The Evolving Relationship between Mathematics and Cryptology: 1951 - 1952

Chris Christensen
Department of Mathematics and Statistics
Northern Kentucky University

Soviet cipher machines

Memorandum from Admiral Stone

REF ID:A66038

~~SECRET~~

AFSA-00E/jcw
Serial: 00104
23 Feb 51

~~SECRET~~

MEMORANDUM FOR THE CHAIRMAN, RESEARCH AND DEVELOPMENT BOARD

SUBJECT: Special Cryptologic Advisory Group

1. For some time, the Armed Forces Security Agency (AFSA) has been augmenting its efforts on assigned tasks and improving its potential for attacking new problems. Special emphasis has been laid on the procurement of additional qualified personnel. The Agency now has a highly competent and experienced staff, but it is believed that a definite group of outstanding technical consultants in certain fields of interest to AFSA would provide a valuable source of advice and assistance to the AFSA organization in meeting special problems.

Stone's proposed SCAG membership

- John von Neumann, Institute for Advanced Study
- Stewart S. Cairns, University of Illinois
- Charles B. Tompkins, George Washington University
- Claude Shannon, Bell Labs
- Howard Engstrom, Engineering Research Associates
- Hassler Whitney, Harvard
- Saunders Mac Lane, University of Chicago
- Dean Montgomery, Institute for Advanced Study
- R. K. Potter, Bell Labs
- Joseph Desch, National Cash Register

Invitation from Wenger

REF ID:A66037

~~CONFIDENTIAL~~

~~PERSONAL & CONFIDENTIAL~~ 13 April 1951

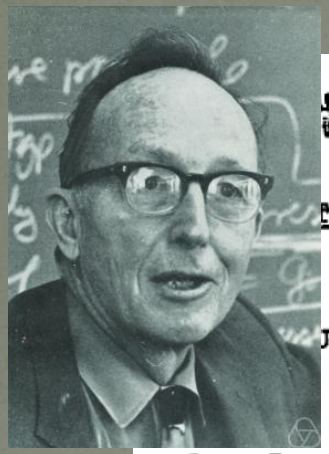
Mr. Joseph R. Desch
National Cash Register Co.
Dayton, Ohio

Dear Desch:

As you may have surmised, certain activities with which you were connected during World War II have continued since that time. In fact they have been receiving added emphasis in recent months as a result of the increasing tension of the international situation. In order to insure that our effort will be as effective as possible under the circumstances, we have recently obtained permission to establish a group of consultants to advise on some of our more difficult problems with which all three of the Military Services are vitally concerned. The group is being sponsored by the Research and Development Board of the Department of Defense, whose Chairman, Mr. William Webster, is taking a personal interest in the project.

The group is now being organized and it is hoped to include in its membership, initially, about ten of the top flight mathematicians and electronics engineers who are likely to be able to help on our particular problems. The membership will gradually be expanded as needs develop. In considering possible candidates, you were, of course, one of the first that came to mind. I am writing, therefore, to ask if

Memorandum from Donald Miller



REF ID:A65811

SCAG file

4 June 1951

M FOR AFSA-OOT

Conversation with Professor MacLane.

1. I succeeded in reaching Professor MacLane in Chicago by telephone at 2230 yesterday. Our conversation was rather extended because he raised a number of questions.

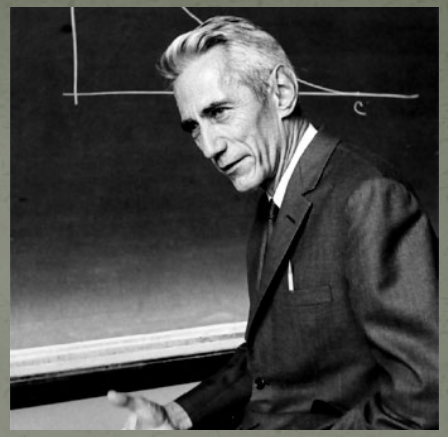
2. Professor MacLane said he had received my letter of 25 May and had written (but was not sure he had mailed) a reply, which he then summarized orally. Apparently he is not enthusiastic about the prospect of being invited to join SCAG, but from the tenor of his remarks I take it that he is open to persuasion.

