from: OOY

Office Memorandum • UNITED STATES GOVERNMENT

~~TOP SECRET - Security Information~~
(Enclosure contains code-word matter)

TO : Dir.

DATE: 13 June 1952

FROM : Dep.

SUBJECT: Utilization of Analytical Machinery.

1. After you told me to study this subject, I found that, before I could really start, I had first to determine what the problems are, and that before I could start to do that I had to find out what machinery we have and what it does. This sounded easy, but a search revealed that we had no catalogue of this information. I have therefore had to make my own. Here is a copy of it. Although it has been carefully checked and rechecked with the technicians involved, it is undoubtedly subject to revision and improvement on many counts, and it is hoped that the responsible operators will soon collaborate on an authentic, properly staffed-out catalogue; meanwhile you may find it useful to retain this first tentative effort for reference until a better one comes along. All other interested parties have copies.

2. Downgraded to ~~CONFIDENTIAL~~ on removal of the inclosure.

W. S. L. GOODWIN
Captain, U.S. Navy

Incl - 1
"Machines Used in Cryptanalysis";
Draft/AFSA Inspector/13 June 1952

Copies to: C/S
DD(R)
Mr. Friedman

~~TOP SECRET~~
~~TOP SECRET~~

Machines Used in Cryptanalysis

1. There has not been available a listing of cryptanalytical machines which puts them in their logical relationship to one another and in their proper perspective from the relatively "lay" standpoint of the users, or of management authorities broadly interested in the application of machinery to cryptanalysis as a whole. The AFSA Technical Committee's paper "T/CA2" attempts a categorization, but its arrangement appears to be from the standpoint of the development engineers, with only indirect reference to purposes and results. This listing is an attempt to fill the gap and, at the same time, to present speed and performance data in terms of practical accomplishment, rather than in terms of the various internal and contributory processes which have too often in the past been cited in statements of the machines' capabilities.

2. The machines have been listed under three major categories by applicability; i.e., "broad", "narrow", and "specific". These applicability categories as used here are of course only relative, with arbitrary division lines and some overlaps and anomalies. Within these major categories, the machines are listed by purpose under two heads; viz, "analysis" (having as primary purpose the tallying and presentation of statistics for analysis) and "solution" (having as primary purpose the "solving" (at least tentative and partial) of individual messages). Here, too, there is an arbitrary line, and some anomaly. Within the two purpose categories, in turn, the sub-listing is according to function, as described in the next paragraph.

3. Because the functional categories "comparator" and "computer" hitherto used are sometimes considerably overlapping and have therefore led to some confusion, three new function categories have been adopted for this listing; i.e., counters, selectors, and operators, representing three degrees of capability on an ascending scale in that order. All three "look" at everything fed into them; the counter counts everything it looks at, the selector is capable of choosing parts of what it looks at and counting or indicating only them, the operator is capable of putting parts or all of what it looks at through certain processes other than or in addition to counting. It would seem that each of the two higher classes would embody the essentials of the classes below it, and this is, in general, the case; operators can be used as selectors or counters, and selectors can be used as counters, but not necessarily efficiently (in this connection, see the notes appended to IBM, ATLAS, ARMER, NOMAD, GATHERER, AND CORINE; notes 4 to 8, inc., and note 15). As for the relationships of the new function categories to the old, about all that can be said is that everything that has been or might validly be called a "computer" is an operator, but the reverse is not necessarily true.

4. At the end of the listing is a category of machines used in preparation which might be listed under that as a function but which, because the machines solely serve and are used in conjunction with other machines, partake of the applicability and purposes of the machines they serve (sometimes several, sometimes only one) rather than having applicability and purposes of their own. These are listed solely because they impose, on the other machines, various speed and time limitations which must always be kept in mind as the "speed" entries for the other machines are used in estimates of capacity and availability.

5. Analogue machines whose purpose is simply decryption or "hand testing" or the generation of specific key for other machines(either separately or as applique units) are not separately listed herein (Note 1; see page 2). In addition, machines which, although having individual names, are essentially appurtenances of the conventional IBM complex (such as MISTRESS) or which are peripheral to other machines (such as BEAR) are not listed.

Machines Used in Cryptanalysis (continued)

6. The categories and subcategories described above (minus "preparation") are briefly defined and related below for convenience.
Broad applicability - Applicable in cryptanalytic attack against any cryptographic system, or systems of more than one broad category.
Narrow applicability - Applicable in cryptanalytic attack against only one category of cryptographic systems or only a few systems.
Specific applicability - Applicable in cryptanalytic attack against only one specific system.
Purpose "analysis" - Having as its purpose the tallying of statistics or the finding of phenomena and symptoms to be used in cryptanalysis.
Purpose "solution" - Having as its purpose the solution of individual messages or parts of them; that is, their rendering into at least partial intelligible text, or into at least partial encrypted text requiring a distinct further or different solution technique.
Function, counting - Tallying complete statistics of its kind on the data fed to it.
Function, selecting - Tallying or indicating "hit" statistics; that is, selecting, counting, or indicating irregularly occurring events in the data fed to it.
Function, operating - Performing combining operations with the data fed to it.
It will be noted that the distribution of subcategories in the listing is markedly biased; for example, that the "counters" are confined to the "analysis" function, that the "solvers" are crowded toward the "specific" end of the applicability scale, that several categories (more, in fact, than otherwise) are completely blank. The fact that this is merely a bias rather than a rigid or necessary correlation is the principal reason why the older and simpler categorizations (which are partly based on approximate groupings in terms of current usage rather than logic) have sometimes been confusing and misleading to persons other than those who are intimate with the field. A third dimension is needed, and has here been introduced.

7. In addition to the anomalies and overlaps within each echelon of categories, there are anomalies and overlaps between echelons, brought about by the exigencies of choice where choice exists. For example, GOLDBUG and COMINT, listed under their "highest" capability as analysis operators, and as such of narrow applicability, have, if regarded as analysis selectors (which they also are), broad applicability.

