United States Patent [19]

Rosenblum

[11] **4,182,933**

[45] **Jan. 8, 1980**

[54] **SECURE COMMUNICATION SYSTEM WITH REMOTE KEY SETTING**

[75] Inventor: **Howard E. Rosenblum**, Silver Spring, Md.

[73] Assignee: **The United States of America as represented by the Secretary of the Army**, Washington, D.C.

[21] Appl. No.: **800,371**

[22] Filed: **Feb. 14, 1969**

[51] **Int. Cl.**[2] **H04K 1/00**; H04L 9/00

[52] **U.S. Cl.** ..... **179/1.5 R**; 178/22

[58] **Field of Search** 179/1.5; 178/22; 325/32

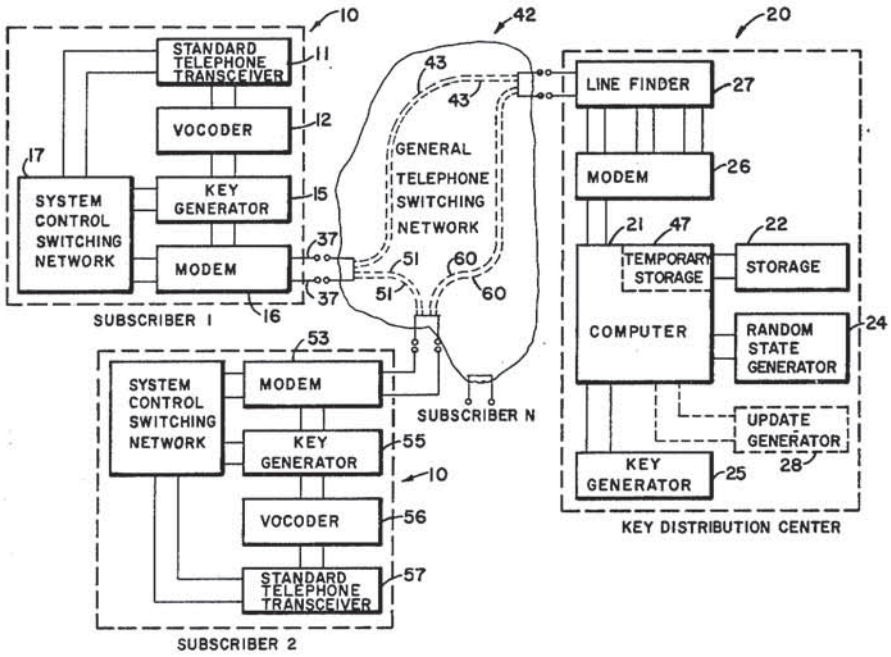
Primary Examiner—Howard A. Birmiel

Attorney, Agent, or Firm—John R. Utermohle

[57] **ABSTRACT**

An apparatus for maintaining secure communication between subscribers. A centrally located key distribution center, which includes a data processor, is utilized as a source of remotely selected working variables which are utilized to enable secure communication between a plurality of selected subscribers. Each subscriber in the system has a unique variable which identifies him to the data processor, and enables a secure communication with the data processor, which will then provide him with the working variable of the subscriber that he wishes to call. The key distribution center also reiteratively replaces the working variable of the caller, and the called subscriber if desired, each time contact is made with the key distribution center.

10 Claims, 2 Drawing Figures



DOCKET ALARM

Find authenticated court documents without watermarks at docketalarm.com.

