July 13, 1929.

MEMORANDUM TO Commander Strubel:

I am attaching hereto a copy of a memorandum I made under date of July 3, 1929, regarding the proposed change in the construction of cipher device, M-94, as discussed in our conversation yesterday. I would be very glad to have your opinion as to the feasibility of the proposed scheme, and whether or not you would like to perform some joint experiments.

William F. Friedman,
Code & Cipher Section, OCSO.

Proposal for Modifying Cipher Device M-94.

1. This proposal contemplates a change from disks to sliding strips, each to be long enough to accomodate an alphabet of 52 letters (a repeated 26-letter alphabet).

2. The strips, instead of being flat, to be square prisms of brass, wood, bakelite, etc. (any nonwarping material), a cross section of which would be approximately 1/4" square. Prisms approximately 14" long would serve nicely. They may be hollow in the case of brass or metal prisms WFF

3. A set would consist of 25 prisms to correspond with present 25 disk device. Each prism to be numbered as is the case at present with the disks.

4. Each side or face of a prism to bear a mixed alphabet, all alphabets to be different, making the 25 prisms equivalent to a set of 100 single-alphabet strips. Thus the original 25-alphabet system becomes a hundred-alphabet system without any increase in apparatus size, etc.

5. Each alphabet on a given prism to be labeled a, b, c, or d. (Alphabets 1a, 1b, 1c, 1d would be entirely unrelated among themselves, and unrelated to any other alphabet of any other rod, as indicated under 4.)

6. Use key words or phrases as at present, developing a key of 25 numbers, as at present.

7. In setting up, the "side up" on each prism would be indicated

by a subsidiary indicator developed from the key. An example:

Divide up the normal alphabet into 4 sections, making the respective total frequencies of these sections as nearly equal as possible:

ABCDE	FGHIJKL	MNOPQR	STUVWXYZ
a	b	c	d

A key letter receives the indicator a, b, c, or d, depending on which section it falls into.

Choosing the key word REPUBLICAN, and deriving the numerical key:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Key:	R	E	P	U	B	L	I	C	A	N	R	E	P	U	B	L	I	C	A	N	R	E	P	U	B
	20-	8	-17-	23-	3-	15-	11-	6	-1	-15-	21-	9	-16-	24-	4	-14-	12-	7	-2	-16-	22-	10-	19-	5	
	c-	a-	c	-d	-a-	b-	b	-a	-a	- c-	c	-a	-c	-d	-a	-b	etc.								

A refinement would be to use a different sequence of a, b, c, d for the 2nd, 3rd... repetition of the key word proper.

8. The foregoing is only an example. Many other methods of indicating a completely systematized-random arrangement of indications of "side up" could be used.

9. It is possible to use a different set-up as regards the "side up" for different messages, even though the same numerical key is employed. Thus, assume that the first five numbers of the key are 21-4-17-6-12. For one message the combination of "sides up" might be 21a-4c-17a-6d-12b; for another message it might be 21c-4d-17b-6c-12a, etc. Various methods of indicating these changes may be devised.

10. One step further: the changes in "side up" might be made for successive lines of 25 letters within a message. Considering only the first five prisms the number of permutations of the four sides is 4^5, or 256. This would allow much room for variation and would undoubtedly considerably increase the difficulty of analysis. Only practical considerations of facility in employment place a limit upon the variability applicable within a message or between successive messages.

11. The prisms might be skillfully hinged at the middle, allowing them to be folded double, decreasing the storing size to half-length. Or they might be hinged to fold triple, or quadruple, etc. This is important for military field use.

William F. Friedman

William F. Friedman,
O.C.S.O.

July 3, 1929,
Washington, D.C.

July 1

Cm . Kingman says Na has entered patent on vertical continuous strip form (issued to Mr Farrar). It is being held up as "secret". They are proceeding to patent leather form. We may proceed to patent our improved form.

May 15, 1935

F.