8. The descriptive matter in the listing has to strike a mean between, on the one hand, the desirability of completely objective attribution in broadest possible terms and, on the other hand, the necessity of keeping the data reasonably down to earth and in terms of the known or more usual cryptanalytic applications. For this reason it must be kept in mind throughout that, in most cases, the given inputs and functions are exemplary rather than limiting. Thus (to pick the first item in the list), although ALCATRAZ is stated to receive "texts" and to make "digraphic and columnar frequency counts", it must be remembered that what it actually does is to make counts of the occurrences of any thirty-six kinds of things taken two at a time, and that "texts" and "digraphic frequency counts" merely happens to be a typical expression of this ability in its usual cryptanalytical applications; many other cryptanalytic applications of this counting capability can be imagined, some of them conceivably useful.

INDEX (by page numbers)

PURPOSE, ANALYSIS			PURPOSE, SOLUTION	
Counters	Selectors	Operators	Counters	Selectors	Operators
		BROAD APPLICABILITY			
		(in order of versatility)			
ALCATRAZ, 4	(GOLDBERG, 5)	Force of clerks, 9	None	WARLOCK II, 14	None
FREAK, 4	(CONNIE, 5)	Conventional IBM complex, 9		AFSAF-12, 14	
Frequency	AFSAF-27, 5	NOMAD, 10		MEDUSA, 15	
Counters, 4	70mm. comparator, 5	ATLAS II, 10			
CADILLAC, 4	TESSIE, 6	ABNER(Baker), 10			
	(AFSAF-12, 6)	EDPM, 11			
	AFSAF-41, 6	ATLAS I, 11			
	DRILLA, 7	TPM, 11			
	ROBIN, 7	AFSAF-1-1, 12			
	IDA, 8	IBM 604, 12			
	COPPERHEAD, 8	Desk calculators, 12			
		O'MALLEY, 13			
		(REMINGTON, 13)			
		NARROW APPLICABILITY			
					(in order of development)
AFSAF-30(PLUTO), 16	None	GOLDBERG, 16	None	None	CHUG, 18
AFSAF-35, 16		CONNIE, 17			PICCOLO, 18
		STORK, 17			DEMON II, 19
		MATHEW, 17			SKATE I, 19
		SIMON, 17			DEMON III, 20
		(IBM &			SKATE II, 20
		JOHN, 17)			SHED, 21
		MIKE, 17			(PRINCESS, 21)
					DUCHESS, 21
					COUNTESS, 21
		SPECIFIC APPLICABILITY			
None	None	None	None	BOMB, 22	None
				AFSAF-18, 22	
				HECATE, 23	
				WARLOCK I, 23	
				REPO, 23	
				AFSAF-33, 23	

Preparation Machines -- pp. 24-25

NEOID APPLICABILITY
PUMPKIN, ANALYSIS
Counters

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
AIGHMAT	1	Cards or two T/T tapes or one T/T tape.	Texts of up to 36 ch.	4ch/sec (cards) or 6ch/sec (tapes) plus printing time.	Less than 5%	Digraphic and columnar frequency count.	Typed page (tabulation), 4 seconds per line.
FREAK	1	One or two T/T (grey) tapes	Texts of up to 32 ch.	5000ch/sec for monographic, 156ch/sec. for digraphic (32ch.), plus printing time.	70%	Monographic or digraphic frequency count.	Typed page (tabulation), or T/T tape, or both. 10ch/sec.
Frequency counters	7	One T/T tape	Text of up to 32 ch.	6ch/sec. plus recording time.	5%	Monographic frequency count.	Counters, manually recorded.
CADILLAC	2	One T/T tape or manual keyboard	Text of up to 32ch.	6ch./sec.	5%	Monographic character or band frequency count and measures of frequency roughness (by characters or bands) and character-to-character or band-to-band repeat rate.	Typed page

BROAD APPLICABILITY (continued)
PURPOSE, ANALYSIS (continued)
Selectors

Machine	No.	Input medium	Input form	Capacity and speed	Problem characteristic time	Function	Output
IDEMIX and OSMIX		See under "Narrow Applicability, Analysis, Operators", and para. 7 of explanatory matter preceding list.					
AFSAF-27 ("elaborated 70-mm. comparator") (still under development)	1	Two 70 mm. punched paper tapes. 16 levels. Provision for third tape run in selected alignment with one of the other two.	Texts of up to 32nk.	Up to 12,500 ch. in each tape. For rare-event-location runs (its principal capability) with full-length tapes, makes repeated passes of tapes at about 18 sec. per pass, thus accomplishing examination of about 1 to 4 message to message lineups per second.	8%	Locates polygraphic coincidences (solid, or broken in selectable specific ways), or selectable specific isomorphs, or coincidence counts in terms of up to 10 specific characters, or any one of several of these or a selectable coinciding combination of them, within width of 17 characters at any or all lineups of pairs of texts. Can also be used for same purposes as 70 mm. comparators.	Stops and prints and makes diagrammatic record of 17-wide condition which causes the stop. For coincidence-count runs, gives printed page tabulation.
70mm. comparator	2	Two 70mm. punched paper tapes, 32 levels.	Texts of up to 32nk.	Holds two texts of 1800 characters each, and tallies through alignments of these at 17 message-to-message line-ups per minute (thus requiring about 3h. 30 min. to complete the 3600 lineups of two full 1800ch. tapes). It is thus about 150-200 times faster than a single human tallier.	10%	Coincidence counts, single or multiple (including broken) up to decagraph, or patterns within width of 10ch, at all lineups of pair of texts.	Printed tape

BROAD APPLICABILITY (continued)
PURPOSE, ANALYSIS (continued)
Selectors (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
[illegible]	2	Two 35mm photo-films. 32 levels.	Texts of up to 32ch.	35,000 characters per film at 120ch. per minute.	Less than 5%	Locates polygraphic (up to decagraphic) coincidences, solid or broken, within widths of 30 characters, at all lineups of all pairs of messages. Can be used to point out high I.C. in the 30-character width.	Stops and points.
AFSAP-12	See under "Broad Applicability, Solution, Selectors"						
AFSAP-41 ("Mod. 2 5202") (still under develop-ment)	1	Two 35mm. photo-films. 80 levels (40 x 2). Program by manual set.	Texts of any alpha-bet, with or with-out weight-ed data, or one text against weighted data of any kind (such as key-gen-erated weight).	45,000 ch. of text in each film, examined up to 600ch. at a time, at net rate of about 17ch./sec. or 3000 message-to-message lineups per second; or up to 90,000 of continuous data (such as key-generated weight) against texts of up to 600ch. at a time, at about 30 sec. per text.	0%	Locates rare message-to-message lineups showing coincidence counts, monographic or poly-graphic, above a selectable high criterion (automatically tapered with overlap) or plants texts in known short key stream by any underlying frequency characteristics translatable into key-generated weights.	Stops and points, with "hit" counts on dials, manually recorded.