3. The first question Professor MacLane raised was whether the work involved would be related to his mathematical interests, which are primarily in abstract algebra. His second question was: "How much time and energy would be required?" I endeavored to reassure him on both points, but was unable to be specific concerning the second. He then remarked, referring to his wartime experience with OSRD, "I was burnt once and I don't want to be burnt again." This remark, I believe, is related to his first question; apparently the work he was assigned to perform for OSRD was of a dull and routine nature, far removed from his mathematical interests.

11 June 1951 “Dear Saunders,”

Thirdly, I understand what you mean about the military "research" assigned to you in World War II (wasn't that the same stuff Mackey worked on?). Let me assure you emphatically that our work is nothing like that. We do not deal with dirty differential equations, we don't carry slide rules, and in general our problems are not amenable to the methods of what is usually called "applied mathematics". I don't mean to say that we are unconcerned with calculation, approximation, and numerical methods, but we have competent people to deal with those aspects of the problems. Our pressing need is for a high order of abstract thinking, for new ideas and approaches rather than mere technical facility.

Letter from Mervin Kelly



REF ID:A66029

COPY

BELL TELEPHONE LABORATORIES
Incorporated
463 West Street, New York 14, N. Y.
CHelsea 3-1000

M. J. Kelly
President

LT. GEN. WALTER B. SMITH, Director
Central Intelligence Agency
Washington 25, D. C.

Dear General Smith:

While there have been several other approaches to enlist Dr. Shannon's services in connection with military activities and it has been our judgment that, in general, he could best contribute in his particular field by carrying on his researches independently, the matter with which your letter deals is of a more compelling nature and we shall, therefore, be glad to encourage and assist Dr. Shannon in participating to the extent of the preliminary examination you suggest. During this phase, we propose that Dr. Shannon's services be contributed by the Laboratories, with reimbursement to him by the Government for incidental travel and living expenses. If this preliminary review indicates the need for Dr. Shannon's continued participation in the program, we should like to reconsider with you the extent and scope of such participation and the basis on which it should be arranged. I trust this will be agreeable to you and I assure you of our desire to be helpful.

