

rc

February 24, 1933.

Mr. George A. Graham,
Signal Corps Laboratories,
Fort Monmouth,
N. J.

Dear Graham:-

The attached sketch (modification of wiring diagram on blue print ES-B-1177A) shows what I wish to do. I see no reason why it won't work. I have tried it with temporary conductors set up by fastening clips to the upper and lower homologous contacts of the disc transmitter. By introducing the second tape transmitter to vary the short-circuiting of the left and right contacts of the disc transmitter, two revolving tapes of unequal length can be used to step together and produce a single, very long resultant key. One of the indirect results is to speed up encipherment or decipherment, because the cipher wheel need not go through an average displacement of 13 steps for each letter. If you will try this scheme out you will soon see what I mean. The cryptographic security is not materially reduced by this modification.

I hope you can send me a second transmitter soon. If you try this out, let me know your reaction.

Very truly yours,

William F. Friedman

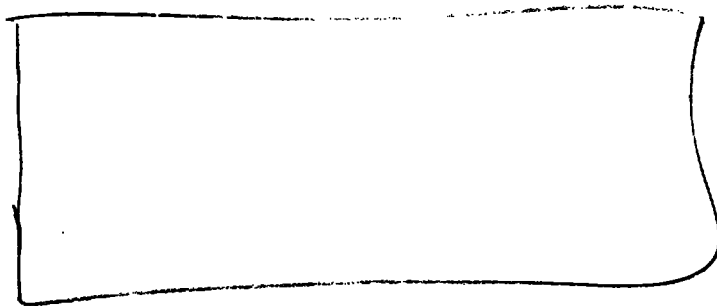
Enc.
Sketch

W. F. Friedman
DATE 2-25-33
SIC PC

In the first place, the ~~use~~ use of key tapes is very much simplified, without reducing the cryptographic security to any appreciable degree. In the second place, as an indirect result, the speed of encipherment or decipherment is increased ~~also~~ not by any speeding up of the driving mechanism, but by virtue of the fact that the ~~cipher wheel~~ ~~control~~ circuit for stopping the cipher wheel can now be closed by any one of several permutations of pins on the periphery of the wheel and the first ^{so} operative permutation ~~is~~ that presents itself to the disc transmitter levers will stop the ~~cipher~~ wheel. Thus, the angular displacements of the cipher wheel become much shorter between successive encipherments or decipherments, with the result that the operator does not have to wait very long between key depressions ^{before} ~~to~~ ~~wait~~ for the wheel ~~to have~~ has come to a halt.

(1) If a second tape transmitter is added in the present circuit for ~~controlling~~ controlling the displacements of the cipher wheel, then two unequal-length, circular tapes may be employed to yield a single resultant cipher key of great length. For example, a tape of 1000 characters operating coincidentally with one of 999 characters will yield a ^{potential} single resultant key of 999,000 characters in length.

(2) The circuits controlled by the above-mentioned secondary ^{tape} transmitter can be introduced as shown in the ~~accompanying~~ sketch below, which represents a portion of the wiring diagram on blue print ES-13-1177-A, modified to the extent under discussion.



(3) By this modification in design, two important objects are accomplished.