~~TOP SECRET~~ ~~SUEDE~~

BROAD APPLICABILITY (continued)
PURPOSE, ANALYSIS (continued)
Selectors (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem characteristic	Function	Output
DELLA (project-ed)	2	Two magnet-ic tapes.	Texts of up to 32mb.	Up to 2,000,000 ch. of text in each tape, divided into messages of not more than 1024 ch. each. Using full tape capacity makes complete Round-Robin run in 72 hours. With 1,000,000 ch. in each tape, makes complete run in 18 hours. Thus, with msgs. averaging 1000 ch. each, examines 15,000 message-to-message lineups per second and with msgs. averaging 500ch. each, examines 30,000 lineups per second (similarly in inverse proportion for other average message lengths). DELLA is thus about 165 times faster than a single ROBIN, a bit less than 50,000 times faster than a 70mm. comparator, and about 8,000,000 times faster than a single human tallier.	Less than 5%	Monographic or polygraphic (through 6j-graphic) coincidences counts or isomorph counts at all lineups of all pairs of a collection of messages (the "Round Robin" operation), recording and placing only those which (by a scoring system involving the weighting of polygraphic coincidences) exceed selectable criteria (automatically tapered with overlap).	Punched tapes.
ROBIN	15	Two T/T (gray) tapes.	Texts of up to 32mb.	About 20,000 ch. of text in each tape (not more than 30,000), divided into not more than 64 messages per tape, of not more than 2048ch. per msg. With msgs. averaging 500ch. each examines 200 message-to-message lineups per second, and with average msg. length 1000ch. examines 100 msg.-to-msg. lineups per second (similarly in inverse proportion for other average msg. lengths). This means that actual ROBIN-hours running time for a complete Round Robin on 1000 msgs. averaging 1000ch. each (and thus requiring one billion lineups (strictly 998,000,000 when the alignments of each msg. with itself are eliminated)) is 2800 hrs. (3000 when handling and changeover is considered). A ROBIN is thus about 300 times faster than one 70mm. comparator, and 50,000 times faster than a single human tallier. (Note 11)	6%	Monographic coincidence counts at all lineups of all pairs of a collection of messages (the "Round Robin" operation), recording and placing only those which (by a scoring system involving additional weight for digraphic coincidences) exceed selectable criterion (automatically tapered with overlap).	Punched cards (during run) giving coincidence counts and alignments.

~~TOP SECRET~~ ~~SUEDE~~

BROAD APPLICABILITY (continued)
PURPOSE, ANALYSIS (continued)
Selectors (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
IDA	1	Two T/T tapes specially prepared in AFE-AFK.	Text repeat patterns as coded by AFF-AFE	8000 to 10,000 characters of original text in each tape at 1 to 8 message-to-message line-ups per second as average message length varies between 1000ch. and 2500ch.	50%	Counts coincidences and non-coincidences of repeat patterns (isomorphs) at any or all lineups of all pairs of all messages, recording only those above a selectable criterion (automatically tapered with overlap) of frequency of either coincidence or non-coincidence.	Punched cards.
COPPERHEAD	2	Two 70mm punched plastic tapes. 5 x 5 levels	Digital or literal (of up to 32ch) terms	25,000 groups in each tape at 300 groups per minute.	10%	Locates split-group, equal-interval coincidences (of up to 5ch. digital groups, 4ch literal groups) within 100-group intervals at all lineups of all pairs of messages.	Stops and prints.

BROAD APPLICABILITY (continued)
PURPOSE, ANALYSIS (continued)
Operators

(Note: This sub-category is listed in approximate order of versatility and scope, without regard to speed)

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
Area of clerks with paper and pencils. (Note 2)	One in each AFSA-02 section	Page copy and oral.	Texts and program (of any alphabet)	Unlimited data at very slow speed. Instantly available contained working primary has low and capriciously variable capacity, but externally stored auxiliary very large and of extremely high availability and great flexibility in use.	Less than zero	Performs, in sequence, all selection, tallying, and arithmetical and logical operations, involving repeated reference to all data, with amounts of data limited only by size of force. Can slide, sort, and collate. (Note 3). Extremely flexible in employment, permitting simultaneous handling of unrelated problems and multiple-parallel handling of large problems.	Page copy or steps and points as appropriate.
Conventional IBM complex with various crypt-analytic appurtenances (Note 4)	Varies with problem.	Punched cards. Program by manual set.	Texts (of up to 47ch) and program.	Unlimited data, at no faster than 100 groups per minute, or sub-multiples thereof, reduced by various operational dead-time factors ascribable to non-automatic nature of sequences of different operations. (Note 15)	Less than zero.	Performs, in sequence, elementary selection, tallying, and arithmetical and logical operations, with very large amounts of data, which require repeated reference to all data. Sequence is automatic only within individual simple operations, and logic is introduced during the processes by human manipulation. Can slide, sort, and collate. (Note 3). Can handle a number of unrelated problems simultaneously, and can handle single large problems by multiple-parallel attack.	Punched cards, which are transcribed to page tabulation at 150 lines (of up to 120ch. each) per minute.

