

[54] **HIGH SECURITY ELECTRICAL KEY**

[72] Inventors: **Robert A. Hedin**, Yorba Linda; **Robert H. Du Quesnay**, Buena Park, both of Calif.

[73] Assignee: **Eaton Yale & Towne Inc.**, Cleveland, Ohio

[22] Filed: **Feb. 22, 1971**

[21] Appl. No.: **117,271**

[52] U.S. Cl. **340/149 R**, 317/134

[51] Int. Cl. **H04q 9/00**, G05b 1/00, H01h 47/00

[58] Field of Search 340/149, 150, 151; 200/46; 235/61.11, 61.11 A, 61.12; 317/134

[56] **References Cited**

UNITED STATES PATENTS

3,411,046 11/1968 Swannick 317/134
3,445,813 5/1969 Price 340/150

Primary Examiner—Donald J. Yusko

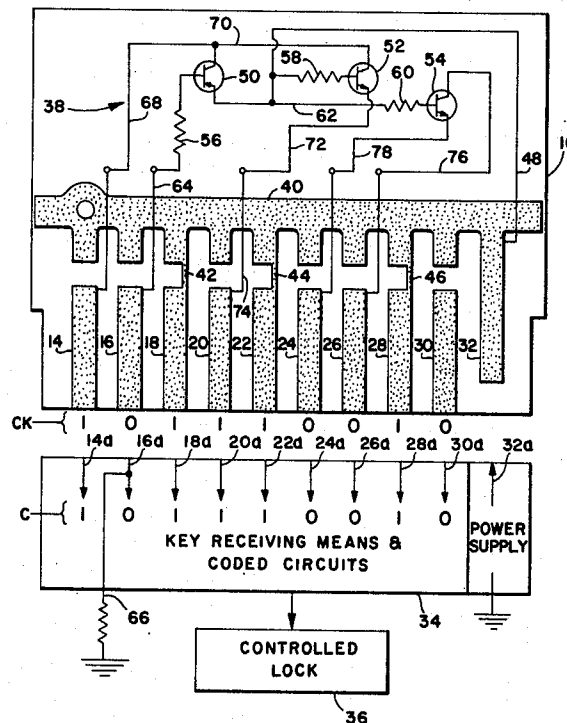
Attorney—Teagno & Toddy

[57]

ABSTRACT

A key for use with an electrical security system includes a plurality of contacts for conveying a binary coded permutation of electric signals to key receiving means of the system for actuating the system when the key is the proper key, a plurality of conductor paths for interconnecting at least a portion of the plurality of contacts, and control means associated with the conductor paths for controlling the conductivity therethrough. The control means has a first condition when the key is engaged with the key receiving means and second condition when the contacts are disengaged from the key receiving means. When the control means is in its first condition the contacts convey the predetermined binary coded permutation to the key receiving means so as to actuate the security system and when the control means is in its second condition the contacts are inoperable to convey the predetermined code stored on the key. Accordingly, deciphering of the key by an unauthorized person is prevented when the key is disengaged from the key receiving means and the control means is in its second condition.

