Famous First Facts, NSA
Part I: Pre-Computer Machine Cryptanalysis

BY SAMUEL S. SNYDER

~~Top Secret Umbra~~

This paper discusses the most important first uses of pre-computer machines and special attachments in U.S. cryptanalysis in the 1930's and 1940's by the U.S. Navy and U.S. Army predecessors of NSA; first use of punched-card equipment, U.S. Navy Code and Signal Section; Naval Communications ("NC") machines and devices; NC-1, Serializing Modification; NC-2, Cross-Foot Machine; NC-3, Dupe Eliminator; NC-4, Improved Cross-Foot Machine; NC-5, Patternizer; NC-6, Difference Scoring and Weighting Device; NC-7, Collator Percentage Matching Device; NC-8, Plugboard Switching Device; paper tape reading the punching equipment and hookup with electrical typewriters (CXCO machines); other electromechanical and photoelectric machines for specialized cryptologic operations; S.I.S. applications for punched-card equipment: U.S. code production, reconstruction of Japanese codes, standardization of indexing procedures, pattern studies, linguistic studies, and analysis of selected parts of messages; the punched-card randomizer; the electromechanagrammer ("Gee-Whizzer").

A reference book[1] on the shelf of most public libraries, titled as is this article (but without the "NSA"), is full of fascinating information spanning a great variety of subjects. Browsing through this book, one finds answers having varying degrees of uselessness, depending on one's questions. One even finds, in areas touching NSA's fields of expertise, an occasional error of fact. For example, credit for building the first solid-state computer is given to Remington Rand UNIVAC, Philadelphia, Pa. We at NSA might have told the author that our SOLO, delivered by Philco Corporation to this Agency in March 1958, was the first. It is not my intention to attack the editors of that scholarly work, or to upset the delicate balance affecting NSA's necessary policy of anonymity, by pointing out such errors. Rather, I would like to take the reader with me while I look at a few "firsts" in

[1] Joseph Nathan Kane, *Famous First Facts* (Bronx, N. Y.: H. W. Wilson Co., revised 1969).

machine applications in cryptanalysis. For those who have come into the NSA community relatively recently, especially where NSA machine applications dominate their work, these few stories may be of interest.

Harking back some 40 years, we find U.S. cryptologic activities in their infancy: three small groups of three or four people each were in the War Department, the Navy Department, and Treasury's Coast Guard. In the Navy Department, the Code and Signal Section (also known as OP-20-GX), under Miss A. M. Driscoll, was responsible for cryptanalytic work. The War Department effort, under Mr. William F. Friedman, was known as the Signal Intelligence Section. Mrs. Elizebeth Smith Friedman headed a small group of cryptanalysts in the Coast Guard.

In 1931, Navy's OP-20-GX was working on a certain Japanese Naval system which was basically a 3-kana[2] code with kana additive encipherment. This system had been partially readable by the Navy analysts, but in 1932 the Japanese changed the system. It is likely that this was one among many changes in the cryptosystems of foreign governments that resulted directly from appearance in 1931 of Yardley's *The American Black Chamber*.[3] It was soon apparent that the new system, also enciphered kana, used a new 4-kana code. This presented an especially challenging task for the analysts, since it was the first time they were confronted with simultaneous change of underlying code and cipher. The labor necessary to perform the analysis of the traffic in the new system was obviously beyond the capacity of the staff, using hand methods. At this time, the possibility of using punched card equipment was investigated. In another area of the Navy Department, such machines were already being used for administrative and accounting applications. Some part-time use of this equipment was arranged, to test the feasibility of the proposed cryptanalytic application. No money was available for rental of IBM equipment for OP-20-GX until the fiscal year 1933.

In the fall of 1932, with $5000 for FY-33, OP-20-GX installed a small complement of punched card equipment:

2 duplicating keypunches
1 sorter
1 tabulator-printer

This machine installation undoubtedly constitutes the first use of machines in cryptanalysis in the United States. Capt. Thomas H.

[2]Kana refers to the modern Japanese 48-syllable system for representing in writing the pronunciation of Japanese words.