BROAD APPLICABILITY (continued)
PURPOSE, ANALYSIS (continued)
Operators (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem characteristic time	Function	Output
NOMAD (projected) (Note 5) (Note 6)	1	Magnetic tape, loaded into internal memory for operation.	Texts (of any alphabet) and program	300,000,000 characters (approximate practical working limit) of contained data with 6000 ch. of data and program in instantly available working primary and 35,000 of program in auxiliary. Loads at 150ch/sec. Can comb through entire data load at up to 150,000 ch./sec.; time, about one-half hour. (Note 5)	Order of 5%	Same as IBM complex, except that all sequence and logic (once programmed in) are automatic; and cannot handle unrelated problems simultaneously nor utilize multiple-parallel attack.	Magnetic tape, which is transcribed to page tabulations at 150 lines (of up to 120ch. each) per minute.
ATLAS II (projected) (Note 6) (Note 7)	1	T/T tape, partly loaded into internal memory for operation.	Texts (of any alphabet) and program	100,000ch. of contained data, with 6000ch. of data and program in instantly available working primary. Unlimited externally-stored data. Loads at 150ch/sec. (Note 15)	Order of 5%	Performs in automatic sequence elementary selection, tallying, and arithmetical and logical operations with medium-large amounts of data, and involving repeated reference to all data. Can slide, sort, and collate. (Note 3)	Punched cards or T/T tape, transcribed to page at usual rates.
ABNER (still under development) (Note 6) (Note 8) (BAKER, ABNER's relay analogue, has same data but much lower speed)	1 (One more projected)	T/T tape, punched cards, and magnetic tape, partly loaded into internal memory for operation.	Texts (of any alphabet) and program	8000ch. of contained data and program. Unlimited externally-stored data. Loads at 300ch/sec. (Note 15)	Order of 5%	Same as ATLAS II.	Punched cards. T/T tapes. Page. Magnetic tapes.

BROAD APPLICABILITY (continued)
PURPOSE, ANALYSIS (continued)
Operators (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
UNIVAC Electronic Data Processing Machine (tentatively projected)	2	Punched cards and magnetic tapes, partly loaded into internal memory for operation.	Texts (of any alphabet) and program	60,000ch. of contained data, with 12,000ch. of data and program in instantly available working primary. Unlimited externally stored data. Speed not yet known.	Order of 5%	Same as ATLAS II, but with fewer built-in orders usable for crypt. work. Can slide, sort, and collate in only a limited sense (because not well adapted to operating with individual characters or bands).	Punched cards and magnetic tape, transcribed to page at usual rates; also direct printer capable of 150 lines (of up to 120ch. each) per minute.
ATLAS I (Note 6) (Note 8)	1 (One more projected)	T/T tape, loaded into internal memory for operation.	Texts (of any alphabet) and program	64,000 ch. of contained data and program. Loads at 150ch/sec. (Note 15)	10%	Same as ATLAS II and ABNER except cannot readily slide, sort, or collate (Note 3); hence, with data in depth, practically confined to work on fixed alignments.	Page and T/T tapes.
IBM TPM (tentatively projected)	1	Punched cards and magnetic tape, loaded into internal memory for operation.	Texts (of up to 47ch) and programs.	72,000,000 ch. of contained data with 10,000ch. of data and program in quickly available working primary and 48,000 in auxiliary. Speed, slower than NTRAD by factor of not more than 1/60.	Order of 5%	Same as NTRAD, except less flexible for crypt. purposes because limited to modulus 10 for operations.	Magnetic tape.

BROAD APPLICABILITY (continued)
PURPOSE, ANALYSIS (continued)
Operators (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
AFSAF-1-1 ("elaborated CONRAD") (projected)	1	Two T/T (gray) tapes. Program by manual set.	Texts (of up to 64ch) and program.	20,000 to 30,000 characters of text in each tape, at 15 to 10 tape-to-tape lineups per minute, thus (for 25,000ch. tapes) examining about 25 to 5 message-to-message lineups per second as average message length varies from 200ch. to 1000ch.	Ranging from less than 5% to 25% depending on variety of usage.	For any or all message-to-message alignments of one or two series of messages, monographic or polygraphic (up to pentagraphic, and all in one run) coincidence counts, recording only those above selectable criteria (automatically tapered with overlap); or differencing (natural or selectable arbitrary), recording frequencies of differences; or counts of specific selectable isomorphs within width of 32; or combinations of the foregoing differently weighted (for adding and selection by aggregate weight for recording) by selectable weights; or similar selection functions after conversion of each of the streams of data through a selectable single wired-chanel-cycle. Can operate on individual bands of characters.	Typed page (tabulation) 12 lines of 38ch. each per sec., or punched cards.
IBM 604 calculator (Note 9)	2	Punched cards. Program by manual set.	Mathematical data, in digits.	Unlimited data at 100 cards per minute, 60 simple operations per card.	Less than 5%	Perform a variety of arithmetical computations.	Data punched on input cards.
Desk calculators (Note 9)	75	Manual set.	Mathematical data, in digits.	10 adding operations per second.	Negligible	Perform a variety of arithmetical computations.	Counter dial, manually recorded.

BROAD APPLICABILITY (continued)
PURPOSE, ANALYSIS (continued)
Operators (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
O'MALLEY 'UNIVAC is generally similar with differences of no significance in this listing) (Note 9)	1	Punched cards. Program by manual set.	Mathematical data, in digits.	Unlimited data at up to 35 multiplications made and summed per second.	Less than 5%	Specialized arithmetical computation. Gives summations of products of pairs of numbers having up to 4 digits.	Typed page.

BROAD APPLICABILITY (continued)
PURPOSE, SOLUTION
Counters

None

Selectors

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
WARLOCK II (projected)	1	Manual set	Text of up to 32ch.	Up to 80 ch. against unlimited key stream at 100,000 positions per second. Thus, for example, would average about 8 minutes per message	0.3% per million of key-stream length	[redacted]	Stops and points; prints and runs
AFSAF-12	1	One T/T tape, loaded into internal memory for operation, plus data stream (such as cipher key generated stream) generated by another machine.	Text and data (key) in any alphabet.	Up to 500 bands (for 32-alphabet, 100 ch.) of text loaded internally from T/T tape at 8ch/sec., then slid through externally generated data stream of unlimited length at up to 2,000 bands (for 32-alphabet, 400ch.) per second.	Less than 5%	By locating alignment yielding high or low coincidence count (over selectable criterion in each case) places cipher text in any known key stream capable of being used to generate frequency data for fast input to the machine.	Stops and points.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

BROAD APPLICABILITY (continued)
PURPOSE, SOLUTION (continued)
Selectors (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
ANDREW	2	Two 70mm photo-films. 160 levels (80 x 2)	Texts (of up to 80ch.), and weight stream based on known key-stream, or two series of texts.	300,000 to 350,000ch. of key against texts of up to 324 ch. each, at 5000ch. of key per second. Thus averages 35 seconds per message to place a series of them. When used to locate high message-to-message coincidence, examines 8500 message-to-message line-ups per second (disregarding time-out for hits).	4M	Places cipher texts in known short key-stream by monographic frequency characteristics of underlying matter. Can be used to check all line-ups of all pairs of a collection of messages, to locate rare message-to-message lineups having coincidence above selectable high criterion (automatically imposed with overlap). (Note 11)	Stops and points.

