other.
- kappa plain constant**. A mathematical constant employed in coincidence tests such as the phi test, to denote the probability of a coincidence of a given plaintext element or unit. 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 mathematical constant employed in coincidence tests such as the phi test 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**. Kilocycle.
- kcs**. Kilocycles per second.
- key**, n. 1. In cryptography, a symbol or sequence of symbols applied to successive textual elements of a message to control their encryption or decryption. 2. A *specific key*. 3. A device used by radio operators to break a continuous wave in a prearranged manner, e. g., by Morse code, so that intelligence can be transmitted.
- key book**. A book containing key text, or plain text forming specific keys.
- key crib**. Key known or assumed to have been used in a cryptogram.
- key 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 in a given cryptoperiod.
- key phrase**. An arbitrarily selected phrase used as a key or from which a key is derived.
- key punch**. A machine used to punch information in the form of holes into cards.—To operate such a machine.
- 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.—adj. *keyword*.
- keyword mixed alphabet**. An alphabet constructed by writing a prearranged key word or key phrase, (repeated letters, if present, 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 controlled movement imparted to a rotating element of a cipher machine.
- kilocycle**. One thousand cycles per second. Abbr. kc. See also FREQUENCY.
- 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.
- landline**, n. A wire circuit between two pieces of communication equipment which are physically separated.
- lane**, n. A path, electrical, physical, or both, in one direction connecting two correspondents regardless of the route involved.
- language index**. An alphabetical listing of language units showing preceding and following textual matter and appropriate *indicative information*, compiled from

~~CONFIDENTIAL~~

messages, newspapers, books, or any other source. If the language unit is the word, it is a *plaintext index*; if the language unit is a code value, it is a *bookbreakers' index*.

language specialist. See LINGUISTIC PERSONNEL.

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.

lateral difference. See DELTA DIFFERENCE.

Latin square. A cipher square in which no row or column contains a repeated symbol.

level, n. 1. A row of an IBM card. 2. An information channel on punched paper tape or magnetic tape.

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.

lineation, n. The sequence of symbols identifying the lines of a code book.

line-up, n. *An overlap*, q. v.

linguist, n. See LINGUISTIC PERSONNEL.

linguistic personnel. In cryptology, those persons skilled in languages; the specific categories of linguistic personnel engaged in cryptologic work are:

linguist—One who has expert knowledge of a foreign language.

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

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

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

translator—A reader who translates written materials from a foreign language into English.

scanner—A reader who examines foreign-language texts to assess their intelligence content.

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

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

transcriber—A listener who converts foreign language voice transmissions into the written form of the foreign language.

voice translator—A listener who translates recorded foreign language voice transmissions into written English.

interpreter—A listener who translates (or summarizes) foreign-language voice transmissions into either written or spoken English directly from the actual transmissions.

link, n. The existence of direct communication facilities between two points.

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

listener, n. See LINGUISTIC PERSONNEL.

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. Cf. NUMERICAL KEY.

literal system. Any cryptosystem in which the plaintext and ciphertext symbols produced or accepted are the normal alphabetical characters and digits.

lobster, n. The phenomenon of simultaneous motion of all rotors in a wired-rotor cipher machine.

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

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 text, which weights are actually logarithms of the probabilities of the textual 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, machine, or device by the preparing agency.

loran, n. A long range radionavigation position-fixing system utilizing the difference in time 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 in the other Services.

low frequency. 1. The range of radio frequencies from 30 to 300 kilocycles. Abbr. LF. 2. Having a low probability of occurring, as the elements of a frequency distribution.

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 held by commands in low echelons, employing a cryptosystem which has wide distribution, fair physical security, and temporary cryptographic security.

lug, n. One of the projections on the cage of a Hagelin machine.

~~CONFIDENTIAL~~

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 units are subtracted each from the other by modular arithmetic.

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

manned intercept position. The necessary personnel and equipment to intercept one radio signal, 24 hours per day if necessary.

manual cipher, n. A cipher system in which the enciphering and deciphering are performed by hand; or a message produced by such a system. Cf. MACHINE CIPHER.

manual Morse. Morse code keyed by hand.

mark, n. *Mark impulse, q. v.*

mark 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 *space impulse, q. v.*

marking bias. In teleprinter transmission, the condition existing when marks are longer than spaces; sometimes referred to as plus prevalence.

master block. To sort traffic as nearly as possible into its original order.

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 cryptanalytic reconstruction. The master decode contains all possible code groups in the system under study, and all partial or complete identifications with their appropriate validity symbols.

matching, adj. 1. Shifting of two or more monoalphabetic frequency distributions so as to bring them into proper alignment for amalgamation into a single monoalphabetic distribution. 2. The assembly of two or more copies of identical intercept traffic.

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. The 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. Megacycle.

mcs. Megacycles per second.

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

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 frequency. The range of radio frequencies from 300 to 3,000 kilocycles. Abbr. MF.

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, n. 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. The component of a communication center whose function is to accept, prepare for transmission, receive, and deliver messages.

