~~CONFIDENTIAL~~

S/A SST
Mr. FRIEDMAN

DRAFT SAMPLINGS

for the

Unabridged Cryptologic Glossary

OFFICE OF TRAINING

1. The enclosed terms are circulated for the purpose of standardization of the definitions and for fixing the exactness of meanings. In many cases these terms have different meanings in different parts of the Agency. In some cases the terms have changed in meaning since their conception. In other cases the terms can stand on their own merits as defined but have been submitted for verification. Lastly there are those terms which need more than one definition. It is to solidify this amorphous mass into a clear cut, useable whole that these terms are submitted for comment.

2. When a term has been approved for use it will go into an unabridged cryptologic glossary, which, when finished, will be TOP SECRET and will have a CODEWORD annex.

3. It is requested that serious thought and consideration be given to these terms and their definitions and that the available space following each term be used for comments, corrections, suggestions, and revisions to the presentterminology.

4. It is further requested that these comments be returned by 6 JUN 1955 in order that they may be used in conjunction with other materials to produce the completed Unabridged Cryptologic Glossary at the earliest possible date.

After entering comments, tear off this page. The enclosure is self-addressed for return to the Office of Training.

~~CONFIDENTIAL~~

TO: Office of Training
Glossary Group

UNABRIDGED CRYPTOLOGIC GLOSSARY

Suggested Terms and Definitions, with Corrections
(first circulation)

TO: Office of Training

FROM: S/ASST NITZBERG MAN

Date _____

The enclosed terms have been circulated within this area of the Agency for consideration and comment by all concerned. In each case where it has been felt that a change in the term or a change in the definition of the term was needed the suggested change has been entered in the space provided.

Suggested Terms and Definitions for the
UNABRIDGED CRYPTOLOGIC GLOSSARY

accumulate, v.t. To add numeric quantities by normal arithmetic. The usual implication is that there will be more than two addends.

Machine terminology.
Comment:

address, conjunctive. An address group, the meaning of which is incomplete unless used in combination with one or more other address groups.

A communication term as defined in ACP 167.
Comment:

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

Comment:

agent. In intelligence usage, one who obtains or assists in obtaining information for intelligence or counterintelligence purposes, but who has no obvious connection with any intelligence agency or officer.

This definition comes from JCS. Do we use it in the same sense in this Agency?
Comment:

antenna, n. An elevated and/or extended system of conductors used for the transmission and/or reception of electromagnetic waves. Also called aerial.

authentication test element. An element on which an authentication of a message, transmission, or station is based.

This is variously defined in several places. Is the above definition adequate?

bandwidth, n. The bandwidth occupied by an emission is the band of frequencies comprising 99 percent of the total radiated power extended to include any discrete frequency on which the power is at least 0.25 percent of the total radiated power.

As defined in ACP 167.

base number. In meteorology, a one-, two-, or three-digit number identifying a meteorogical observation center and almost always transmitted as the first element in a meteorological report. Also called station indicator or IMC number.

beam/lobe switching. A method of determining the direction of a remote object by comparison of the signals corresponding to two or more successive beam angles, differing slightly from the direction of the object. Beam switching may be either continuous and periodic, or discontinuous.

As defined in ACP 167.

book message. 1. In COMINT usage, a circular message; q.v. 2. In U.S. communication usage, a message which is destined for two or more addressees and is of such a 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.

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

card coding. The arrangement of punched holes in an IBM card which will be interpreted by an IBM machine as a number, a letter, or a special character.

Machine Terminology.

casebook number. A number designation for a circuit, sub-net, or net.

catalog, n. A systematically arranged record of all the relevant data of a complete set of hypotheses.

chaff, n. Electromagnetic-wave reflectors in the form of narrow metallic strips used for creating radar echoes for confusion purposes. See window.

chain addition. A cryptographic process wherein a sequence or group is disguised by the elements within it; the first digit is added to the second, the second to the third, etc., and the last to the first.

channel, n. A facility for telecommunications on a system or circuit. The number of independent channels on a system or circuit (derived by frequency or time division) is measured by the number of separate communication facilities that can be provided by it. Note: The term channel is also used frequently in conjunction with a figure or letter to identify a particular facility existing between two stations.