Sincerely yours,

/s/ Mervin J. Kelly

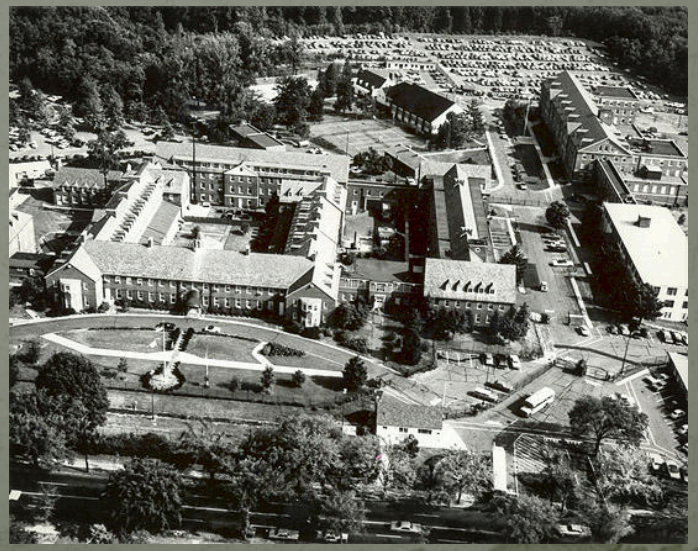
President

SCAG members

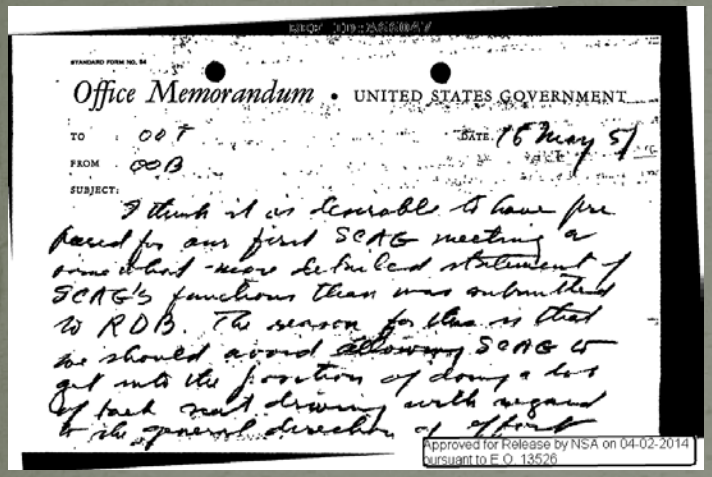
- John von Neumann, Institute for Advanced Study
- Stewart S. Cairns, University of Illinois
- Charles B. Tompkins, George Washington University
- Claude Shannon, Bell Labs
- Howard Engstrom, Engineering Research Associates
- Hassler Whitney, Harvard
- Saunders Mac Lane, University of Chicago
- Dean Montgomery, Institute for Advanced Study
- R. K. Potter, Bell Labs
- Joseph Desch, National Cash Register
- John C. McPherson, International Business Machines
- John Howard, Engineering Research Associates

SCAG conferences

- 4 – 5 June 1951
- 10 – 11 July 1951
- 12 – 13 September 1951
- 6 – 7 December 1951
- 12 – 13 March 1952



Wenger to Friedman 16 May 1951



Office Memorandum • UNITED STATES GOVERNMENT

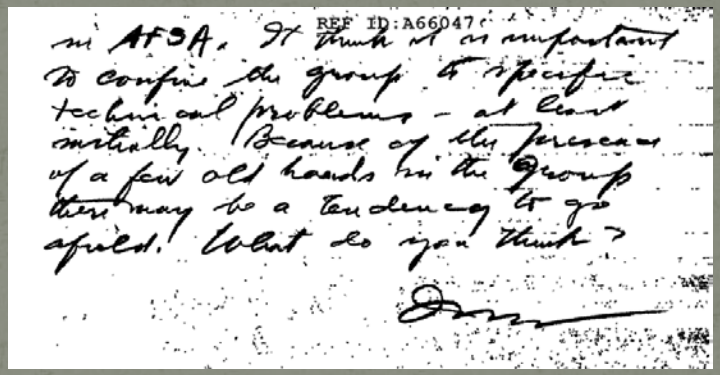
TO : OOT

DATE: 16 May 51

FROM : OOB

SUBJECT:

I think it is desirable to have prepared for our first SCAG meeting a somewhat more detailed statement of SCAG's functions than was submitted to RDB. The reason for this is that we should avoid allowing SCAG to get into the function of doing a lot of back seat driving with regard to the general direction of [illegible]



in AFSA. I think it is important to confine the group to specific technical problems – at least initially. Because of the presence of a few old hands in the group there may be a tendency to go afield. What do you think?

I think it is desirable to have prepared for our first SCAG meeting a somewhat – more detailed statement of SCAG's functions than was submitted to RDB. The reason for this is that we should avoid allowing SCAG to get into the function of doing a lot of back seat driving with regard to the general direction in AFSA. I think it is important to confine the group to specific technical problems – at least initially. Because of the presence of a few old hands in the group there may be a tendency to go afield. What do you think?

The 1st conference, Friedman

The technical sessions will therefore be confined strictly to the presentations required to develop the technical background SCAG will need in order to understand the nature of that problem, and in broad outline to present the directions in which our past experience with similar problems

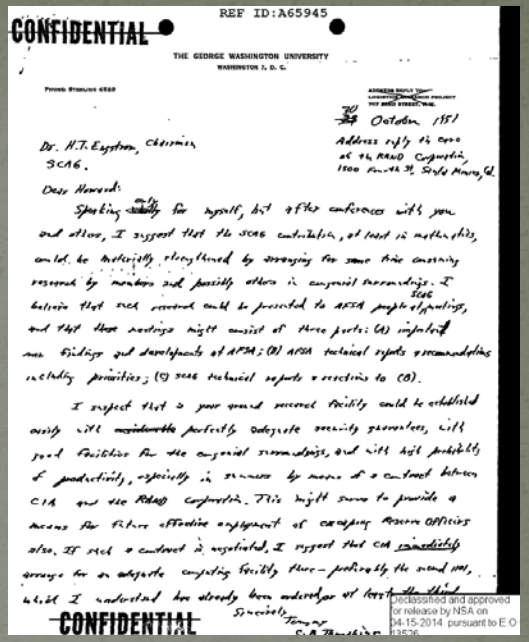
~~TOP SECRET~~

indicates the research should travel. The specific problem is one which involves a cipher machine of apparently quite complex construction. I say "apparently quite complex construction" because not only have we never seen the machine but also we have been unable to gather by covert intelligence any information whatever concerning its construction. What little we know about it has been derived by deductive and inductive reasoning, based upon our studies of the cryptograms produced by the machine and collected for us by our intercept stations.