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

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

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

message heading. The part of a message containing all components preceding the text.

message indicator. A group of letters or numbers placed within an encrypted message to designate the keying elements applicable to that message.

message keying elements. That part of the key which changes with every message.

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

message print. A machine reproduction of messages usually 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 register. A traffic analysis log of the messages intercepted on a certain link or net for one day, entered in chronological order. Cf. PROFORMA SHEET

~~CONFIDENTIAL~~

message serial number. A reference number assigned by the originator to each outgoing 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 units are subtracted each from the other by mod-10 arithmetic.

minor group. That one of two code or cipher units which, when subtracted from the other unit, 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 plain code text is cryptographically subtracted from the key. In the process of decipherment, the enciphered code text is cryptographically subtracted from the key. Cf. SUBTRACTIVE METHOD.

minus prevalence. See SPACING BIAS.

mission, n. 1. The objective; that is, the task together with its purpose, thereby clearly indicating the action to be taken and the reason therefor. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit. 2. In radio intercept, a definite task 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 non-constant 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.

mode, n. In *flexible multiplex*, q. v., any of the various multiplex phases employed; for example, two-channel mode.

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.

modified one-part code. A basically one-part codebook which has been altered in some fashion, e. g., by introduction of intrusives, by random repagination, by random shuffling of orderly blocks of meanings throughout the code or within each page, etc. Although both a decoding and an encoding book may be required, such a code differs from a two-part code in that some pattern is visible in the relationship between certain groups and meanings. Cf. HYBRID CODE.

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

modulation, n. The process in which the amplitude, frequency or phase of a carrier wave is varied with time in accordance with the waveform of superimposed intelligence.

modulo, adv. With respect to a *modulus*, q. v. (Abbr. 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.

monitoring, n. The act of procuring one's own or other friendly forces' communications for the purpose of maintaining standards, improving communications, or for reference.

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

monoalphabeticity, n. A characteristic of encrypted text which indicates that it has been produced by means of a single cipher alphabet or an unenciphered code system using a single code book. 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.

monome, n. A single digit. A contraction of monome.

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. Abbr. MOA.

multilateral, 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.

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

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

multipartite alphabet. A multilateral alphabet in which each letter of plain text is represented by a

~~CONFIDENTIAL~~

- cipher unit of two or more characters whose functions are clearly defined. See BIPARTITE ALPHABET, TRIPARTITE ALPHABET.
- multi-part message.** A message broken up because of length and sent in parts.
- multiple-address message.** A message which is destined for two or more addressees, each of whom is informed of all the addressees who are to receive identical messages. The addressees are indicated as action or information or a combination of both.
- 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 callsigns of the stations called are used (in contrast to collective call).
- multiple flash.** A system within a DF net whereby one or more stations, other than net control, may flash targets.
- multiplex, adj.** Pertaining to a communication system permitting the simultaneous use of several channels on a single link.
- multiplex link.** A link between a transmitter and a receiver whose characteristics are such as to permit the simultaneous transmission of more than one channel of intelligence.
- multiplex signal.** The telegraphic signal from a multiplex system.
- multiplex system.** A telegraphic system in which two or more messages at a time are transmitted.
- multitone, n.** A transmission of more than one audio tone, usually used to transmit two or more channels.
- MUX.** *Multiplex*, q. v.
- NCS.** A *net control station*, q. v. Also indicates Naval Communication Station.
- near depth.** Depth which, but for some minor inconsistencies in the progression or identity of keying elements, would be true depth.
- net, n.** A number of associated groups all controlled at a common location and presumably serving the same common superior headquarters.
- net authentication.** Identification used on a communication net to establish the authenticity of the several stations.
- net callsign.** A collective callsign 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. Abb. 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.
- no current impulse.** In standard American single-channel start-stop teleprinter systems, the condition which corresponds to a space in Baudot systems.
- NOFORN.** An abbreviation placed on an item of written material to indicate: "Not releasable to foreign nationals or their representatives."
- non-borrowing subtraction.** Subtraction to the modulus ten; i. e., the tens digits are disregarded. Cf. CRYPTOGRAPHIC ARITHMETIC.
- non-carrying sum.** A sum produced in cryptographic (mod 10) arithmetic.
- non-commutative, adj.** As applied to bipartite matrices, so constructed that row and column coordinates must be read in a certain prescribed order, for example, in 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 represented in the cipher text by the same unit.
- nonliteral system.** Any cryptosystem designed for the transmission of data in which the symbols or signals produced or accepted are other than the normal alphabet and digits, (e. g., teleprinter, IFF, ciphony, cifax, civision, etc.).
- non-Morse, adj.** Pertaining to methods of electrical 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 or which is of such an extremely long cycle that for practical purposes the sequence does not repeat.
- 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*, q. v.
- 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 textual unit or letter relative to other textual units or letters, as disclosed by the statistical study of a large volume of homogeneous text. Also called characteristic frequency.
- 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.