characteristic distribution. The distribution of plain-cipher pairs within a conversion square.

checker, n. One who reviews a translation for accuracy by comparing it with the original text or transmission.

circular message. 1. A message destined for two or more different recipients, encrypted in cryptographic keys held in common by all recipients of the message. Usually, but not necessarily circular messages pass from superior to subordinate. 2. A book message, q.v.

circular keys. Cryptographic keys used to encrypt circular messages, i.e. messages passing to two or more different recipients, the keys being held by each of the recipients. Recipients of messages in a certain circular key normally are not authorized to encrypt messages using the same circular keys.

cluster, n. A series of plain equivalents in a code each possessing some feature common to all others in the series. A cluster may be formed of various inflections of a verb or of various phrases each of which contains the same important noun.

code, combat. A code or cipher, the purposes of which are simplicity and speed in addition to as much security as is possible without prejudicing unduly such simplicity and speed.

As defined in ACP 167.

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.

conjugated matrices. Two separate matrices each containing a different sequence used in a two-square checkerboard.

counter, n. An electrical or mechanical device which can accept numeric quantities, hold them, add (or subtract) them, and yield their totals to be punched, printed, or to control other operations.

Machine terminology.

daily film. A RAM film on which is recorded a cipher text or text subjected to a key in use for a single day or for a single message.

decode, n. In cryptanalysis, the listing of a code book in order by the code group. In machine terminology, a short term for "message decode," that is, the message with meanings applied.

Machine terminology.

de-ghosting. The process of recovering the latent group.

difference book. A list which presents a large sorted set of differences of code groups and the code groups which produce the differences.

Machine terminology.

distance measuring equipment. A radio-navigation aid in the aeronautical radio-navigation service that determines the distance of an interrogator from a transponder by measuring the time of transmission to and from the transponder.

As defined in JANAP 121 A.

dummy letter. A character, usually one of several characters or groups of characters with no plain text significance, inserted within a cryptogram with the intent to delay or prevent its solution; a null. q.v.

edit, v.t. 1. In cryptology, to prepare textual material for the next step in processing. 2. To emend.

facility, n. 1. An activity which provides the means for assisting or making easier any function, often of a technical or testing nature; sometimes used in the plural. 2. Any part or adjunct of an activity which contributes to the performance of its function by providing some specific types of physical assistance.

As defined by JCS.

ferret, n. Aircraft, ship, or ground vehicle especially equipped for the detection, location, recording, and analyzing of electromagnetic radiation.

As defined by JCS.
Should this be limited to "electromagnetic"?

filter, v.t. To reduce or narrow down reports of aircraft to definite information about hostile aircraft.

finnery, n. Cycle interruption in machine ciphers effected by the arbitrary advancement of one or more of the wheels. Named for the Finns who were the first to be observed using it.

frequency, alternative. A frequency or a group of frequencies which may be assigned for use on any channel, or on a particular channel, at a certain time or for a certain purpose to replace or supplement the frequencies normally used on that channel.

As defined in ACP 167.

frequency count. A frequency distribution.

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

frequency list. A frequency distribution in tabular form, with frequencies listed in order from high to low. NOTE: The Machine Division calls this an inverse frequency list, q.v.

frequency table. A frequency distribution.

G. Used as a symbol in code recovery and in translated text to mean "garble" or "garbled".

garble, n. Any instance of unintentional departure from the correct in any part of a message or transmission.

As defined by JCS.

H. Used as a symbol in code recovery to indicate "hypothetical meaning".

Hagelin, n. 1. One of a number of machines invented by Mr. Boris Hagelin. 2. Specifically models C-36 and C-38, the prototypes of the U.S. Army M-209 which produces a polyalphabetic cipher, (with a key so long as to be nonrepeating) by means of rotors and movable lugs. 3. Loosely, traffic enciphered on such a machine.

heading, n. 1. The part of an order containing the designation of the issuing unit, place of issue, hour and date of issue, file notation, classification, serial number, and reference to map(s) used. (JCS) 2. That part of a message which contains the call preamble, address, and message instructions. 3. That portion of a complete intercept message not actually transmitted by the original correspondent but applied by the intercept operator. 4. Loosely, that part of a message preceding the text. 5. The direction in which a ship or aircraft is pointed with reference to true, magnetic, or compass north. (JCS) 6. The orientation of an antenna.

