

~~SECRET~~~~SECRET~~

22 May 1953

MEMO FOR THE FILE

SCAMP

Prof. Cairns has arranged for the following people to participate in the seminar at Los Angeles.

1 July - 31 Aug	cleared	2 months	Prof. S. S. Cairns	U. of Ill.	Topologist	ANABRANCH	
	cleared	2 months	Mr. J. C. Koken	U. of Ill.	Topologist	ANABRANCH	
		2 months	Prof. D. W. Hall	U. of Md.	Topologist		
		2 months	Prof. C. Wexler	U. of Ariz.	War time cryptanalyst		
	cleared	2 months	Prof. T. Botts	U. of Va.	Topologist, War time cryptanalyst		
15 June - 15 Sept	cleared	3 months	Prof. J. A. Ward	U. of Ky.	Algebraist		
		2 months	Prof. E. H. Hanson	N. Tex. State	War time cryptanalyst		
1 July - 31 Aug		2 months	Prof. G. A. Hedlund	Yale	Topological Groups		
		2 months	Prof. W. Karush	U. of Chicago	Eigenvalues		not cleared
3 - 24 Aug		5 weeks	Prof. T. Kapitansky	U. of Chicago	Combinatorial analysis		" "
Rest of Aug		1 week	Prof. A. A. Albert	U. of Chicago	Algebraist		
1-15 July		2 weeks	Dr. S. Ulam	Los Alamos	Monte Carlo methods		
	cleared	2 weeks	Dr. R. A. Leibler	Sandia	Probability		
1 July 31 Aug		2 months	Mrs. L. Walters	AFSA	Librarian		

Various members of SCAG have indicated they will be there part of the time.

15 June 15 Sept	3 months	Dr. C. Tompkins	I.N.A.
dates used in	short time	Dr. H. T. Engstrom	E.R.A.
	3 weeks	Prof. J. von Neumann	I.A.S.

Shannon - Adm Wenger
phoned him this morning
Sorry he can't get away
17 June 53 Z

Representatives of AFSA will be

5 weeks, July	Dr. H. Campaigne
5 weeks, July	LCDR A. M. Gleason
3 weeks, August	LCDR M. Hall

others yet to be nominated by O2 and O4.

Others

Lowell J. Paige	- UCLA	(3 weeks)
A. E. Roberts	- ERA	(less than week)
D. C. Spencer	- Princeton	(3 days)

~~SECRET~~~~SECRET~~

- 2 -

Memo for the file SCAMP.

Problems proposed as starting points for this research are:

1) Matrix algebra, particularly solving for matrices X such that $X^{-1}RX = B$ or with fragmentary A_s $X^{-1}R^sX = A_s$ or finding X and Y such that

$$X^{-1}R^sY^{-1}R^{-s} + tYR^{-t}X = B_{s,t}.$$

This is the wheel-wiring recovery problem. One method of solution is matrix projection.

2) Computations with group characters; this may be another way to recover wheel wiring.

3) Cycle structures (combinatorial topology).

4) Logical reduction of hypotheses. This is another potential way of attacking burst messages.

5) Determination of the finite geometries of a given order. This is of interest because it may be possible to solve it by matrix projection.

6) Invent a measure for security. This may be possible using information theory. Our present crude measure is in terms of minimum time of breaking; 24 hours or 5 years for example.

7) Determine what level of security is needed in a privacy system. This depends on satisfactorily solving 6), and may involve the theory of games.

cc O2T
O4
O0T
O3
Reading file

~~SECRET~~~~SECRET~~