

Invention of a Cipher System and Apparatus for Plural-Unit-
Code Telegraph Printer.

1. As an example of a plural-unit-code telegraph printer, I will select the teletype or similar device, wherein the individual characters to be transmitted are represented by permutations of electrical spacing and marking impulses taken in groups. In the teletype system the groups are all of equal length, five units, according to the Baudot or 5-unit code of 32 permutations; but the groups may be of irregular lengths, as for example in the recently developed radio-printer of the IBM Corp., which uses some 42 permutations of 2 to 6 units. In the teletype system the characters are "set up" on 5 relays, and a distributor sends the marking ^{and spacing} impulses distributed in time; in the IBM system the characters are set up on 6 relays, and an electronic system ^{distributes} sends the marking and spacing impulses, ~~distributed in time.~~

2. For cipher purposes it is ^{possible to employ a system} ~~necessary to disguise the distribution~~ involving changing marking intervals into spacing intervals, ~~or vice versa~~ ^{of the marking and spacing intervals.} In the old AT&T system this is done by means of two interacting key-tape transmitters using 5-unit-code perforated tapes; in the IT&T system this is done by means of 10 cam wheels which interact in pairs to influence the individual units of the characters to be transmitted.

Thus, by changing the card inserted there would be, in a single column, 7 keying characters. For example, in the card shown in Fig. 1 there are in Column 1, holes in positions 9, 6, 7, 6, 5, and 4 were effective, the keying character is representable by the number effective, then the keying character is representable by the figures 9, 6, 7, 6, 5, and 4, and 3 were effective, which would give a different cipher result.

3. In the present system I propose to use one or more sets of ^{80-column} Hollerith cards. ^{In these cards I perforate} ~~bearing~~ cipher keying perforations in ⁷⁵ ~~80~~ columns, ^{and I leave} ~~and other~~ ⁵⁷ columns for card-identifying purposes, ^{so that the cards may be arranged} ~~thus affording a maximum of 17,676~~ and rearranged automatically by means of a card sorter whenever desired. ~~cards in a set; or, if more cards are desired in a set, one need only reduce~~ ~~the number of columns devoted to cipher-keying purposes.~~

4. These cipher-keying perforations consist of holes through which sensing brushes can make contact with a contact roller and set up ^{ciphering} circuits to be described. Let us consider a card as follows:

Fig. 1

In each column there are 12 loci for holes, and in a given key card the holes are distributed at random throughout the 1st, ⁷⁵ columns. In the IBM printer there are 6 relays, so that a column of 12 loci can be used ^{radio-} merely by shifting the initial point of each grouping to the left or right. ^{if the cards are inserted in the cryptographic mechanism and one advanced in the direction shown in Fig. 1} for 7 key letters. With ⁷⁵ columns, therefore there can be $75 \times 7 = 525$ keying characters. And a set of 1000 cards will provide $525 \times 1000 = 525,000$ keying characters.

*columns at a time
until all 75
columns of plain
characters have
been employed,
and then feed in
the next card.
Suppose also that means are provided*

5. Now suppose means are provided to feed the cards into the
to orient the card from left to right, and to advance the card one step (or
cryptograph, one card at a time from the pile, ^{and} ^{to} cause the keying-

character units to interact with the plain-text character-units, in a manner

similar to that used in AT&T or IT&T systems, namely, two similar signs give
a spacing unit, and two dissimilar signs give

^ a marking unit (+ + → -, - - → -, + - → +, and - + → +). This sort of a system

of interaction is, of course, reciprocal and at the other end of the line, if an

identical pack of keying cards is inserted and started at the identical keying

character as at the enciphering end, decipherment will take place correctly.

6. Now suppose also that two packs of cards are used, these to interact

as in the AT&T case of two cipher-key transmitters. Suppose one pack has 1000

cards, the other 999. The first deck has ^{525,000} ~~560,000~~ keying characters, the other

^{524,475}
~~75~~ x 7 x 999 = ~~559,440~~ characters. Their interaction will yield a potential

^{525,000} x ^{524,475}
key of ~~560,000~~ x ~~559,440~~ = characters.