Hollerith machine. (Brit.) Any standard punched card machine of the kind manufactured by the International Business Machine Company. Invented by Herman Hollerith of the U. S. Census Bureau.

I. C. Index of Coincidence.

idiomorph, four-square digraphic. A special type of digraphic idiomorph, partial or complete, peculiar to cipher text produced by a four-square system involving a matrix in which the arrangements of the letters in the plain component sections are known.

infinite key. A keying sequence the length of which extends or can be prolonged to an infinite number of elements. A non-repeating key. Also known as indefinite, unlimited, running, or continuous key.

information, national elements of. That information which is required by the Federal Government to assure the most effective accomplishment of the intelligence mission related to the national security of the United States.

inverse frequency list. See frequency list.

inversion. A change in the normal order of words and phrases. See transposal.

Kasiski method. A method of solving polyalphabetic substitution by factoring to find the period. Named for Major Kasiski but developed by Auguste Kerckhoffs.

Is this term still in use?

key bank. An ordered listing or file of expanded text, potential or recovered, showing the unique or multiple key or keys immediately preceding and following the sorted group with proper identification of the source, whether crib or overlap.

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

language consultant. One who has an expert knowledge of a difficult language or of a group of languages, and who is called upon to solve complex linguistic problems in those languages.

level, n. The "rows" of a card, referred to as 12, 11, 0 or ten, 1, 2, ..., 9. In tape, one of the five (or seven) streams of single bauds along the tape.

Machine terminology.

line-up, n. An overlap. The line-up is said to be absolute if the exact position in the additive book of the starting point is known; if the starting points are only known relative to each other, the line-up is said to be relative. ---v.t. To set in depth.

listening watch (radio communication). A continuous receiver watch established for the reception of traffic addressed to, or of interest to, own unit with complete log optional.

As defined in ACP 167.

M. 1. Used as a validity classification in code recovery to mean: "English meaning is certain enough for unquestioned translation, but precise wording or complete form is undetermined." 2. In COMINT translation, used as an abbreviation for "missing".

MAI. Master additive (indicator additive) indicator.

map, line route/route diagram. A map or overlay for signal communication operations that shows the actual routes and type of construction of wire circuits in the field.

As defined by JCS and in ACP 167.

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

muto message. A message which has been relayed because it was originally misaddressed.

net, n. 1. A number of associated groups all controlled at a common location and presumable serving the same common superior headquarters. (Combined) 2. A group of inter-communicating radio or landline stations.

net, controlled. A group of stations on a common channel of communication with one station designated as control and all other stations transmitting only when granted permission to do so.

non-COMINT. Information from a source other than communication intelligence. This term is synonymous with and preferable to the term "collateral" as it applies to the communication intelligence field.

NSD. 1. A trigraph applied to a message which does not bear (in clear or cipher) a recognized discriminant. Short for new system discriminant. 2. Navy abbreviation for Naval Supply Depot.

O. Used as a symbol in code recovery meaning: "Omit part of this for correct meaning."

offset position. This term has been submitted for inclusion but without a definition. We suggest the following:

1. In cryptanalysis, that condition which exists when the plaintext component appears one or more spaces to the right or left, usually the right, of the normal window setting. 2. In machine terminology, the position to the right of the control position of the Master IBM card in which the information is punched into secondary cards.

one-way difference table. A difference book listing only the smaller of the two complementary differences obtained when selected pairs of code groups are subtracted (non-borrowing). Cf. reciprocal difference table.

P. 1. U. S. 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. 2. Used as a validity classification in code recovery to mean: "Identified portion is certain, but meaning is incomplete."

paper tape. A medium for input and output with certain machines, and for storage of information. A character is represented in one frame of a tape, which is normally a vertical arrangement of five levels in which hole and no-hole define the character. There is a tape wide enough for seven level coding, as well as tape to contain only five levels. The density of tape coding is ten frames or characters per inch.

Machine terminology.

parallel cipher alphabets. Cipher alphabets having the same components but with different juxtaposition.

parapolygraph.

Is this term still used?

phantom circuit. A telephone or telegraph circuit obtained by superimposing an additional circuit on two existing physical circuits by means of repeating coils.