17 Claims, 2 Drawing Figures



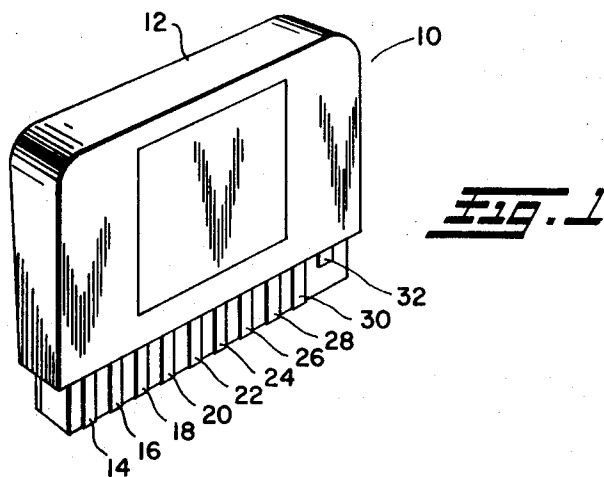


Fig. 1

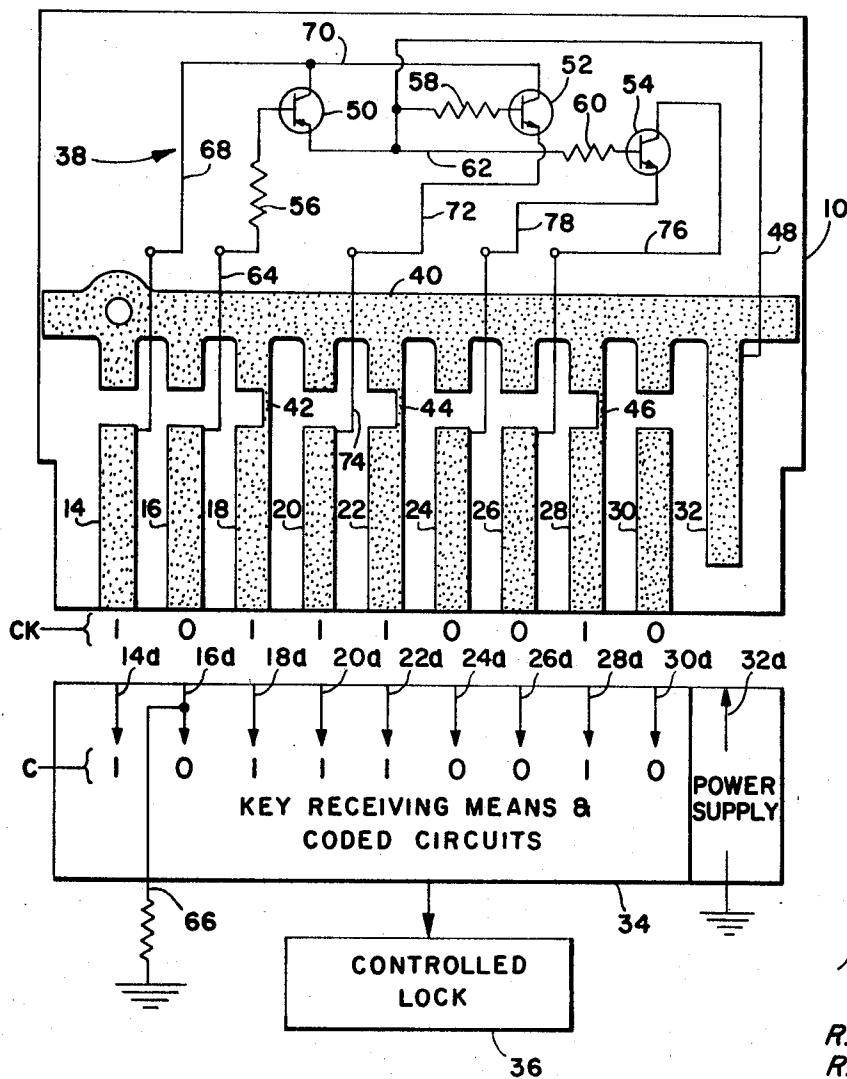


Fig. 2

INVENTORS
R. A. HEDIN
R. H. DUQUESNAY

James & Gaddy
ATTORNEYS

HIGH SECURITY ELECTRICAL KEY

The present invention relates to a key for controlling electric locks and security systems, and more specifically to a key having binary coded information stored thereon and means for preventing deciphering of the coded information stored on the key.