[3]Herbert O. Yardley, *The American Black Chamber*, (Indianapolis, Indiana: Bobbs-Merrill, 1931).

Dyer, USN (Retired), then Lieutenant, JG, was placed in charge of the machine operation, and probably deserves the title of "father of machine cryptanalysis." The equipment was instrumental in producing a breakthrough in this initial application, and of course in many other problems later.

Old-timers (pre-computer days) at NSA who "cut their machine teeth" on punched card equipment may not know about the following technical detail about IBM card systems of the early 1930's. Capt. Dyer recalls that when he made the above-related small beginning, the representation and manipulation of alphabetic data in punched cards was in its infancy. There were only two "zones" for alphabetic 2-hole codes: the "12" and "11." The rest of the alphabet was accounted for by arbitrary assignment of certain numeric punches to selected alphabetic characters. Thus, "zero" represented the letter "O," "one" equated to "I," "2" stood for "Z," "6" for "G," and so on. Obviously this scheme precluded uses for mixed alphabetic and numeric material. Within a year or two, IBM perfected and introduced its 3-zone system for 2-hole coding of alphabetic material.

Early in 1941, the punched-card machine operators in Navy's Code and Signal Section felt the need to overcome certain awkward and inconvenient aspects of their work. For example, it was repeatedly necessary to number, in sequence, the individual cards in a set, starting with a certain number, to identify each card. To do this, one had to have ready a "master" deck, select the starting number, and perform the reproduction of the identifying numbers into the detail cards in a separate pass through the reproducer. A similar chore was the counting of sets of blank cards, for insertion after each master, or line card. A more sophisticated function was that known as "cross-footing" or summing two 5-digit fields in a card and punching the sum into the same card. These requirements, and a few others, were brought to the attention of Captain Redmond, then Director of Naval Communications, who promised to bring these needs to the attention of his good friend, T. J. Watson of IBM Corporation. The result of this contact was a visit by Mr. Watson's "second in command," during which these requirements were described by Messrs. Peter Deffert and Lewis Holland of OP-20-GX. This visit by the IBM executive was repeated a few days later by a senior IBM engineer, who took entensive notes. According to Mr. Holland, "this was the extent of our R & D, paperwork, etc."

The result of these initial contacts was the beginning of a series of "NC" (for Naval Communications) machines and devices. These are briefly described below:

NC-1: Serializing Modification.—Within a few months, about August 1941, Mr. Dell Newcomb, the IBM customer engineer assigned

to the Navy installation, installed a modification to the IBM Type 513 reproducing gangpunch. This performed the required serial numbering function mentioned earlier, with excellent results.

NC-2: Cross-Foot Machine.—This new machine, built up from the IBM summary punch, accomplished the fundamental requirement of adding two numbers and punching the result into the same card, at the rate of 100 cards per minute. This was quite an improvement over the 10-to-15 cards per minute of the previous procedure. The *NC-2* was the first instance of use of "matrix calculation" in accounting machines.

NC-3: Dupe Eliminator.—About the same time as the *NC-2*, this single-purpose machine was completed and delivered. It processed presorted decks of message cards, noted cases of duplicate message numbers, and flagged instances of repeated messages, at about 400 cards per minute.

NC-4: Improved Cross-Foot Machine.—A better name might be "general-purpose deciphering machine," although this would not apply to the machine in its original form. The *NC-4* combined several card-handling operations in one machine, such as inserting blank detail cards, reproducing additive key into detail cards, cross-footing (performing noncarrying arithmetic), and checking the result for divisibility by 3.[4] When first delivered (about December 1941) the *NC-4* 10 x 10 matrix was "hard-wired." In succeeding years it underwent several modifications which added to its flexibility by making this process pluggable: first 10 x 10, then 26 x 26, and eventually 32 x 32.[5] An additional function was the application of meanings to code groups. The *NC-4* was a real workhorse during World War II, and many copies were in use at the Naval Security Station and at Pearl Harbor and Melbourne.