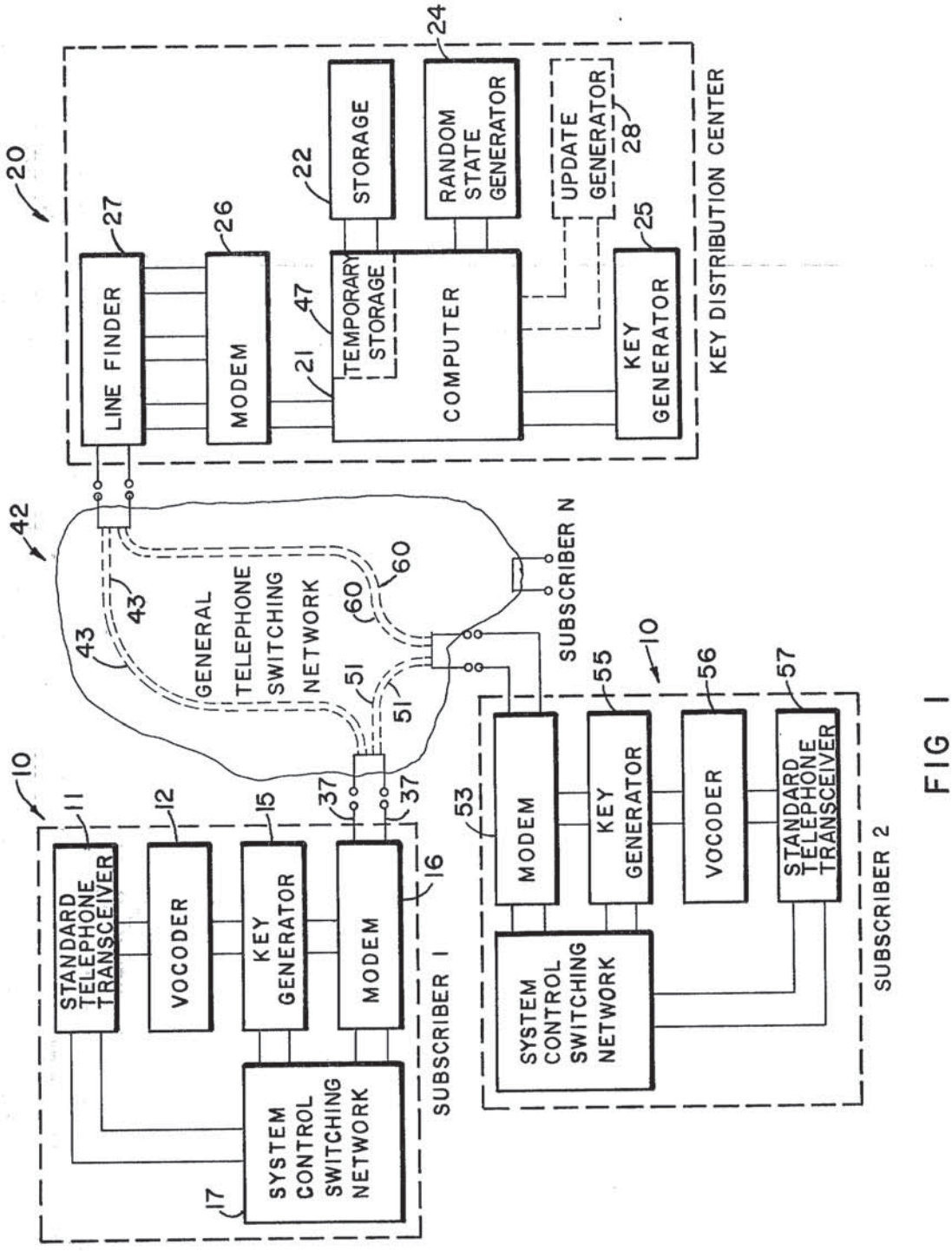


FIG 1

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

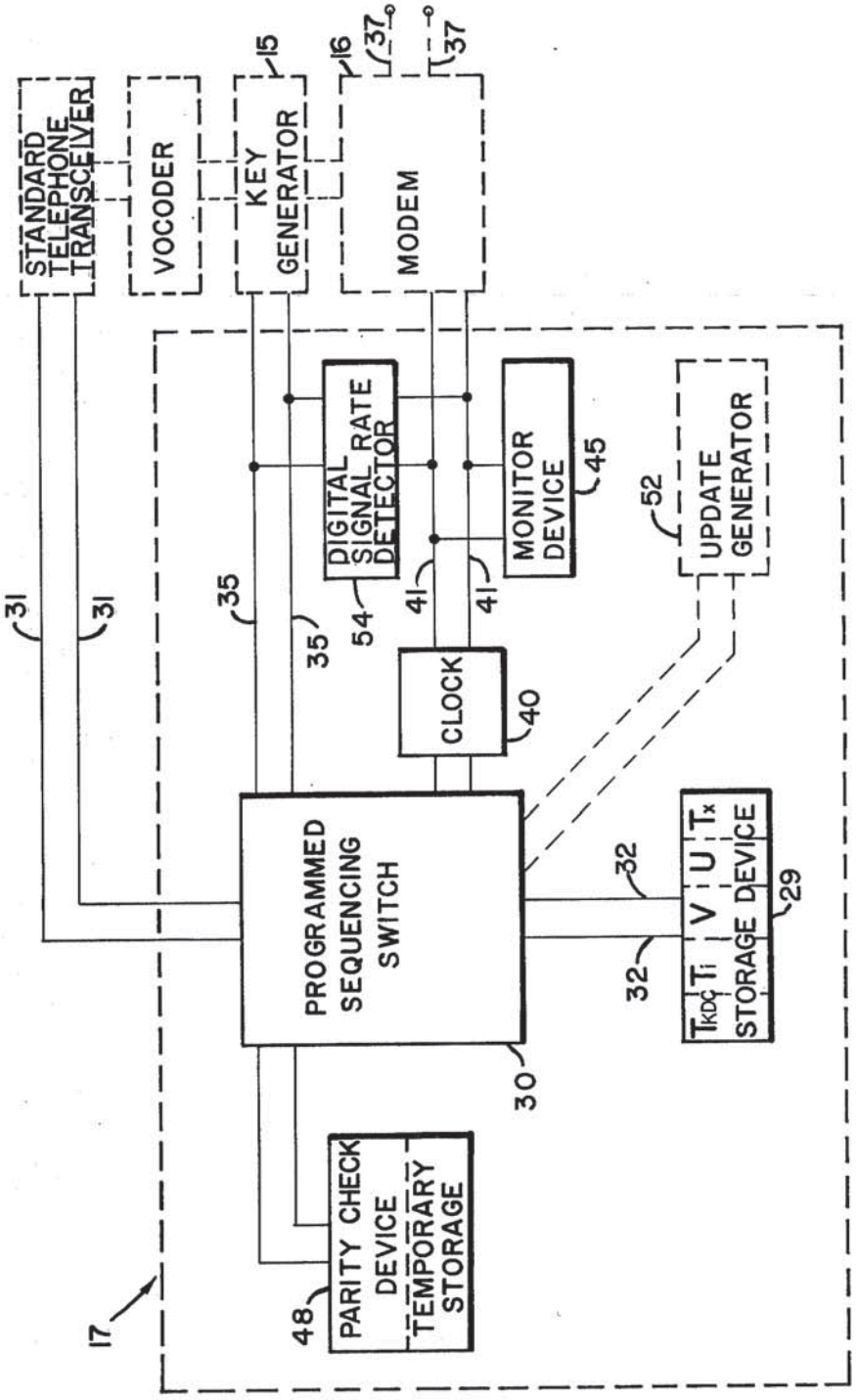


FIG 2

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

SECURE COMMUNICATION SYSTEM WITH REMOTE KEY SETTING

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention is a communication system, more particularly it is a secure communications system for maintaining secure communication between subscribers.

2. Prior Art

Prior art secure communication systems which utilize at least one working variable for enciphering and deciphering secure messages transmitted therein, do not remotely select these working variables for purposes of retransmission of a secure message between subscribers in the system. These prior art systems utilize a working variable which must be known to all subscribers receiving the secure message. This working variable, known by the subscribers, must be inserted into their enciphering/deciphering means in order to maintain secure communication. If each subscriber to the system has a different working variable, the one initiating the message in such a system must have at his disposal the working variable of the subscriber he wishes to call so that he may insert it in his enciphering/deciphering means in order to maintain a secure message between subscribers. This requires a substantial inventory of working variables at the place of message initiation, and reception, thus minimizing the security of the system.

Another feature of prior art secure communication systems, which has limited desirability from a security viewpoint, is the requirement that in order to change the working variables utilized in these systems these variables must be changed in accordance with a predetermined schedule, known to all subscribers in the system; thus, there is once again a minimization of security.

