Description of document:	A Study of the Mathematical Effort in the National Security Agency (NSA) prepared by The Mathematics Panel, NSA Scientific Advisory Board, 31 May 1957
Requested date:	24-December-2012
Release date:	06-January-2020
Posted date:	03-February-2020
Source of document:	FOIA Request National Security Agency Attn: FOIA/PA Office 9800 Savage Road, Suite 6932 Ft. George G. Meade, MD 20755-6932 Fax: 443-479-3612 Online FOIA Request Form

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 69540A
6 January 2020

This is the final response to your Freedom of Information Act (FOIA) request of 24 December 2012 for "A Study of the Mathematical Effort in the National Security Agency, dated 27 May 1957." Your request has been processed under the FOIA and the document you requested is enclosed. Certain information, however, has been deleted from the enclosures.

Some of the withheld information has been found to be currently and properly classified in accordance with Executive Order 13526. The information meets the criteria for classification as set forth in Subparagraph (c) of Section 1.4 and remains classified TOP SECRET and SECRET as provided in Section 1.2 of Executive Order 13526. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage and/or serious damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)). The information is exempt from automatic declassification in accordance with Section 3.3(b)(1)(3) of E.O. 13526.

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in this document. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

Since these deletions may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures.

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving your appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

  NSA/CSS FOIA/PA Appeal Authority (P132)
  National Security Agency
  9800 Savage Road STE 6932
  Fort George G. Meade, MD 20755-6932

  The facsimile number is (443)479-3612.
  The appropriate email address to submit an appeal is FOIARSC@nsa.gov.
- Request must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Rd - OGIS
College Park, MD 20740
ogis@nara.gov
(877)684-6448
(202)741-5770
Fax (202)741-5769

Sincerely,

for Shawn C Lucas

JOHN R. CHAPMAN
Chief, FOIA/PA Office
NSA Initial Denial Authority

Encls:
a/s

~~SECRET~~

~~SECRET~~

A STUDY OF

MATHEMATICAL EFFORT

IN THE

NATIONAL SECURITY AGENCY

Prepared by

The Mathematics Panel

NSA Scientific Advisory Board

31 May 1957

~~SECRET~~

~~SECRET~~

~~SECRET~~

A STUDY OF

MATHEMATICAL EFFORT

IN THE

NATIONAL SECURITY AGENCY

Prepared by

The Mathematics Panel

NSA Scientific Advisory Board

31 May 1957

~~SECRET~~

~~SECRET~~

TABLE OF CONTENTS

INTRODUCTION

There is a wide variety of Agency problems which have been attacked by mathematical methods, and many of them have been solved by these methods. The spectacular success attained in solving certain cryptanalytic problems in the past may have created the false impression that the mathematical approach is the only approach to cryptanalytic problems and that it is useful to the Agency only when applied to such problems.

Since the end of World War II, many new cryptologic problems have arisen and many more may be expected in the future. It is characteristic of these problems that they are becoming more and more difficult and that this trend will undoubtedly continue. New cryptologic technology has generated a large number of problems which are essentially mathematical or can be formulated in mathematical terms.

If the Agency is to continue to be effective in dealing with an increasing number of progressively more difficult problems, it will necessarily have to increase the effectiveness of the use of mathematics and machine aids in solving such problems. It is therefore pertinent to assess the present mathematical effort and to inquire how its effectiveness might be increased. As a result of questions of this nature, the Mathematics Panel of NSASAB has made a study of the Agency's mathematical effort, both within and outside the Agency.

The Panel's basic conclusions can be summarized as follows: The Agency has many extremely difficult and challenging mathematical problems, strong mathematicians (but not enough of them), and very able consultants. The proportion of the Agency's mathematical skills applied to activities promising immediate or short term results has been too great when compared with that devoted to

long-range problems. Barriers of security and organizational structure have hampered communications and mutual support among mathematicians.

Important applications, both to present unsolved problems, and to the problems of the future, may be expected from increased external mathematical support, from increases in mathematical personnel and improvements in mathematical training, and from reorganization of the mathematical effort.

The order of presentation of the results of the study is as follows: Findings and Recommendations, Discussion, Appendices.

SECRET

FINDINGS ON
RESEARCH AND TRAINING

FINDING RT-a. There exists no large body of theory or technique, mathematical or statistical, recognizable as being applicable to the Agency's critical cryptanalytic problems, which has not already been exploited.

More than 35 leading U. S. mathematicians and statisticians have served, or continue to serve, the Agency as consultants. Their fields of mathematical interest are extensive and diverse and their knowledge of the world's published mathematics is great. Many of them have been concerned with the Agency's most crucial problems, and have combed all known and partly known regions of mathematics for aid in their solution. (See Discussion A, Appendices III and IV.)

FINDING RT-b. In those areas of mathematical and statistical theory and technique which have proved most useful to the Agency's cryptanalytic effort, the total amount of U. S. mathematical knowledge outside the Agency has been small.

These areas have not recently been applied to other fields, and have not, until very recently, received intensive study by mathematicians interested in them without regard to applications. Problems in these areas are difficult and recent interest in them has been stimulated largely on the part of mathematicians who have become familiar with the Agency's mathematical problems. Project SCAMP has played a particularly useful role in stimulating interest in these areas of mathematical theory. (See Discussions A, C and Appendix IV.)

FINDING RT-c. The Agency has not been able to carry out enough long-range research directed toward the identification and development of special fields of mathematics and statistics of particular interest to the Agency.

This has been due partly to a reluctance on the part of some Agency personnel to encourage such activity, and partly to the unusual susceptibility of a cryptanalytic organization to the extreme pressures of immediate problems. Such fields as abstract theory of rotor maze information, Bayesian statistics, theory of stochastic search, and theory of special iterative convergence schemes might have been, and still should be, further developed as basic mathematical research with a good expectation of eventual dividends in cryptology. (See Discussion A.)

FINDING RT-d. Despite increasing demands, the number of Agency personnel with formal mathematical training has decreased over the period from World War II, through the Korean Campaign to the present. Nevertheless, the growing complexity of cryptographic systems and the increasing power of cryptanalytic techniques will continue to increase the demand for more and deeper mathematics and statistics in cryptology and cryptanalysis.

While personnel with less formal mathematical training are making increased use of quantitative techniques and showing good understanding of them, the gap between the mathematical needs of the Agency and its mathematical resources is steadily growing. (See Discussion A.)

FINDING RT-e. The Agency suffers from a lack of an adequate program of training courses and seminars in mathematics and statistics.

Some effort has been made at the Agency to provide mathematical training and to conduct seminars, but the effort has been sporadic.

While recruitment of more mathematicians seems imperative, many more able persons, analytically trained in other disciplines, are available in the Agency or by recruitment. Able persons in mathematics with partial training are also available. (See Discussion B.)

RECOMMENDATIONS ON RESEARCH AND TRAINING

RECOMMENDATION RT-1. A special group should be set up to do long-range basic mathematical research in areas relevant to cryptology.

The Agency has a deep and pressing need for research of a more basic and long-range character than any at present in progress. In particular, attention must be given today to:

(a) understanding and organizing the essentials and common elements of present cryptologic, especially cryptanalytic, techniques (leading toward a unified science of mathematical cryptology),

(b) the nature and feasibility of attacks which will be required by systems likely to be used in the future,

(c) precise formulation of parts of outstanding unsolved problems which are sufficiently small to offer hope of successful attack. (See Discussion A.)

RECOMMENDATION RT-2. This long-range research group should not be located in the Agency, either physically or organizationally.

The great advantages of close contact with the Agency and its problems are clear. Unfortunately, careful study and consideration makes it equally clear that the degree of insulation from day-to-day pressures required to encourage long-range basic research cannot be provided at the Agency in the foreseeable future. Such a group might be operated under an outside contract with enough contact with the Agency's long-range problems to keep the group effectively stimulated and to preserve proper direction of effort. Under such an independent arrangement every effort should be made to provide for the utilization, on certain classes of problems, of mathematicians of very high ability who are not clearable under the Agency's rigid standards. (See Discussion A.)

RECOMMENDATION RT-3. Project SCAMP should be continued and expanded.

Expansion might include not only further increase in size within its present scope, but also coverage of special topics as are mentioned in (a) under RECOMMENDATION RT-5 and a combination of SCAMP-like activities with the long-range research group discussed in RECOMMENDATIONS RT-1 and RT-2. (See Discussion C and Appendix IV.)

RECOMMENDATION RT-4. The staff of the Office of Mathematical Research (MATH) should devote about half of its time to immediate or to short-range problems and half to long-range problems.

MATH is not putting enough effort on long-range research. It must constantly strive to prevent the pressure of immediate practical problems from blocking its research efforts on the longer-range problems. It will be unable to protect and augment its long-range research program until its staff for long-range problems is increased so there is something like a 50-50 distribution of effort between immediate and long-range problems. (See Discussion A.)

RECOMMENDATION RT-5. The Agency should look further, both to special outside groups and to the mathematical community as a whole, for support.

In particular:

(a) SCAMP-like activity should be expanded, to the extent that leadership can be found, toward topics of special interest such as Bayesian statistics, the theory of search (including search guided by scoring techniques), partial permutations, and the development of a theory of iterative decompositions (e.g., rectangle convergence). Such activity might usefully be conducted, even if leadership and participants are not fully cleared, when this part of the activity can be located away from SCAMP.

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

(b) Every effort should be made within the Agency to relate results of SCAMP and other outside researchers to Agency problems.

(c) The spread of knowledge of, and research in, special topics such as those listed in (a) should be encouraged, perhaps [redacted] This may be done through projects, conferences and summer institutes, and possibly by the statement and publication, in unclassified form, of challenging problems in such areas. (See Discussion C and Appendix IV.)

RECOMMENDATION RT-6. The Agency should conduct regular, highly classified meetings for the presentation of original mathematical papers by members of its staff.

Specifically, the Agency should arrange for suitable groups of able mathematicians from among its consultants, recruiting further as may be desirable, to serve as mathematically critical audiences for the presentation of mathematical papers related to cryptology and other Agency functions, by members of its staff. These meetings, which might be held once or twice a year, would serve a function which would otherwise require an American Cryptologic Society. Such a program should be entered upon with the understanding that it is not intended to assist in day-to-day problems, or even to enlarge the scope or improve the content of particular papers presented, but rather as a means of improving future research at the Agency by developing an increased sense of mathematical quality and a deeper mathematical professionalism among the full-time staff of the Agency. Such meetings should also further arouse the interest of the audience in types of mathematical problems of interest to the Agency. (See Discussion B.)

RECOMMENDATION RT-7. Seminars among Agency staff (and consultants) for the discussion of mathematical and cryptologic results and techniques should be established and actively encouraged.

The principal purposes should be the dissemination of information on cryptologic techniques within the Agency, the

development of esprit de corps among all Agency mathematicians, and the introduction of some of the more recent mathematical concepts and ideas to Agency mathematicians. For the first purpose, speakers would come from within the Agency, while for the last purpose external speakers, some of whom may have worked on SCAMP, are needed. Both types are needed for the middle purpose, and the use of both should be encouraged. Seminars should have regular meeting times, at least once a month, and should be regularly attended.

Attendance at seminars should be given sufficient priority to allow relatively regular attendance in the face of other pressures. Recognition of the importance of attending such seminars will be required at high administrative levels. (See Discussion B.)

RECOMMENDATION RT-8. The Agency should redouble its efforts at instituting a substantial and growing training program in mathematics.