NC-5: Patternizer.—This machine examined 10-character selections of text and formed a pattern ("idiomorph") reflecting occurrences of repeated characters. Example:

Text: REAREXITIT
Pattern: ABCABDEFEF

Although this was an interesting and classical cryptanalytic process, the *NC-5* did not have a large number of practical applications during the war.

[4] One characteristic of many war-time Japanese systems was their use of 4-digit codes having the limitation of divisibility-by-3, for garble-checking.

[5] Actually the model of NC-4 which was expanded to accommodate full alphabets was a different machine, designated IBM Type 797, the Coordinating Reproducer.

NC-6: Difference Scoring and Weighting Device.—A modified reproducer was connected to a specially built accumulator to analyze high-frequency differences in additive systems, and recovering plain code by statistical means. Only one model was built; it was used in certain Japanese Naval additive systems during World War II.

NC-7: Collator Percentage Matching Device.—An attachment, the *NC-7* device, was connected to a standard IBM collator, making it possible for the collator to select, or perform other collator functions, subject to a "percentage" match control. Thus, control could be set to select when, say, any 15 columns out of 25 achieved a match. The capacity for match-sensing was a maximum of 74 columns of digital information, or 37 columns in the case of alphabetic data. The *NC-7* was built by local Navy personnel, rather than by IBM, which was the case in all the earlier NC-series equipment.

NC-8: Plugboard Switching Device.—This device simplified the changing of plugboards for those problem situations where succeeding stages in processing required different plugboards. Prewired plugboards could be manually or automatically switched into operation and connection with a tabulator, collator, or reproducer. Use of the *NC-8* thus saved operational time through elimination of delays in removing and replacing plugboards.

Two other early machine developments deserve mention: (1) the series of transcribing and deciphering machines based upon paper tape reading and punching equipment and their hookup with electric typewriters, known as CXCO machines, and (2) the electromechanical and photo-electric machines, built under Navy sponsorship for the most part, for specialized cryptologic operations. The first is well documented in the *NSA Technical Journal*, Vol. XVI, No. 4 (Fall 1971): "The CXCO Story," by Captain John A. Skinner, USN. The second series of machines includes a host of special-purpose or limited-purpose devices and machines too extensive to be detailed here; however, one of the first electromechanical machines, MIKE, and the first photoelectric machine, the 70-mm Comparator, will be briefly described. MIKE, built in 1944, was a monograph and digraph counter. Input was numerical or alphabetic material punched in paper tapes and read by a "double-headed" tape reader. The paired combination was formed by means of a matrix, which transmitted an impulse for a digraph to one of 676 dial counters. At the same time each letter of the pair was counted on a visual counter, one of 52, corresponding to rows and columns of the matrix. The totals had to be read visually and copied out by hand. (For a time, an experimental process of photographing these dial settings was tried, without great success.) MIKE was superseded by ALCATRAZ, which included

facilities for automatically printing the results. The 70-mm Comparator was based on a principle suggested by Vannevar Bush of M.I.T., and the first model of such a machine arrived at the Navy early in 1941. It used rolls of paper, the opaque backing commonly used on camera film rolls, as an information medium. Very small holes were punched along its horizontal dimension, corresponding to letters of text, one line per character. The width, somewhat more than 70 millimeters, was divided into positions corresponding to letters of the alphabet. Two such rolls of tape were threaded around a series of rollers and past a bank of ten photo-cells which scanned from one to ten successive text positions. Coincidences between the two tapes registered in one or more counters, and an eleventh photo-cell recorded the extent of overlap by means of a separate feed-hole level on the tape. After each pass of the tape loops, the relative juxtaposition of the two tapes was changed by advancing one tape from 1 to 10 positions. A printed record of results was made on a typewriter. Many models of the 70-mm Comparator were built, and of course equipment to punch the tape. It was used both by the Navy and War Department offices very successfully in a number of problem situations.

