

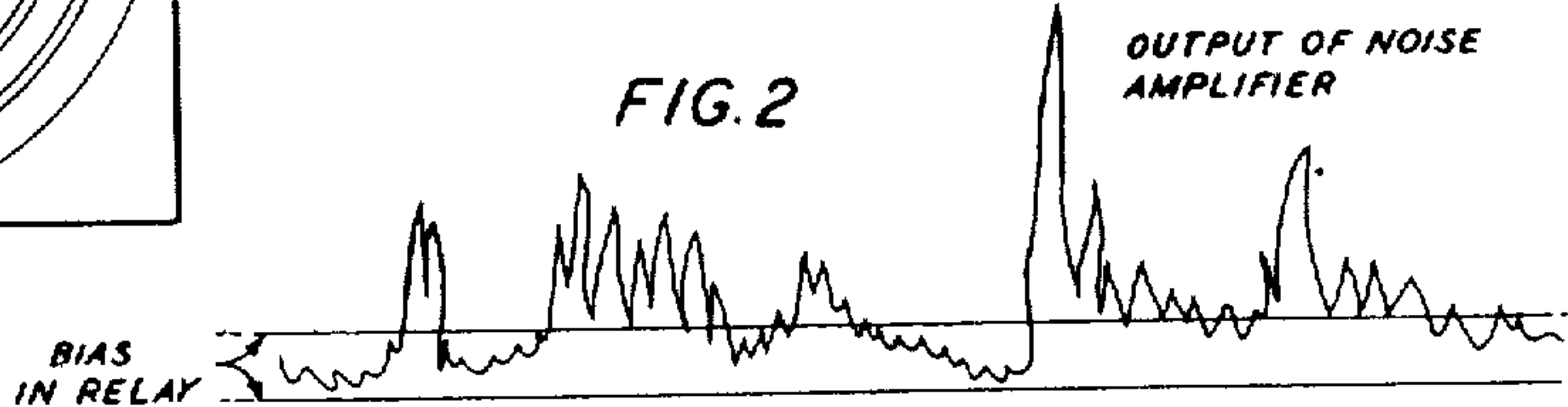
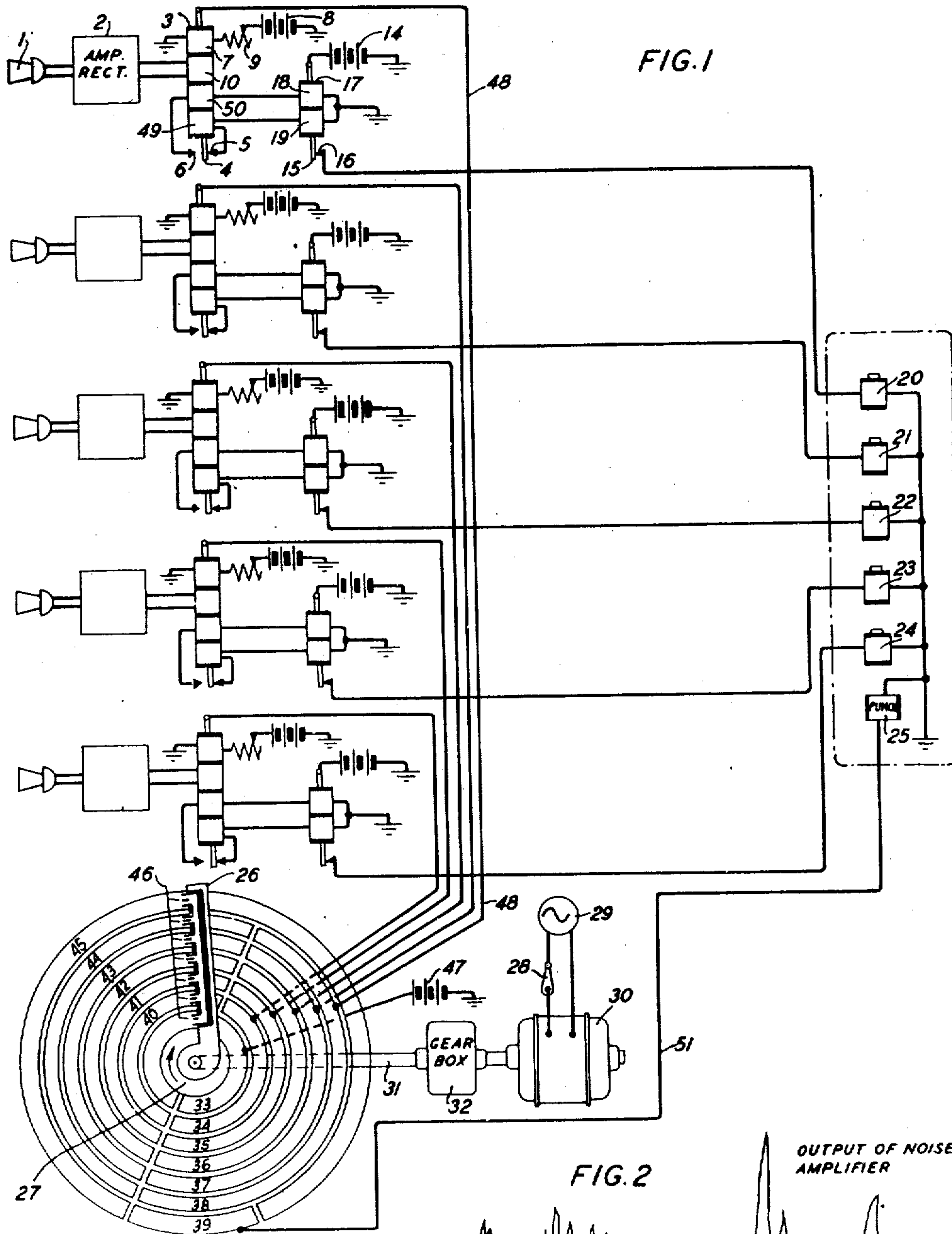
Aug. 20, 1946.