~~CONFIDENTIAL~~

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.

notate, v. t. To assign a case number.

notation, n. *Case number, q. v.*

notch, n. An indentation, located on the periphery of a rotor of a cipher machine, which controls the stepping of components in the machine.

NR. *Station serial number, q. v.*

NTX. U. S. Naval Teletypewriter exchange.

null, n. 1. In cryptography, a symbol or unit of encrypted text having no plaintext significance. 2. In DF, an *aural observation, q. v.*

numerical key. A key composed of a sequence of numbers. Cf. LITERAL KEY.

numerically-keyed columnar transposition. A columnar 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 OPERATIONAL 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. *Order of battle, q. v.*

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

off-line equipment. The equipment normally used in off-line operations.

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

Cf. ON LINE OPERATION.

off-phase. See PHASE.

offset, adj. Applied to messages in depth or repetitions in these, beginning or occurring at different points of the key.—v. t. To shift information by punching it into a different field of another IBM card in the same file.

offset depth. A depth in which the two messages start at different places in the key stream.

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. Cf. STAGGERED DEPTH.

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.

on-and-off keying. A method of keying a transmitter whereby the power of a transmitter is turned off or on in accordance with the keying. Abbr. OOK.

one-channel system. See SIMPLEX LINK.

one-deep reading. The keying-in of assumed plain text or plain code of a single message.

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

one-place garble. A garble of only a single element of a code group. Cf. DOUBLE GARBLE.

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.

one-time tape. A perforated tape used as the keying element in a one-time teleprinter system.

on-line equipment. The equipment normally used in on-line operations.

on-line operation. A method of operation in which the processes of encryption, transmission, reception, and decryption are performed automatically and simultaneously. Cf. OFF LINE OPERATION.

on phase. See PHASE.

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

OOK. *On-and-off keying, q. v.*

open code. A system of disguised secret writing 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.

operational signal. In joint and combined usage, a trigraph beginning with "Q" (in international usage, "Q" or "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.

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

operation service. A notation entered at the bottom of each page of intercept copy or at the end of each message consisting of (1) operator's estimate of the readability of the copy, (2) intercept time, (3) operator's personal sign, (4) intercept position number.

OPM. Operations per minute. The cycle rate of a transmission system.

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. The composition, strength, location, and combat values of all units in line or in reserve of one's own, friendly, or enemy forces. Abbr. O/B.

ordinary relay. A type of relaying in which electrical impulses are sent to their destination without correcting their form. Quite often distortions of the impulses are amplified. Cf. AUTOMATIC RELAY.

originator, n. The command by whose authority a message is sent. The originator is responsible for the functions of the drafter and releasing officer.

O/S. Outstation, q. v.

out of phase. See PHASE.

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. Cf. DEPTH. 3. In the Hagelin machine, the condition arising when there are two effective lugs on the same bar. Also called double key.—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 message in page form which is the result of a transmission.

page printer. A teleprinter which produces page copy.

page symbol. 1. That part of the indicator in an enciphered code system, indicating the page in the key book on which the initial key is located. 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.

pancake random. A significantly flat frequency distribution.

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.

parallel link. A link serving the same two stations as another link, usually by a different type of communication.

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

partial depth. A depth of messages in which most, but not all, of the cryptographic elements used in any given message are the same as those used in the other message.

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 show 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, or 3 and 3.—v. t. In Hagelin solution, to resolve the actual key into the separate key contributions made by the individual wheels.

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 encrypted text. Cf. LATENT REPETITION.

patent symmetry. See DIRECT SYMMETRY.

pattern. See IDIOMORPH.

peg, n. See PIN.

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 the recurrence of a cycle.

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 two or more alphabets. Also called repeating key method.

periodic system. A system in which the enciphering process 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. Cf. GARBLE TABLE.

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

personal sign. A sign composed of one or more letters, normally initials, used when endorsing station records and messages to indicate individual responsibility of operating and supervisory personnel.

phase, n. 1. A period or interval. 2. The relationship between two sequences of text, of key, or both, 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.

~~CONFIDENTIAL~~

phi (ϕ) test. A test applied to a frequency distribution to determine whether it is monoalphabetic or not. See also KAPPA PLAIN CONSTANT and KAPPA RANDOM CONSTANT.

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

pilot channel. A channel of a multiplex system which is employed for administrative and operational circuit matters rather than for transmission of regular traffic.

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

pilot Morse. A Morse communication link used exclusively for synchronization of radioprinter transmission.

pin, n. An adjustable peglike projection on a rotor which can be set to control the movement of another component of a cipher machine, especially a Hagelin-type machine. Also called peg.

pinch, n. A document or fragmentary document obtained by clandestine means and containing information about foreign communications, cryptography, or communication intelligence.—v. t. To obtain a pinch.

pin pattern. A given arrangement of the active and inactive pins on a Hagelin-type wheel.

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

plain code. Unenciphered code.

plain component. The sequence of plaintext symbols in a cipher alphabet.