Such a training program should eventually include work at all levels, make as much use as possible of assistance from educational institutions, and hold to a high standard. Its graduate level courses should carry graduate credit to the greatest extent possible. Such a program will require leadership from MATH, cooperation from mathematicians throughout the Agency, support from the Director, and, at the graduate level, affiliation with one or more strong educational institutions. (See Discussion B.)

RECOMMENDATION RT-9. Serious attention should be given to the preparation of texts and portions of texts on cryptology and to the revision of existing material.

There is a serious lack of textbook material on cryptology. This makes it difficult for the newcomer to acquire a background and working knowledge in the field in a reasonable length of time.

Subjects to be covered should include quantitative cryptology, applied and abstract, and modern statistical practice in cryptology.

SECRET

Consideration should be given to preparing some of the material for non-mathematicians (or the less mathematically sophisticated) as well as for mathematicians.

Summer (or longer period) employment of selected consultants for the specific purpose of preparing such texts or portions thereof should be encouraged. Serious efforts should be made to keep such material reasonably up-to-date. (See Discussion B.)

~~SECRET~~

FINDINGS ON
PERSONNEL AND RECRUITMENT

FINDING PR-a. The mathematical and statistical personnel of the Agency are technically strong, able and sophisticated.

As an organization dealing with applications of mathematics, the Agency is outstanding. It makes excellent use of available mathematical techniques, and very substantial use of available statistical techniques. However, several organizational improvements might be made to utilize better the talents available both inside and outside the Agency. (See Discussion A.)

FINGING PR-b. The level of mathematical ability among the Agency's full time staff does not reach, and probably could not be raised to that of "world-renowned" mathematicians.

It is most improbable that such people can be recruited during peacetime on a full-time basis — either by the methods already used by the Agency or by any others we have been able to envisage. However, some expansion of the number of people at the highest level now reached in the Agency, and possibly some slight increase in that level itself, seems possible under conditions envisaged in RECOMMENDATIONS RT-1 and RT-2. Utilization of "world-renowned" mathematicians on the Agency's long-range mathematical problems during peacetime can be accomplished, if at all, only by such methods as presented in RECOMMENDATIONS RT-1, RT-3, RT-5, RT-6.
(See Discussion A.)

FINDING PR-c. Despite the existence of a vigorous and well directed recruiting program by PERSONNEL, the needs of the Agency for mathematicians exceed the available supply.

This situation is aggravated by intense competition both in the fields of pure mathematics and of logical design of machines

and programming. The competition is increasing and must be countered with even greater recruiting effort on the part of the Agency. Successful recruitment of personnel at the Ph. D. level can be accomplished only through the initiative of MATH. Recruiting effort is not being sustained at a sufficiently high level to compete effectively for the available talent.

FINDING PR-d. The greatest single potential source of fully-trained mathematicians which might be made available to the Agency consists of mathematics Ph. D.'s who are performing their military service.

Not only would such mathematicians provide badly needed abilities during their required service, but recent experience suggests that a substantial fraction would be sufficiently stimulated by contact with the Agency's problems to remain at the Agency in a civilian capacity. Similar considerations also apply in large part to mathematicians whose training has not yet reached the Ph. D. level.

FINDING PR-e. Certain security procedures are a source of serious difficulty in recruitment. In particular, the use of the polygraph is repugnant to many scientifically trained persons, including mathematicians, who would make desirable Agency employees.

The recruiting problem in the case of mathematicians is serious enough to warrant the expense and delay associated with a full field investigation of persons who do not wish to submit to the polygraph procedure.

SECRET

RECOMMENDATIONS ON

PERSONNEL AND RECRUITMENT

RECOMMENDATION PR-1. The Agency should more fully exploit its associated (outside) talent as an aid in recruiting.

This would require the placing of approved NSA information already available in PERSONNEL in the hands of Board members, Panel members, and Consultants, for use in recruiting among students and possibly colleagues. Action already taken in providing PERSONNEL with the names of NSA associated mathematicians and suggesting that recruiters visit such persons when recruiting at their institutions is a step in a desirable direction.

RECOMMENDATION PR-2. The Agency should prepare, for use in recruiting, an account, in as mathematically interesting a form as possible, of mathematical problems related to its work.

It is most difficult to interest able young mathematicians in working on mathematical problems on whose nature, challenge, and interest they have no information. An unclassified brochure indicating the nature of some of the Agency's mathematical problems could greatly reduce this difficulty. Material for the brochure should be sought both in the open literature (e.g., papers from the Agency and from SCAMP, [redacted] and in documents which could appropriately be declassified. In such an account, a description of the duration and extent of John von Neumann's relations with the Agency should be considered. (b)(3)-P.L. 86-36

RECOMMENDATION PR-3. The Agency should take more initiative in using its consultants.

Outside consultants must be urgently and individually invited if, in face of other demands on their time, they are to

SECRET

come to NSA for as much time as they can give, and as the problems warrant. The NSA staff must use active persuasion, and must realize that it is unlikely that mathematical research workers will respond to general invitations to spend relatively long periods of time at the Agency. (See Discussion C.)

RECOMMENDATION PR-4. Recruiting of mathematical personnel, especially at the M. A. and Ph. D. levels, should be done by fully qualified mathematicians or mathematically knowledgeable technical people.

This procedure has been occasionally followed by the Agency, with gratifying results. It should be conducted vigorously as part of a planned and continuing program. At the M. A. and Ph. D. levels, it should be done under the leadership of MATH.

RECOMMENDATION PR-5. A determined effort should be made to establish procedures whereby mathematicians and statisticians performing military service will be assigned to work at the Agency upon its request.

The existing procedures are entirely inadequate. Far too few of the total number of requests for such assignments have resulted in actual assignment to the Agency. This is particularly noticeable in the case of mathematicians and statisticians. It is of the utmost importance that this largest single potential source of trained mathematicians and statisticians be fully exploited by the Agency. NSA should take the initiative to insure that in the assignment of draftees the Agency will receive a share of mathematicians and statisticians commensurate with the requirements of its mission.

RECOMMENDATION PR-6. Contacts should be established with commercial and educational institutions, preferably through consultants, with the objective of notifying the Agency when mathematicians and statisticians employed by them are about to enter military service.

Consultants should be informed of the importance of such notification and should understand clearly the procedure to be followed in notifying the Agency.

SECRET

RECOMMENDATION PR-7. Every effort should be made to use mathematicians and statisticians who are performing their military service (or equivalent) under conditions which will make continuation with the Agency in a civilian capacity most likely.

All reasonable devices should be employed to this end. For example, the U. S. Public Health Service is authorized to commission from civilian life, and it exercises this authority, not only for doctors but also for statisticians. The Agency should explore the possibility of obtaining similar authority.

RECOMMENDATION PR-8. When mathematicians or statisticians who would make desirable Agency employees object to being polygraphed, their security clearance should be obtained through a full field investigation.

These mathematicians can be effectively used in training programs, and quite possibly in connection with outside contracts not requiring high-level clearance, while the result of the field investigation is being awaited.

RECOMMENDATION PR-9. The Agency should become an Institutional Member of the American Mathematical Society, the Institute of Mathematical Statistics, and analogous professional organizations.

Such an Institutional membership would allow the privileges of membership for several mathematicians and statisticians of the Agency. It would keep the Agency's name before the mathematical and research community, thus improving its recruiting position.

The Agency should also institute a plan for paying expenses of its research mathematicians and statisticians to at least one national meeting of one of these societies per year.

These actions would promote morale and professionalism among the Agency's mathematicians and statisticians.

SECRET

FINDINGS ON

ORGANIZATION AND FUNCTIONS

FINDINGS OF-a. There is need for a stronger focus of mathematical leadership in the Agency than exists at the present time.

This is needed not only to strengthen the Agency's mathematical research effort, but also to strengthen its programs of recruiting and providing specialized training for mathematicians, supplying mathematical support for other research groups, arranging seminars, and similar activities. (See Discussion B.)

FINDING OF-b. There is need for a small number of applied mathematicians in RADE and in ANEQ who would provide direct and immediately available mathematical aid on problems which arise in these two R/D Offices.

The effectiveness of a group concerned with problems of an engineering nature can be increased by integrating a few applied mathematicians-at-large into the group. (See Discussion D.)

FINDING OF-c. There is need for some operations research activity in the Agency, directed toward, for example, increasing the effectiveness of the intercept effort, improving the direction finding program, and minimizing the time and effort required to intercept, transmit, and process traffic.

The members of such a group must, as a team, combine operations research experience, knowledge of mathematical techniques useful in formalizing manageable approximations to real problems and skill in their use, and sufficient engineering background to understand the nature of the problems and to ask the right questions. (See Discussion D.)

~~SECRET~~

FINDING OF-d. There is need for a systems analysis by a group of mathematicians and mathematically inclined engineers of the problems involved in the mechanization of the various steps involved in the reception and preparation of intercept material, its transmission, processing and analysis.

There is a tendency in the Agency to concentrate effort on the various major and minor components of the entire system used in the primary activity of the Agency. More attention should be given to the system as a whole and interaction between its components. (See Discussion D.)

~~SECRET~~

RECOMMENDATIONS ON
ORGANIZATION AND FUNCTIONS

RECOMMENDATION OF-1. The Office of Mathematical Research (MATH) should carry the burden of leadership of the Agency's mathematical community in fields of common interest.

Eventually a central organization for mathematics may have to be established which would be responsible for the recruiting at the higher levels and for the advanced training of the mathematicians of the Agency, for supplying mathematical support to the various research groups of the Agency and for other mathematical functions. But until such an organization is established, MATH should carry the mathematical leadership of the Agency, at least in such matters as the advanced training program, regular seminars, special meetings for original papers, and the development of an Agency spirit among all its mathematicians. (See Discussion B and Appendix II.)

RECOMMENDATION OF-2. The general objectives of the various mathematical groups should be clearly and consistently stated.

Especially in view of the unusual day-to-day pressures on the Agency, clear statements of objectives, adequately illustrated, are essential if friction between groups, failures to act due to divided responsibility, and undue deflection from work of long-term value are to be avoided. (Appendix II presents drafts of possible statements of mission for MATH and two of its divisions as an illustration.)

RECOMMENDATION OF-3. A small number of applied mathematicians should be integrated into both RADE and ANEQ.

Their mission should include (1) discovery and formulation of problems of an engineering nature which are susceptible to mathematical analysis, and (2) efforts to solve such problems,

as well as problems which are already clearly recognized as mathematical in nature. (See Discussion D.)

RECOMMENDATION OF-4. An operations research (OR) group should be established in the Agency.

This should consist initially of three of four persons, one or two of whom have had substantial OR experience. It should be so placed in the Agency organization as to have enough flexibility to attack, with a minimum of organizational restraint the Agency's most critical OR problems wherever they may be found. The choice of the location of the OR group within the Agency structure should be guided by the advice of one or two of the country's top OR people who have had wide military OR experience. (See Discussion D.)

RECOMMENDATION OF-5. Analytical aspects of the problems of mechanized data handling should have the full-time attention of a small group combining mathematical and engineering talents.

The Agency is struggling with the very difficult problems involved in mechanizing its data handling. Adequate systems studies, some at the broadest level and others concerned with more detailed aspects of information flow (symbolic representation, transmission, etc.), are essential. (See Discussion D.)