Operators

Name

MAJOR APPLICABILITY
PURPOSE, ANALYSIS
Counters

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
AFSAP-30 (PEPTO)	1	Manual set	Stepping pattern and starting position within cycle.	Up to ten 36-point rotors (or more of fewer points) at about 700,000 steps per second.	5%	Duplicates selectable notched-rotor cipher machine cycle, to indicate point in cycle at any desired number of steps, or number of steps to reach any desired point in cycle.	Steps and points
AFSAP-35	1	Manual set	Stepping pattern and starting position within cycle.	Up to fifteen 80-point rotors (or more of fewer points) at no faster than 3½ steps/sec.	Less than 5%	Same as PEPTO except records rotor alignments at selectable intervals in cycle and affords greater flexibility and selectability of motions, including multiple stepping.	Typed page and T/T tape.

Selectors

None

Operators

GOLDBERG (Note 6)	1	One or two T/T tapes loaded into drum for operation. Program by manual set.	Texts (of up to 64ch) and program.	Four tracks of up to 4300 characters each on a revolving drum, loaded from T/T tape in 9 minutes per two tracks, then operating at 30 message-to-message lineups per minute for coincidence count (provided criterion such that no more than about 10% of lineups are counted; slower if more) or 15 per minute for difference count (print-out time included).	Ranging from less than 5% to 30% depending on variety of usage.	For any or all alignments of text to text, monographic and polygraphic (to pentagraphic, and all in one run) coincidence counts, recording only those over selectable criterion (monographic count only can be identified by individual characters or by total count, as desired); or differencing (natural or selectable arbitrary), recording frequencies of differences; or counts of specific selectable isomorphs up to 5 wide. Can perform a variety of other selection tasks. Will sum squares of its own tallies. Can operate on individual bands of characters.	Typed page (tabulation) 4 seconds per line.

~~TOP SECRET~~ [illegible]

NAVY APPLICABILITY (continued)
PURPOSE, ANALYSIS (continued)
Operators (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
CORNIH (Note 6)	1	Two T/T (grey) tapes. Program by manual sub.	Texts (of up to 64ch.) and program.	20,000 to 30,000 characters of text in each tape at 15 to 10 tape-to-tape linkups per minute. (Counter capacity does not permit use of the 20,000-30,000 tape length for a series of different messages)	Same as GOLDBERG	Same as GOLDBERG, except cannot square and sum, and somewhat less flexible in differencing and adding operations.	Typed page (tabulation) 12 lines of 30ch each per sec.
STURK	1	One T/T tape and manual sub.	Text (of up to 32ch.) and crib.	Unlimited text against up to 30ch. crib, at 8ch./sec.	Less than 5%	Differences out additive key at all alignments of short crib with text, and indicates any alignment yielding key having above selectable criterion of frequency roughness, thus placing crib in cipher text where key is known to be additive key of short cycle (15 or less) or rough for any other reason.	Steps and points.
MATHEW and SIMON (IUKE and JOHN similar but limited to digital texts)	6 and 1	Two T/T tapes	Texts (of up to 32ch.) or text and key.	Unlimited at 8ch/sec.	Less than 5%	Adding or differencing (natural or selectable arbitrary) by selectable modulus on characters of aligned pairs. Of cipher text, key, and plain text, will produce any one from the other two.	(MATHEW only) page and T/T tape (CIC-O), or (SIMON only) printed frequency count of result.
RUKY (projected)	1	One T/T tape or keyboard, and manual sub.	Text and key of up to 26 ch.	25 plugged-up characters of text or alphabets of [illegible] against unlimited key or text.	Ranging from less than 5% to 50% depending on variety of usage.	Applies selectable substitution key to text and produces trial decrypts (long stream can be either) for inspection by analyst.	Typed page.

~~SECRET~~

~~TOP SECRET CURRY~~

NARROW APPLICABILITY (Continued)
PURPOSE, SOLUTION

Counters

None

Selectors

None

Operators (in order of development)

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
CEDO (Note 10)	11	Manual set.	Aligned digital (base 10) texts.	Up to 20 unlimited texts at no faster than 10ch. per minute. Up to 5ch. at a time.	Negligible	Differences trial numeral additive key with each character of known alignment, in depth of up to 20, to yield trial "P/I" up to 5 wide for recognition by operator. Thus provides a hand-desk method of performing (for digital texts and additives only) SKATE II's multiple depth operation, with the human operator supplying both "memories".	Manually recorded dials.
PEDCOB	3	Manual set	Digital texts and crib for "narrow" applicability, 30ch. for specific applicability.	Up to 20ch. of crib against two texts of 60ch. each, at 8ch./sec.	Less than 5%	[redacted]	Typed page.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

NATRO" APPLICABILITY (continued)
PURPOSE, SOLUTION (continued)
Operators (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
DEMON II (Note 10)	2	Two T/T tapes. Program by manual set.	Texts (of up to 30ch.) and program.	Unlimited texts at theoretical limiting speed of about 5ch./sec. (tape feed rate for no hits) and practical speed of ½ to 3ch. per second depending on degree of success (the more successful the run, the slower it goes.)	Ranging from less than 5% to 20% depending on variety of usage.	[redacted]	Punched cards containing all successful key portions and resultant "P/L" texts, plus original cipher groups involved.
SKATE I (Note 10)	1	Punched cards. Program by manual set.	Texts (of up to 32ch.) and program.	Same as DEMON II	Ranging from less than 5% to 15% depending on variety of usage.	Same as DEMON II except has 192 5ch. cribs in test memory and 2000 in recognition memory.	Same as DEMON II.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