Keys that utilize open and closed electrical circuits to convey a binary coded permutation to a lock or security system are known in the art. One such key is disclosed in the Hedin and Balzano U.S. Pat. Re. No. 27,013, issued Dec. 22, 1970. The Hedin and Balzano patent discloses a key having a plurality of contact members engageable with contacts of a lock or security system. Certain of the contact members are in a closed circuit and others are in an open circuit so that a binary code may be applied to the lock system to effect actuation thereof. Another known key utilizing a binary coded permutation to operate a security system is disclosed in the Hedin application entitled "Keys for Electronic Security Apparatus," Ser. No. 23,272, Filed Mar. 27, 1970, which discloses a key that may be termed a memory key. The memory key, unlike the key disclosed herein, need have no permanent code but is equipped with memory elements that will retain different codes that may be impressed upon them. The key disclosed herein will permanently retain a particular code that will be the normal code of the key, and will offer a different code only when put to improper use.

While the binary coded keys of the prior art offer security that is satisfactory for many purposes, it is possible to utilize procedures that will decipher the keys and there is need for a key that will offer the best security.

Accordingly, an object of the present invention is to provide a new and improved key for actuating a security system which has means therein to prevent the deciphering of the code stored on the key.

Another object of the present invention is to provide a new and improved key for actuating a security system which has key receiving means, the key including a plurality of contacts, a plurality of conductor paths interconnecting at least a portion of the plurality of contacts and means located in the plurality of conductor paths for controlling the conductivity of the paths, and wherein the means for controlling the conductivity has a first condition which enables the contacts to convey binary coded permutation to the key receiving means and a second condition in which the contacts are inoperable to convey the binary coded permutation.

Still another object of the present invention is to provide a new and improved key for actuating a security system, the key having a plurality of contacts some of which receive information from the key and at least one of which is a power contact for applying power to the key, the key including a plurality of key contacts for conveying information to the contacts of the security system, a power receiving contact engageable with the power contact of the security system and through which power will be directed to at least one of the plurality of key contacts, and means interconnecting at least a portion of the plurality of key contacts and having a first condition when said key contacts engage with the plurality of contacts of the security system, the power receiving contact then engaging with the power contact, to interconnect the key contacts in a predetermined manner to enable the key contact to direct a predetermined code to the contacts of the security system, and a second condition effective when the key contacts are disengaged from the plurality of contacts of the security system to prevent the key contacts from conveying the predetermined code.

A further object of the present invention is to provide a new and improved key for actuating a security system having key receiving means, including a plurality of contacts for conveying a predetermined binary coded permutation to the key receiving means to actuate the security system, a plurality of conductor paths interconnecting at least a portion of the plurality of contacts, and control means having a first condition enabling the contacts to convey the predetermined binary coded permutation to the key receiving means and a second

condition disguising the predetermined binary coded permutation when the contacts are not engaged with the key receiving means, and wherein the control means when in its second condition enables the contacts to convey a plurality of binary coded permutations to thereby prevent deciphering of said predetermined binary coded permutation.

Further objects and advantages of the present invention will become apparent from the following detailed description thereof taken in conjunction with the following drawings wherein:

FIG. 1 is a perspective view of a key embodying the present invention; and

FIG. 2 illustrates schematically the circuitry of the key and the security system.

A binary coded key 10 having a body member 12 and a plurality of contacts 14, 16, 18, 20, 22, 24, 26, 28, 30, and 32 is illustrated in FIG. 1 and 2. The key 10 is operable to be engaged with a key receiving means of a security system which controls access to a secured area. The security system is schematically illustrated as including key receiving means and coded circuit 34 and a lock 36 which is controlled by the circuitry 34. The key receiving means and coded circuits may be in a preferred embodiment similar to the circuitry disclosed in the Hedin and Balzano patent already referred to U.S. Pat. Re. No. 27,013 entitled "Key Actuated Electronic Security System," issued Dec. 22, 1970. As is described in the Hedin and Balzano patent the key receiving means is operable to receive information stored on the key 10 upon engagement therewith. The key receiving means directs the information to the coded circuits and if the information directed to the coded circuits is correct, i.e., a correct code, the coded circuits effect operation of the lock 36 to provide for access to the secured area.