~~SECRET~~

FINDINGS ON

INFORMATION FLOW

FINDING IF-a. The organization and dissemination of mathematical and statistical knowledge within the Agency is inadequate.

General lack of expository and research publication, oral or written, and a tendency not to engage in formal scholarly reading and discussion, normal in other groups of similar professional attainments (at universities, for example), has reduced the effectiveness of much of the ingenious mathematical work done at the Agency.

The mathematical and statistical material in the Agency seems not to be sufficiently well indexed and cross referenced.

FINDING IF-b. There is inadequate liaison between Agency personnel concerned with cryptologic problems and personnel concerned with similar problems elsewhere.

Some liaison between NSA groups and the various Department of Defense groups working on cryptologic problems would increase the efficiency of the mathematicians working on these problems. Furthermore, the variety of non-literal secure communication problems which now arise in the National Defense effort, in particular in missile guidance, is so great that cryptologic research even beyond the Department of Defense must sooner or later be regarded as inevitable.

Whenever research on various cryptographic devices by groups outside the Agency involves mathematical work which is a repetition of work already done and familiar to the Agency, the country-wide shortage of mathematicians for cryptographic work is made more serious.

~~SECRET~~

RECOMMENDATIONS ON

INFORMATION FLOW

RECOMMENDATION IF-1. Relatively rapid communication of new mathematical generalizations and the principles of new mathematical techniques among Agency mathematicians should become a regular policy.

While security and compartmentation may require some delays in communication, these should be held to a minimum. If necessary, the establishment of an organizationally broad Senior Mathematical Staff, to whom information might be more rapidly communicated, should be considered.

RECOMMENDATION IF-2. The completion of mathematical work which leads to new techniques or new results should be followed by the preparation and circulation of informative abstracts and then by the preparation and circulation of a formal paper.

The abstracts must be informative enough to indicate to mathematicians who need the new techniques or results that they should contact the author. It is possible that many such abstracts could appear in the NSA Technical Journal.

RECOMMENDATION IF-3. Preparation of accounts of the present status of moderately broad fields of cryptology and of other special mathematical techniques should be encouraged.

This would be parallel to the preparation of texts mentioned in RECOMMENDATION RT-9. The accounts might be brief but bibliographies must be adequate.

SECRET

RECOMMENDATION IF-4. More nearly adequate systems of indexing and cross-referencing of material on cryptologic techniques involving mathematics and statistics should be provided and used.

The indexing of material by mathematical method irrespective of class of cryptographic system is inadequate. It is often necessary, at present, to know at least names of authors to find material which is known to exist and be relevant to a specific problem.

RECOMMENDATION IF-5. Technical liaison between the groups concerned with research in cryptographic principles at Air Force Cambridge Research Center and in MATH should be made adequate.

Research on various cryptographic devices by one group could easily involve mathematical work which is a repetition of that already done and familiar to another. Such a situation can only aggravate the country-wide shortage of mathematicians for cryptographic work.

RECOMMENDATION IF-6. Department of Defense mathematical groups working in cryptology and traffic processing should exchange information on fields of mathematical activity.

Efficient use of mathematicians in the general field of the Agency's activities would be greatly aided by a broader sharing of knowledge of fields of mathematical activity. Groups in the Agency, in AFSS, ASA, NSG, and AFCRC should certainly be included. These, in fact, might form the nucleus of the hypothetical American Cryptologic Society referred to in RECOMMENDATION RT-6. A real attempt should therefore be made to determine where cryptologic work is being done, what exchanges of literature would help the work of these groups, and to what extent these exchanges can appropriately be made. Information on fields of mathematical activity and needs for technical liaison should be assembled, presumably by a committee, and made available to all such groups to an extent consistent with security regulations.

SECRET

FINDINGS ON

MACHINES AND PROGRAMMING

FINDING MP-a. Use of the mathematical resources of the Agency has been, and continues to be, seriously hampered, and its effectiveness on critical problems is seriously reduced by difficulties in data processing.

The effective use of presently available mathematical skills in urgent cryptanalysis is still severely limited by apparent inability to convert available traffic rapidly enough into a form susceptible to processing — both recent traffic and, in some instances, traffic at least nine years old is currently held up. Problems of data handling and data organization in a form suitable for analysis continue to be among the Agency's most serious problems. The Agency's data-handling problem is much larger than any other known industrial or military data-handling problem, and has certainly required special study and mechanization. (See Discussion D.)

FINDING MP-b. Use of the mathematical resources of the Agency has been hampered, and its effectiveness reduced, by difficulties of communication with machines and by limitations of computing and analytical machine capacity for analysis. These problems could easily become more serious.

There is a need for a vigorous prosecution of the program for increasing the capacity of general and special purpose computing machines, and for developing automatic programming, more extensive diagnostic programs and other techniques which will bring the analyst nearer to the machines which serve him. (See Discussion A.)

~~SECRET~~

RECOMMENDATIONS ON

MACHINES AND PROGRAMMING

RECOMMENDATION MP-1. The development of languages, systems and devices simplifying the use of machines should be pursued energetically.

The development of a suitable machine crypto-language, and its use in automatic programming is unusually important, as is the development of still more flexible and extensive diagnostic programs (going far beyond STETHOSCOPE, for example). Outside facilities should be used to the greatest extent possible. (See Discussion D.)

RECOMMENDATION MP-2. The gap between cryptanalysis and programming should be narrowed.

In particular,

(a) the individual cryptanalyst should be more closely related to the machine codes or pseudo-codes of his own problems, and

(b) there should be greater opportunities for training and experience for both cryptanalysts and programmers in each other's field. (See Discussion A.)

RECOMMENDATION MP-3. Particular care should be given to insuring wide knowledge of the strengths and weaknesses of the various computing equipments.

This is needed so that

(a) such equipment will be effectively used, and

(b) demands for new equipment will be expressed in terms of operations sufficiently elementary to be entirely clear to designers. (See Discussion D.)

~~SECRET~~

RECOMMENDATION MP-4. Utilization of computing equipment can and should be improved by raising the quality of programmers.

Both the quality of programmers as hired and career opportunities for programmers should be improved. The existence of places for top-level skills and grades in programming should be recognized.

SECRET

DISCUSSION A

MATHEMATICS AND CRYPTANALYSIS

1. Type and Extent of Mathematics Required by the Agency's Cryptanalytic Problems.

It is far too easy to underestimate the scope and quality of the mathematics required in cryptanalysis. Nearly every member of the Mathematics Panel who did not grow up with cryptomathematics was surprised, perhaps even shocked, when he first encountered modern mathematical cryptanalytic techniques and unsolved problems. Each tended to feel, during the months of waiting for clearance, that he could make some approach which would almost surely be helpful, only to find, when at last the problems and techniques could be put before him, that his particular approach was one of those which had already been exploited. Even if he had been warned that this would be the case, he would not have believed it.

It is not true that presently available mathematical knowledge of clear applicability has been neglected; nor is it likely that any highly skilled mathematicians could dent the more difficult cryptanalytic problems in a week or a month. This does not mean that mathematics is not a promising tool in attacking cryptanalytic problems. It only means that it is not necessarily an immediate or short-range tool for major problems.

There are many problems where mathematics could give immediate or short-range results. The Agency is, and has been, attacking some of these. If its mathematical staff were larger it would undoubtedly have attacked more of them. Rather than showing reluctance in attacking them, it has probably shown too much eagerness, thus expending too much of its mathematical capacity on problems where shorter-range gains are to be anticipated.

~~SECRET~~

Many of the difficult problems of current cryptanalysis — and the cryptanalysis of the near future — are also susceptible to mathematical attack with reasonable hope of success, but not to short-term attacks of the sort developed under day-to-day pressure. The attacks on these problems which offer hope of success demand patient development: of new mathematical concepts, of specialized branches of mathematics rather than isolated mathematical theorems, of an abstract science of cryptology.

The things which are needed are not those which are easy to do, especially under stress of day-to-day and month-to-month needs. There must be mathematically trained persons to "put out fires"! There must be persons to conduct "research"! which might perhaps better be called "development"! along lines which promise short-term gains. But there must also be persons — of very high ability — in an atmosphere just remote enough to encourage long-range basic research, and close enough to current problems (and perhaps even to "traffic") to stimulate thought and preserve proper direction of effort.

2. Scales of Effort: Past, Present, and Future.

A crude estimate suggests that about 150 "mathematicians" worked for the Agency's predecessors during World War II. Some 25 to 75 mathematician-years of effort may have gone into the successful analysis of a single system under wartime conditions, when such a system carried very many messages, sent by large numbers of communicators, some of whom were relatively untrained. Moreover, the analysts were motivated and driven by the force of a shooting war and the critical value of reading particular pieces of traffic. This observation is not a criticism of present analysts. It is a recognition of a fact of human behavior. During the War, an engine change in a B-29 often required a week in the Zone of the Interior, and not more than a day in the Marianas. Cryptanalysis has no Zone of the Interior once a shooting war is on or imminent.

During World War II, the available material was better and there were many mathematicians who were highly motivated.

SECRET

After World War II, many countries realized that the advance of cryptanalysis had made their communications security measures inadequate and introduced much more secure systems. Today, the cryptanalyst — mathematician or not — faces less traffic, better trained communicators, better communications procedures, and much harder systems. If mathematics is to help, it is going to take more mathematicians, not fewer, and very deep mathematical considerations, not routine work.

Some methods will have to be found to provide dozens of mathematician-years, a sizeable fraction coming from mathematicians of very high ability.

3. Mathematics on the Team.

If mathematics is to contribute greatly to cryptanalysis, it cannot "go it alone"! In the cryptanalytic process, narrowly defined, it will have to share the load with other special skills. In the broader scope of Agency activities it must depend on data collection, data processing and high-speed computation, to name three potential towers of strength. It would be entirely unwise to look only at mathematics' share of the problem — unwise and dangerous.

If we could have had our present-day knowledge of the technical situation in 1945, and could have redisposed a few man-years of research and development effort, it is probable that the best thing we could have done then, to forward mathematical cryptanalysis now, would have been to expend these few man-years on the development of a typewriter — of a simple typewriter which would provide punched paper tape as well as typed copy and which could be supplied to all intercept positions. For if we had, automatic data processing should by now be years ahead of its present state, and backlogs of unprocessed traffic would be far smaller.

Without some data processing, mathematical cryptanalysis would be helpless. Without exceptionally good data processing, mathematical cryptanalysis cannot be highly efficient. Data processing is only one of the other members of the team; the others can have equally important influences.

SECRET

4. The Nature of the Long-Range Need.

It was said above that the difficult problems would require new mathematical concepts, whole new branches of mathematics, an abstract science of cryptology. These are not empty words; some comprehension of their meaning is important.

Much has been heard, in both the popular and the scientific press, of "cybernetics", of "information theory" and of similar words. All this refers to a new branch, or, if you will, new branches of mathematics which have been developed over a period of years. These branches are related to older branches; yet if they did not exist today, we would be unable to do nearly so well in studying mathematically either the relative range of different types of radar or the controllability of a stabilized and guided missile. If 12 months ago these branches of mathematics had not been in existence, and we had urgent need to study problems like those just mentioned, we could not, had we wished, have developed these branches in time.

There has been no notable development of a broad abstract theory of cryptanalysis, and little development even of specialized theories as, for instance, for pin-wheel machines. An abstract theory of cryptanalysis has not been developed and stored up against today's needs — we cannot use it today. If we wish to use it tomorrow or the day after, we shall have to begin to work on it today.