The 1st conference

- Gleason: WW II attack on Enigma as background for wire-wheel problems. Questions about one-time additives and irregular stepping.
- Raven: exposition of ALBATROSS' place in Soviet communications and what had been recovered.
- Shepard: round robin search for depths on ALBATROSS.
- Roberts: project SWEATER.
- Tours: GOLDBERG, DEMON, a BOMBE, ATLAS, ABNER, ATLAS II, NOMAD, ROBIN, CONNIE.

The Tompkins' proposal


REF ID:A65945

CONFIDENTIAL

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON 7, D. C.

October 1951

Dr. H.T. Engstrom, Chairman
SCAG.

Address reply to Exec
at the RAND Corporation,
1500 Fourth St. Santa Monica, Cal.

Dear Howard:

Speaking only for myself, but after conferences with you and others, I suggest that the SCAG contribution, at least in mathematics, could be materially strengthened by arranging for some time consuming research by members and possibly others in congenial surroundings. I believe that such research could be presented to NSA people at meetings, and that these meetings might consist of three parts: (A) important new findings and developments at NSA; (B) NSA technical reports recommendations including priorities; (C) SCAG technical reports & reactions to (B).

I suspect that a year around research facility could be established easily with considerable perfectly adequate security precautions, with good facilities for the congenial surroundings, and with high probability of productivity, especially in summers by means of a contract between CIA and the RAND Corporation. This might serve to provide a means for future effective employment of cooperating Western Officers also. If such a contract is negotiated, I suggest that CIA immediately arrange for an adequate computing facility there – preferably the second 1101, which I understand has already been ordered, or at least the third.

Sincerely,

CONFIDENTIAL

Declassified and approved for release by NSA on 04-15-2014 pursuant to E.O. 13526

… I suggest that the SCAG contribution, at least in mathematics, could be materially strengthened by arranging for some time consuming research by members and possibly others in congenial surroundings. … I suspect that a year around research facility could be established …especially in the summers by means of a contract between CIA and the RAND corporation. … If such a contract is negotiated, I suggest that CIA immediately arrange for an adequate computing facility there – preferably the second 1101[72] which I understand has already been ordered, or at least the third. (Friedman A65945)

The reaction within AFSA

Raven: "… a thickly veiled rehash of the CIA proposal of last year prepared by Mr. Engstrom."

Reaction within AFSA

Kullback:

2. In the cryptologic business the biggest asset that an organization can have is continuity of personnel. A cryptologic organization cannot be successfully operated, in my opinion, on an assumption that any time some difficult problem arise "experts" will be brought in who will solve the problem and then go about their own business again.

3. If SCAG can make a contribution to the problem for which it has been assembled, it is only because of continuity of AFSA personnel to formulate the problem in terms of which SCAG members can attack it, for without such a formulation it is doubtful if any outstanding scientist without a long period of training in cryptology could make a real contribution.

4. Are we to favor outside experts by providing them with congenial surrounding and expect competent AFSA personnel to operate under conditions considered less favorable?

4th conference

of potential problems and contractors. The chairman is to recommend to the Director AFSA that basic research be considered as an objective on its own, with ALBATROSS a separate problem.

The SCAG report

- Recommendation one: More programming and computing time should be allocated to the Robert's method and related approaches.
- Recommendation two: An expanded program should be initiated in high-speed machine developments.
- Recommendation three: A senior technical director should be appointed, reporting directly to the Director of AFSA.
- Recommendation four: A separate research organization should be established in AFSA and other organizational changes should be made.
- Recommendation five: More use should be made of outside contractors for basic research and machine development.