The key receiving means includes a plurality of contacts 14a, 16a, 18a, 20a, 22a, 24a, 26a, 28a, 30a, and 32a which are operable to engage with the contacts 14-32 respectively of the key 10 upon insertion of the key 10 into the key receiving means. The key 10 will then be operable to convey a binary code via the key receiving means to the code circuitry. If the binary code is a proper code the controlled lock 36 will be actuated and entry to the secured area may be effected as is described in the aforementioned patent. A particular code is assumed simply for the purpose of describing the invention, and that code is indicated in FIG. 2 by a group of "0" and "1" information bits C contained in the coded circuits 34, and by corresponding bits CK contained in the key.

The contacts 14-30 disposed on the body 12 of the key 10 are operable to form either closed or open circuits with the contact 32 which is a power contact. The contact 32 is operable to be engaged with the contact 32a of the key receiving means which is associated with a power supply, schematically illustrated in FIG. 2, to thereby apply power to the contact 32 upon insertion of the key 10 into the key receiving means. If a closed circuit is completed between the contact 32 and one of the other contacts, a potential will be applied to the one contact and the contact will convey to the key receiving means a 1 bit of information. If an open circuit is formed between the contact 32 and one of the other contacts, the one contact will convey a 0 bit of information to the key receiving means. As is schematically illustrated in FIG. 2 the contacts 14-30 form open and closed circuits with the contact 32 to convey information in the form of binary bits to the coded circuits and key receiving means 34. The contacts 14, 18, 20, 22 and 28 are operable in the present embodiment of the invention to convey 1 bits of information to the key receiving means and coded circuits 34. The 0 and 1 bits of information form a binary coded permutation which is utilized to actuate the lock 36. It should be appreciated that while specific bits of information are illustrated associated with specific contacts these may be easily varied to form a variety of codes.

In the form that has been chosen to illustrate, the key contacts 18, 22, 28 and 30 merely utilize an earlier development shown in the application of R. A. Hedin, Ser. No. 27,686, filed Apr. 13, 1970, entitled "Method and Apparatus for Producing

Encoded Electrical Keys." Thus, when the key 10 is engaged in the key receiving means, power will be transmitted via the contact 32 to a bus bar 40 located on the upper portion of the body member 12. The bus bar 40 will then apply a potential directly to the contacts 18, 22, and 28 via the conductive portions 42, 44 and 46 disposed between the bus bar 40 and the contacts 18, 22, and 28, respectively. Thus, the contacts 18, 22 and 28 will convey 1 bits of information to the key receiving means via the conductive portions disposed between the bus bar 40 and the contacts. The contact 30 may have been formed with a conductive portion connecting it with bus bar 40, but that portion has been removed and therefore no potential will be applied thereto and thus the contact 30 will convey a 0 bit of information to the key receiving means. By utilizing the earlier Hedin development mentioned above, the owner of the key may remove any of the conductive portions 42, 44, 46 so as to make limited changes in the code, enabling him to establish a code that is unknown to the manufacturer of the key.

Supplying power to the power contact 32 also effects energization of control means 38 disposed in the upper portion of the key body 12. The control means 38 is associated with circuitry which provides conductor paths between certain of the contacts so that either 0 or 1 bits of information can be conveyed by the contacts associated with the control means 38. The control means 38 is energized via the line 48 which is connected to the upper portion of the contact 32. Energization of the control means 38 will enable the contacts 14 and 20 to convey 1 bits of information to the key receiving means and the contacts 16, 24 and 26 to convey 0 bits of information to the key receiving means.