In the secure communication system of the present invention, the security liabilities of prior art systems are overcome by providing for an automatic reiterative replacement for the working variables of the system subscribers, and by providing a means by which the working variable of the subscriber which is called is remotely selected for purposes of retransmission by the subscriber initiating the call. By reiteratively replacing the working variables automatically, there is no need for conforming to a rigid schedule known to all parties. By accomplishing remote selection and reiterative replacement by some means external to the subscribers to the system, at some central location, an absolute maximization of system security is provided. This is due to the singular remote location of the necessary information, as opposed to the multiplicity of locations, one at each subscriber, necessary in prior art systems, as well as the fact that the actual working variable which is utilized, at any given time, is unknown to all subscribers in the system, the setting of the enciphering/deciphering means of the subscribers being accomplished automatically with information received from a remote selection means. Furthermore, the security of the system of the present invention is enhanced due to the ease of reiterative replacement, which may occur as often as once per message instead of once per day, or once per plurality of messages, as in prior art systems.

Prior art subscription television systems employing remote selection of switch setting information in order to allow the subscriber to receive a scrambled subscription television picture cannot provide for remote selection of a working variable in the sense that the switch setting information received is not utilized to transmit a secure message between the subscriber and another subscriber, but rather merely to receive information already existent.

SUMMARY OF THE INVENTION

An object of this invention is to provide a new and improved secure communication system which overcomes the disadvantages of the prior art.

Another object of the present invention is to provide a new and improved secure communication system wherein the information necessary to enable secure communication is remotely selected.

Another object of the present invention is to provide a new and improved secure communication system wherein the information necessary to enable secure communication is reiteratively varied.

SUMMARY

With these objects in view a secure communication system may include a remotely selectable means for selecting a key-setting variable and a unique variable and transmitting the remotely selected key-setting variable, the remotely selectable means including a means for reiteratively replacing the key-setting variable when the key-setting variable is remotely selected, the reiterative key-setting variable replacement replacing the key-setting variable necessary to maintain secure communication the next successive time remote selection occurs; a first means for initiating remote selection, for receiving the transmitted remotely selected key-setting variable, and for transmitting a secure communication enciphered in accordance with key-setting variable, the first receiving means being unique to the unique variable; and a second means for receiving communications from the first receiving means using the most recently obtained key-setting variable to enable secure communication between the first and second receiving means.

Other objects and many of the intended advantages of this invention will be readily appreciated as the invention becomes better understood by reference to the following description when taken in conjunction with the following drawings wherein:

FIG. **1** is a functional diagram of a system which is a preferred embodiment of the present invention, and

FIG. **2** is a functional diagram of a portion of the system shown in FIG. **1**.

Referring now to FIG. **1**, which is a functional diagram of the entire system of the present invention, a general telephone switching network is shown, although the basic theory underlining the system is functional with any type of communication media. A subscriber has a secure module **10** comprising a standard telephone transceiver **11**; a standard vocoder **12**, or other speech-to-digit converter means such as a delta-modulation coder, or other digital communication device, such as a teletypewriter; a key generator **15**; a modem **16**, which is a standard modulator-demodulator communication device for accomplishing conversion of a digital signal to an analog type signal, and vice versa, for direct delivery to and from a telephone network; and a system control switching network **17**, shown in more detail in FIG. **2**, which supervises the overall operation of the subscriber module **10**. Each subscriber to the system has an identical secure module with re-

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

spect to structure, differing only in its associated security parameters, as will be explained herein below.

The key distribution center **20** is the heart of the system in that it provides the remote selection capability, as well as the reiterative replacement capability, of the present invention. The key distribution center **20**, which is centrally located with respect to the subscribers to the system, comprises a standard computer **21**, which has an associated storage means **22**; a random state generator **24**, for generating random variables to enable reiterative replacement, to be described later; a key generator **25**; a modem **26**; and a standard communication line-finder device **27**, which acts as a concentrator and selects the open terminal pair of the modem **26** when contacted by a subscriber, the modem **26** shown as a singular modem having a plurality of terminal pairs, rather than a plurality of modems, for illustrative purposes. The key distribution center **20** may also contain an update generator **28**, shown by hidden lines, when an alternate embodiment of the general system is utilized, to be explained later.