[redacted]

MACHINE APPLICABILITY (continued)
PURPOSE, SOLUTION (continued)
Operators (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
DEMON III (Note 18)	1 (one more projection)	Two T/T tapes loaded into drum for operation. Program by manual set.	Texts (of up to 32ch.) and program.	Unlimited at essentially same speeds as DEMON II. (Although drum loads at 100ch./sec., and internal operations are extremely rapid, the limiting factor is the output punch, which holds DEMON III's rate of production to same order as that of DEMON II.) Has drum storage of 16,384 polygraphs (up to pentagraph) usable for "text memory" plus working data from fed-in texts.	Same as SKATE I		Same as DEMON II
SKATE II (Note 20)	1	Punched cards. Program by manual set.	Texts (of up to 32ch.) and program.	Unlimited texts. Speed same as SKATE I for same problems, slower for others (by varying amounts, depending on depth of data and intervals used in examination). Theoretical limit of speed on problem of text placement in key stream about 9ch./sec.	Same as SKATE I		Same as DEMON II

MARGIN APPLICABILITY (continued)
PURPOSE, SOLUTION (continued)
Operators (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem characteristic time	Function	Output
WIND (projected) (Note 10) (Note 12)	2	Punched cards loaded into drum for operation. Program by manual set.	Texts (of up to 32ch.) and program.	Unlimited texts at double SKATE II's theoretical limiting speed. Practical speed for SKATE II problems about 1½ times SKATE II's speed except can do text placement in key stream at speed of order of 150ch./sec. Has drum storage of 48,000 characters, usable in groups of any length as "text memory" plus working data.	Probably same as SKATE II.	Same as SKATE II plus (1) can handle depths greater than 10, (2) can handle anomalies in alignment of depths greater than two, and (3) more flexible in unit lengths of crib handled and in text placement in key stream, and able to handle longer stretches of key stream. (Note 11)	Same as SKATE II
Machines of PRINCESS program (1 DUCHESS, 2 COUNTESSES) (projected) (Note 10)	3	Two T/T (grey) tapes or punched cards or both.	Text (of up to 32ch. for one COUNTESS, 10ch. (digital) for other machines)	Unlimited key, and unlimited text examined (in the COUNTESSES) 1024ch. at a time, or (in DUCHESS) 300ch. at a time. 60ch./sec. (one COUNTESS) or 300ch./sec.	Less than 5%	Places single cipher texts in known additive key stream by frequency roughness, in 1024ch. or 300ch. width, of underlying in-phase (on-beat) quadri- or penta-graphs (for example, code groups). As two special cases of this, can detect unenciphered code (key all zero) and can do some placement when underlying matter is plain language.	Stops and prints, and resumes.

[redacted]
~~TOP SECRET CRUM~~

SPECIFIC APPLICABILITY
PURPOSE, ANALYSIS
Counters

None

Selectors

None

Operators

None

PURPOSE, SOLUTION
Counters

None

Selectors

Machine	No.	Input medium	Input form	Capacity and speed	Problem characteristic time	Function	Output
BOMBE	2 (Note 13)	Manual set.	Brief text and crib; 26ch.	Up to 16ch. each of text and crib, at 50 seconds per wheel order for complete 3-wheel cycle. Thus, assuming 100% success in choice and placement of cribs, places messages at rate of about 4 to 6 per hour if there is no choice of wheels; rate lower as additional wheel possibilities are added, or as cryptanalysts drop below perfection in cribbing.	75%	To place individual message in Enigma cipher machine cycle by checking rigidly placed crib through entire cycle.	Stops, points, and prints.
AFSAF-18 (super-[illegible]cher)	1	Manual set	Brief text and crib; 26ch.	Up to 25ch. each of text and crib at about 7 cycle positions per sec. (about 36 min. per wheel order for complete 3-wheel cycle). Thus places messages at about one-tenth the speed of BOMBE.	Less than 5%	Same as BOMBE.	Stops and points.

[redacted]

SPECIFIC APPLICABILITY (continued)
PURPOSE, SOUGHT (continued)
Selectors (continued)

Machine	No.	Input medium	Input form	Capacity and speed	Problem changeover time	Function	Output
SPEAKE	2	One T/T tape and manual set.	Text and brief crib; 26ch.	Unlimited text and up to 12ch. crib. 2½ seconds for complete cycle at each alignment. Speed of dragging thru 24ch. per minute.	Less than 5%		Stops and points.
WARLOCK I	1	Manual set.	Text of 26ch.	Up to 75ch. of text run through [redacted] in 7 3/4 hours. (Thus averaging 3-4 hrs. to place one message. If one constant substitution element of the machine setup is known, as it sometimes is, the average time per message placement is reduced to about 9 minutes.)	30%		Stops and points.
HYPO (Note 14)	2	Two 35mm. photo-film. 169 lev-els, 4 lines per frame.	Text (of 26ch.) and key.	Single message texts of any length. One message per hour in 4-rotor machine, two per hour in 3-rotor machine.	8%		Stops and points.
AFSAF-33	1	Special punched cards and one T/T tape.	Crib and tentay 25ch.	Drags a 20ch. crib through un-limited texts (trying full machine cycle at each align-ment) at 6ch./sec.	10%	To place individual messages in B-211 cipher machine cycle by dragging brief crib through texts, testing entire cycle at each alignment.	Stops and points.