The control circuitry 38 includes a PNP transistor 50, and a pair of NPN transistors 52 and 54. A resistor 56 is connected to the base of the transistor 50, and resistors 58 and 60 are connected to the bases of the transistors 52 and 54 respectively. The potential applied to the line 48 will bias the base of transistor 52 through the resistor 58 and the base of the transistor 54 through a line 62 and the resistor 60. The potential on line 48 will also be applied through the conductor 62 to the emitter of the transistor 50. The base of the transistor 50 is connected through the resistor 56 and a lead 64 to contact 16. When contact 16 engages with the contact 16a of the key receiving means, there will be a difference of potential in effect grounding the base of transistor 50, as represented schematically by ground 66 connected to contact 16a of the key receiving means. Since the base of transistor 50 is grounded and a positive potential is applied to the emitter thereof through the line 48 and the line 62, the transistor 50 will conduct.

Conduction of transistor 50 will complete a circuit between the emitter and collector thereof to apply a potential through a line 70 to the lead 68. The lead 68 is connected to the contact 14 and thus a potential will be applied to the contact 14 which will enable the contact 14 to convey a 1 bit to the contact 14a of the key receiving means. The contact 16 will convey a 0 bit of information to the contact 16a of the key receiving means. It should be appreciated that while a small potential might be applied to the contacts 16 and 16a due to grounding of the base of transistor 50, the potential will not be great enough to effect the conveyance of a 1 bit of information to the key receiving means.

Conduction of the transistor 50 will also enable a positive potential to be applied along the line 70 which is connected to the collector of transistor 52. Since at this time a potential is applied to the base of the transistor 52 through the resistor 58 from the line 48, the transistor 52 will conduct and complete a circuit through the collector emitter thereof to line 72. The line 72 is connected to a lead 74 which is connected to the contact 20 and the potential on line 72 will then be applied through lead 74 to the contact 20. The potential applied to the contact 20 will enable the contact 20 to apply a 1 bit of information to the contact 20a of the key receiving means.

The application of power to the line 48 effects the biasing of the base of transistor 54 through the resistor 60. However, since no potential is applied to the collector of the transistor the transistor 54 will remain in an off condition and the leads 76 and 78 which are connected to the collector and emitter thereof respectively will not have a potential applied there along. The leads 76 and 78 are respectively connected to the contacts 26 and 24 of the key 10 and thus a 0 bit of information will be conveyed by the contacts 24 and 36.

The purpose of transistor 54 will be better understood if at this point a different condition is assumed. Thus, assume that, by some means such as a testing instrument, a potential is applied directly to the contact 26 of the key 10. The application of a potential to the contact 26 would effect a potential along the line 76 to the collector of transistor 54. If at this time the base of the transistor 54 is biased by potential on line 48, the potential which is applied to the collector would turn transistor 54 on and power would flow through the collector emitter circuit thereof to the line 78 to apply a potential to the contact 24. In the assumed condition, where a potential is applied directly to the contact 26a the contact 24 will indicate a 1 bit of information. That naturally departs from the predetermined code of the key and therefore indicates false code.

It should be appreciated that when a potential is applied to key contact 26, as when the key is in position engaging the key receiving means, the transistor 54 will conduct and the key 10 will convey a binary coded permutation which has a 1 bit of information at the contact 24. If however, a zero potential is applied to the contact 26 the transistor 54 will not conduct when the key engages the key receiving means and accordingly a 0 bit of information will be conveyed by the contact 24. Thus, it should be apparent that the binary coded permutation that will be conveyed by the key will depend upon the potential applied or not applied to the contact 26. This enables the key to convey a plurality of binary coded permutations. Since the key will convey its proper binary coded permutation only when a potential is applied to a certain key contact or contacts, in this example including the contact 26, the proper permutation will be disguised when the key is removed from the key receiving means.

At this point, attention may be called to the fact that the key can be utilized to offer a second code permutation that may be desired. Thus, in the circuitry described, the contact 24 can offer either a 1 or a 0 bit of information. Therefore, depending upon the predetermined binary coded permutation needed to actuate the security system, a potential may or may not be applied to the contact 26 and the transistor 54 may or may not be utilized to direct a 1 bit of information to the contact 24.

