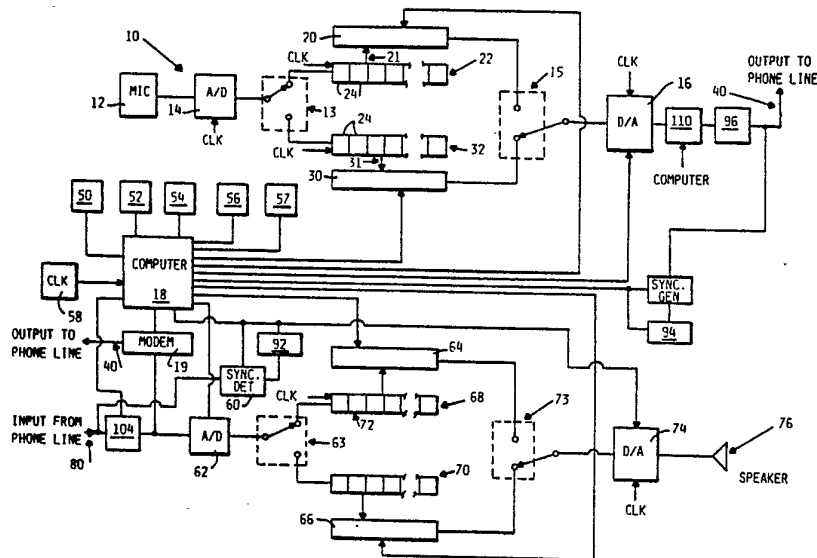




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification⁴ : H04M 1/70, 3/16, H04L 9/00 H04L 1/14, H04K 1/00, 1/04 H04K 1/06	A1	(11) International Publication Number: WO 87/ 00377 (43) International Publication Date: 15 January 1987 (15.01.87)
(21) International Application Number: PCT/US86/01364 (22) International Filing Date: 26 June 1986 (26.06.86) (31) Priority Application Number: 749,939 (32) Priority Date: 27 June 1985 (27.06.85) (33) Priority Country: US (71) Applicant: CODART COMMUNICATIONS, INC. [US/US]; 320 Tesconi Circle, Suite G, Santa Rosa, CA 95401 (US). (72) Inventors: MAISEL, Douglas, Andrew ; 56 Panoramic Way, Berkeley, CA 94704 (US). McREYNOLDS, John, Frederick ; 1297 Grizzly Peak Boulevard, Berkeley, CA 94708 (US). WEISMAN, Joe ; 519 Clip- per Street, San Francisco, CA 94114 (US). CARL- SON, Charles, Edward ; 56 Panoramic Way, Berke- ley, CA 94708 (US).		(74) Agents: WATT, Phillip, H. et al.; Fitch, Even, Tabin & Flannery, Room 900, 135 South LaSalle Street, Chi- cago, IL 60603 (US). (81) Designated States: AT (European patent), AU, BE (Eu- ropean patent), CH (European patent), DE (Euro- pean patent), FR (European patent), GB (European patent), IT (European patent), JP, LU (European pa- tent), NL (European patent), SE (European patent). Published <i>With international search report.</i>

(54) Title: SCRAMBLING APPARATUS**(57) Abstract**

A novel time-element scrambling system and the component parts thereof for communication over a non-secure communication link (40, 80) such as a telephone line. The scrambling and unscrambling operations are specified by a scrambling code which is exchanged by the two apparatuses (10, 10) at each end of the communication link (40, 80) in an encrypted form (using a public-key code) when the communication link (40, 80) is first established. Thereafter, each apparatus (10) uses the scrambling code to scramble its communications with the other apparatus (10). The generation of these two codes and their exchange by the two apparatuses (10, 10) is transparent to the users. The manner in which the codes are generated guarantees that the next code that will be generated may not be predicted by examining the apparatus (10) in question at any time substantially in advance of the time at which the communication link (40, 80) is established or afterward.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GA	Gabon	MR	Mauritania
AU	Australia	GB	United Kingdom	MW	Malawi
BB	Barbados	HU	Hungary	NL	Netherlands
BE	Belgium	IT	Italy	NO	Norway
BG	Bulgaria	JP	Japan	RO	Romania
BR	Brazil	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	LI	Liechtenstein	SN	Senegal
CH	Switzerland	LK	Sri Lanka	SU	Soviet Union
CM	Cameroon	LU	Luxembourg	TD	Chad
DE	Germany, Federal Republic of	MC	Monaco	TG	Togo
DK	Denmark	MG	Madagascar	US	United States of America
FI	Finland	ML	Mali		
FR	France				

-1-

SCRAMBLING APPARATUSBACKGROUND OF THE INVENTION

The present invention relates to devices for scrambling and unscrambling voice communications which are to be transmitted and received over ordinary or non-secure communication links.