One reason why not enough has been done — one reason which has to be faced, evaluated and discarded — is related to the famous sign on a cryptanalytical office door: "We don't write history here, we make it"; and to the plaint of today's cryptanalyst with a specific mathematical problem: "Why do you keep solving the X machine again and again?". If we are to develop the powerful abstract theory we hope to have in due course, we shall have to begin at the beginning, and develop the science by starting with simple examples. We shall have to keep solving the X machine year after year — and the Y machine and the Z machine! And we shall have to spend some of our time solving systems so simple that today's cryptanalyst would laugh at them, e. g., simple

substitution. For it is only by beginning at or near the beginning that we can build up, unfortunately slowly, the new concepts, the new points of view, the new theorems, and the new techniques which would constitute a useful abstract theory of cryptology.

SECRET

DISCUSSION B

SOME ASPECTS OF THE MATHEMATICAL ACTIVITIES INSIDE NSA

1. The Agency and Mathematics.

The problem of the Agency and Mathematics is obviously of concern to many informed persons in the Agency. In a significant number of cases emotional involvement is evident. This involvement seems often to be due to an unnecessary identification of mathematics with mathematicians, or to a failure to recognize the diversity of the many activities appropriately called mathematics.

A very substantial and increasing fraction of the activities of the Agency are mathematical, in the broadest sense of that word. But most major sections of this part need not be carried out by professional mathematicians. Any attempt to specify mathematical training as a sine qua non for analytic work at the Agency would be a great mistake. The qualities of puzzle-solving ability, persistence, symbol understanding, imagination and creative thinking, when combined with general intelligence, are the prime requisites. These are the crucial abilities. If these can be combined with mathematical ability, possibly untrained but better still trained, their value to the Agency will be enhanced. But they will be valuable in any case. The present proposal of the Agency to recruit able students trained in disciplines other than mathematics, for example in classical languages, appears reasonable and sound from this point of view.

However, we must not press this point too far. First, because the requirements of puzzle-solving ability, persistence, symbol understanding and creative thinking would serve quite well to specify a natural mathematician (though not, perhaps, a natural worker with numbers). Some of those persons most useful to the Agency may deny that they are mathematicians, yet.

SECRET

those characteristics which make them most useful as cryptanalysts would have made them good mathematicians had they chosen to develop in that direction.

Secondly, there are increasing sections of Agency work where formal mathematics is of growing importance. Mathematicians will be needed in increasing numbers to deal with these sections. It would be a serious error, however, to recruit ready trained "mathematicians" whose crucial abilities were too far below the level of other persons whithout formal mathematical training who were also available. It would be an even more serious error not to go on and train these other very able persons who lack formal mathematical training. Mathematical training, after such persons reach the Agency, could and should be most rewarding.

If almost all analysts could realize that they frequently act as informal mathematicians, often as very good ones, much of the debate about the place of mathematics in the Agency would resolve itself.

2. Varied Aspects of Mathematics.

Gradation in what various persons mean when they say "mathematics" or "mathematicians" is most noticeable in the Agency.

Some say "mathematician" meaning one who can do simple arithmetic, or perhaps one who can provide the right formula for various standard situations.

Others say "mathematical analyst" or "crypto-mathematician" when they mean a person well versed in the standard techniques of formal analysis.

Others think of those who work in R/D (in "MATH"), or of those who psychologically and intellectually could do so, when they say "mathematician".

Still others might think, and it is unfortunate that too few have so thought, of those who set up and develop new fields of mathematics ultimately relevant to cryptographic progress.

These four stages are well marked, though there are many gradations in between. Pure mathematicians will wish to delete the first stage on the ground that it is arithmetic and handbookery — not mathematics. Many practical cryptanalysts will wish to delete the fourth stage (and some the third) on the ground that it is at least nonsense, and perhaps worse. Neither deletion can be allowed, if we are to be concerned with the use of the nation's mathematical resources by the Agency. All stages, and all intermediate gradations, use mathematical resources, and each is, in its way and time, useful. We must be careful not to conceive of mathematics too narrowly.

3. Mathematical Esprit de Corps in NSA.

There are some deficiencies in mathematical morale in the Agency. These deficiencies handicap the activities of the Agency in three main ways:

(a) Those with little or no formal training in mathematics fail to realize the extent to which they think and act mathematically.

(b) Among those with formal training in mathematics or its equivalent, there is insufficient feeling of being an NSA mathematician rather than a mathematician within some particular part of the Agency.

(c) Those currently doing research or development in the application of mathematics to cryptanalytic problems fail to have an audience of sufficient scope and mathematical depth to allow them to develop their own abilities through discussion and evaluation of their results and problems.

The first of these failures cannot be attacked directly. Pressure against mathematics has diminished greatly in the Agency during the last few years, however, and a substantial

SECRET

influence in this improvement seems to have been from a more tolerant and understanding attitude on the part of the formally most advanced mathematicians. It is to be hoped that this tendency will continue.

One cause of the second failure seems to be a matter of informal organization. No group or groups of mathematicians seem to have accepted the responsibility of leading the Agency's mathematicians to know one another better — and to learn from one another. Such responsibility must be exerted informally and tactfully across many organizational boundaries. The task is not an easy one, but it can be done.

There are several ways to attack the third failure. This is not the least crucial of the three, for it must take much of the responsibility for the lack of long range research at the Agency. The recent institution of The NSA Technical Journal represents one attack which has already begun. While the institution of suitably highly classified meetings intended for the reading of papers (presumably before a moderate group of able consultants) has been attempted, it has not been successfully established — though it is badly needed.

4. Organizational Problems of Mathematics in the Agency.

In the absence of clear statements of responsibility and authority or clear definitions of research in connection with the mathematical effort, misunderstandings are likely to arise which will impede progress. The Agency has been fortunate in the small number of such misunderstandings which have arisen. We suspect that such misunderstandings might best be avoided in the future by a careful reappraisal of the assignments made to major units. However, it is undoubtedly more reasonable to suppose that careful writing of the assignments made to MATH can be attained more quickly than more widespread reallocation of assignments, and we have undertaken to furnish what we believe to be a reasonable start for such an assignment. In particular, we have appended to this report (Appendix II) drafts of assignments for the Office of Mathematical Research and the divisions in it devoted to cryptanalytic research and machine studies.

We might note in passing that such an assignment consists properly of two parts (like those of the military mission as defined by the Joint Chiefs of Staff in their Dictionary of Military Terms). For our purposes these are a description of activities contemplated (which may be only indicative of the type of activity desired) and a general statement of objective written in terms which permit evaluation of results expected or results attained.

Continuing attention must be given to the relations between PROD and R/D. Certainly any problem which has not been solved and which cannot be solved directly is in some measure a research problem, and the best team which can be justified should be assigned to its attack. Each team is by its nature a task force, to be disbanded when the problem is solved or abandoned. There is little point in transferring a problem from PROD to R/D until it is reduced to direct attack, and then returning it to PROD, but there will always be some friction and difficulty of communication unless clear assignments of responsibility and authority are made within the task group and accepted by all major groups contributing to the solution of the problem.

5. The Question of a Central Organization for Mathematics.

Consideration might be given to the establishment of a central organization for mathematics in the Agency. Such an organization would be responsible for the recruiting and specialized training of mathematicians, supplying to research groups, task forces and other Agency activities the best procurable approximation to an adequate supply of mathematicians. The responsibilities of such a central organization would have to cut across the various offices using mathematicians, perhaps in a way similar to that in which the responsibilities of the Commander, Destroyers and Cruisers, of the Pacific Fleet cut across the responsibilities of the Commanders of that fleet's various Task Forces. It would clearly have difficulty in functioning effectively unless similar organizations were concerned with similar specialized skills. The extent of such an organization might vary from a single person, perhaps one of the Agency's competent mathematicians who is now not engaged in mathematical work, to a substantial group of mathematicians, most of whom would be on loan to research groups and task forces at any given time.

~~SECRET~~

Institution of such an organization or organizations would be a major change in the Agency's policy, and should not be undertaken without most careful consideration. It may be necessary, however, if the Agency's utilization of its presently available mathematical manpower is to be sufficiently improved.

6. The Internal Training Program.

While sustained effort at recruiting more mathematicians is imperative, many able analytically trained persons are available in the Agency or by recruitment, with training in other disciplines. Able persons with partial training in mathematics are also available. For such persons the Agency should organize a substantial and growing training program in mathematics. This program would eventually operate at all levels, including:

(a) Conventional graduate courses in mathematics.

(b) Special graduate courses in areas of particular interest to the Agency.

(c) Suitably classified courses in cryptology.

(d) Undergraduate mathematics courses.

(e) Mathematical training at precollege levels.

It should make as much use as possible of assistance and cooperation from educational institutions, especially in connection with (d), (e) and some aspects of (a).

It should utilize both frequent monitoring of actual classes and reviews of course content, examination content and marking to maintain a high standard in (a), (b), and (c). Those of its consultants who come from universities should be called on in this connection.

The teaching of cryptology, especially cryptanalysis should be conducted by competent professional cryptanalysts. Real traffic should be used in the examples, and a suitable amount of machine time made available for students' analyses.

SECRET

DISCUSSION C

SOME ASPECTS OF THE AGENCY'S OUTSIDE MATHEMATICAL ACTIVITIES

1. Nature and Merits of Outside Mathematical Activities.

Outside activities, for present purposes, will mean work done for NSA by mathematicians whose primary employment is elsewhere. Such work is done partly by individual consultants and partly through contracts with universities and industrial organizations. Among contracts, SCAMP is in a class by itself, since it covers the entire range of NSA mathematical interests and involves, as summer participants, a wide variety of research workers from all over the country.

The efforts of NSA mathematicans are primarily directed, at present, toward the solution of immediate and pressing problems. The pressure for immediate results of practical value, combined with the need for more research workers, makes it difficult for any one to devote an adequately long period to the uninterrupted study of a fundamental problem. The Office of Mathematical Research is thus prevented from devoting more than a relatively small effort to basic research. In addition to practical pressures and personnel shortages, there is difficulty in achieving, at the Agency, the degree of privacy sometimes needed for creative thinking. While the hindrances to fundamental research within the Agency could be partly cured, their existence is one of the factors making outside activities valuable.

Aside from the considerations in the foregoing paragraph, outside activities permit NSA to enlist the occasional services of mathematicians not available on a permanent, full-time basis. Many of them, despite a preference for other employment, have become intrigued with problems of the Agency and have made significant contributions toward their solution. A list is appended (Appendix III) of approximately one hundred mathematicians, other

than present full time employees, who are at present, or have been at some time in the past, associated with NSA. Included in this list are former employees, consultants and advisors, SCAMP participants, and mathematicians who have worked under outside contracts. Some fit into more than one category. A gratifying percentage of this group consists of mathematicians whose research has won them a high place in modern mathematics. The outside mathematicians are in a position to contribute not only by working on NSA problems but also by influencing appropriate young mathematicians to consider NSA employment. More than thirty institutions of higher education appear on the list of mathematicians associated with NSA.

The extended use of outside mathematicians is not without its disadvantages. It involves NSA personnel in the repeated, difficult and time-consuming task of initiating outsiders into the intricacies of Agency problems. Occasionally, such efforts are partly wasted, for some of those initiated lose interest.