Just a few words about the Treasury's Coast Guard cryptologic activities. The Cryptologic Unit was established in 1931 to solve messages between smugglers and other criminals operating in violation of laws administered by the Treasury Department. After World War II began in 1939, the unit monitored possible nonneutral communications affecting vessels of belligerents. Punch card machines were used to assist these activities, beginning in 1935 with Remington Rand equipment, and continuing from 1937 with IBM machines. Mrs. Elizebeth Friedman was in charge, and her small staff included Lt. Leonard T. Jones, Robert O. Gordon, Vernon E. Cooley, and Miss Mary Joe Dunning, among others. The last three named transferred to the War Department's S.I.S. in 1939. In November 1941 the Coast Guard unit was transferred to the Navy Department, becoming a part of OP-20-GX.

The War Department's Signal Intelligence Section, under Mr. William F. Friedman, was originally primarily responsible for cryptographic work for Army needs. The section devised field codes and several small enciphering devices for Army use. In connection with these efforts, in order to assess the security of such systems the S.I.S. also engaged in theoretical studies in cryptanalysis, being prevented from practical work in the field by lack of traffic and also because, in Mr. Friedman's words, ". . . the Army regulation applicable thereto

specifically restricted cryptanalytic operations on foreign communications to wartime."[6]

Although the need for machine assistance was acutely felt, no money was available for this purpose until late in 1934. According to Mr. Friedman, he did not even know of Navy's use of IBM equipment until the summer of 1934. An IBM installation in the Munitions Building, ". . . used for accounting purposes in connection with the C.C.C.—the Civilian Conservation Corps—. . ."[7] was transferred to S.I.S. upon Mr. Friedman's urgent request.

The first S.I.S. applications for punched card equipment were related to code production. An amusing story is told concerning S.I.S. compilation of code books using punched cards. Two equal-size decks of cards were punched, one containing code groups and the second containing plain-text meanings. The object was to assign one code group to each meaning in random order. The earliest method employed for the randomizing process was simply to throw the meaning cards into the air, pick them up one by one, and then use the IBM reproducer to punch meanings into the code group cards. Of course, after printing a "decode" copy (in code group order), the deck of cards would be sorted alphabetically according to meanings, to produce a copy of the code book in "encode" order. In one incident during such a code book production, the number of cards in one deck was *one fewer* than those in the other deck, after "up-in-the-air" randomizing. After searching for some time, (you guessed it!) we found the missing card, stuck in a crack over a doorway!

By the time I started work at S.I.S. in August 1936, the Section had grown to the respectable size of nine civilians (I was number 10) and two student officers. It had been the custom for several years for the Army to assign two regular officers to the S.I.S. for two years' study of cryptology under Mr. Friedman's supervision. Captain Harrod G. Miller and First Lieutenant Harold G. Hayes (later Col. Hayes, one of A.S.A.'s early directors) were on active duty in S.I.S. in 1936. We occupied one room and a vault room (in which classified material was locked nightly), and, down the hall from our regular offices, a machine room. The complement of IBM punched card equipment consisted of one each alphabetic duplicating key-punch, sorter, gang punch-reproducer, and tabulator.

By this time the S.I.S. was actively pushing cryptanalytic activity on Japanese diplomatic codes. We were already receiving intercepted messages from two or three stations, and two new Army stations, at

[6] William F. Friedman, *Six Lectures on Cryptology*, (Fort George G. Meade, Md.: Office of Training Services, NSA, April 1963), p. 171 (CONF).

[7] Ibid., p.170.

Panama and Hawaii, were being set up about this time by Dr. A. Sinkov and Dr. S. Kullback, respectively. The Japanese messages were usually in one of a series of 2- and 4-letter codes that changed every three to six months. With the help of indexes prepared on the IBM equipment, new codes were relatively easily reconstructed by our team of three or four cryptanalysts and one Japanese linguist, the late John Hurt.