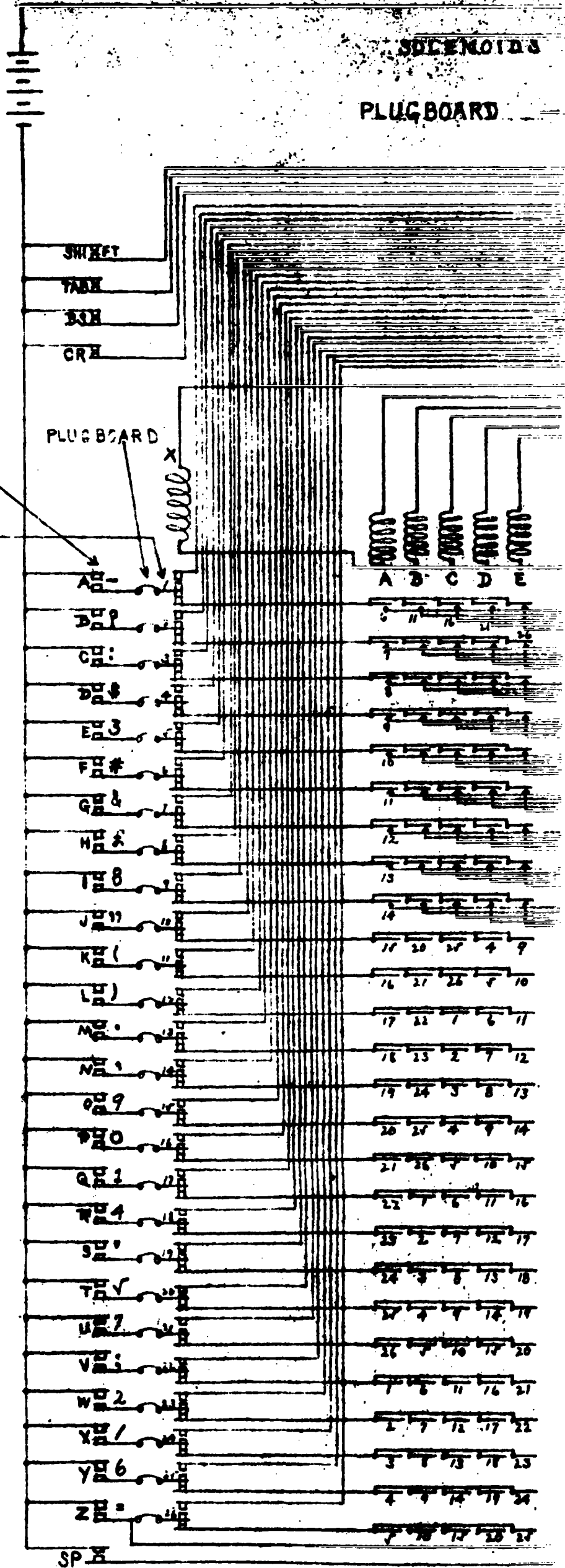
7. The circuits:

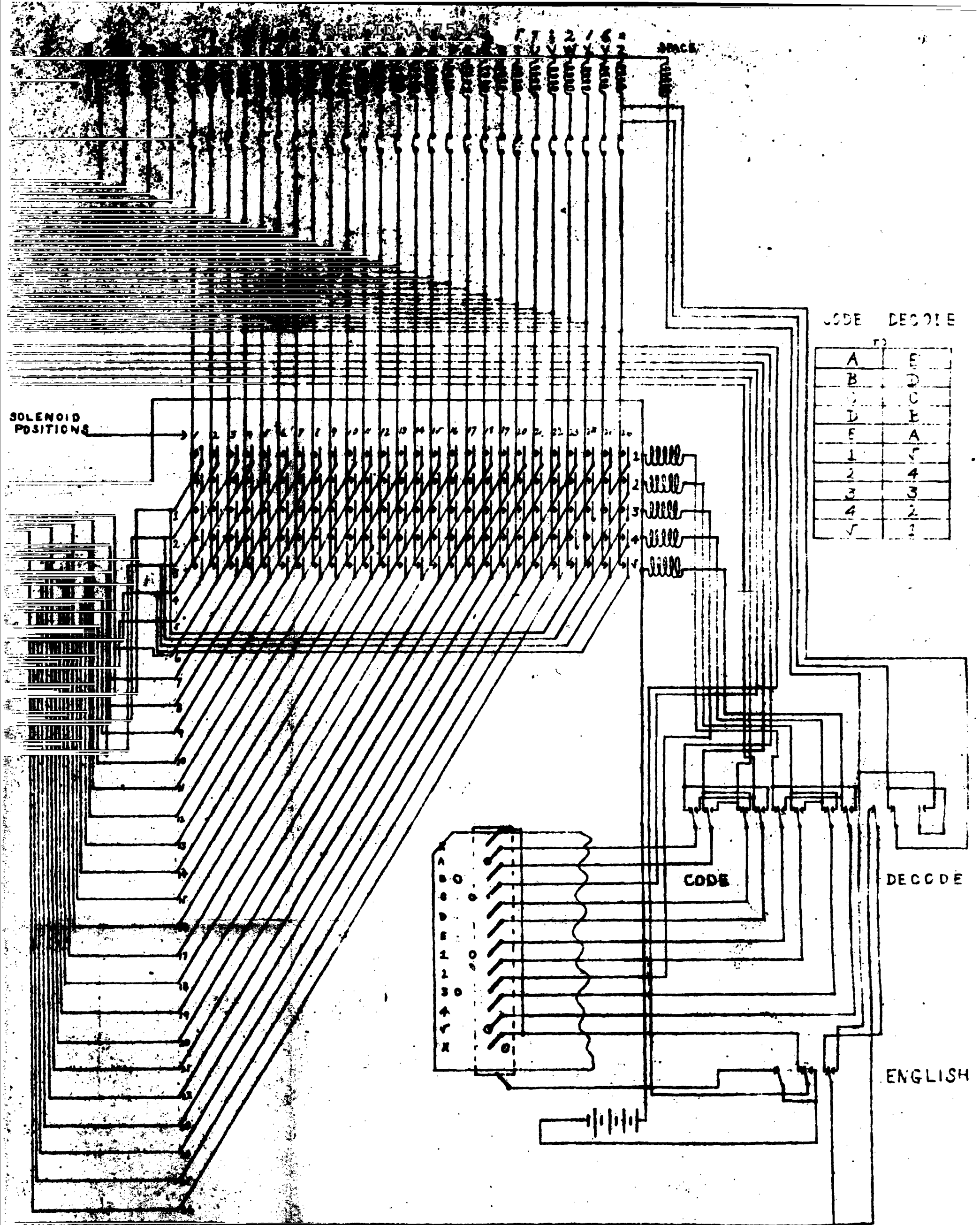
a. For 1 pack of cards, as in Part 5

b. For two packs of cards, as in Par. 6

A					B					C					D					E					X	
1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5		
A	F	E	D	C	B	K	J	I	H	G	P	O	N	M	L	J	T	S	R	Q	Z	Y	X	W	V	A
B	G	F	E	D	C	L	K	J	I	H	Q	P	O	N	M	V	U	T	S	R	A	Z	Y	X	W	B
C	H	G	F	E	D	M	L	K	J	I	R	Q	P	O	N	W	V	U	T	S	B	A	Z	Y	X	C
D	I	H	G	F	E	N	M	L	K	J	S	R	Q	P	O	X	W	V	U	T	C	B	A	Z	Y	D
E	J	I	H	G	F	O	N	M	L	K	T	S	R	Q	P	Y	X	W	V	U	D	C	B	A	Z	E
F	K	J	I	H	G	P	O	N	M	L	U	T	S	R	Q	Z	Y	X	W	V	E	D	C	B	A	F
G	L	K	J	I	H	Q	P	O	N	M	V	U	T	S	R	A	Z	Y	X	W	F	E	D	C	B	G
H	M	L	K	J	I	R	Q	P	O	N	W	V	U	T	S	B	A	Z	Y	X	G	F	E	D	C	H
I	N	M	L	K	J	S	R	Q	P	O	X	W	V	U	T	C	B	A	Z	Y	H	G	F	E	D	I
J	O	N	M	L	K	T	S	R	Q	P	Y	X	W	V	U	D	C	B	A	Z	I	H	G	F	E	J
K	P	O	N	M	L	U	T	S	R	Q	Z	Y	X	W	V	E	D	C	B	A	J	I	H	G	F	K