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. CO-DRESS.

plain language. *Plain text*, q. v.

plain text. 1. Normal text or language which, with no hidden or secret meaning, conveys knowledge. 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.

plaintext index. A type of *language index* in which the word is the basic unit and is shown in context with the words preceding and following. It may be derived from enciphered or unenciphered plaintext messages or from newspapers, magazines, books, or other documents.

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

plus prevalence. See MARKING BIAS.

Poisson table. Table of the Poisson distribution. A special 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 or 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.

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.

POROCO. *Position rotating coverage*, q. v.

Porta system. A forerunner of the Vigenere 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.

portmanteau group. A code group equivalent to a whole phrase, such as: "I refer to my telegram number," or "in this event." The term may also refer to a combination meaning such as "period the," or "period end quotes."

position, n. 1. The order or place of a given symbol within its code group. 2. A terminal equipped to receive radio signals and manned by one or more operators.

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

position rotating coverage. A type of intercept assignment where certain cases are grouped together for the purpose of obtaining as much intercept as possible. Abbr. POROCO.

possible compromise. A loss of accountability when it has not or cannot be determined if classified information or material came into hands of unauthorized individuals.

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

post-card grille. See RECTANGULAR GRILLE.

practice message. A message passed on a communication link only to familiarize personnel with message handling techniques and procedures.

practice system. A cryptologic system devised primarily to generate practice. See PRACTICE TRAFFIC.

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. One of the components contained in the heading of a message whose elements include the degree of precedence, the date-time-group, and message instructions.

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.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

- 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 call.** A call for establishing communications.
- 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.
- preliminary key.** See INITIAL KEY.
- primary frequency.** A radio frequency assigned for normal use on a particular circuit.
- primary period.** *Basic period*, q. v.
- 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 of a group of individuals or a commercial firm.
- probable word.** A word assumed or known to be present in the underlying plain text of 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, plain dress message used to expedite the handling of traffic, usually between operators.
- procedure sign.** A prosign. One or more letters or characters or a combination thereof, used to facilitate communication by conveying, in a condensed standard form, certain frequently used orders, instructions, requests, and information related to communications.
- procedure word.** A word or phrase limited to radiotelephone procedure and used in lieu of a prosign. Abbr. Proword.
- proforma message.** A message in standardized form, designed to convey intelligence by conventions of arrangement and abbreviation.
- proforma sheet.** A printed form used by traffic analysts to record or log basic data for study of messages and other activity. A traffic analysis log.
- program (computer).** The sequence of instructions to a computer which enables it to carry out a computation.
- 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 of a code system.
- pseudo-polygraphic system.** A polygraphic substitution system in which at least one of the letters in each polygraph is enciphered monoalphabetically.
- pseudo-solution.** A false solution to a cryptogram, call-sign system, routing system, etc., which gives a seemingly plausible answer, but in fact is based on insufficient raw material to give a true solution.
- psychological random.** As applied to cryptographic key, sequences which have been generated manually and which exhibit the idiosyncrasies of the person responsible.
- P→C (read "P" to "C") sequence.** In transposition cipher solution, a sequence the successive terms of which indicate the positions that the successive plain text letters occupy in the cipher text. Also known as encipher sequence. Cf C→P SEQUENCE.
- 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.
- punched papertape.** 1. A medium for storing binary information in a number of levels (usually five or six in number), using punched holes for the binary coding.
2. *Chadless or chadded tape*, q. v.
- pyrotechnics code.** A prearranged code in which meanings are assigned to the various colors and arrangements of pyrotechnics.
- Q.** A symbol used in DF bearing observation classification to indicate "insufficient time for accurate measurement or classification."
- Q code.** A code adopted by the International Telecommunications Conference at Cairo, 1938. See Q SIGNAL.
- Q signal.** In joint and combined usage, a trigraph beginning with "Q" used to facilitate the handling of traffic, to direct net operation, or to convey certain originator's instructions in a message. See OPERATING SIGNAL.
- quinteliteral alphabet.** A cipher alphabet in which each plaintext letter is represented by a 5-character equivalent.
- R.** 1. 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.
2. *Readability of radio signals.*
- 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.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

radio deception. The radiation or reradiation of radio waves in a manner intended to deceive the enemy. Radio deception includes sending false dispatches, using deceptive headings, employing enemy call signs, etc.

radio direction finding. See DIRECTION FINDING.

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. Abbr. RFP.

radio frequency. Any frequency at which electromagnetic radiation can be used for communications. Cf. RADIO SPECTRUM.

radiogoniometry. See DIRECTION FINDING.

radio printer. A radio teleprinter. See TELEPRINTER. Abbr. 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 collocated transmitters and receivers operating in any number of radio links, but serving the same organization.

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

radiotelephone position. An intercept position specially equipped and reserved for the exclusive use of radiotelephone intercept.

radiotelephony, n. Transmission of voice signals by radio. Abbr. 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 which variations are indistinguishable from those due to chance.

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. Abbr. RAM.