For the first few years, our use of IBM equipment followed a system best described as "haphazard." The analysts who used the equipment were self taught as to punch-card techniques, since the only known IBM uses were in the accounting field. Each analyst requiring an index of cipher text, for example, worked out a procedure, punched cards of raw traffic reading from sheets edited by himself, then wired up plugboards and operated the machines to produce printed listings. At the conclusion of the job the analyst could be seen returning to the vault from the machine room, often with a machine listing under one arm and one or two boxes of cards under the other. (Occasionally if the volume was great, we had the use of a small truck which we pushed from one end of the fourth wing to the other.) Incidentally, if the analyst-operator was careful and more than usually systematic, he would remember to write down the column numbers of the fields of information punched in the cards, and a few words about the particular process, to be saved along with the cards. But, of course, each analyst's columns and procedures were his own and different from those of the other analysts.

Even though IBM operations were unsystematic, this was an exciting time for machine developments. The procedure for preparing indexes, already mentioned, was undergoing refinement and generalization. The idea of generating a separate card for each code group, using a master line card followed by a set of blank cards, was developed by two or three of us analysts working cooperatively. The use of an X-punch control card, later refined by using a Q-punch on-line card (which can be interpreted by the machines as an X-punch whether read forward or backward), became possible only when we prevailed on our IBM customer engineer, the late Dell Newcomb, to short-circuit one of the relays of the reproducer. For many months after this, our indexing procedure included as one vital step, the insertion of a paper clip across a certain set of contacts on a particular relay![4] It is not an exaggeration to say that this IBM indexing procedure (with or without the paper clip!) became the backbone of all NSA punched card operations, and was the forerunner of the important computer programs known as KWIC indexes (Key-Word in Context).

[4]Mr. Newcomb later received a cash award from IBM Corporation for his proposed modification in the reproducer which accomplished the same thing, *sans* paper clip.

In 1938, Mr. Friedman realized that the state of affairs in the machine room was chaotic. He directed Larry Clark to begin preparing written descriptions of IBM procedures and about the same time assigned me to work full time in the machine room. As first machine-room supervisor for S.I.S., my duties at first were divided approximately as follows: 50% card-punching, 30% machine operations, and 20% planning new procedures. One of my first innovations was the standardization of our indexing procedures. As I have mentioned, until this time each analyst worked out his own methods, punched his own cards, wired plugboards, and operated the equipment. The problem was not only the differences in fields of the card used by different individuals, but also differences due to variations in size of groups to be indexed. The size of groups indexed could vary from single letter (or digit) to five characters. There might be other variations in collateral information needed; that is, message identification, date, routing, and the like. Also, there were differing requirements for number of groups preceding or following the indexed group, as well as differences in extent of consolidation of messages—from separate indexes of single messages to mammoth studies of hundreds of messages. The final solution was based on use of uniform fields for punching master cards, which not only simplified things for the card punch operator, but reduced to only a handful the number of reproducer plugboard wirings required to be kept on hand.

My assignment as full-time supervisor of machine room operations lasted about a year. I had asked Mr. Friedman for a transfer back to cryptanalytic duties as soon as a professional punch card man could be hired. In October 1939 our first full-time key-punch operators were employed. In December 1939 Mr. Ulrich Kropfl was obtained for the job of machine room supervisor, and I spent a few weeks with him to familiarize him with our problems and procedures. Within a year after Mr. Kropfl came, he had hired several other key-punch operators, and soon additional machine operators. The machines were used for a variety of jobs, including pattern studies, linguistic studies, analyses of selected parts of messages, and the like. The work horse continued to be the index; it contributed heavily to the success of our attacks on Japanese Red and Purple machine ciphers, as well as to other lesser known successes.

Very little was done before the beginning of the Second World War in the area of special machines or attachments for cryptologic purposes. Although it never became operational on a large scale, probably the very first attachment or modification to punched-card equipment for cryptologic purposes was a device for randomizing punched cards.