R. D. PARKER

2,406,032

TELEGRAPH SIGNAL ENCIPHERING MECHANISM

Filed Nov. 23, 1942



INVENTOR
R. D. PARKER
BY John E. Cassidy

ATTORNEY

UNITED STATES PATENT OFFICE

2,406,032

TELEGRAPH SIGNAL ENCIPHERING
MECHANISM

Ralzemond D. Parker, Brooklyn, N. Y., assignor to
Bell Telephone Laboratories, Incorporated,
New York, N. Y., a corporation of New York

Application November 23, 1942, Serial No. 466,645

9 Claims. (Cl. 178—22)

1

This invention relates to secret telegraph systems and particularly to the full automatic production of a purely random key tape for use in enciphering and deciphering permutation code teletypewriter signals.

In a system of secret telegraphy presently known in the art, in connection with which this invention may be used, the enciphered code elements as transmitted are the resultants of the elements of the regular permutation code signals modified by the elements of what is known in the art as a key tape. The key tapes are prepared and supplied to each terminal in advance. The key tapes at each terminal are identical and are operated in synchronism. Each character element of the enciphered code may be made marking or spacing by suitable mechanism, depending upon whether each element of the regular permutation code representing the character and the corresponding element as randomly punched in the key tape are alike or unlike.

Previous proposals for making random ciphering or key tapes or equivalent devices have followed two general procedures.

In accordance with one procedure, tapes have been prepared at random manually by operators. This method has two undesirable features. First, it is laborious and time consuming. Second, it seems doubtful whether a human operator can actually prepare a mathematically random tape and the deviation from randomness may be such as to aid unauthorized parties in deciphering messages. In any case, the effort to make the tape random increases the arduousness of the task and adds a mental strain to the work.

In accordance with the second procedure, key tapes have been prepared mechanically. Mechanical devices for producing random key tape, however, are complex and expensive. As a result, few, if any, such devices have been suitable for or applied to the making of key tape. The invention herein represents an improvement over presently known mechanical devices for the preparation of key tapes. The mechanism of this invention is relatively simple and inexpensive to produce and to operate. With properly chosen noise sources the resultant key tape produced by the invention herein should be perfectly random. By this is meant that when a sufficient number, say one thousand characters, are punched in a tape by means of the mechanism described herein it should be found by actual count to contain substantially equal numbers of all of the thirty-two possible characters provided in a five-element permutation code.

2

An object of the invention herein is the provision of improved means for and methods of producing random key tape for use in enciphering and deciphering permutation code telegraph signals. Another object of the invention herein is to simplify and cheapen the mechanism required to produce purely random key tape.

A feature of the invention herein is the control of each of the punch selecting magnets of a permutation code tape perforator by the randomly occurring noise in a separate source of noise for each punch selecting magnet. A further feature of the invention herein is the controlling of the operation of each of the punch selecting magnets of a multielement permutation code tape perforator by means of a separate polar relay controlled by a separate amplifier-rectifier connected to a separate source of randomly occurring noise.

These and other features of the invention will become apparent from the following description when read with reference to the associated drawing in which:

Fig. 1 shows the mechanism of this invention; and

Fig. 2 shows a diagram used in explaining the invention.