Part of the task performed at NSA is that of distilling mathematical problems from the practical questions giving rise to them, and formulating these problems for mathematical attack. There is a natural reluctance, therefore, to set up a nice problem for others to solve. On the other hand, such formulations are useful to NSA mathematicians both in their own attacks and in collaborative efforts between Agency and outside mathematicians.

Questions are sometimes raised of the weakening of security as a result of the dissemination of information to consultants and contractors. These questions, while involved in outside mathematical activities, are broad in scope, and we shall not undertake any detailed discussion of them here.

2. Past and present outside mathematical activities.

We are not in a position to give a comprehensive picture, either quantitatively or qualitatively, of the work done for the Agency by mathematical consultants. We were informed by Dr. Sinkov that A. A. Albert, J. B. Rosser, E. H. Spanier, and J. W. Tukey have all made valuable contributions in

SECRET

connection with PROD problems. This is perhaps worth special mention because the problems arose outside the Office of Mathematical Research. It would be a major undertaking merely to list, to say nothing of assessing, the work done by consultants for and with the Office of Mathematical Research.

Without attempting to be exhaustive, we mention, among past contracts: (1) ANABRANCH (1947-1953) with S. S. Cairns as chief investigator and with J. C. Koken as the best-known assistant (The work under this contract was primarily concerned with cycle studies and exerted a significant influence on the development and analysis of the Koken machine and various rotor machines.); (2) a contract at North Carolina State College (Jack Levine and C. L. Carroll); (3) a contract with Brooklyn College (James Singer); (4) a contract with I. Heller at George Washington University; (5) a contract with Engineering Research Associates (A. E. Roberts). Among current contracts, we mention (6) CAVE, with Bell Telephone Laboratories, in the basic field of speech cryptography and cryptanalysis, a long-range general undertaking; (7) an ONR contract with Stanford, involving D. H. Blackwell; (8) a contract with Iowa State (R. J. Lambert, C. G. Maple, B. Vinograde, C. E. Langenhop); (9) a contract with General Kinetics (A. E. Roberts).

A condensed but fairly comprehensive account of SCAMP was prepared by Dr. W. A. Blankinship for presentation at the Mathematics Panel meeting of 13 - 14 December 1956. His report has been reproduced and is appended (Appendix IV). The present remarks are distilled from his condensation which, in turn, was largely gleaned from the annual reports of the several SCAMP chairmen.

SCAMP was born in 1951, passed through infancy, childhood and adolescence during the next four years and reached maturity in 1955. It is a continuing year-round project which grows thin in the winter and expands during the summer into a two-month symposium involving approximately a dozen outside fully-cleared mathematicians. In the early years, the participants could not all be cleared in time, and the early programs were consequently quite restricted in scope. In addition to

the outside participants, there is always a corps of NSA members, varying in numbers and composition from year to year.

The project is carried out on the UCLA campus through a contract on behalf of NSA between the ONR and the University of California. The location was and is motivated by: (1) the physical facilities, including secure offices and conference room, an adequate library, the digital computer SWAC, and the other machines, equipment and personnel of the UCLA Numerical Analysis Research; (2) the fact that the Los Angeles area has developed into a summer mathematical center to which it is relatively easy to attract desirable SCAMP participants.

In mathematical scope, SCAMP has, during recent years, increased its coverage so as to embrace the entire range of major mathematical interests of the Agency: combinatorial analysis, numerical analysis (computers), linear algebra, group theory, finite fields, statistics and probability, and Fourier analysis.

The annual SCAMP program, in its recent form, includes a two-week pre-SCAMP session at NSA, where new SCAMP participants are given relevant information concerned with the Agency (organization, personnel, modus operandi), with basic cryptanalytic and cryptographic techniques, and with the scope of NSA interests, and where presentations and discussions are conducted of some of the important problems to be submitted to the Summer Symposium.

When the Summer Symposium starts, the participants are supplied with a list of problems (with their backgrounds and various comments) prepared for SCAMP by NSA personnel. Those problems are discussed at a few conferences early in the session. It is made clear that the participants are not confined to the listed problems, but are free to pursue whatever research appears most appropriate to them, with due regard, of course, to the mission of SCAMP. There has been a consistently stimulating atmosphere conducive to fruitful individual and collaborative efforts.

Although productivity is not well measured by numbers of papers, we note that SCAMP has produced about one hundred papers

~~SECRET~~

distributed over about twenty different general topics, including [redacted] permutation matrices, [redacted] [redacted] statistical scoring methods and statistics of cipher text streams.

There appears to be general, though not universal, agreement that the output of SCAMP has been of great value to NSA; in particular, that it more than repays not only its financial cost but also the great expenditure of time and effort by the Agency in preparing proposed problems, in briefing outside participants, in supplying participants from its own staff and in a variety of other ways.

SCAMP produces not only papers, but also a pool of competent, informed and interested mathematicians, many of whom will prove useful as consultants or as aids in recruiting personnel from among graduate students. The value of these informed mathematicians generally increases with repeated participation in SCAMP or in consulting activities. On the other hand, there is of course a certain amount of wasted effort where participants lose interest and drop out after a relatively brief exposure to such activities.

Among expected future efforts, we note that Project PARALLEL will be partly a mathematical activity. It would be inappropriate for us to comment on it further in its present planning stage of development.

~~SECRET~~

DISCUSSION D

ADDITIONAL AREAS FOR MATHEMATICAL

SUPPORT IN NSA

1. Internal Mathematical Support for RADE and ANEQ.

There is a need for a small number of applied mathematicians in each of RADE and ANEQ. Their purpose would be to facilitate the application of engineering effort on problems usually not specifiable ahead of time. Mathematicians, aware of the set up and scope of these offices, who can see their problems from the inside, are essential. Thus when one of these offices needed outside mathematical support, it would have available a mathematician's analysis of the real mathematical problem already translated into a mathematician's language. Engineering problems which could really profit from mathematical support could be recognized and supported most easily in this way (e.g.: noise and interference problems for radio propagation). Such mathematical support should not be regarded or treated as "support" in the usual sense, but should rather be continually integrated into the total R/D effort.

A fair proportion of RADE personnel are communications engineers. It is widely recognized that there need be no sharp line between the communications engineer and the applied mathematician in the field of random processes and communication theory. This area of applied mathematics should be further stressed. However, there are many places within RADE where good use could be made of a less specialized mathematician with a substantial knowledge of the engineering problems and practices of the office.

Most ANEQ engineers are, in a broad sense, computer engineers. Many R/D computer units, outside the Agency, have found it profitable to bolster their engineering groups with a sprinkling of mathematicians, some preferably trained in logic. Even when ANEQ is separated into two offices to protect the Research or long-range side of R/D, both offices will (perhaps unequally) need this internal mathematical support.

Mathematicians within RADE and ANEQ would be expected to:

a. Provide direct and immediately available aid on relevant problems. For example, a study of radio interference and natural noise coupled with the communication theory of radio propagation certainly needs at least one full-time mathematician-communication theorist. A mathematical statistician (statistics and random processes) should be working in RADE-2 on the Morse translation and related problems — one mathematician has been at times borrowed from MATH. Any fair sized group (more than a dozen engineers) on circuit and component development can profitably use a mathematician of its own. The proposed new group on Systems in the new ANEQ office should probably have two, if it is to fulfill the broad premises of its charter.

b. Communicate effectively with other mathematicians or for other mathematical support throughout the Agency. For example, they should be aware of the limitations and uses of the available digital computers in (and out of) the Agency. They should know the fields and interests of other mathematicians, say, in MATH, so as to enlist their support most efficaciously when needed. (b) (1) (b) (3)

c. Know the office's operations thoroughly enough to recognize the desirability of mathematical effort on new problems as they arise. For example, in a study like [redacted] a suitable mathematician-communication theorist available within the office would have been helpful. The presence of mathematicians in each office should facilitate liaison between RADE and ANEQ on data processing equipments which fall partly in the purview of each — mechanizing Morse translation is an obvious example. This, of course, is part of a very general need for better and easier intra- and inter-divisional communication on a technical level universally throughout the entire Agency.

d. Provide mathematical education and inspiration to the other members of the division. For example, they should give occasional seminars on advances in, say, information theory, or the game-theoretical aspects of optimum design and use of D/F intercept antennas. They should ensure that engineers and others generally are aware of and up to date on the status, power, and limitations of mathematical and computer analysis, in exactly the

SECRET

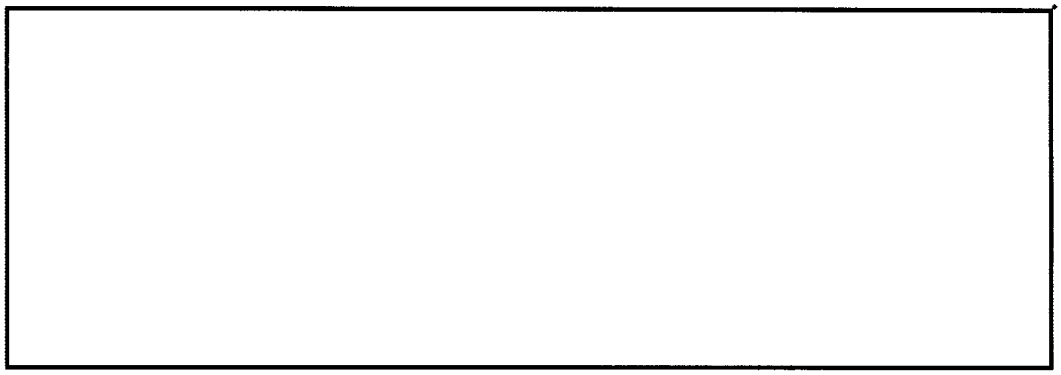
same way that mathematicians ought generally to know what is feasible to design and implement concretely.

Experienced inter-disciplinary mathematicians are hard to find. And yet, almost any R/D group can profitably find a place for such mathematicians. Even junior mathematicians should be encouraged, not only to continue their education, but to retain their mathematical identity. In any case a small but definite influx of mathematicians into every reasonably sized working group should be encouraged.

2. Operations Research.

A further area of mathematical support for NSA activities which we believe should be explored and developed is that of operations research (OR). The success with which OR techniques were applied to the evaluation of military tactics and strategy under combat conditions during World War II is too well-known to require discussion here. OR studies often resulted in clear indications as to how to improve the effectiveness of operations. These activities have been continued in all three services since the war for the purpose of evaluating new weapons and weapons systems, new tactics and strategies in maneuvers or under simulated combat conditions, with a view to determining directions of changes for improvement. OR groups are now being established by some of the large corporations for the purpose of dealing with inventory control, plant location, merchandising procedures, and other operational problems of the companies.

An OR group should be established in the Agency. This should be an independent group consisting initially of three or four individuals, including one or two who have had substantial OR experience. Their sole assignment should be to delineate and work toward the solution of operations problems which are susceptible to this method of attack. The nature of these problems is such that they cannot be precisely formulated in advance of a preliminary OR study. However, three particular problems to which those methods might usefully be applied must be mentioned:



An OR approach to improving the quality of direction finding, which seems to be hampered by insufficient training of operators, poor site locations, and various other factors, is needed. A systematic OR effort on this problem with due analysis of such factors as errors of D/F bearings, the geometry of site location, quality of operator training, etc., may well indicate practical ways and means of producing significant improvements.

A systems analysis approach to the problem of minimizing the time and effort required to intercept, transmit, and process intercepted traffic for analysis, one which looks toward automation of the whole process, is badly needed and would be an important OR activity. A fuller discussion of this problem is given in the next section.