When the key 10 is engaged with the key receiving means the binary coded permutation is applied to the key receiving means via the contacts 14-30 of the key 10. The binary coded information, which consists of the 1 bits of information applied by the contacts 14, 18, 20, 22, and 28 and the 0 bits of information which are applied by the contacts 16, 24, 26, and 30, is controlled by the presence or absence of conductive portions between the bus bar 40 and the contacts 14 to 30, the operation of the control means 38, and the electrical condition of the key receiving means contacts 14a to 32a. It should be apparent from all of the foregoing that the control means has a first condition when the key 10 is engaged with the key receiving means and the contacts 14 to 32 engage the contacts 14a to 32a and a second condition when the key is not engaged with the key receiving means. The second condition of the control means is such as to effectively prevent deciphering of the code stored on the key 10 when the key is not engaged with the key receiving means. Moreover, the body 12 of the key is preferably made of a material which prevents X-ray of the key, and which also renders the circuitry destroyed if the key is taken apart. Thus, if the key 10 falls into the hands of an unauthorized person, he cannot duplicate the code stored on the key without destroying the key.

There are three general types of testing that might be attempted to determine the binary coded permutation of the key. Perhaps the most obvious test would be to use a battery and a light to test the conductivity of the different terminals by engaging the contacts of the battery and light with different contacts of the key. A test such as this applied to the key would show that the terminals 18, 22, 28 and 32 are closed circuits. A person using this test would have no way of knowing that the contacts 14, 20 are also closed circuits. Thus, deciphering of the code by this method would not be productive.

A more sophisticated test would be to use an ohmmeter and measure the resistance of all the terminals. In this type of test it should be appreciated that the resistances of the terminals 14, 16, 20, 24, 26 and 32 would all be about the same due to their connection with the control means 38. Therefore, the distinction between these terminals could not be found by using an ohmmeter. In a further attempt to decipher the key, power might be applied to one of the terminals and the output of the different terminals measured. However, it should be apparent that if power were applied to the terminal 32 it would be necessary to ground terminal 16 in order for the code to be deciphered thereon since transistor 50 will not conduct unless there is a certain potential through terminal 16. Thus, unless it is known specifically what terminals to ground and what terminals to apply power to, it will be exceedingly difficult or impossible to decipher the key. Moreover, since it is also possible to apply power to more than one of the leads, i.e., such as the lead 26 to bias transistor 54 into condition to thereby obtain from the key a different code in which the contact 24 would convey a 1 bit of information, it would be impossible for an unauthorized person to know exactly which of the codes he might find would be the correct code.

It should be appreciated that while only 10 terminals have been shown in conjunction with the key, more or less terminals could be utilized depending upon the degree of security and the number of possible combinations desired to be utilized with the key. For example, a plurality of contacts such as the contacts 14-32 naturally may be disposed on the opposite side of the key in a parallel relation to the contacts 14 to 32 shown in FIG. 1. This of course would substantially increase the number of code changes which could be stored on a key thereby adding to the complexity of deciphering of the key. Moreover, the complexity of the control means can be varied to connect more or less contacts to it as the security is desired to be increased or decreased respectively. It should be realized that the control means illustrated is for a particular key and, using that key as an example, persons who are skilled in the art will be able to vary the control means to enable different codes to be stored on the key 10.

From the foregoing it should be apparent that a new and improved key for actuating a security system has been provided. The key includes a plurality of contacts receiving power from the security system and in return conveying information to the security system. Interconnecting at least a portion of the plurality of contacts is a control means which is operable, when the contacts of the key engage contacts of a key receiving means of a security system to effect the application of a predetermined code from the key to the key receiving means of the security system. When the key is removed from the security system the control means takes another condition which is different from the condition of the control means when the key engages with the key receiving means of the security system. The second condition of the control means is such as to effectively prevent deciphering of the predetermined code stored on the key by an unauthorized person.

While the key of the present invention has been described in relation to a security system that comprises a lock mechanism, it is to be understood that the key will be of equal value where a security system will perform other functions such as identification of the key or the operation of different types of mechanism.