General description

Fig. 1 shows five amplifier-rectifiers indicated by rectangles at the left of the drawing. The input of each amplifier-rectifier is coupled to a different source of random noise by means of an independent receiver. The irregular outputs of amplifiers arranged so that the gain is so high that tube and resistance noise is great may be coupled to a rectifier without employing a receiver if desired. The rectified noise currents from each of the five noise sources control the operation of an individual polar relay. The armature of each of the polar relays assumes one or another of its two positions depending upon the intensity of the noise. It is locked in engagement with one or the other of its two contacts depending upon the position it has assumed, under the control of battery supplied once per punching cycle to either of two locking windings on the polar relay through the segments of a rotary distributor. Each of the five polar relays controls the operation of a second polar relay which, in turn, controls the energization of an individual punch selecting magnet in the tape perforator. The selecting magnets of the perforator will control their respective punches so that corresponding positions in a key tape will be

punched or remain unpunched, depending upon the position assumed by the armature of each of the corresponding relays. The punch perforating magnet associated with the five selecting magnets will be energized once for each rotation of the distributor arm after the punches have been set in position to operate those of the five punches which have been set in the punching position by the selecting magnet.

Detailed description

At the left of the drawing each receiver, such as 1, is coupled in any convenient manner to a separate source of random noise. The source of noise may be any convenient source, such as the noise produced by static in a radio receiver, subject, however, to requirements explained hereinafter. The receiver 1 is coupled to an amplifier-rectifier 2. The rectified output of the amplifier is supplied to winding 10 of relay 3 to control the operation of its armature 4 between its opposed contacts 5 and 6. A biasing current is supplied over a circuit extending from ground, through battery 8, variable resistance 9 and the winding 7 of relay 3 to ground. The magnitude of the current is adjusted by means of variable resistance 9 so as to maintain the armature 4 of relay 3 in engagement with each of its two contacts 5 and 6 approximately one-half of the time.

Fig. 2 is a current versus time graph. The irregular line therein simulates the output current of a noise amplifier-rectifier, such as amplifier-rectifier 2 when connected to a source of noise suitable for use with this invention. This source of noise might be an amplifier adjusted to have such a high gain that tube and resistance noise is very noticeable in its output. The horizontal line in Fig. 2 indicates the magnitude of the biasing current in winding 7 of relay 3 relative to the rectified noise current in winding 10. A suitable source of noise for the purpose of this invention is one in which the variations above and below a fixed level fluctuate rapidly and are approximately equal in duration. Each source 1 may be selected to be of a different type of noise, for example, one source may be a rapidly operated typewriter, another static from a receiver, another a musical instrument, etc. In every case best results will be obtained by adjusting the amplification until the noise from the source results in approximately equal numbers of marking and spacing conditions. Reference to Fig. 2 indicates that the magnitude of the current output of a noise amplifier exceeds the magnitude of the biasing current about one-half the time. Fig. 2 is intended to exemplify a suitable rectified noise current pattern and a biasing current of proper magnitude with relation to the pattern of the noise current.

The effects of the biasing current and of the noise amplifier output current in windings 7 and 10 of relay 3 are arranged to oppose each other so that each effect tends to actuate the armature 4 of relay 3 in the opposite direction. If it is assumed that the effect of the biasing current in winding 7 tends to actuate the armature 4 of relay 3 to engage with contact 5 and that the effect of the output current of the noise amplifier in winding 10 of relay 3 tends to actuate the armature 4 of relay 3 to engage with contact 6, it is apparent that the armature will engage each contact approximately one-half the time.

When switch 28 is closed power is supplied from power source 29 to motor 30. Motor 30 is coupled

to drive shaft 31 through gear box 32. When motor 30 rotates the arm 26 of rotary distributor 27 is rotated. On the face of the distributor 27 there is a continuous conducting ring 33 to which is connected a ground source of battery 47. On the face of the distributor there are also five segmented rings comprising conducting segments 34 to 39, inclusive, and non-conducting segments 40 to 45, inclusive. As the brush arm 26 rotates current is supplied during a portion of its rotation by means of interconnected conducting brushes 46 from ring 33 to segments 34 to 39, inclusive, simultaneously. When the brushes 46 are in position to bridge the gap between ring 33 and segment 38, a circuit may be traced from ground, through battery 47, ring 33, brushes 46, segment 38 and conductor 48 to armature 4 of relay 3. Depending upon whether or not the effect in winding 10 of relay 3 of the output current of the noise amplifier 2 is at the moment of sufficient magnitude to preponderate over the effect of the biasing current in winding 7 of relay 3, armature 4 of relay 3 will be in engagement with either of its contacts 5 or 6. If the armature 4 is in engagement with contact 5 the circuit extends through winding 49 of relay 3 and winding 19 of relay 17 to ground, operating the armature 15 of relay 17 to engage contact 16. If the armature 4 is in engagement with contact 6 the circuit extends through contact 6, winding 50 of relay 3 and winding 18 of relay 17 to ground, operating the armature 15 of relay 17 toward the left to disengage from contact 16. When current flows through winding 49 of relay 3 armature 4 is locked in engagement with contact 5. When current flows through winding 50 of relay 3 armature 4 is locked in engagement with contact 6. The armature 4 of relay 3 remains locked to either contact 5 or 6 while brush 46 traverses segment 38. As a result of this, armature 15 of relay 17 will be maintained in one or the other of its two positions while brush 46 traverses segment 38. If the armature 15 of relay 17 is in engagement with contact 16 a circuit may be traced from ground, through battery 14, armature 15 and contact 16 of relay 17 and through the winding of selector magnet 20 to ground, energizing the selector magnet. When the winding of the selector magnet 20 is energized its associated punch is set in the perforating position. The selector magnet could of course control the operating element of some other form of recording device as well as punched tape such as a magnetized tape or disc.