RATT. Radio teletypewriter. See TELEPRINTER.

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.

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. 1. A person engaged in the recovery of key. Cf. *Stripper*. 2. See LINGUISTIC PERSONNEL.

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

receipt method. A 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 bearing. In DF, a bearing of exactly opposite direction, 180 degrees away from an observed bearing.

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, n. The machine process by which a predetermined set of data is matched against one or more pieces of temporary data. If a match occurs, a record is made; if no match occurs, testing continues.

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; discs, wire, etc.).

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

- recording serial number.** The individual recording identification assigned to each intercept site for the exclusive use of radiotelephone intercept.
- recover, v. t.** To solve; to reconstruct (e. g., cryptographic data or plain text.)
- recovered code.** A codebook whose groups have been identified by cryptanalysis. Cf. COMPROMISED CODE.
- 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. 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 multilateral 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 callsign.** A collective callsign 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 accounted for periodically.
- register number.** A number assigned to registered matter for accounting purposes.
- relate columns.** *Equate columns, q. v.*
- 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 base.** Digits or letters arbitrarily assigned, especially to code groups, keys, or substitution tables, when the true digits or letters are not yet determined, in such a manner that the assigned characters differ from the true by an amount which is constant for each code group, key or table. See RELATIVE CODE and RELATIVE KEY.
- 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.
- relative key.** Key developed to reduce enciphered code to a relative base; not true key, but differing from the true key by an interval constant for each segment of code-group length; (i. e., constant for each segment of 4 if it is applied to 4-digit code, or 5 if to 5-digit code, etc.).
- 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.
- reperforator, n.** A teleprinter equipment which produces a copy of text on *chadless tape*.
- repetitive 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.
- reserved frequency.** A frequency allocated to a radio link or net for use when contact cannot be established on the normal assigned frequency.
- reversed polarity.** The transmission of teleprinter impulses of opposite to normal polarity or with mark and space impulses interchanged, as opposed to normal or direct signals.
- 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 plaintext digraph and its cipher digraph equivalent which permits the elements of each to be reversed without disrupting the equivalency (e. g., ABp = CDc and BAp = DCc).
- 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.*
- ring, n.** A movable metal collar bearing symbols, usually the letters of the alphabet, on a rotor.
- rod square.** See FRIEDMAN SQUARE.
- room circuit.** A circuit which has no connection with outside stations and which is used for encipherment and decipherment in off-line operation.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

root callsign. 1. A *basic callsign*, q. v. 2. A callsign allotted to a number of associated radio stations, each of which applies its individual suffix for differentiation. Cf. SUFFIX CALLSIGN. 3. The basic callsign used to generate enciphered callsigns.

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

rotating grille. See REVOLVING GRILLE.

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

rotor, n. A disk 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 periphery of a rotor serving to indicate its position at commencement of enciphering.

roughness, n. A pronounced variation in relative frequencies of the elements considered in a frequency distribution. Cf. SMOOTHNESS.

route transposition. A method of transposition in which the cipher-text equivalent of a message is obtained by transcribing, according to any prearranged route, the letters inscribed in the cells of a matrix into which the message was inscribed earlier according to some 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 in routing the message to the final recipient.

routing indicator. In U. S. Military usage, a group of letters assigned to identify a station within a teleprinter network.

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" (Roger) method. See RECEIPT METHOD.

R/T. *Radiotelephony*, q. v.

RTT. Radio teletypewriter. See TELEPRINTER.

run, n. 1. A *listing*, q. v. 2. A sequence of identical elements.

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. See LINGUISTIC PERSONNEL.

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

scramble, v. t. 1. To make unintelligible to casual interception, as in telephone and teleprinter transmission. 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 radio 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. Cf. TOP SECRET; CONFIDENTIAL.

secret ink. Any of several chemicals used for writing or printing which has 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 which 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.).

security, n. The protection of information and material from any possible access by any unauthorized person.

segmented code. See BLOCKED CODE.

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.).

senior rotor. Of two sequential rotors, the rotor which controls the motion of the other.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