What we claim is:

1. A key for actuating a security system having key receiving means, said key comprising a body member, a plurality of contacts mounted on said body member for conveying a binary coded permutation of signals to the key receiving means, a plurality of conductor paths each of which interconnects at least two of said plurality of contacts to enable said contacts to convey a binary coded permutation of signals to the key receiving means of the security system, and control means disposed in said plurality of conductor paths for controlling the conductivity of said plurality of conductor paths, said control means having a first condition wherein the conductor paths conduct in a predetermined manner and said contacts convey said binary coded permutation of signals to the key receiving means and a second condition in which said conductor paths are prevented from conducting in said predetermined manner and said contacts are inoperable to convey said binary coded permutation of signals.

2. A key for actuating a security system as defined in claim 1 wherein said control means is operable to render at least one of said conductive paths, which is disposed between at least a first and second one of said contacts, conductive when said control means is in one of said first and second conditions and nonconductive when said control means is in the other of said first and second conditions, said first one of said contacts being operable to convey a 1 bit of information when said conductive path is conductive and a 0 bit of information when said conductive path is non-conductive, said bits of information forming a part of said binary coded permutation of signals.

3. A key for actuating a security system as defined in claim 2 wherein said second one of said contacts is a power receiving contact operable to have a potential applied thereto upon engagement of said power receiving contact with the key receiving means, said power receiving contact transmitting said potential to said control means to thereby actuate said control means to said first condition.

4. A key for actuating a security system as defined in claim 1 further including a power receiving contact operable to have a potential applied thereto upon engagement with said key receiving means and wherein at least one of said plurality of contacts is operable to apply a potential to the key receiving means upon engagement therewith when said control means is in said first condition, said power receiving contact directing said potential to said control means to thereby actuate said control means to said first condition to control the potential applied by said one contact to the key receiving means.

5. A key for actuating a security system as defined in claim 4 wherein a second one of said plurality of contacts is operable to have a potential applied thereto upon engagement with the key receiving means and a third one of said plurality of contacts is operable to apply a potential to the key receiving means upon engagement therewith, said second contact directing said potential to said control means to thereby control the potential applied by said third contact to the key receiving means, said second contact having no potential applied thereto when said third contact is utilized to convey a 0 bit of information to the key receiving means to actuate a security system with one predetermined binary coded permutation and said second contact having a potential applied thereto to enable said third contact to direct a 1 bit of information to the key receiving means to effect actuation of a security system by another predetermined binary coded permutation.

6. A key for actuating a security system as defined in claim 1 further including a power receiving contact operable to have a potential applied thereto upon engagement with the key receiving means and wherein said control means includes switch means disposed in at least one of said plurality of conductor paths for controlling the conductivity therethrough, said power receiving contact being connected with said switch means, said switch means having a conductive condition when a potential is applied thereto by said power receiving contact and said power receiving contact is engaged with the key

receiving means and a nonconductive condition when said power receiving contacts are disengaged from the key receiving means.

7. A key for actuating a security system as defined in claim 6 wherein said switch means includes a transistor having its base, collector, and emitter connected to first and second ones of said plurality of contacts and to said power receiving contact, said transistor having a nonconductive state when said plurality of contacts and power receiving contact are disengaged from the key receiving means and a conductive state when said plurality of contacts and said power receiving contact engage with the key receiving means and a predetermined potential is applied to said first and second of said plurality of contacts and to said power receiving contact, said transistor when in said conductive state enabling said plurality of contacts to convey said binary coded permutation of signals to the key receiving means.