The randomizer, or strictly speaking the "mis-sorter," was invented by Mr. Frank B. Rowlett about 1936. It consisted of (1) a commutator disk with a rotating brush, mounted on the back of an IBM sorter, and (2) a group of five brushes mounted at the sorter reading position, in place of the single brush normally used in conventional sorter operation. The different points, or divisions, of the commutator disk delivered electrical signals from the five brushes to the leaves[9] of the sorter. Thus, the rotation of the brush on the commutator, by reading random punches in five card columns, caused the cards to fall into sorter pockets in random, or mis-sorted, order. There were some synchronization problems to be solved, but these were soon cleared up, and the randomizer was actually used for a time in connection with code book production. There was the obvious drawback that, with only one pass, the rearranged cards were only partially "shuffled"; that is, cards occupying early positions in the original deck would still be in relatively early positions in the shuffled deck. To get around this, one made at least three passes with the randomizer, and combined with this some manual shuffling. This device, plus the procedure of using the sorter, achieved the unpredictability which satisfied the requirements.

Among the Japanese diplomatic systems current in the 1930's and early 1940's, a series of 2- and 4-letter codes accounted for a large share of the traffic. Some of these were enciphered by keyed-columnar single transposition, with keys changing daily. Using manual anagramming methods, we found it fairly easy to stay current; much of the traffic in such systems was readable within a short time. In some cases changes and corrections to one system were transmitted by the Japanese in another readable system!

In the spring of 1941 the Japanese complicated the system further with use of blanks and nulls in the enciphering matrix, and traffic became heavier, so that it was more difficult to keep up with the workload. Machine help was sought. At first this took the form of preparing sets of punched cards containing logarithms of frequencies of digraphs and assembling for printout those cards corresponding to a group of letters to be slid, or juxtaposed, against the other letters of the message. The cards contained two sets of 26 logarithmic values, that is, the values of digraphs formed with the chosen group of letters taken both as initial and as final letters of digraphs. Printouts had to be scanned along a diagonal to find a high frequency setting, which turned out to be very tedious. To generate the series of diagonals and provide a means of calling attention to the highest totals, it was necessary to devise a procedure or a device which could feed new log values to the tabulator counters while dropping the old ones from the total and

[9]The mechanical guides that determine which of 12 pockets the cards will fall into.

operating in synchrony with the tabulator. This was accomplished by use of two 6-point, 25-position rotary selector switches. I won't include here all the technical details, since this has been very well covered in a previous *NSA Technical Journal* (Vol. VIII, No. 1, Winter 1963). The results were spectacular, inspiring the nickname "Gee-Whizzer." This attachment, officially called Electromechanagrammer, was undoubtedly the first practical special-purpose cryptologic attachment to punched card equipment in the U.S. cryptologic agencies.

Many other attachments and special-purpose machines were built, particularly under pressure of war-time needs, similar to those already briefly described in the section on Navy Code and Signal Section. Since this discussion has been limited to describing some "firsts"in U.S. machine cryptology in the pre-computer era, we will not go into more detail. The actual items of equipment built numbered in the hundreds, and the variety of design and problem applicability was almost unlimited. Indeed, the one universally true statement that would summarize our experience might be that no sooner has a machine been built for some purpose than other unforeseen uses are discovered. In fact, it is in this sense that the modern computer finds its true destiny.

ACKNOWLEDGMENTS (b)(3)-P.L. 86-36

Thanks are due to the following persons for providing assistance in the preparation of this study: Mary Joe Dunning; CAPT Thomas H. Dyer, USN (Retired); Lewis P. Holland; Wilfred H. Lapierre; [redacted] Martyn Miller; Frank B. Rowlett; CAPT John A. Skinner, USN; John R. Stapleton and [redacted].

BIBLIOGRAPHY

National Security Agency History, Vol. 2: "General Cryptanalytic Problems."

CAPT L.E. Safford, USN, "History of Radio Intelligence in U.S. Navy, 1922-1941" (S-3443).

Signal Security Agency: "History, Machine Branch, to 1944."

U.S. Navy, OP-20-G: "Chronologic Documented Notes on History of Research Section, 1940-46" (S-31,551).

U.S. Navy, OP-20-G: "Rapid Analytic Machines Panel Report" (April 1947, S-14,707).

War Department, S.I.S.: "Mechanism for Facilitating Solution of Certain Types of Transposition Ciphers" (SECRET, undated, S9098).

War Department, S.I.S.: "Description of J-Series Systems, J-16 through J-19" (SECRET, undated, S-1622).