Each of punch selecting magnets 21 to 24 will be controlled simultaneously in the same manner as described for punch selecting magnet 20 by means of corresponding independent noise sources, amplifier-rectifiers, rotary distributor segments and relays as shown on the drawing.

As brush 46 sweeps over segment 39 a circuit is established from ground, through battery 47, ring 33, brush 46, segment 39, conductor 51 and the winding of punch perforating magnet 25 to ground, operating the perforating mechanism. Each of the punches that has been set in the punching position will perforate the tape in corresponding positions and the tape will be moved into the succeeding position in a well-known manner. Rotary arm 26 rotates clockwise as indicated by the arrow. Segment 39 subtends a smaller arc than the other conducting segments 34 to 38 and brush 46 engages it later than it engages segments 34 to 38 to provide time for the setting of the punches before magnet 25 is energized.

5

The armature 4 of relay 3 will remain locked in position in engagement with either contact 5 or contact 6 until the rotary arm 26 has swept brush 46 onto the non-conducting segments 44. If magnet 20 is energized it will remain energized for substantially the same interval. When brush 46 sweeps onto the non-conducting segments, relay 4 will be unlocked. The armature 4 of relay 3 will then be free to assume position for the next character.

Each of the other circuits controlling selecting magnets 21 to 25 will be released simultaneously in a corresponding manner.

What is claimed is:

1. In a mechanism for producing key tape for enciphering permutation code telegraph signals a plurality of means for punching a tape in a plurality of positions, a plurality of sources of noise and a plurality of means individually responsive to variations in the intensity of noise in said plurality of sources for controlling said punching means individually.

2. In an enciphering mechanism for controlling the enciphering of a plurality of elements of a multielement permutation telegraph code combination a plurality of separate independent sources of noise, a plurality of noise receiving means connected individually to said sources and means responsive to the variation in the noise in said sources for controlling variations in the individual elements of said permutation code combination.

3. In a mechanism for producing key tape for enciphering permutation code telegraph signals a plurality of separate independent sources of noise, a plurality of noise receivers connected individually to said sources, a plurality of amplifier-rectifiers responsive individually to said receivers and a plurality of means responsive to said amplifier-rectifiers for determining the character of individual elements in a particular code combination recorded in said key tape.

4. In an enciphering mechanism for preparing key tape for enciphering permutation code telegraph signals a number of selecting mechanisms corresponding to the number of elements in a particular permutation code, means for controlling said elements comprising an amplifier-rectifier individual to each of said elements and means for controlling said rectifiers individually

6

in response to variations in noise in individual noise sources.

5. In a mechanism for manufacturing key tape for enciphering permutation code telegraph signals a polar relay, means responsive to variations in noise for controlling the operation of said relay, a pair of opposed contacts on said relay and a second control means comprising a biasing winding on said relay for maintaining the armature of said relay in engagement with a particular one of said contacts approximately one-half of the time.

6. In a mechanism for manufacturing key tape for enciphering permutation code telegraph signals a polar relay, a first control on said relay responsive to variations in noise, a second control on said relay comprising a biasing winding, a third control on said relay comprising a locking path connected to a first contact on said relay and a fourth control on said relay comprising a second locking path connected to a second contact on said relay.

7. In a mechanism for manufacturing key tape for use in enciphering permutation code telegraph signals, a plurality of amplifiers connected to a plurality of noise sources, a plurality of polar relays individually responsive to variations in the noise in said sources, a transmitting distributor, means comprising said distributor and a plurality of locking windings on each of said relays for locking the armatures of said relays in either of their alternate positions and means for energizing a plurality of selecting magnets in response to the operation of said relays.

8. In a mechanism for producing key tape for enciphering permutation code telegraph signals, a plurality of amplifiers set at inordinate gain to produce noise, a tape producing recording means and means interconnecting said amplifiers and said recording means for controlling said recording means in response to noise variations in said amplifiers.

9. The method of producing permuted sets of two conditions which comprises selectively determining each condition of the set as a function of a characteristic at a given instant of a given source of noise and combining the two conditions thus determined in permutations.

RALZEMOND D. PARKER.