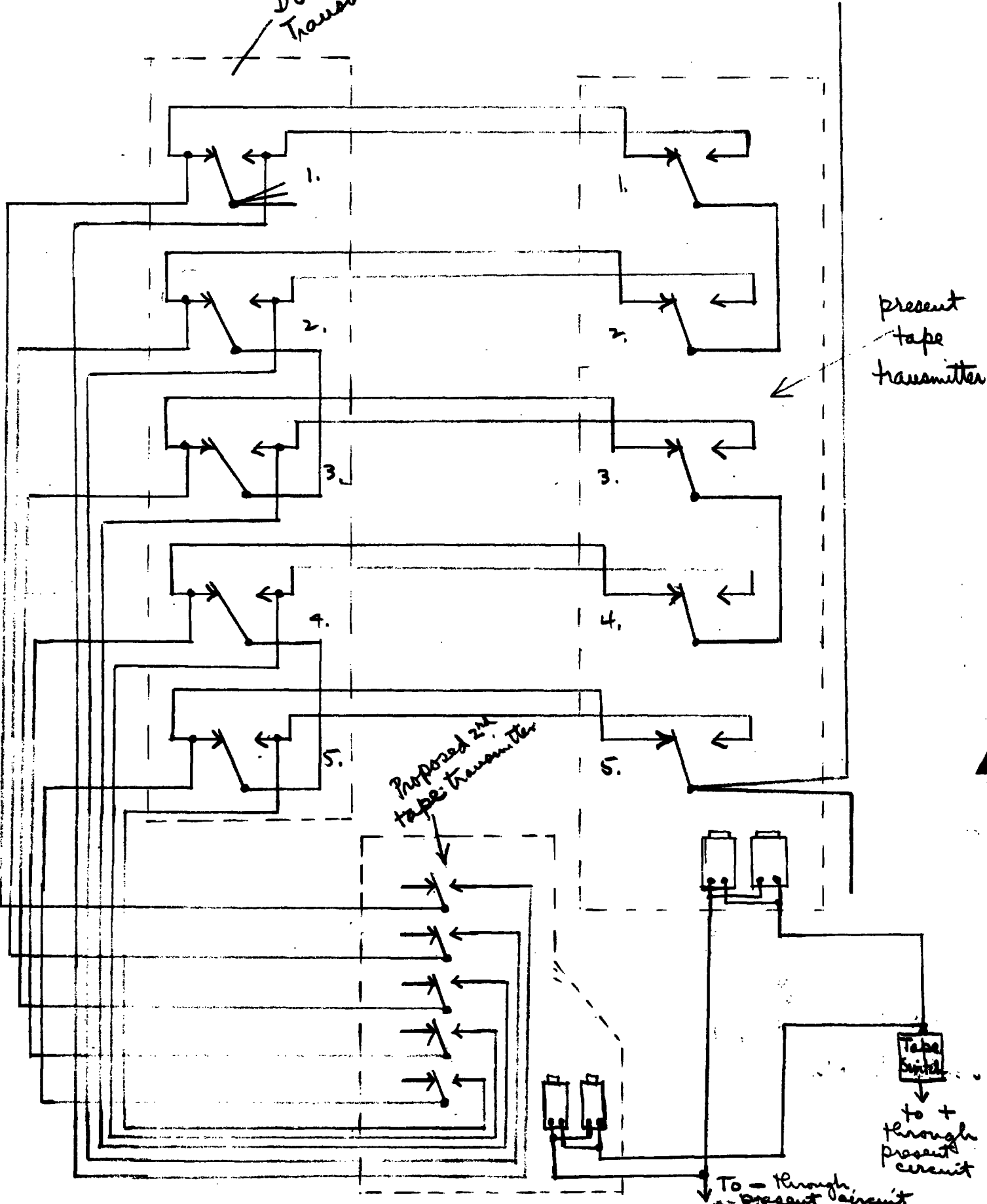
Disc Transmitter

present tape transmitter

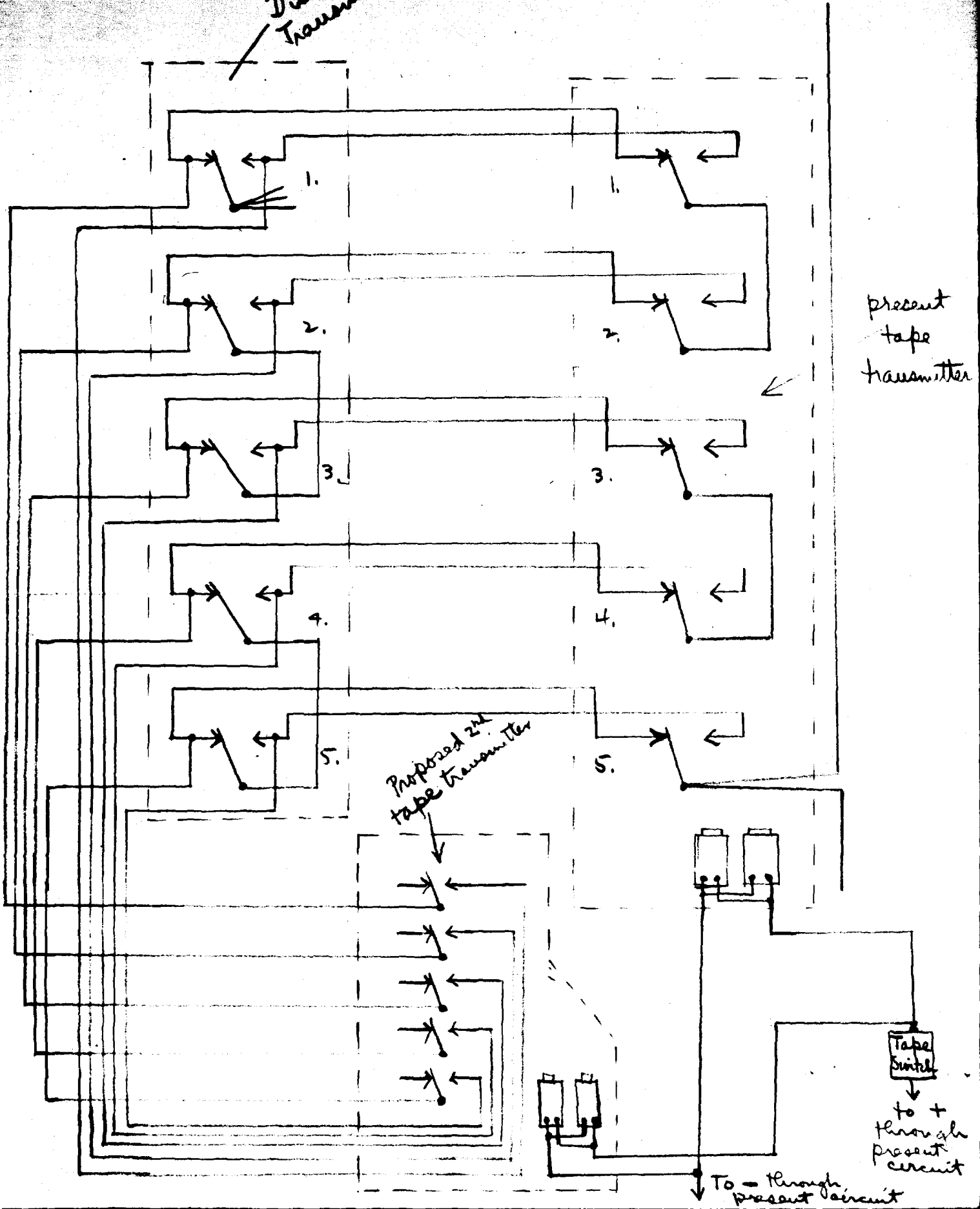
Proposed 2nd tape transmitter

Tape Switch
to +
through present circuit

To - through present circuit



*Diss
Transmitter*



*present
tape
transmitter*

*Proposed 2nd
tape transmitter*

Tape Switch
to +
through
present
circuit

*To - through
present circuit*

- ⊖ + + +