Just as the key distribution center **20** is the heart of the entire system, the system control switching network **17**, shown in more detail in FIG. **2**, is the heart of the subscriber module **10**, as it controls the sequence of operations occurring in the subscriber module **10**, from the initiation of a call to another subscriber in the system, until the cessation of contact with the called subscriber, and the going off line. The system control switching network **17** contains a storage device **29**, which may be any type of standard storage device comprising either a permanent storage (read only) and temporary storage (read-write) portion, or be completely of the read-write variety. The selection of storage device **29** is merely a matter of choice, the system functioning equally well with other types of storage. For purposes of explanation, we will assume that a permanent storage-temporary storage type of storage device **29** is utilized.

A subscriber module storage device **29** would have in its permanent storage a unique key-setting variable, designated U, this unique key-setting variable being of a predetermined bit length, and being used for purposes of secure communication with the key distribution center computer **21**, to be explained subsequently; the unique telephone number of the subscriber, designated T_i, consisting of the predetermined number of digits which are necessary to uniquely identify the subscriber in the system, the number of digits being dependent on the number of subscribers in the system; and the number of digits necessary to contact any subscriber in a world-wide system, for example **12** digits; and the unique telephone number of the key distribution center **20**, designated T_{KDC}, consisting of the predetermined number of digits necessary to contact the key distribution center **20** from any point in a world-wide system, for example **12** digits. The temporary storage portion of the subscriber module storage device **29** would contain a key-setting variable, designated V, this key-setting variable being utilized to maintain a secure communication between any subscribers in the system having this key-setting variable; and, after a call has been initiated to another subscriber in the system, this operation to be subsequently explained, the telephone number of the subscriber being called, designated T_x, consisting of the predetermined number of digits necessary for contacting the called subscriber anywhere in the secure communication network, for example, **12** digits.

The key-distribution-center-computer-associated-storage device **22**, which may be a drum storage, a tape storage, a disc storage, or any other acceptable computer-associated-storage means, would contain the unique variables and key-setting variables, associated with the telephone identification numbers of the subscribers, T_i, T_x, for all the subscribers in the secure communication system.

The function of the various key-setting variables in this system is to determine the key that is produced by the associated key generators, the key that is generated being generated from the key-setting variable, whether directly or indirectly, the generated key being utilized to encipher the communication in order to enable a secure message to be transmitted, and/or received. The key-setting variables associated with the key generators can be electrically changed so as to alter the key which is produced by the associated key generator, and thus vary the enciphering/deciphering of the message, enabling a more secure system than possible in prior art devices. In one embodiment of the general system, the key-setting variable of the called subscriber is directly utilized as the dynamic working variable, which is the variable which is ultimately utilized by the associated subscriber key generators to enable secure communication between associated subscribers whose key generators are set in accordance with the dynamic working variable. In an alternate embodiment of the general system, the key-setting variable of the called subscriber is not directly utilized as the dynamic working variable, but instead is combined with an indicator variable, which is a variable which denotes the function to be performed on the key-setting variable to update it, to obtain the dynamic working variable which is utilized to set the associated subscriber key generators.

The normal operating condition of all the subscriber modules **10** in the secure communication system of the present invention, when the telephone transceiver **11** is on-hook, in the particular embodiment where the key-setting variable is directly utilized as the dynamic working variable, is to have the associated working key-setting variable, V, filled into its associated key generator **15** while the subscriber is on-hook, so that he may receive a secure communication immediately after contact is established without any further operation being necessary in order to place him in the secure mode, unless it is desired to override this automatic operation with a manual switch means, to be explained later. The normal operating condition of all the subscriber modules **10** in the secure communication system of the present invention, when the telephone transceiver **11** is on-hook, in the alternate embodiment where the key-setting variable of the called subscriber is combined with an indicator variable to obtain the dynamic working variable, is to have the associated key generator **15** blank while the subscriber is on-hook.

OPERATION

The operation of the secure communication system of the present invention, in order to enable a secure communication between subscribers for the system, differs slightly for each embodiment, the differences to be subsequently explained, the choice of embodiment being dependent on the degree of security desired.

PREFERRED EMBODIMENT

The operation of the system when the particular embodiment, wherein the key-setting variable is di-

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.