- 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.
- sequential**, adj. Characterizing a multiplex signal in which the intelligence bauds of each channel are sent in orderly sequence. When all bauds of channel 1 have been sent, those of channel 2 are sent, etc., until all channels have been transmitted.
- serial number**. A number assigned to a document by the originating office for the purpose of counting the copies prepared and of controlling their distribution. It may be used for local accounting purposes, but is not to be confused with a register number.
- seriation**, n. A process of inscribing plain or cipher elements in two rows and subjecting the vertical pairs to further cryptographic treatment.
- service code**. An international commercial communicator's code consisting of five-letter pronounceable groups. It is published in several languages and contains sections on navigation, communication, and general subjects.
- service message**. A message between communications personnel pertaining to any phase of traffic handling, communication facilities or circuit conditions.
- set**, v. t. To find the *setting*.
- 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. 4. A frequency transposition.
- shoran**, n. An abbreviated name for a short range radio navigation system. It is a precision position finding 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, machine, or device for purposes of brevity and security.
- SIGINT**, n. 1. Former term for COMINT, q. v. 2. Intelligence derived from the study of intercepted signals apart from the message externals and content.
- sigma** (σ), n. A symbol for the standard deviation.
- 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. It consists of all information-transferring media except direct unassisted conversation or correspondence.
- signal operation instructions**. A series of orders issued periodically for technical control and coordination of the signal communication activities of a command. They 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. Abbr. 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 relay**. See ORDINARY RELAY.
- simple substitution**. Monoalphabetic uniliteral substitution.
- simple transposition**. See SINGLE TRANSPOSITION.
- simplex circuit**. *Simplex link*, q. v.
- simplex link**. A radio link so constituted that communication between the two stations is possible in only one direction at a time.
- simplex operation**. In the operation of a cipher machine, the use of a separate arrangement of rotors for each message or transmission.
- simplex star**. A star in which all stations use the same frequency.
- simplex working**. A system of radio frequency usage in which two or more stations communicate with each other on the same frequency.
- single-channel system**. A teleprinter system so constituted that communication is possible in only one direction at a time.
- single position**. A receiving terminal manned by one operator.
- single position index**. An index having a monographic control field.
- 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 digraph**. A digraph formed by the systematic selection of non-adjacent letters of text.
- 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

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

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.

slide, n. 1. In the Hagelin machine, the relative displacement between the indicating wheel and the printing wheel. 2. The interval between two different juxtapositions of the same cipher and plain components. 3. A *cyclic permutation*, q. v.—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. A run which tests the placement of a crib in a message by sliding the crib against the message text.

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. The lack of pronounced variation in relative frequencies of the elements considered in a frequency distribution. Cf. ROUGHNESS.

snap bearing. In direction finding, a quick bearing taken when the target station is on the air only a very short time.

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.

sort, v. t. To arrange data systematically according to some predetermined principle or pattern.

space. See SPACE IMPULSE.

space 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 mark impulse.

spacing bias. In teleprinter transmission, the condition existing when spaces are longer than marks. Sometimes referred to as minus prevalence.

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. Abbr. 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. Cf. GENERAL PURPOSE SYSTEM.

special solution. A solution which depends on circumstances which are not 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 use 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 use 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.

speech privacy. *Ciphony*, q. v.

speller. 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. See LINGUISTIC PERSONNEL.

spread band. A transmission system in which a signal is transferred from its normal position to another position in the spectrum.

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.

~~CONFIDENTIAL~~

- 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. Abbr. SOP.
- standing signal instructions.** Signal instructions containing items of operational data not subject to change, and instructions for the use of the SOI. Abbr. SSI.
- star, n.** A number of stations with a common control station, all traffic normally being routed through that control. The two principal types of stars are simplex stars and complex stars.
- star with lateral.** A star operating with some regular lateral working, (i. e., working between outstations) In many such nets, lateral working will be a regular procedure between some, but not all, of the outstations.
- starting point.** A point in a key where enciphering or deciphering begins.
- start-stop system.** A teleprinter system in which certain impulses are used for synchronization purposes to start and stop the receiving printer.
- station, n.** 1. *Radio station*, q. v. 2. *Intercept station*, q. v.
- station authentication.** A security measure designed to establish the authenticity of a transmitting or receiving station.
- station indicative.** See BASE NUMBER.
- 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. Abbr. NR.
- stator, n.** A stationary element in a cipher machine, (e. g., an endplate, a separator or a rotor), that does not move during the operation of the machine.
- stencil, n.** See GRILLE.
- step, v. t.** To move a rotor from one enciphering position to another.
- stepping, n.** The motion of a rotor from one enciphering position to another.
- stereolog, n.** A set of messages related by the fact that they contain a stereotype so that part of the underlying plain text is identical throughout the set.
- 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.
- strand, n.** A segment of a page containing a systematic arrangement of code groups, often part of a series reappearing on other code pages.
- strip, n.** *Sliding strip*, q. v.—v. t. To remove key, especially from enciphered code.
- strip board.** See CHANNEL BOARD.
- strip-cipher device.** A cipher device employing sliding alphabet strips.
- stripper, n.** Who who recovers keys, particularly from depths.
- stutter group.** A group consisting of a repeated single digit, as 55555 or 11111, usually a four or five digit group. A stutter group may be used as a *flag group*, q. v.
- 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.** A method of enciphering code in which the key is cryptographically subtracted from the plaincode text. In the process of decipherment, the enciphered code is added to the key. Cf. MINU-END METHOD.
- subtractor, n.** A number or series of numbers from which numerical code, cipher, or plain text is subtracted in the process of encipherment or decipherment.
- suffix callsign.** A callsign which is transmitted with an additional character or characters following the regular, or *root callsign*, q. v. Suffix callsigns are of several types: 1. Callsigns designating individual *mobile units* or elements of units such as aircraft, vessels, tanks, etc. Numbers are most frequently used as suffixes but letters or words may appear. 2. Callsigns associated with unit moves. The advance headquarters uses the normal callsign for the unit, (e. g. XYZ) with the suffix "1" (e. g. XYZ1). Since the physical separation of the two parts of the unit is temporary, no separate callsign allocation is normally made in such cases. 3. International-type callsigns with digit suffixes. Various suffixes to a given letter callsign designate different transmitters at a single station.
- sum check, n.** A digit of a textual group which is the sum (mod 10) of the other digits in the group.—v. i. 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.
- superencipher, v. t.** To subject an encrypted text to a further process of encipherment.
- superencipherment, n.** A form of superencryption in which the final step involves encipherment.
- 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.
- super-high frequency.** The range of radio frequencies from 3000 to 30000 megacycles. Abbr. SHF.