L	Q	P	O	N	M	V	U	T	S	R	A	Z	Y	X	W	F	E	D	C	B	K	J	I	H	G	L
M	R	Q	P	O	N	W	V	U	T	S	B	A	Z	Y	X	G	F	E	D	C	L	K	J	I	H	M
N	S	R	Q	P	O	X	W	V	U	T	C	B	A	Z	Y	H	G	F	E	D	M	L	K	J	I	N
O	T	S	R	Q	P	Y	X	W	V	U	D	C	B	A	Z	I	H	G	F	E	N	M	L	K	J	O
P	U	T	S	R	Q	Z	Y	X	W	V	E	D	C	B	A	J	I	H	G	F	O	N	M	L	K	P
Q	V	U	T	S	R	A	Z	Y	X	W	F	E	D	C	B	K	J	I	H	G	P	O	N	M	L	Q
R	W	V	U	T	S	B	A	Z	Y	X	G	F	E	D	C	L	K	J	I	H	Q	P	O	N	M	R
S	X	W	V	U	T	C	B	A	Z	Y	H	G	F	E	D	M	L	K	J	I	R	Q	P	O	N	S
T	Y	X	W	V	U	D	C	B	A	Z	I	H	G	F	E	N	M	L	K	J	S	R	Q	P	O	T
U	Z	Y	X	W	V	E	D	C	B	A	J	I	H	G	F	O	N	M	L	K	T	S	R	Q	P	U
V	A	Z	Y	X	W	F	E	D	C	B	K	J	I	H	G	P	O	N	M	L	U	T	S	R	Q	V
W	B	A	Z	Y	X	G	F	E	D	C	L	K	J	I	H	Q	P	O	N	M	V	U	T	S	R	W
X	C	B	A	Z	Y	H	G	F	E	D	M	L	K	J	I	R	Q	P	O	N	W	V	U	T	S	X
Y	D	C	B	A	Z	I	H	G	F	E	N	M	L	K	J	C	R	Q	P	O	X	W	V	U	T	Y
Z	E	D	C	B	A	J	I	H	G	F	O	N	M	L	K	T	S	R	Q	P	Y	X	W	V	U	Z