8. A key for actuating a security system having a plurality of contacts some of which receive information from said key and at least one of which is a power contact for applying a potential to said key, said key comprising a body member, a plurality of spaced apart key contacts mounted on said body member, each of said plurality of key contacts having a first end portion and a second end portion that is engageable with the plurality of contacts of the security system for conveying information to the security system to effect actuation thereof, a power receiving contact engageable with the power contact of the security system for directing a potential to at least one of said plurality of key contacts, and control means mounted on said body member interconnecting said first end portions of at least a portion of said plurality of key contacts, said control means having a first condition when said key contacts engage with the plurality of contacts of the security system and said power receiving contact engages with the power contact and a second condition when said key contacts are disengaged from the plurality of contacts of the security system, said control means when in said first condition interconnecting said key contacts in a predetermined manner to enable said key contacts to direct a predetermined code to the plurality of contacts of the security system, said control means when in said second condition interconnecting said key contacts in a second predetermined manner to prevent said key contacts from conveying said predetermined code.

9. A key for actuating a security system as defined in claim 8 wherein said predetermined code directed to the security system when said control means is in said first condition is a binary coded permutation, said binary coded permutation including 0 and 1 bits of information, each of said plurality of key contacts being operable to convey a 1 bit of information when said key contacts receive a potential applied thereto from said power receiving contact and a 0 bit of information when said key contacts are prevented from having a potential applied thereto by said power receiving contact, said control means when in said first condition enabling at least one of said key contacts to have a potential applied thereto by said power receiving contact and when in said second condition preventing a potential from being applied from said power receiving contact to said one key contact.

10. A key for actuating a security system as defined in claim 8 wherein said power receiving contact is connected to said control means, said power receiving contact upon the application of a potential thereto by the power contact actuating said control means to said first condition.

11. A key for actuating a security system as defined in claim

10 wherein said power receiving contact directs said potential to said control means to thereby control the potential applied by other of said key contacts to the plurality of contacts of the security system.

12. A key for actuating a security system as defined in claim 8 further including a power receiving contact operable to have a potential applied thereto upon engagement with the key receiving means, and wherein said control means includes switch means disposed in at least one of said plurality of conductor paths for controlling the conductivity therethrough, said power receiving contact being connected with said switch means, said switch means having a conductive condition when a potential is applied thereto by said power receiving contact and said power receiving contact is engaged with the key receiving means and a nonconductive condition when said power receiving contact is disengaged from the key receiving means.

13. A key for actuating a security system as defined in claim 12 wherein said predetermined code is a binary coded permutation of signals that said key contacts direct to the plurality of contacts of the security system, said binary coded permutation of signals being controlled by the conduction and non-conduction effected by said control means between said power receiving contact and said plurality of key contacts, each of said key contacts conveying a 1 bit of information when said control means effects conduction between said key contact and said power receiving contact and a 0 bit of information when said control means prevents conduction between said key contact and said power receiving contact.

14. In a key for applying a particular binary coded permutation of electric signals to an electric security system and having a plurality of contacts through which the signals are applied to the system, said particular permutation comprising a normal code of the key, circuit means interconnecting contacts of said plurality of contacts on the key, control means forming a part of said circuit means and changing state when potential is applied through a certain combination of said contacts to the circuit through portions of said circuit means through which said potential will act when said control means are in a changed state to establish said particular permutation of signals the said plurality of contacts, and the establishing of said signal permutation through said control means circuit portions being dependent upon the changed state of the control means so that said control means will withhold the normal key code when a potential is applied through a contact combination that differs from said certain combination.

15. A key for applying a particular binary coded permutation of electric signals to an electric security system as defined in claim 14 in which said circuit means include portions whereby said control means make one contact of said plurality of contacts relatively conductive and nonconductive so as to offer alternately a 1 bit signal or a 0 bit signal.

16. A key for applying a particular binary coded permutation of electric signals to an electric security system as defined in claim 14 in which said circuit means include a portion that causes said control means to change state in response to a potential applied through a further contact of said plurality of contacts.

17. A key for applying a particular binary coded permutation of electric signals to an electric security system as defined in claim 14 in which said circuit means include resistive elements offering a limited degree of conductivity between contacts of said plurality of contacts.

* * * * *