8 January 1952

Memorandum

TO: Chief, R & D

FROM: Math. Division

SUBJECT: Possible Contract for basic research.

1. The possibility of contracting for basic mathematical research on cryptologic problems was discussed at the last SCAG meeting. A summary of the views of the Math. Div. are given here. These cover three points, contracts already let, subjects suitable for further contracts, and potential contractors. The list of problems certainly could be extended, and the formulations should be extensively reworked. The list of contractors is the result of conversations with Tompkins, von Neumann, and others.

2. The Armed Forces Security Agency has already let contracts for mathematical research.

a) Brooklyn College has contracted with us (although ONR is technically the contractor) to administer research in combinatoric problems (Latin squares, enumeration of substitutions, classification of substitutions by parallelisms; etc.). This project is supervised by Prof. Singer. The contract is new and Prof. Singer is not yet fully cleared; however, some specific problems have been presented and some results have been received.

b) Under a contract with ONR, Stanford University administers a project in statistics, Prof. Girschick in charge. This contract was initiated by ONR without cost to our agency, although Stanford devotes much of the time to our problems and have sent a number of papers on subjects of interest to us.

c) AMARANCH is a project sponsored by the Armed Forces Security Agency, (again with ONR as fiscal agent) at the University of Illinois to study cycle structures. This project was formerly at Syracuse University but was moved when its sponsor, Prof. Cairns, went to Illinois. Many results have been achieved which have proved valuable in the design of our own cryptographic systems, in particular the Koken rule of motion.

8 January 1952

Possible Contract for basic research.(cont.)

d) Project SWEATER has for its object the replacement of complicated logical processes by numerical algorithms. It was started several years ago by Dr. Tompkins, then at ERA, as a contract with BuShips. (Task 15 of NObs42001, now under Task 3). Dr. Tompkins has since left ERA, and the project now headed by Mr. A. M. Roberts. An outstanding result of this contract is the so called Robert's method, which although still in an experimental stage, is considered one of the best hopes of solving one of our most important problems.

e) Through an ONR contract, Prof. Wilks of Princeton University has been cleared for talks on our statistical problems and has shown some interest in our work.

3. There are many other problems suitable for contract projects. Brief statements of some of these problems are given here together with an estimate of the relative urgency of their solution. Any precise formulation of these problems will require a great deal of work, hence contracts for them will necessarily be vague and will require the contractor to reformulate the problem in the light of his own experiences in studying the subject. In writing a contract the Agency would specify some particular illustration of the problem and request research on problems related.

a) Logical reduction of hypotheses. Given a large number of hypotheses, some consistent and some inconsistent, to find the maximum consistent subset. This is the most important problem facing the Agency, containing immediately the solution of our most important cryptanalytic problem. URGENT.

b) Classification of data. Given a number of observations, each from one of two universes, to classify them according to their parent universe. This problem and its variations are continually recurring in cryptanalytic problems. VERY IMPORTANT.

8 January 1952

Possible Contract for basic research, (cont)

c) Measures of goodness of fit. Most statistical techniques now known require samples much larger than those available in our problems. IMPORTANT.

d) Measures of significance. The question of whether to proceed further or start again on a cryptanalytic process depends on measuring the significance of the partial result obtained. In some cases we have measures and would like to refine them, in others we have no objective measures at all and are forced to depend on intuition. IMPORTANT.

e) Solution of simultaneous modular equations. Since cryptologic manipulation concerns finite sets, the problems can often be conveniently represented in modular fields. The problems of solving simultaneous equation in these fields, especially when some of them are in error, are most important to the Agency. Since this problem is rather poorly defined, it is difficult to assign it a priority, however, it includes a) as a special case.

f) Various statistics problems, such as calculating the distribution functions of certain statistics, their expected values, etc. Most of these problems will arise in connection with other problems on this list and should probably be treated in this connection.

g) The theory of permanents. The enumeration of wired wheel classes can be done by considering the permanents of certain matrix. DESIRABLE.

4. Any potential contractor would build his program about a key man. For example, when we had a contract with Syracuse University, Prof. Cairns directed and conducted the work. When he left Syracuse they made no pretense of being able or willing to continue the work. They would not again consider such work unless they had again a man with the interest, ability, and special knowledge needed to "spark-plug" the program. This is likely to be the critical factor in finding a contractor, either commercial or academic.

8 January 1952

Possible Contract for basic research. (cont)

As an example of the attitude of the Universities, a portion of the annual report of the president of M.I.T. is quoted. "These 'Hartwell type' projects --- impose heavy burdens on our staff. --- [We] accepted them in response to insistent appeals from the Government and only after becoming convinced ---."

However, it is plausible that a contractor could be found, and here is a list, with a few relevant comments for each, of agencies which might be considered.

The list below is roughly in order of estimated feasibility.

a) Princeton University. The work could be done at the Forestal Center, already equipped with secure stowage. Prof. S. S. Wilks has consulted with us in the past. The University has high prestige and is centrally located. There will soon be a computer at the Institute for Advanced Study.

b) RAND Corporation. Secure spaces and stowage are available. Dr. M. M. Flood may be available. Other mathematical work is being done there, and prestige is high. The location is remote.

c) Bell Laboratories. Secure spaces and stowage are available. Dr. Shannon is there. They have computers. One of our former outstanding employees, Dr. R. A. Leibler, is now working for a Bell subsidiary, the Sandia Corporation.

d) Johns Hopkins University. They have set up the Applied Physics Laboratory in Silver Springs to handle one Government contract, where they have secure spaces. Prof. A. H. Clifford, who is now here on extended active duty but may be back there next year, is extremely competent to direct such work.

e) N.R.A. has an Arlington laboratory with secure spaces, and Dr. Engstrom and Mr. Roberts have experience in directing such a program.

f) The University of Illinois. Prof. Cairns and Mr. Koken have experience in such research. There is not now any extensive secure stowage available. There is a computer soon to be finished.

6 January 1953

Possible Contract for basic research. (cont)

g) Harvard University. Prof. A. M. Gleason may be back there next year. The school has enough prestige to attract most mathematicians. There is a computer, but one not very good for our problems.

h) M.I.T. There is no one there now to be the center for such a program, but they have secure spaces and prestige. There is an excellent computer with one graduate student who knows our problems.

i) Ohio State University. Prof. M. Hall hopes to return there next year and could manage a program. No secure spaces there now.

j) George Washington University. Dr. Tompkins is there. They now have contracts with the Navy, and have secure stowage. They are within easy reach of this Agency.

k) U.C.L.A. or the Bureau of Standards Institute for Numerical Analysis. The two are located together and for our present purposes are almost indistinguishable. There is not now a central figure for such a contract, but they already have contracts for classified research. Prestige is good, and a computer is available.

l) The Bureau of Standards, Washington. They have classified contracts, and would be anxious to undertake the service. The plant is extremely accessible. They have a computer.

m) University of Michigan. Prof. H. W. Meise was formerly assigned to this Agency. He is a very competent mathematician. The prestige of the University is good.

n) Brooklyn College. Profs.A. Landers and Singer have had contact here. New York City has certain attractions.

5. We have assumed here that a single contract was needed to deal with several problems. This gives flexibility of assignment and simplicity of coordination. However, it may be worth considering the alternative of a number of small contracts.

A. M. Gleason
H. M. Campaigne