The extent to which the OR effort is developed will depend on the success with which it deals with the problems it encounters. Such an OR group should be placed in the NSA organization so that it will have enough flexibility to tackle OR problems wherever they exist with a minimum of organizational restraint.

3. Mathematical Support of Mechanization.

There are many obvious needs for further mechanization of the various steps involved in collecting and processing data. Many of these needs have long been recognized and steps have been taken

SECRET

to implement them. For example, conversion of data from typewriter to paper tape, to punched cards, to magnetic tape, is clearly less efficient than direct preparation of magnetic tape. Again, Project LIGHTNING includes provision of improved high speed input output equipment as a part of a high speed computer. The need for proper preparation of the input to such a system is obvious.

There is little if any need for special mathematical support in applying immediate remedial measures. But effective mechanization requires a long range study of the requirements of the entire system from antenna to final output, to produce a completely integrated system. This goal may be somewhat visionary, but a consideration of some of the major steps involved will serve to illustrate the kind of mathematical support which would be valuable if not absolutely necessary to attain this, or a more limited, objective.

The system we are considering comprises three major functions: (a) reception and preparation of data, (b) transmission, (c) processing and analysis. All three functions give rise to problems which are susceptible to mathematical analysis, and the integration of the three functions requires a study of their mutual interactions which can profitably employ methods essentially mathematical in nature.

Many of these problems have been studied, some of them in considerable detail. As an example, Project FARMER represents advanced thinking about data processing equipment for the solution of this particular type of problem. Further reference to FARMER will be made below.

Consideration needs to be given to the form of the data which are to be forwarded to the control processing point to insure that they are in a form consistent with the methods of mechanization employed at that point. For example, should notes and corrections arising in the process of editing be interpolated in the body of the message, or should they be lumped at the beginning or end of the message? Every effort should be made to develop reliable methods to reduce the number of messages to be transmitted to the central processing point.

SECRET

All messages which are to be handled automatically must be coded in one form or another. Among the existing codes which are commonly used are the Baudot Code used in Teletype and an eight digit code used with the IBM Data Transceiver. These, of course, are only two examples to illustrate the meaning of the word coding. Most data processing machines do not directly accept data in the form on which they are delivered to the machines. This leads to inefficient mechanization since an extra step of code conversion must be introduced.

An important aspect of the coding problem is consideration of the use of error detecting codes, such as is used by the IBM Data Transceiver, and of error correcting codes. Error detecting codes have been used in some computers, but their use is not widespread. The advantages of such codes are most apparent when data are transmitted over a noisy channel, but a quantitative evaluation of their effectiveness is a complicated process which is worthy of further attention. Much remains to be done in a study of different types of such codes and evaluating their relative effectiveness in combatting different types of interference.

The transmission problem has many aspects which may be treated analytically. The coding problem has been mentioned above. In addition, there are a number of problems relating to the type of signals which make the most efficient use of the communication channels which are available.

The coding problem and the transmission problem are of great importance and the results of a study of these problems may have far reaching effects. It is our opinion that these problems should be made a specific assignment of a small group composed of mathematicians and mathematically inclined engineers.

The formulation of machine requirements is a vast subject which can only be outlined briefly. If we consider a machine to be a unit which performs conventional arithmetic operations, it can be stated that formulating machine requirements is a subject on which much has been done and which is fairly well understood. A program for extensive mechanization makes such a concept of a machine too restrictive. The FARMER concept is that of several

machines of different types which may communicate among themselves. As mechanization becomes more complete, the concept must be extended to include the sources of data and the means by which such data are concentrated at a central point, filed, and retrieved when needed. Later the data may require distribution to different parts of the system. All this gives rise to the necessity of studying both the flow of information in the system and the amount of equipment which is required to maintain efficient operation.

[redacted] Such studies will be of particularly great importance as the results of LIGHTNING become available. We will then be faced with the problem of making efficient use of a system composed of components which differ in their processing capabilities by several orders of magnitude. We will at the same time have equipment which is capable of handling problems of such magnitude that their solution has never been attempted by conventional methods and equipment. The need is clear for long range planning to cope with these situations before they arise.

Another type of problem, which has already been the subject of study, is the development of automatic coding methods to reduce the time and effort spent in programming more or less general purpose machines. Further effort is required along these lines, and the need becomes greater as the actual computation time is reduced.

Adequate treatment of the problems of a system study and machine requirements could well occupy the full time attention of an R/D group of four to six people. The group should include both mathematicians and engineers, or mathematical engineers. It is realized that work of this sort is presently being done, but it is felt that its importance is such that it should be made a full-time assignment for a small group, which might be an existing group or one formed especially for this purpose.

~~SECRET~~

APPENDIX I

THE ORIGIN OF THE STUDY

At a meeting of the Scientific Advisory Board held 17 February, 1957 and in subsequent discussion with the Director, NSA, and with the Executive Secretary, NSASAB, it was agreed that the NSASAB Mathematics Panel would undertake a study of the Agency's Mathematical effort. The scope of the study was to include mathematical support to cryptologic problems (not including ALBATROSS) and to all non-cryptologic problems. The principal sources of this support are within the Agency, but significant contributions have come from outside mathematicians, notably through SCAMP.

The following individuals comprise the membership of the NSASAB Mathematics Panel:

A. A. Albert, University of Chicago
D. H. Blackwell, University of California, Berkeley
S. S. Cairns, University of Illinois
A. M. Gleason, University of Illinois
Saunders MacLane, University of Chicago
Claude Shannon, Bell Telephone Laboratories
C. B. Tompkins, University of California, Los Angeles
J. W. Tukey, Princeton University
S. S. Wilks, Princeton University, Chairman.

Some NSASAB members, as well as Panel members, participated in the study, which was carried out by four groups having the following memberships:

Group 1 (Cryptanalysis):
*W. F. Friedman
A. M. Gleason, Harvard University
Saunders MacLane, University of Chicago
*J. C. McPherson, IBM
C. B. Tompkins, UCLA
J. W. Tukey, Princeton University, Chairman

Group 2 (Cryptography):

A. A. Albert, University of Chicago, Chairman
A. M. Gleason, Harvard University

Group 3 (Outside Activities):

*H. P. Robertson, California Institute of Technology
*S. S. Cairns, University of Illinois, Chairman

Group 4 (Mathematical Support of Engineering and Traffic Analysis):

D. H. Blackwell, University of California
*A. W. Horton, Jr., Bell Telephone Laboratories
*S. S. Wilks, Princeton University, Chairman

The study groups had the benefit of the advice and assistance of the following persons:

Group 1:

E. H. Land, Polaroid Corporation

Group 2:

E. C. Paige, Jr., University of Illinois
E. H. Spanier, University of Chicago

Group 4:

J. J. Eachus, Datamatic Corporation
W. J. Lawless, IBM
O. G. Selfridge, Lincoln Laboratories
E. M. Williams, Carnegie Institute of Technology

(Those marked * are members of NSASAB.)

SECRET

APPENDIX II

EXAMPLES OF MORE SPECIFIC MISSIONS

The following pages contain draft proposed missions for the Office of Mathematical Research of R/D and two of its four divisions. Each mission consists of a list of activities illustrative, but not exhaustive, of those to be performed in order to attain the general objective stated at the end of the mission.

Office of Mathematical Research

1. Maintain high competence in cryptology; in the mathematical theory, use and general design of advanced computing equipment; and in other areas of statistics and mathematics of concern to the Agency — including the development of new techniques and results whenever necessary.

2. State, develop and publish an abstract quantitative science of cryptology.

3. Train suitably chosen persons from any part of the Agency in this science, its application, and pertinent mathematical subjects (such as Bayesian statistical theory) with which they may not be familiar.

4. Apply this science in outstanding problems as appropriate to carrying out the above assignments.

5. Attack outstanding problems of great depth and importance which are seemingly not amenable to procedures in current use, and abstract and publish methods of analysis used in such attacks.

6. Furnish mathematical advice to other Agency groups.

SECRET

7. Provide facilities (such as regularly scheduled formal professional seminars, frequently with outside speakers) to maintain and increase the competence and interest of mathematicians throughout the Agency.

8. Relate the work of external research groups to the needs of the Agency by collecting mathematical problems throughout the Agency at all times, transmitting these problems to the outside groups, and ensuring that the results of these outside groups become a part of working knowledge throughout the Agency.

9. Encourage the development of broad esprit de corps among all Agency mathematicians and facilitate the interchange of information about techniques.

General Objective: To make available powerful methods of analysis — cryptologic, mathematical and statistical — for application to current and, particularly, to future problems of the Agency.

Cryptanalytic Research Division (Part of the Office of Mathematical Research

1. Cooperate in attacks on suitable outstanding current problems and abstract and publish methods of analysis used in such attacks.

2. Formulate unsolved mathematical problems, abstracted from outstanding cryptanalytic problems, in a form suitable for research efforts within the Office of Mathematical Research, in the SCAMP project or by other contractors.

3. Prepare expository and textual material, and aid in the application and teaching of current abstract cryptanalytic science.

~~SECRET~~

4. Instruct suitably chosen members of the Agency staff in abstract cryptanalytic science and in pertinent mathematical subjects, borrowing personnel from other divisions for this when their training or competence indicates a particular suitability for such assignment.

General Objective: To contribute to making available powerful methods of analysis for application to current and, particularly, to future problems of the Agency, by observing and predicting developments in the applied cryptologic science and by appraising and advancing the potential effectiveness of currently developing abstract cryptanalytic science in the light of these developments.

Methods Research Division (Part of the Office of Mathematical Research)

1. Provide leadership in applying available electronic computing equipment to problems arising or expected to arise in the Agency.

2. Formulate general design plans for equipment which might be more powerful than that currently available in attacking Agency problems, and which might reasonably be expected to be producible in the foreseeable future.

3. Code for available or engineeringly feasible equipment solutions to problems currently most efficiently done by hand, and formulate sets of machine improvements or developments, feasible or not, which would bring machines more closely into competition with hand methods in these problems.

4. Pay particular attention to machines proposed for problems involving decisions, including so-called thought machines, language machines, machines for document transcription, machines for automatic transcription of spoken information to written form, etc.

5. Furnish advice to other groups.

6. Remain advised concerning current research studies on the structure of and redundancies in languages.

7. Develop and expound mathematical fields and techniques especially related to machine computation, such as: further developments of Boolean algebra, logical formulations of the coding problem, methods of automatic coding, and optimum representation of required operations in terms of elementary ones.

General Objective: To contribute to making available powerful methods of analysis for application to current and, particularly, to future problems of the Agency, by recognizing and providing facilities for performing automatically and economically the tasks which require no ingenuity other than that used in their formulation, and by presenting in concise and convenient form aspects of Agency problems which seem to require human ingenuity or inventiveness for solution.