~~CONFIDENTIAL~~

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).

supersession date. The date on which cryptographic procedures, keys, codes, etc., are changed.

supplement, n. A publication, related to a basic publication, prepared for purposes of promulgating additional information or summaries.

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 in a different manner.

syllabary, n. In a code book, a list of individual letters, combination 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, tri-graphs, 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. A proforma message giving complete meteorological data obtained from a single observation at a single station.

synoptic hour. A fixed hour at which meteorological observations are made at all meteorological stations in a particular area (e. g. Europe).

synoptic period. 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. See CRYPTOSYSTEM.

tape-to-card process. Any method of automatically transferring data from punched paper tape or magnetic tape to punched cards.

systematically-mixed cipher alphabet. A cipher alphabet in which the component that is mixed has been disarranged by systematic procedure.

system indicator. See DISCRIMINANT.

T/A. *Traffic analysis*, q. v.

tactical callsign. A callsign which represents and identifies a tactical command or communications facility.

tail, v. i. Of two messages, to exhibit tailing. Cf. TELEGRAM TAIL.

tailing, n. 1. 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. 2. The practice of beginning the encipherment of one message with machine components aligned as they were after processing of 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 near-by machine as a check on the encipherment.

tandem group. An immediate repetition of a plain-code group which serves as a garble check.

tandem operation. In cryptography, electrically or mechanically coupling two cipher machines to produce automatic decipherment simultaneous with encipherment.

tape copy. A message in tape form which is the result of a transmission.

tape-to-card process. Any method of automatically transferring data from punched paper tape or magnetic tape to punched cards.

target, n. Radio intercept. A specific point, area, station, group of stations, etc., toward which intercept activities are directed. Cf. MISSION.

task, n. An assignment to an intercept operator to cover the transmission of a link, group, or net.

technical report. In the COMINT field, a working aid or a report of traffic analytic or cryptanalytic results.

telecommunications, n. Any transmission, emission, or reception of signs, signals, writing, images and sounds, or intelligence of any nature by wire, radio, visual, electronic, or other means.

telecon. A *teleconference*, q. v.

teleconference, n. A conference between persons remote from one another but linked by a telecommunications system. Abbr. telecon.

telegram tail. That part of an internal number series designating the area or service originating the telegram.

telemetering, n. Measurement with the aid of intermediate means which permit the measurement to be interpreted at a distance from the primary detector.

teleprinter, n. An electrically-operated instrument used in the transmission and reception-printing of messages by proper sensing and interpretation of electrical signals. Also called teletypewriter, radioprinter. A specific variety of teleprinter is the Teletype, a trademarked machine manufactured by the Teletype Corporation.

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 in telephone service. Abbr. TWX.

terminal, n. Equipment required to receive and reproduce, or to transmit in usable form one radio signal.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

- test element.** A character used for the derivation of an authenticator.
- 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.
- textual element.** An individual letter, a word, or a unit of encryption from the actual text of a message.
- tfc. *Traffic*, q. v.**
- three frequency Morse.** A morse-based system in which a carrier is shifted among three frequencies and in which dot, dash, and space are represented each by one of the three frequencies.
- thripple, v. t.** In meteorological ciphers, to substitute two three-figure groups for a five-figure group so that the sum (noncarrying) 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.** A ciphony system in which successive sections of speech are divided into short elements and these short elements are sent in a scrambled time sequence.
- time of delivery.** The date and time at which a message is delivered to an addressee. Abbr. TOD.
- time of intercept.** The time at which a message was received by an intercept operator. Abbr. TOI.
- time of origin.** The time at which a message was originated. Abbr. TOO.
- time of receipt.** The date and time at which a communication agency completes reception of a message transmitted to it by another communication agency. Abbr. TOR.
- time of transmission.** The time at which a message is transmitted. Abbr. TOT.
- 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.
- TINA, n.** A term used to designate the research and development of techniques and equipment employed in Morse operator analysis.
- TOD. *Time of delivery*, q. v.**
- 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. Cf. SECRET; CONFIDENTIAL.
- TOR. *Time of receipt*, q. v.**
- TOT. *Time of transmission*, q. v.**
- tracer, n.** An inquiry sent out requesting information concerning overdue or lost communications or articles.
- traffic, n.** All transmitted and received communications. Abbr. tfc.
- traffic analysis.** The branch of cryptology which deals with the study of the external characteristics of signal communications and related materials for the purpose of obtaining information concerning the organization and operation of a communication system. Abbr. T/A.
- traffic analyst.** A person versed in the art of *traffic analysis*.
- 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*, q. v.
- 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.** See LINGUISTIC PERSONNEL.
- 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.** 1. In electrical or electronic communication systems, an equipment which translates information from one code to another. 2. See LINGUISTIC PERSONNEL.
- transmission security.** That component of communication security which results from all measures designed to protect transmissions from interception, traffic analysis, and imitative deception.
- transmitter callsign.** The callsign of the radio station actually transmitting a message by radio.
- transmitter-distributor, n.** A device which reads baud tape and converts the code into electrical impulses which it relays to other equipments. Abbr. TD.
- transparency, direct.** That characteristic of cipher text which indicates that certain plaintext elements may have been self-enciphered.
- transparency, inverse.** In a digraphic system that characteristic of cipher text which indicates that certain cipher digraphs may be merely reversals of the corresponding plaintext digraphs.
- transposal, n.** The exchange of position of two or more adjacent textual elements, usually by error. Also known as inversion.
- 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.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