Reply from General Canine

~~SECURITY INFORMATION~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL - SECURITY INFORMATION~~

Serial:

17 MAY 1952

Dr. R. K. Potter
Bell Telephone Laboratories
463 West Street
New York, New York

Dear Dr. Potter:

I have devoted considerable time to studying the Special Communications Advisory Group (SCAG) Report which was submitted to me on 17 March 1952 and which I found not only quite interesting but also very useful.

The five principal recommendations made in the Report have been given special attention and I have directed that those recommendations or parts of them which can be carried out as matters entirely within my responsibility are to be implemented without delay and to the maximum practicable degree.

Reply from General Canine

With the completion of the task set before SCAG, certain members have indicated a belief that the group should be reorganized and reestablished on a different basis. I share this view and am having prepared a new charter accordingly. When this has been done, I shall probably communicate with you at an early date with a view toward ascertaining your interest in further participation in SCAG affairs.

In closing I wish to express my earnest appreciation of the time, thought, and effort which you personally gave to make the work and deliberations of the first SCAG so fruitful.

Sincerely,

(sgd) Ralph J. Canine

RALPH J. CANINE
Major General, US Army
Director, Armed Forces Security Agency

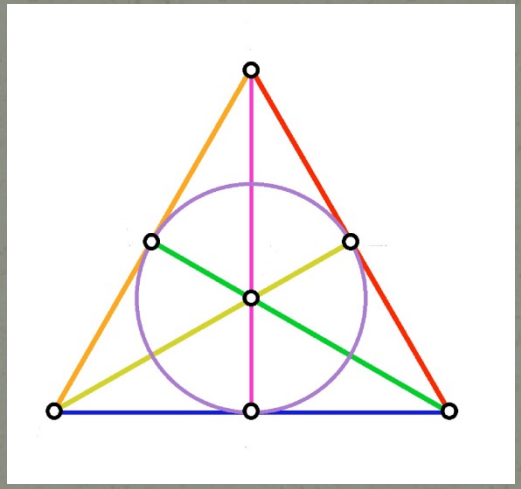
Special Committee Advising on Mathematical Problems (SCAMP)

1952, the trial year

A. A. Albert	T. Botts	D. W. Hall	E. H. Hanson
G. A. Hedlund	J. C. Koken	J. A. Ward	C. Wexler
S. S. Cairns*	H. T. Engstrom	C. Tompkins	J. von Neumann
H, Campaigne	A. M. Gleason	M. Hall	
L. Paige	A. E. Roberts	D. C. Spencer	R. A. Leibler

Multi-month summer symposium

Report on the first SCAMP



Levenson, Dribin, and Gretchell

… we feel that the two months of SCAMP's existence failed to produce any results of value to the Office of Operations.

… unless future programs be more clearly related to operational problems, the Office of Operations should not participate in such conferences.

R. H. Shaw

(1) The introduction of new, competent scientific thought on important unsolved problems many of which have been around so long that the Agency personnel assigned to them have begun to grow stale;

(2) The opportunity for the Agency's better cryptomathematicians, or mathematical cryptologists, to free themselves for an extended period from the extensive morass of administrative and executive detail with which all too many of them are saddled and to participate full time in the attempted solutions of significant problems with which they are technically competent to solve;

(3) The opportunity for bona-fide mathematicians employed by AFSA to recover a bit of their professional skill through informal discussion with recognized leaders in mathematical specialties.

R. H. Shaw

There is a real danger in projects such as SCAMP … that the Agency may make itself an enthusiastic but unwitting sort of computing machine for the use of "outside experts" who do not have any real responsibility for the operation of the Agency but who are very much aware of the advantages to pure research of having so large and rich an organization to support their personal research goals.

National Security Agency Scientific Advisory Board (NSASAB)

4 – 5 February 1953

S. S. Cairns*	University of Illinois
H. P. Corwith	Western Union Telegraph Company
Howard Engstrom	Engineering Research Associates
John C. McPherson	IBM
Howard P. Robertson	California Institute of Technology
John von Neumann	Institute for Advanced Study
Samuel P. Wilks	Princeton University

To advise the Director on scientific matters related to the mission of the NSA.

ALBATROSS