PL 86-36/50 USC 3605
EO 3.3(h)(2)

Operators

None

PREPARATION

Machine	No.	Input medium	Input form	Speed	Problem changeover time	Function
031 punch	40	Hand	Any, of up to 47ch.	Hand	Less than 5%	Produces punched cards.
4 punch	55	Hand	Any, of up to 47ch.	Hand	" " "	" " "
026 punch	9	Hand	Any, of up to 47ch.	Hand	" " "	Produces interpreted punched cards.
063 card to tape	2	Punched cards	Any, of up to 47ch.	8ch/sec	" " "	Produces T/T tape.
043 tape to card	3	T/T tape	Any, of up to 47ch.	8ch/sec	" " "	Produces punched cards.
CXCO ("Letter-writer")	39	Hand or T/T tape	Any, of up to 64ch.	Hand or 8ch/sec.	" " "	Produces T/T tape and page copy in any form for machine analysis.
Mod. 2	2	Two T/T tapes	Any, of up to 64ch.	8ch/sec.	" " "	Produces binary-coded tape or modulus 2 differences, in T/T tape form.
70mm comparator punch	2	One T/T tape	Text, of up to 32ch.	8ch/sec.	" " "	Produces 70mm. punched paper tape for use in 70mm. comparator.
AXE-AYE	2	One T/T tape	Text, of up to 64ch.	2ch/sec.	" " "	Makes T/T tape in which are coded repeat patterns in text within span of twelve characters, for use in IDA or IBILIA. Uses three frames of pattern data per frame of original text tape.
COPPER HEAD punch	2	1 T/T tape or punched cards.	Digital or literal (of up to 32ch.) text, in up to 5ch. code groups	8ch/sec or 100 cards per min.	" " "	Produces 70mm. punched plastic tape for use in COPPERHEAD.

[redacted]

PREPARATION (continued)

Machine	No.	Input medium	Input form	Speed	Problem changeover time	Function
RHETA camera	1	1 T/T tape or punched cards	Text, of up to 32ch.	8ch/sec or 100 cards/min. plus darkroom	20%	Produces 35mm. film for use in THESEUS.
RPO camera	1	1 T/T tape or punched cards	Text (of up to 26ch) and key (made in separate runs)	8ch/sec. or 100 cards/min. plus darkroom.	20%	Produces 35mm. film for use in RUFUS.
AMBER camera	2	T/T tapes or punched cards or both	Texts (of up to 4ich.) or text and key-generated frequency weights. (made in separate runs)	300ch./min. (tape) or 100 cards/min plus darkroom	20%	Produces 70mm. photo-film for use in AMBER.
AFSAF-40 ("5202 camera") (projected)	1	One or two T/T tapes	Texts (of up to 4ich.) or text and key-generated weights.	8ch./sec.	20%	Produces 35mm. photo-film for use in AFSAF-41 ("Mod. 2 5202")
AMBER-DELIA tape maker (projected)	1	Punched cards or T/T (grey) tape	Text (of up to 4ich.) and program	128ch/sec.	Less than 5%	Produces magnetic tape for AMBER and DELIA
NOMAD tape maker (projected)	1	Punched cards or T/T (grey) tape	Text (of up to 4ich.) and program.	320ch/sec 1000ch/sec.	Less than 5%	Produces magnetic tape for NOMAD

Notes

Note 1 – Under this limitation the following are omitted from the list: OPHIR, MAINIE, M-8, SATIR (and other Hagelin analogue devices), B-211, STONEHOE, and AFSAF-13.

Note 2 – The most costly machine in the list.

Note 3 – Definitions. Sliding – Moving two streams of data relative to each other to permit their being operated on or compared at every possible desired alignment of one with the other.
Sorting – Rearranging the order in which the data of a stream of data are available for use.
Collating – Shuffling two streams of data into one in a desired order. As a special case, shuffling a small body of new data into an already ordered stream of old data.

Note 4 – There are various devices having separate names (such as MISTRESS) which are essentially appurtenances of the conventional complex rather than independent machines, and which are therefore not listed separately. In addition to its usefulness as an operator, IBM is outstandingly useful as a counter of polygraphs of trigraph and higher and as a selector of relatively frequent occurrences. Useful for "solution" as well as "analysis". Particularly applicable where long and complex listings and arrangements of written data are wanted in connection with the needs of analysis.

Note 5 – As now conceived, NOMAD will be comparable to the entire IBM complex with a speed advantage over IBM of the order of 100 to one, but without the flexibility in employment afforded by the discontinuity of IBM processes and the safety inherent in IBM's essential multiplicity, replaceability, and dispersion.

Note 6 – Outstandingly useful as selectors, and limited in use as such only by the demands on them for use as operators. Except for GOLDBUG and COMET, have wide applicability to "solution" as well as "analysis".

Note 7 – ATLAS II is essentially a more capacitous ATLAS I with provision for keeping the active data more available, so that ready sliding ability is added. This enables it to do all that ATLAS I can do more readily, and in addition to add to the processes the sliding features.

Note 8 – ATLAS I and ABNER are unsurpassed among machines now available in operations with multiple depths of data (with ATLAS I, for lack of sliding ability, alignment in depth should be supplied) where weighting is involved, and where there are complex interrelationships involving choices in the course of and as part of the automatic operation. The "bootstrap" operation is a noteworthy case in point.

Note 9 – The IBM 604, the desk calculators, O'MALLEY, and MONROE may be regarded as constituting a special category by function, that of "calculators". As distinguished from all of the other machines listed, which receive and perform various functions with text and key, they are purely mathematical; receiving, using, and producing nothing but mathematical information.

Notes (continued)

Note 10 – These narrow solution operators are all of "narrow" applicability only in that they are applicable solely to additive systems and not to wired-wheel systems. Additive systems constitute a broad class of cryptography, and these operators are applicable to a large number and variety of individual systems within that class. The term "narrow" is thus used relatively merely to distinguish these machines from those which can be used against both wired-wheel and additive systems.

Note 11 – For message placement in a key-stream, AMBER is applicable to all problems, including those where there is no phase or "beat" in the placement (as with underlying plain text which can start at any key position), while SKATE II and SIXD are particularly applicable to problems where there is phase or beat (as with underlying code groups, particularly where there are likely to be level starts of messages at known intervals in the key stream). It will be noted, too, that, for a "Round Robin" with short messages, AMBER is of the order of 25 times as fast as a single ROBIN, and thus might have the edge on the entire 15 machine ROBIN battery; but it must not be forgotten in this connection that there is film preparation time to consider in addition, and that AMBER, unlike ROBIN, merely locates high coincidences, without giving the statistics on them, and is, by the nature of its operation, not particularly useful for locating more than the few very highest.

Note 12 – Useful as an "analysis" operator also, and in this employment is comparable to GOLDBERG.

Note 13 – There are a number of others in storage.