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 multiliteral 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 base. Those digits or letters assigned to code groups, keys, substitution tables, etc., which are determined to be the actual digits or letters in the original encrypting materials used by the originators of the encrypted text.

true periodic repetition. A repetition in 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 cipher units display no evidence of monoalphabeticity, nor evidence of relationships within any group; that is, in a true polygraphic system, changing one letter in any plaintext polygraph affects the equivalent ciphertext unit in its entirety. Cf. PARTIALLY POLYGRAPHIC SYSTEM and PSEUDO-POLYGRAPHIC SYSTEM.

TT, TTY. 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-digit differential. A two-element differential in which the elements are digits.

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-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 plaintext groups are arranged in an alphabetical or other systematic 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-point hit. See DOUBLE HIT.

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 DF 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. Abbr. UHF.

undulator tape. Inked tape, q. v.

unilateral, 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.

unilateral frequency distribution. A simple tabulation showing the frequency of individual characters of a text.

~~CONFIDENTIAL~~

- unilateral substitution.** A cryptographic process in which the individual letters of a message text are replaced by single-letter cipher equivalents.
- universal stereotype.** A stereotype commonly used by many originators. Cf. LOCAL STEREOTYPE.
- 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. 2. One of several plaintext meanings which may be represented by a single code group; also called alternative.
- variant callsigns.** Two or more callsigns which may be used interchangeably to identify a particular radio station. Also known as alternate calls.
- variant group.** See VARIANT.
- 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.
- verical digraph.** A pair of letters written one over the other.
- vertical message print.** An IBM listing, used in code reconstruction, which contains essentially the code groups of a message tabulated in a column and, where applicable, includes the meanings of the groups as recovered from earlier traffic. The message print generally has a heading including such indicative data as pertinent callsigns, serial numbers, originators date and time of file, etc., and in most prints the code groups are accompanied by an indication of their frequency in earlier traffic. Abbr. VMP.
- 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. Abbr. VHF.
- very low frequency.** The range of radio frequencies below 30 kilocycles. Abbr. 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.
- VMP.** *Vertical message print*, q. v.
- voice announcement.** Voice intercept operators comments and data recorded for information of the transcriber and analyst.
- voice callsign.** A word or combination of words used in voice transmission to identify a radio station.
- voice intercept operator.** An intercept operator responsible for operating a radiotelephone position.
- voice translator.** See LINGUISTIC PERSONNEL.
- watch, n.** A period during which one is on duty.
- wavelength, n.** The distance in the line of advance of a radio wave from any one point to the next point at which at the same instant there is the same phase; usually measured in meters.
- wave propagation.** The radiation, as from an antenna, of radio frequency energy through 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.
- 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 equisized 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 can be read, serving as a reference point for setting the rotors.
- WMO number.** See BASE NUMBER.
- word pattern.** The characteristic arrangement of repeated letters in a word which tends to make it readily identifiable when enciphered monoalphabetically. See IDIOMORPHISM.
- 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 officially designated representative.
- W/T.** Wireless telegraphy; *radiotelegraphy*, q. v.
- WX.** Abbr. for weather.
- X test.** See CHI TEST.

~~CONFIDENTIAL~~

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. 3. Used followed by a number to indicate the location of a group from the end of a message; i. e., the last group is called Z β , the fifth from the last is called Z4.

zeroize, v. t. 1. To equate two or more elements. 2. To align cryptographic elements of a cipher machine to a fixed original position.

Z. I. Zone of the interior.

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" signals. An *operating signal*, q. v., beginning with the letter Z.

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.)

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~
~~Modified Handling Authorized~~

BASIC CRYPTOLOGIC GLOSSARY

~~CONFIDENTIAL~~
~~Modified Handling Authorized~~