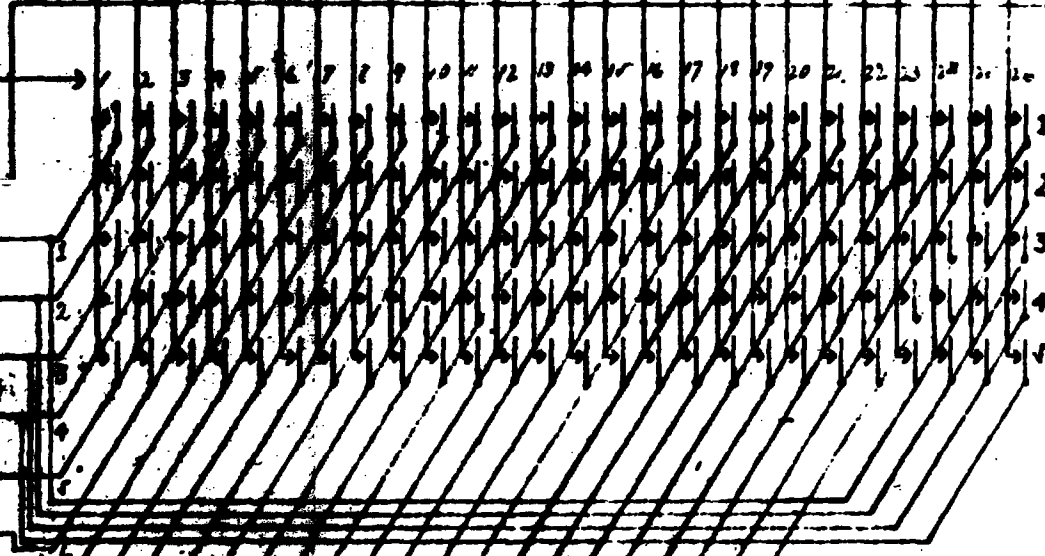
EXAMPLE OF ONE ALPHABET - TOTAL OF FACTORIAL 26 MAY BE USED - CAM SWITCHES AND CORRESPONDING SOLENOID POSITIONS MUST CORRESPOND - EG. CAM SWITCH A POSITION 17 SOLENOID A POSITION 17. USE TWO WIRE PLUGS TO REDUCE TO 26 PLUGGINGS MAXIMUM.





CODE DECODE	
	73
A	E
B	D
C	C
D	B
E	A
1	5
2	4
3	3
4	2
5	1

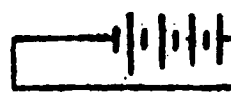
SOLENOID POSITIONS



CODE

DECODE

ENGLISH



TODD/A

DEPARTMENT OF COMMERCE
UNITED STATES PATENT OFFICE
WASHINGTON

June Eighteenth 1940

William F. Friedman:

Sir:

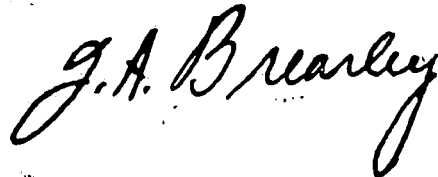
Your APPLICATION for a patent under the Act of 1883
as amended, April 30, 1928, for an IMPROVEMENT
IN
CRYPTOGRAPHIC DEVICE

filed Oct. 19, 1939, has been examined and ALLOWED.

The Letters Patent will be forwarded in due course of
business.

Additional copies of specifications and drawings will
be charged for at the following rates: Single copies, uncerti-
fied, 10 cents each. The money should accompany the order.

Respectfully,



Chief Clerk.

Edgar H. Snodgrass
& Charles A. Rowe
c/o The Chief of the Air Corps.
Munitions Bldg.
Washington, D. C.

Invention of a Cypher System and Apparatus for plural-unit-code telegraph printer.

1. As an example of a plural-unit-code telegraph printer I will select the teletype or similar device, wherein the individual characters to be transmitted are represented by permutations of electrical spacing and marking impulses taken in groups. In the teletype system the groups are all of equal length, five units according to the Baudot or 5-unit code, but the groups may be of irregular lengths, as for example in the recently developed radio-printer of the IBM Corp, which uses some 42 permutations of 2 to 6 units. In the teletype system the characters are "set up" on 5 relays, and a distributor sends the marking impulses distributed in time; in the IBM system the characters are set up on 6 relays, and an electronic system sends the marking impulses distributed in time.

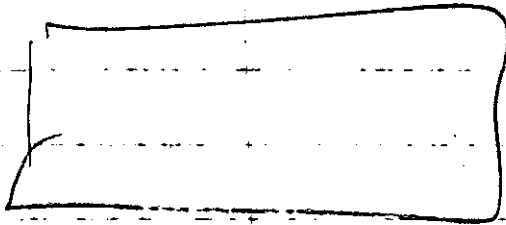
2. For cypher purposes it is necessary

to disguise the distribution of the marking and spacing intervals. In the old AT&T system this is done by means of two interacting key-tape transmitters using 5-unit-code perforated tapes, in the IT&T system this is done by means of 10 cam wheels which interact in pairs to influence the individual units of the characters to be transmitted.