Note 14 – The conditions expressed under "Function" practically limit MEPO to use on Enigma and Enigma-like systems. It is functionally capable of much broader application, but as the Enigma principle is departed from MEPO rapidly yields superiority to AMBER and even to some of the analytical selectors, so that its broader capability is not practically useful, and, despite an inherent versatility which the other specific solution selectors cannot match, has to be listed among them.

Note 15 – Because of the wide variety of their applications, statements of the speed capabilities of these analytic operators are necessarily specific and multiple, and all simplifications are likely to be over-simplifications. Furthermore, comparisons are likely to be artificial, since operations within the capabilities of other machines would hardly be assigned to these, and operations particularly suited to the capabilities of these would usually be impossible for the others. Thus, although this expensive equipment can outperform MEGATF and ALCATRAZ, it would not be sensible or economical to use it for MEGATF's and ALCATRAZ's work, or to waste time devising ways in which this could be done, as long as the two cheaper and less versatile equipments are there to do it. NOMAD's performance is shown in terms of two data-sorting operations only, because sorting of large amounts of data will be NOMAD's outstanding new contribution to the capabilities of the "computers"; actually, in addition, NOMAD will probably be at least comparable to ATLAS II and AMBER for all of the other operations listed. (Tabulation on next page.)

Notes (continued)
(Note 15, continued)

PROBLEM	MORE SPECIALIZED MACHINES	CONVENTIONAL IBM	ATLAS I	ATLAS II	ARDEE
1. 160 (26ch.) mags., each of 1000ch., make columnar frequency count on best of 17 (or up to 26) and print totals.	ALCATRAZ, tape 7 hrs., card 11.5 hrs.	26 hrs.	13.3 hrs.	44 min., assuming high speed punch available.	25 min.
2. [redacted]	MEGATE, 15 min.	Impractical	3 min.	1 min.	0.25 min.
3. Same, slide unknown.	MEGATE, 15 min.	Impractical	27 min.	2 min.	6.5 min.
4. Slide 2000ch. against another 2000ch., all lineups; differencing, and recording lineups yielding differences meeting a selectable criterion of frequency roughness.	GOLDBERG, 30 min.	Impractical	1350 min.	5.5 min.	11.5 min.
5. Same, except 200 against 2000.	GOLDBERG, 30 min.	Impractical	135 min.	4 min.	3 min.
6. Round Robin for monographic coincidences above selectable criterion, 1000 texts of average 1000ch. each.	DELLA, 18 hrs. ROBIN, 3000 ROBIN-hours.	Impractical	Impractical	2170 hrs.	1190 hrs.
7. Slide one text of 1000ch. against 1000 texts of average 1000ch., recording coincidences above selectable criterion.	DELLA, 5 min. ROBIN, 5½ ROBIN-hours.	Impractical	380 hrs.	32 hrs.	2.5 hrs.

Notes (continued)
(Note 15, continued)

	PROBLEM	NSA SPECIALIZED MACHINES	CONVENTIONAL IBM	ATLAS I	ATLAS II	ADREP
8.	[redacted]	O'MALLEY, 90 min.	25 hrs.	22 min.	10 min.	7 min.
9.	Diversion of 30 x 30 circulant matrix.	O'MALLEY, 60 min.	5-16 hrs.	3 min.	3 min.	2 min.
10.	Try 5000 pentagraphic cribs in 100 pairs of depth-of-two texts, averaging 200 groups each. Recognize on 1000 pentagraphic cribs. (One 400 group hits per text.)	DEMON III, 120 hrs.	Impractical	20,000 hrs.	2400 hrs.	1946 hrs.
11.	Try to place 50,000 15-digit stretches of text against (level start) 100,000 15-digit stretches of key by recognition of 400 weighted pentagraphic cribs. (Average two placements per text.)	DEMON III, 210 hrs.	Impractical	500,000 hrs.	100,000 hrs.	20,000 hrs.
12.	Try to place 200 fifty-group texts in 1000 fifty-group stretches of key (sliding) by recognition of 1000 pentagraphic cribs.	SIED, 1.25 hrs.	Impractical	2000 hrs.	140 hrs.	2330 hrs.
13.	Solve key to satisfy depth of 11 texts averaging 100 groups each, using 500 cribs for test and 1000 for recognition.	SIED, 1 hr.	Impractical	3,800 hrs.	190 hrs.	2859 hrs.

Notes (continued)
(Note 15, continued)

	PROBLEM	MORE SPECIALIZED MACHINES	CONVENTIONAL IBM	ATLAS I	ATLAS II	OTHER
14.		WARLOCK I, 20 min.	Impractical	60,000 hrs.	300 hrs.	1067 hrs.
15.		WARLOCK I, 1.5 hrs.	Impractical	60,000 hrs.	300 hrs.	1067 hrs.
16.		HYPO, 20 min.	Impractical	20 min.	4 min.	1 min.
17.		HYPO, 1 hr.	Impractical	40 min.	7 min.	2 min.
18.	BOOTSTRAPS -- test and record roughness of key derived from assumptions of plain text against texts in depth.	NONE (Force of clerks, 1200 man-hours)	37 hrs.	20 min.	15 min.	———
19.	IDIOMORPH FINDING--given 50,000 ch. of text, to find, code, sort, and record all 16-long patterns starting at all possible positions.	NONE (AYE-AYE could find and code, but not sort and list, only 13-wide, in 7 hrs.)	65 hrs.	Impractical	1 hr.	3 hrs.

Notes (continued)
(Note 15, continued)

	PROBLEM	MOST SPECIALIZED MACHINES	CONVENTIONAL IBM	ATLAS I	ATLAS II	ABNFR	NOMAD
20.	[redacted]	NONE	15 hrs.	15 min.	11 min.	———	———
21.	Sorting operation equivalent to sorting 1,000,000 cards on 1 column of alphabetic data.	NONE	60 sorter-hours	Impossible	26 hrs.	80 hrs.	5 hrs.
22.	Sorting operation equivalent to sorting 1,000,000 cards on all 80 columns of alphabetic data.	NONE	4800 sorter-hours.	Impossible	350 hrs.	380 hrs.	5 hrs.