~~SECRET~~

APPENDIX III

MATHEMATICIANS ASSOCIATED WITH NSA

The following list includes those mathematicians, other than present full-time employees, who are now, or have been at some time in the past, associated with NSA. This list was compiled in MATH and is by no means completely exhaustive. The code used to indicate connection with the Agency is as follows:

A - Consultant or Advisor
S - SCAMP Participant
E - Former Employee
C - Contractor
F - Former Contractor

Name	Connection	Present Affiliation
Albert, A. Adrian	A,S	University of Chicago
Allan, Richard E.	E	SW La. Institute
Begle, Edward G.	S	Yale University
Belsky, Martin K.	E	IBM
Billingsley, Patrick P.	E,S	U. S. Navy
Blackwell, David H.	A,S,F	Univ. of Cal. (Berkeley)
Bode, Hendrik W.	C	Bell Telephone Labs
Botts, Truman A.	E,S	Univ. of Virginia
Bruck, Richard H.	S	Univ. of Wisconsin
Bush, Kenneth A.	S	Univ. of Idaho
Cairns, Stewart S.	A,S,F	University of Illinois
Carpenter, Lloyd H.	E	Nat. Bureau of Standards
Carroll, Charles L.	E,F	N. Carolina State College
Chernoff, Hermann	C	Stanford University
Church, W. Randolph	E,S	U.S. Naval Postgraduate School, Monterey

Name	Connection	Affiliation
Clifford, Alfred H.	E	Sophie Newcomb (Tulane)
Coles, William J.	E	University of Utah
Cramer, George F.	E	Sperry Rand
Deacon, Robert C. S.	E	
Dean, Burton V.	E	Operations Research, Inc.
Dean, Lura C.	E, F	CONVAIR
[redacted]	E, S, A	Cal. Institute of Technology
DeFrancesco, Henry F.	E	Westinghouse
Diehl, Henry H.	E	Ohio State University
Dilworth, Robert P.	S	Cal. Institute of Technology
Eachus, Joseph J.	E, A	Datamatic Corporation
Edmundson, Harold P.	E, S	Rand Corporation
Fabens, Augustus J.	E	Stanford University
Fort, Marion K., Jr.	A, S	University of Georgia
Gleason, Andrew M.	E, S, A	Harvard University
Good, Richard A.	S	University of Maryland
Gorenstein, Daniel	S	AFCRC
Greenwood, Robert E.	E, A	University of Texas
Hall, Dick Wick	S	University of Maryland
Hall, Marshall M., Jr.	E, S	Ohio State University
Hanson, Eugene H.	E, S	North Texas State College
Hayden, Seymour	S	AFCRC
Hedlund, Gustav A.	S	Yale University
Heller, Isidore	F	Navy Department
Herbert, E. V.	E	IBM
Hoffman, Alan J.	S	Nat'l Bureau of Standards
Horwitz, Harold M.	E	
Hydeman, William R.	E	Sperry Rand
[redacted]	E, S	Dept. of the Air Force
Johnson, G. Phillip	E	Univ. of Minnesota
[redacted]	E	Rand Corporation
Keisler, Jerome	S	Cal. Institute of Technology
Kennison, Lawrence S.	E	Brooklyn College
Killgrove, Raymond B.	S	Univ. of Cal. (Los Angeles)
Klee, Victor L.	S	Univ. of Washington

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

SECRET

Name	Connection	Affiliation
Koken, John C.	F, S	University of Idaho
Krall, Harry L.	E	Pennsylvania State Univ.
Kunze, Ray	E	
Lambert, Robert J.	E, C	Iowa State College
Langenhop, Carl E.	F	Iowa State College
Lehrer, Thomas A.	E, A	
Levine, Jack	F, E	N. Carolina State College
Levine, Norman	E	University of Pittsburgh
Long, Calvin T.	E	University of Oregon
Lotz, Warren	E	
MacLane, Saunders	A	University of Chicago
Maple, Clair G.	E, C	Iowa State College
Marlow, William M.	A, S	G. W. University Logistics Research Proj.
Martin, Nathaniel F. G.	E, C	Iowa State College
Martin, Peter E.	S	AFCRC
Martino, Michael A., Jr.	E	General Electric
Mattson, Harold F.	S	AFCRC
McCue, Edmund B.	E	
Menger, Karl	F	Ill. Institute of Technology
McMillan, Brockway	A	Bell Telephone Labs
Miller, Donald D.	E	Univ. of Tennessee
Moise, Edwin E.	E	Univ. of Michigan
Mullikin, Thomas W.	E	Harvard University
Newman, Morris	S	Nat'l Bureau of Standards
Nicol, Charles A.	S	Ill. Institute of Technology
Nyquist, Harry	A	Retired Bell Tel Labs
Paige, Eugene C., Jr.	E, A, S	University of Illinois
Paige, Lowell J.	S, A, F	Univ. of Cal. (Los Angeles)
Pall, Gordon	S	Ill. Institute of Technology
Pearl, Martin H.	E	Univ. of Rochester
Pierce, William A.	S	Syracuse University
Pollak, Barth	E	Ill. Institute of Technology
Prange, Eugene A.	S	AFCRC
Quine, Willard V.	S	Harvard University
Rees-Brahdy, Mina S.	S, A	Hunter College

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

SECRET

Name	Connection	Affiliation
Reiner, Irving	A, S	University of Illinois
Richmond, Donald E.	E	Texas Instrument
Rigby, Fred D.	S	Office of Naval Research
Roberts, Alfred E., Jr.	E, C, S	General Kinetics
Rosser, J. Barkley	A, S	Cornell University
Rubin, Herman	C	Stanford University
Rygg, Paul T.	E, F	Iowa State College
Schweppe, Earl J.	Naval Reserve	Univ. of Nebraska
Schmitt, Samuel A.	E	IBM
Shannon, Claude E.	A	Bell Telephone Labs
[redacted]	E	Intelligent Machines, Inc.
Silletto, C. David	E	Lincoln Life Insurance
Singer, James	F	Brooklyn College
Slepian, David	C	Bell Telephone Labs
Spanier, Edwin H.	A, S	University of Chicago
Spencer, Donald C.	S	Princeton University
Standerfer, Catherine S.	E	
Standerfer, John A.	E	CONVAIR
Stern, Mark E.	E	IBM
Swift, Douglas D.	E	
Swift, Jonathan Dean	A, S, F	Univ. of Cal. (Los Angeles)
Tompkins, Charles B.	E, S, A	Univ. of Cal. (Los Angeles)
Topp, Chester W.	E	Penn College
Tukey, John W.	A	Princeton University
Vinograde, Bernard	C	Iowa State College
Walker, Elbert A.	E	University of Kansas
Walker, Robert J.	S, A	Cornell University
Wall, Drury William	A, E	Univ. of N. Carolina
Ward, James A.	S	Univ. of Kentucky
Wexler, Charles	S	Arizona State College
Whiteman, Albert L	S, E	Univ. of Southern Cal.
Wilks, Samuel S.	A	Princeton University

~~SECRET~~

APPENDIX IV

DESCRIPTION OF PROJECT SCAMP: 1952-1956

(Prepared by W. A. Blankinship, NSA)

I. Introduction.

As nearly as I can determine, SCAMP is an abbreviation of the words "Special Committee Advising on Mathematical Problems". It is not in fact a committee, however, but a program. This program is effected in behalf of the National Security Agency by a contract between the Office of Naval Research and the University of California.

The initial proposals leading to project SCAMP were made in 1951 by C. B. Tompkins in his role as a member of SCAG (the predecessor of NSASAB). In March 1952 it was decided to conduct a summer symposium and, on the basis of this experience, to decide whether or not to continue the project.

Initially no fixed objectives were officially adopted for the symposium. A document by C. B. Tompkins dated 18 May 1952, entitled "Notes on a Proposed Research Project and Symposium", was unofficially adopted as embodying the temporary objectives. These objectives were:

"1. To provide a convenient and attractive, but private setting in which workers, ... who have attacked problems in a field of interest to the sponsor of the symposium, may exchange ideas and results;

"2. To provide a facility which may be used to initiate a later constructive research effort, mathematical in nature, directed toward solutions on computing machines or otherwise of problems assigned ... ".

In 1953 the following objectives were officially adopted from a letter by John H. Curtiss to the Chief of Naval Research.

> "a. Increasing the general knowledge available concerning discrete problems and their computational solution.
>
> "b. Educating competent mathematicians in mathematical theory and techniques of interest to the sponsor."

Since the California climate and the eminent mathematical community in Los Angeles provided a considerable initial step toward objective 1, and since objective 2 was likewise enhanced by the availability of the SWAC computer and the NAR computing facilities, it was decided to hold the first symposium at Numerical Analysis Research (NAR), then part of NBS, on the UCLA campus. (NAR was then known as the Institute for Numerical Analysis.) This seems to have been such a good choice that there has been no reason to change in subsequent sessions.

Although SCAMP is a year-around continuing project, the principal activity is the summer symposium held at the UCLA Numerical Analysis Research. SCAMP has been in existence five years now and we feel that each session has been an improvement on the previous ones, although it appears now to have reached full stride.

II. Conduct of SCAMP

Before going into details of individual SCAMP symposia, I will try to describe the manner in which SCAMP is conducted at present.

A. Pre-SCAMP

Some time between 1 January and 1 July a two week preliminary session is held at NSA in Washington, D. C. The purposes of this are:

(a) To acquaint new SCAMP participants with our organization, personnel, and modus operandi.

(b) To acquaint new personnel with fundamental cryptanalytic and cryptographic techniques.

(c) To acquaint all participants with the scope of our undertakings and fields of interest.

(d) To discuss some of the more important problems which will be submitted to the Summer Symposium.

(e) To afford an opportunity for some of the "older" members to work with cryptanalysts on operational problems.

These purposes are accomplished through a series of lectures, conducted tours, sessions left open for reading or informal discussion, and, of course, farming out the old hands to PROD.

The pre-SCAMP session was initiated before the 1954 symposium. It has been unquestionably profitable and will remain so as long as the present rate of turnover of SCAMP personnel is maintained. However, since more or less the same program is presented every year, we would be at a loss to maintain interest for the same set of people for more than two consecutive years.

B. The Symposium

The summer symposium is convened at NAR about 1 July each year and lasts until about 1 September. The symposium is composed of a Chairman with about 15 mathematicians (Actually there are seldom more than a dozen on hand simultaneously, as a few participants are available for only short periods.) from Academic institutions and two or three mathematicians from NSA. We have also had guest participants from the Air Force Cambridge Research Center.

The facilities at NAR include:

(a) A physically secure building containing a conference room and eight offices capable of accommodating 3 persons each (in a pinch).

(b) The mathematical library of NAR.

(c) A library of classified NSA and SCAMP technical papers.

(d) The digital computer, SWAC, with ancillary equipment and personnel.

(e) A very fine coffee mess.

At the beginning of the session a list of problems which have been prepared by NSA is distributed to the participants. These problems are a mixture of pure cryptologic problems and pure mathematical problems extracted from cryptologic ones. As a rule we feel it desirable to present a reasonable amount of cryptologic background along with the problems. For the first week or so formal conferences are held at which the NSA mathematicians discuss the problems — what is known, what has been tried, why we are interested, etc. It is emphasized that the problems presented by NSA are not assignments, but are presented merely as a framework for research. Each participant is to pursue whatever avenues of research his ability and conscience dictate. (Of course, NSA is delighted when one of its problems is solved.)

The entire atmosphere of SCAMP is informal and we hope to keep it so. The participants work both singly and in collaboration. Bull sessions germinate spontaneously so that everybody knows what the others are doing, and there are few papers published the credit for which can be claimed in toto by its author.

The function of the NSA mathematicians is, besides presenting and discussing the NSA problems, to:

(a) Perform research like everybody else.

(b) See that papers are classified correctly and that physical security is maintained.

(c) Evaluate SCAMP results, encourage further research, and suggest new problems.

NSA also provides a secretary who types and reproduces all SCAMP working papers and correspondence, maintains the classified library, arranges for janitorial services, keeps stocks of stationery, etc., and keeps an eye out for security violations.

