1 NAME OR TITLE		CONCURRENCES,	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION	<u>S</u>	edman/	DATE	-	COORDINA-
2		<u></u>		V	FILE
					INFORMATIO
3	<u> </u>	<u></u>			NECESSARY
					NOTE AND RETURN
4					SEE ME
			_	-	SIGNATURE
		proved for rele suant to E.O. 13		Â	L
FROM NAME OR TITLE	NS	A-314	• • • •	1947	Lak
ORGANIZATION AND LOCATION	17	117		一步	105 4

SECTORA56994

SECRET

"ENCIPHERED MOTION" Branching Structure

Introduction:

There has been considerable interest in observational data concerning the proportion of origins, single points, and branch points of a device employing wheels stepped by enciphered motion. To this end a program was written for ATLAS II to compare the empirical results with the expectations under purely random stepping.

The probability P(i) of a branch point of multiplicity "i" for the case where there are n random stepping wheels (each of the "random" wheels steps with probability 1/2, each wheel steps independently of each other, and therefore each of the 2^{n} motion assumptions is equally likely) can be given by the following formula:

$$P(i) = {\binom{2^{n}}{i}} {\binom{1}{2^{n}}}^{i} {\binom{1}{2^{n}}}^{i} {\binom{1}{1 - \frac{1}{2^{n}}}}^{2^{n}-1}$$
(1)

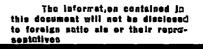
As n increases, (1) approaches $\frac{1}{e(1!)}$ as a limit.

$$P(\mathbf{i})\sim \frac{1}{\mathbf{e}(\mathbf{i}\mathbf{i})}$$
(2)

Note the expected number of origins and single points approaches the same value.

In the ATLAS program, rotor maze wirings were simulated and the motion determined for each setting of the rotors, and after stepping the rotors in accordance with the motion (the maze encipherment of the stepping

LCURED NATIONALS



SECRET

SECIE: A56,994

SECRET

pulses was carried out, etc.) a listing of the initial setting, the next four successive settings, and the 10th setting was recorded. This was done for all settings composed of core settings A, B, or C in each of the rotors stepped by the output of the maze. Examination of these runs and recognition of confluences provided additional information in that for some settings (those composed of B or C on each of the rotors stepped by the output of the maze) all possible predecessors and their immediate successors were present in the print out. 'For these settings actual enumeration would provide the number of them that were origins, single points, branch points of order 2, branch points of order 3, etc.

For example when n = 5 there are 2^5 settings which are either origins, single points, or branch points of degree two or more. We know for a certainty the character of these 32 settings since all their possible predecessors have been examined among the 3^5 initial settings.

A. The first device to be examined was a 10 wheel machine with four metric or cycle guarantee wheels and six wheels stepped by enciphered motion. Each of the latter six wheels has probability 1/2 of stepping. The following is a listing of four samples made on ATIAS. The samples differed in that the metric rotors were set to a new position before each set of runs was made. Shown also is the expected number E(i) of each kind of point for the sample observed.



The information contained in this desemont will not be disclosed in forcion nationals or their reproagateting

C J : VATIONALS

-- SEORET

,

· .

.

•

• •

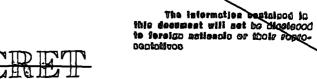
.

.

SAMPLES

REFAID: A56994

	A	B	C	D	E(i)
Origins	24	22	25	27	23.4
Single points	25	22	20	16	23.7
Double points	11	16	14	15	11.8
Triple points	3	2	2	5	3.9
Quadruplis points	1	1	3	1	1.0
Quintuple points	-	1	-	*	.2
,	64	64	64	64	64.0



SPECIAL HANDLINS REQUIRED

NOT RELEASABLE TO TOHEIGN NATIONAL

9



SECRET

• • • • •

> B. The second device to be examined was a 10 wheel machine with five metric or cycle guarantee wheels and five wheels stepped by enciphered motion. Each of these five latter wheels has probability 1/2of stepping. The following is a listing of nine samples made on ATLAS. E(i) is the expected number of branch points of multiplicity (i).

SAMPLES

	A	B	C	D	E	F	G	H	I	E(i)
Origin s	9	14	13	11	12	12	15	13	11	11.6
Single points	14	8	6	11	12	14	11	6	12	12.0
Double points	7	7	11	9	4	2	4	ш	5	6.0
Triple points	2	2	1	-	4	2	2	2	2	1.9
Quadrupl e	-	1	1	1	-	2	·	-	1	•4
points Quintuple points	-	-	-	-	-	-	-	-	1	.1
	32	32	32	32	32	32	32	32	32	32.0

Robert Sengpiehl NSA-314 28 June 1955

SPECIAL HANDLING REQUIRAD MOT RELEASAB E TO , OREIGN MATIOLION,

The information sericised in this decement will not be the te house antionals of the formation senicities