As defined by JCS.

pilot card. An IBM card used for determining the discriminants and finding duplications in traffic received by mail.

pulse, n. A variation in the value of an electrical quantity as a function of time such that the value departs from a given datum for a time interval and then returns to this datum.

radar shadows. Regions obscured from the surveillance of a radar set by obstructions, either natural or artificial.

radio guard. A ship or radio station designated to listen for and record transmissions, and to handle traffic on a designated frequency for a certain unit or units.

As defined by JCS.

reciprocal difference table. Any difference book listing both differences obtained when selected pairs of code groups are subtracted (non-borrowing). Cf. one-way difference table.

recognition, n. The 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, further testing is resumed. Recognition, machinewise, can have the forms of pre-wired boards, drum storage, or card storage.

Machine terminology.

recovery, n. 1. The process of making cryptic text intelligible. 2. Any cryptographic material obtained through cryptanalysis. 3. Any plaintext so obtained.

rope, electronic. Electromagnetic-wave reflectors consisting of long strips of metal foil. A small parachute or other device may be attached to each strip to reduce rate of fall.

scritch, v.t. To test an assumption by examining its implications in conjunction with each of a set of further assumptions in turn, eliminating those cases which yield contradictions and scoring the others.

selector, n. A device which permits information in one channel to be put into either of two or more channels under suitable controls. It can also be used to direct information from either of two or more sources to one destination.

Machine terminology.

service, safety. Any radio service, the operation of which is directly related, whether permanent or temporary, to the safety of human life and the safeguarding of property.

As defined in ACP 167.

stop, n. A point in a run at which a bombe stops; especially one giving a solution of a particular menu.

tabulate, v.t. To abbreviate the length of a report by suppressing the listing of every item, showing only necessary descriptions of each class, and the numbers it produces--as card count totals, or true totals of a numerical quantity.

Machine terminology.

text block. A section of plain text or cipher text written into a square or rectangle.

transposal, n. A change in the relative, usual, or natural place or order of; exchange in position; reverse or rearrange the sequence of. (Webster)

U. Used as an abbreviation for "unrecovered" in COMINT translation.

unique, n. A plain-cipher pair which occurs with a frequency of one in a BPCD or in a characteristic distribution. ---v.t. To reduce a multiple key to a unique key group.

variant pattern. A stereotypic pattern subject to variation.

verify, v.t. To ensure that the meaning and phraseology of a transmitted message conveys the exact intention of the originator.

As defined in ACP 167.

Wd. Abbreviation for "word" in COMINT translation.

weight, n. A number associated with a recognized group or condition in a mass testing of data. It is roughly proportional to frequency, probability, or some other measure of goodness of a result. The sum of weights of several occurrences is often used in conjunction with a threshold to suppress random answers, or guarantees only good ones.

Machine terminology.

X. Used in code recovery as a symbol meaning "unevaluated." Usually applied to code identification received from the field or a sister installation when there is insufficient evidence at NSA for evaluation.

X punch. The single level "11" punch, used for control purposes in IBM processing. It is represented in machine listings by +.

Z. 1. U. S. 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. 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 ∅, the fifth from the last is called Z 4. 4. Used as a validity classification in code recovery to mean: "Precise wording of value is certain but the code group may be garbled."

~~CONFIDENTIAL~~

Distribution List

S/ASST (Mr. Friedman)	- 1	NSA-74	- 1
S/ASST (CAPT Holtwick)	- 1	NSA-75	- 1
P/P	- 3	NSA-76	- 2
COM	- 1	NSA-82	- 1
SEC	- 1	NSA-91	- 1
LIB	- 1	NSA-92	- 1
NSA-062	- 1	NSA-93	- 1
NSA-063	- 1	NSA-94	- 1
NSA-064	- 3	NSA-31	- 2
NSA-61	- 1	NSA-32	- 1
NSA-62	- 1	NSA-33	- 2
NSA-63	- 1	NSA-34	- 1
NSA-64	- 1	NSA-35	- 1
NSA-71	- 2	NSA-41	- 1
NSA-72	- 1	NSA-42	- 1
NSA-73	- 1	NSA-43	- 1

~~CONFIDENTIAL~~