The output of SCAMP consists of a series of informal working papers written by individual participants describing intermediate and final results of their investigations. (These may also include tables which are results of machine computations.) An innovation in the 1956 SCAMP was an informal floating log in which participants recorded stray thoughts and suggestions which could not be pursued at the moment as well as incomplete results which didn't seem to justify a working paper.

At the end of the SCAMP session the Chairman solicits from each participant a written memorandum describing:

(a) His principal activities.

(b) His feeling as to the effectiveness of SCAMP.

(c) Suggestions for the improvement of future symposia.

(d) Nominations for future participants.

These opinions are expected to be frank, and I believe they have been. They should provide a good evaluation of SCAMP from the mathematician's point of view, indicating whether or not he felt he had wasted his time. They are included as appendices in the Chairmen's final reports.

C. Between SCAMPS

The primary business between symposia is that of engaging participants for the next one. This is done by the Chairman with the advice and approval of NSA. We now insist that all participants be fully cleared and this means that negotiations and clearance procedures must be initiated very early, preferably

right at the end of the last symposium. Besides personnel negotiations and fiscal arrangements with UCLA, there is also a certain amount of computing left over from the previous session. This is usually done by Dr. Tompkins, sometimes with the assistance of an interested participant who can find time to return to UCLA for a short period during the winter.

III. Individual SCAMP Sessions:

A. 1952

The first SCAMP (1952) was hampered by the late decision (March) to hold it. In spite of this, Dr. S. S. Cairns, who was appointed as Chairman, did a remarkable job of assembling a competent group of mathematicians for the project and in completing all physical and financial arrangements. On such short notice it was impossible to obtain clearances for these persons in time for the symposium, and hence it was not possible completely to orient the participants towards the type of problems of interest to the Agency. An effort was made to do so but only in very general terms or on a quite elementary level. Nearly all of the effort of the 1952 SCAMP was consequently directed toward research on Finite Projective Planes. This subject had the advantage that it was completely unclassified and of considerable mathematical interest. While results would not be applicable to Agency problems, it was considered quite likely that methods and by-products would be, since both Finite Projective Planes and Cryptology are intimately concerned with permutation matrices, latin squares, and the like. The symposium was quite successful mathematically and I believe most participants felt that their time had been well spent.

B. 1953

The 1953 session, again under the chairmanship of Dr. Cairns, was still hampered by lack of clearances, but less so than the 1952 session. In advance of the session a paper by L. J. Paige and M. Newman was distributed, summarizing all the results achieved by the 1952 session on Finite Projective

SECRET

Planes. Because of the lack of clearances and because many participants of the previous year had questions to resolve, the principal effort was again directed toward F. P. P. However, there was some work done on other problems of more immediate concern to the Agency, namely on [redacted] and a statistical problem. Since there was no formal list of problems submitted by the Agency, these researches were prompted by lectures made by NSA mathematicians at SCAMP.

C. 1954

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

The 1954 session, under the chairmanship of Dr. Mina S. Rees, seemed to be the first session which was really productive from the Agency point of view. This is probably attributable mainly to two factors: (1) The large number of participants with complete clearances, and (2) a list of problems submitted by the Agency. Nearly all of the effort was directed along lines indicated by the problems. I believe this was prompted not by coercion or assignment on the part of the Agency, but rather by the fact that the problems were of real mathematical interest in spite of having practical applications. The most significant results obtained by this session were those pertaining to [redacted]

D. 1955

In 1955, SCAMP seemed to have reached full stride. All participants were fully cleared, a list of 32 Agency problems was presented, and SCAMP was housed in new air-conditioned offices adjacent to the NAR. Most of the problems were of an algebraic or logical nature which fitted exceptionally well with the experience of the mathematicians present. Complete clearance also allowed free exchange of information between NSA mathematicians and the participants as well as allowing the problems to be presented more nearly in their natural settings. The most significant results were obtained in the

theory of [redacted] Dr. Rees was again chairman of 1955 SCAMP. 1955 was also the first year of the pre-SCAMP session which was held in early January at NSA.

Another innovation in 1955 was the addition to the final report of an appendix written by the senior NSA participant describing the results achieved by the symposium in the light of the Agency's interests. The purpose of this was two-fold: (1) to indicate to interested components of the Agency where pertinent results could be found, and (2) to indicate to present and future participants what the significance of the results were. Whether or not these purposes were accomplished is still debatable.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

E. 1956

The 1956 SCAMP under the chairmanship of Prof. E. G. Begle, was as successful as the 1955 session. A list of 35 problems, more or less, was submitted by the Agency (some repeats of 1955 problems). The research and papers produced were more diverse than in previous years, and the overall picture indicated that this was beneficial. In other words the diversification was not a mere scattering of effort but resulted in fruitful results in more directions. Notable results included papers on [redacted]

Another factor which stimulated productive research was the presence of [redacted] has a wide knowledge of mathematical techniques and problems in cryptanalysis and was able to raise many questions of mathematical interest as well as contributing directly to the research effort.

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

F. Summary

Appended hereto are lists of SCAMP participants by year and other pertinent data. All of the things I have said can also be gleaned from the final reports of the chairmen for the appropriate years, the perusal of which I heartily recommend.

~~SECRET~~

SCAMP 1952: S. S. Cairns, Chairman

Outside Participants

T. A. Botts
S. S. Cairns
D. W. Hall
E. H. Hanson
G. A. Hedlund
J. C. Koken
L. J. Paige
C. B. Tompkins
J. A. Ward
C. Wexler

Two weeks or less

A. A. Albert
R. A. Leibler
A. E. Roberts
D. C. Spencer

NSA Participants

P. P. Billingsley
C. Bostick
H. H. Campaigne
R. B. Dawson
D. Dribin
[redacted] (b)(3)-P.L. 86-36
B. C. Getchell
A. M. Gleason
[redacted]
D. D. Miller
[redacted]
L. L. Walters

Two weeks or less

Jane Brewer
J. J. Eachus
A. J. Levenson
R. H. Shaw

Remarks

1. Very few participants fully cleared.
2. No list of NSA problems presented.
3. Effort primarily on Finite Projective Planes.
4. NSA members gave talks indicating, within security limitations
   (a) Areas of general interest to NSA.
   (b) Specific problems of low classification.
   (c) Expository talks on topics such as depths, weighting, measures of roughness, information theory, and permutation problems.
5. Also numerous computations on SWAC re FPP.

~~SECRET~~

~~SECRET~~

SCAMP 1953: S. S. Cairns, Chairman

Outside Participants

A. A. Albert *
R. H. Bruck
K. A. Bush
S. S. Cairns *
W. R. Church
R. P. Dilworth
A. M. Gleason *
R. A. Good *
D. W. Hall *
A. J. Hoffman
J. C. Koken *
M. Newman
A. Oates
L. J. Paige *
G. Pall
W. A. Pierce
M. Rees
C. B. Tompkins *

Two weeks or less

[redacted]
A. E. Roberts *
J. J. Wolf

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

NSA Participants

H. H. Campaigne
H. F. DeFrancesco
R. A. Leibler
O. S. Rothaus
L. L. Walters

Two weeks or less

J. J. Eachus
L. W. Tordella

Remarks

1. * indicates outside participants with full clearance.
2. Paper distributed in advance describing FPP results of 1952 session.
3. Lectures by NSA personnel on wired wheels, the assignment problem, [redacted] some intercept problems, rules of motion for cipher devices, matrix projection.
4. No formal list of NSA problems.
5. Papers (output) included
   14 papers on FPP or related topics
   1 paper on [redacted]
   1 paper on Statistics
   4 papers on Wired Wheels.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

6. SWAC commutations re FPP, latin squares, [redacted]

~~SECRET~~

~~SECRET~~

~~SECRET~~

SCAMP 1954: Mina S. Rees, Chairman

Outside Participants		NSA Participants
A. A. Albert	*	H. P. Edmundson
R. P. Dilworth		Ivan King
M. Hall, Jr.	*	R. A. Leibler
W. H. Marlow	*	[redacted]
F. B. Meek		J. J. Eachus (less than 2 weeks)
L. J. Paige	*	
Gordon Pall		
M. Rees	*	
E. H. Spanier	*	
J. D. Swift	*	
C. B. Tompkins	*	
A. L. Whiteman	*	
D. Gorenstein	(AFCRC)	
S. Hayden	(AFCRC)	

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

Remarks

1. * indicates fully cleared outside participants.
2. List of NSA problems included
   - (a) Wired Wheel problems
   - (b) [redacted]
   - (c) [redacted]
   - (d) [redacted]
   - (e) Distribution of max and min frequencies in a multinomial sample
   - (f) [redacted]
   - (g) [redacted]
   - (h) [redacted]
   - (i) [redacted]
   - (j) [redacted]
3. Papers on

(a)	Wired Wheels	(1)
(b)	Sums of Permutation Matrices	(5)
(c)	Statistical Problems	(3)
(d)	[redacted]	(3)
(e)	[redacted]	(1)
(f)	Partition functions	(1)
(g)	[redacted]	(1)
(h)	FPP	(1)

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

4. The first session really productive from Agency point of view.
5. Recommend reading Chairman's report in full.

~~SECRET~~

~~SECRET~~

~~SECRET~~

SCAMP 1955: Mina S. Rees, Chairman

Outside Participants

A. A. Albert
R. P. Dilworth
W. H. Marlow
L. J. Paige
M. S. Rees
J. B. Rosser
E. H. Spanier
J. D. Swift
C. B. Tompkins
R. J. Walker
A. L. Whiteman
P. E. Martin (AFCRC)
E. A. Prange (AFCRC)

NSA Participants

P. P. Billingsley
W. A. Blankinship
[redacted]

Two weeks or less

[redacted]
R. A. Leibler

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

Remarks

1. All participants fully cleared.
2. Agency list of 32 problems submitted
   (4) Cryptologic
   (15) [redacted]
   (8) Statistical distribution problems
   (1) [redacted]
3. Papers on [redacted]
   (17)
   (3)
   (4)
   (2)
   (1)

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

4. Occupied private and air-conditioned offices adjacent to NAR.
5. Pre-SCAMP orientation session at NSA in January.
6. Problems discussed and applications shown in detail at beginning of session.

~~SECRET~~

~~SECRET~~

SCAMP 1956: E. G. Begle, Chairman

Outside Participants

A. A. Albert	(2 weeks)
E. G. Begle	
S. S. Cairns	
R. A. Dean	
R. P. Dilworth	
V. L. Klee	
C. A. Nicol	
L. J. Paige	
I. Reiner	
J. D. Swift	
C. B. Tompkins	
H. F. Mattson	(AFCRC)
H. P. Edmundson	(RAND)
F. D. Rigby	(ONR)

NSA Participants

Reed B. Dawson

[redacted]

O. S. Rothaus

[redacted]

H. E. White

[redacted]

Two weeks or less

W. A. Blankinship
R. A. Leibler
M. Martino

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

Remarks

1. All participants fully cleared.
2. Pre-SCAMP session in June.
3. 35 Problems submitted of about the same calibre as 1955 problems.
4. Papers:

[redacted]	(11)
Rotor setting	(2)
Statistical scoring methods	(6)
Statistics of cipher-text streams	(2)
[redacted]	(3)
	(3)
Cycle structure of cipher devices	(1)
Maximization techniques	(1)

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

5. Problems and their application discussed in detail at pre-SCAMP and continued at SCAMP.