3. In the present system I propose to use ^{or more} one ~~set~~ sets of Hollerith tabulating cards bearing ^{cipher keying} perforations in ~~columns~~ ~~80~~ 80 columns, leaving 3 columns for card-identifying purposes, thus affording a maximum of 17,676 cards in a set; or, if more cards are desired in a set, one need only reduce the number of columns devoted to cipher-keying purposes. ~~Let us assume for the moment that two sets of cards are used, one containing 1000 cards, the other 999.~~

4. These cipher-keying perforations

consist of holes through which sensing brushes can make contact with a contact roller and set up circuits to be described. Let us consider a card as follows:



In ^{each} column there are 12 loci for holes, and in a given key card the holes are distributed at random throughout the 1st 80 columns. In the IBM printer there are 6 relays, so that a column of 12 loci can be used for 7 key letters. With 80 columns therefore there can be $80 \times 7 = 560$ keying characters. And a set of 1000 cards will provide $560 \times 1000 = 560,000$ keying characters.

5. Now suppose means are provided to feed the cards into the cryptograph, one card at a time from the pile and to cause the keying-character units

$$\begin{array}{r}
 560 \\
 999 \\
 \hline
 560 \\
 \hline
 59940 \\
 4995 \\
 \hline
 559440
 \end{array}$$

4
45
4

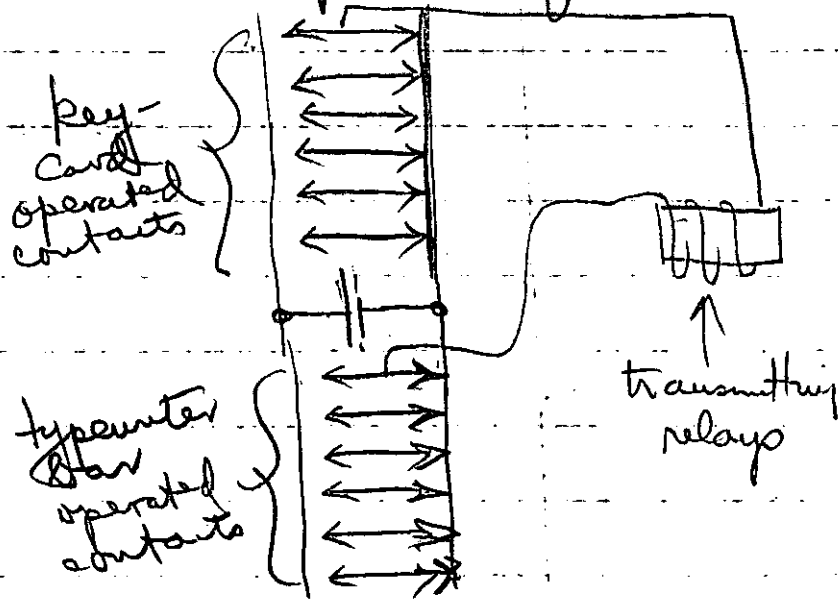
to interact with the plain-text character-units, in a manner similar to that used in AT+T or IT+T systems, namely, two similar signs give a spacing unit, two dissimilar signs give a marking unit. ($++ \rightarrow -$, $-- \rightarrow -$, $+ - \rightarrow +$, and $- + \rightarrow +$) This sort of a system of interaction is of course reciprocal and at the other end of the line, if all identical parts of ^{keying} cards is inserted and started at the identical keying character as at the enciphering end, decipherment will take place correctly.

Now suppose also that two packs of cards are used, these to interact, as in the AT+T case of two cipher-key transmitters. Suppose one pack has 1000 cards, the other 999. The first deck has 560,000 keying characters, the other $80 \times 7 \times 999 = 559,440$ characters. Their interaction

will yield a potential key of
 $560,000 \times 559,440 =$
 characters.

7. The circuits:

a. For 1 pack of cards



6 relays

June 14, 1936

b. For two packs of cards