The first voice-privacy devices were developed soon after the widespread adoption of the telephone. The simplest, and historically the earliest, voice privacy systems utilized the technique of frequency inversion. Here, a mirror image of the message frequency spectrum replaces the original speech signal. This results in the highest-pitched sounds being converted into low-pitched sounds, and the low-pitched sounds being converted into high-pitched sounds. Since the rhythm of the speech is not altered, the residual intelligibility of the scrambled signal is quite high. Furthermore, since the inversion scrambler operates in a fixed and predetermined manner, the scrambled signal may be unscrambled by an opponent equipped with a similar device.

A more sophisticated system related in concept to the inversion scrambler is the band-shift scrambler. Here the frequency spectrum is divided into a number of bands. The various bands are then shifted with respect to each other, possibly in conjunction with inversion of some or all of the frequency bands. This system provides true coded speech privacy, since there are a number of different combinations of shifted frequency bands. To unscramble the communication, one must know how the frequency spectrum was divided into bands and the sequence of the various bands in the scrambled signal. This information constitutes a "key" which an opponent must either possess or deduce in order to unscramble the signal. Unfortunately, the effectiveness of the "keys" is limited in this type of system by the

-2-

system's ability to divide the band width of the telephone lines over which the scrambled speech is to be sent into a sufficiently large number of bands. The maximum number of bands is small enough to allow an
5 opponent to deduce the key by "brute force".

The most secure analog scrambling method which produces a scrambled or cyphered signal presently suitable for transmission over conventional telephone circuits is the time-element scrambler. This technique
10 has been made practical by recent improvements in the cost/performance ratio of microcomputers. In this technique, the speech is divided into a large number of very short duration time-elements. The sequence of these time elements is altered using a scrambling code
15 which may have so many possible values that "brute force" deduction is impossible. Moreover, each successive second or other time segment of speech may be altered using a different code which is specified by the scrambling code. Hence, deduction of the key by
20 examining the patterns in the scrambled speech is also impractical. The unscrambling unit, properly set to the particular code in use and synchronized with the scrambling unit, can reassemble the fragments of speech in the correct sequence to restore intelligibility and
25 substantially unimpaired voice quality to the message. When properly implemented, this type of scrambler offers low residual intelligibility and a sufficiently large number of possible codes to be secure from
30 cryptoanalytic attack by an opponent equipped with any but the most advanced technological and economic resources.

The main problem in constructing a practical time-element scrambler for use by a large population of users lies in the management of the coding keys. The
35 large number of codes needed to prevent cryptanalytic attack results in a typical code having a very large

-3-

number of digits, e.g., greater than ten. Such codes are difficult to remember and consequently are recorded somewhere by the user. This list represents a weak point in the security system, since an opponent may gain
5 access to this list. An opponent may also obtain a list of the codes actually used by the manufacturer of the scrambler via a breach in the manufacturer's security. Although this latter list is clearly much larger than the list maintained by any one user, it is sufficiently
10 short to permit cryptanalytic attack by brute force searching of the known codes. Finally, in systems in which a list of possible codes are stored in the scrambling apparatus, an opponent can gain access to the list by examining the scrambling apparatus at a time
15 prior to the commencement of the secure communication or afterwards in the case of a taped communication.

Since the same code must be inputted into prior art scrambling machines at each end of the communication link, the codes must be exchanged by the parties to the
20 communication at some time prior to the commencement of said communication. Hence these systems are also vulnerable at the time the code is passed between the parties which are to have the secure communication. Two solutions of this problem are possible. First, the code
25 may be passed by courier or other secure means. Although this solution provides the necessary security, it is impractical in a system designed for use by a large number of parties who have not necessarily had prior dealings with each other. Furthermore, the cost
30 of the code passing transaction in both time and money may make this solution unattractive except for the most important of communications.

In principle, a second solution would be to exchange the scrambling code over the non-secure
35 communication link using a public key system. The public key system was developed to allow two parties who

-4-

have not previously communicated with each other to communicate in code by eliminating the need to exchange "code books" over a secure communication link. In a public key system, the party who wishes to receive the coded message, referred to as the receiver, sends an encryption code, E, to the party wishing to send the message, referred to as the sender. The sender uses the encryption code to transform his message into a coded message which he then transmits to the receiver over the non-secure communication link. The receiver then decodes the message using a decrypting code, D, which only he possesses. The unique feature of the public key system resides in the fact that even a third party who overheard the encrypting code, E, can not decrypt the message, since it is essentially impossible to derive the decryption code, D, from a knowledge of E. In fact, even a knowledge of how E was used to encrypt the message is insufficient to decrypt the message.

Given sufficiently fast computing hardware, one could encrypt the entire conversation between two parties using a public key system approach. Unfortunately, such hardware is too expensive at the present time to provide the basis for a secure communication system for a large group of users. However, the public key system could be used to exchange scrambling codes which are to be used by two time-element scrambling machines connected to an non-secure communication link. Here, the first machine would transmit a public key system encrypting code to the second machine which would use the encrypting code to encrypt a scrambling code. The encrypted scrambling code would then be sent back to the first machine over the non-secure communication link where it would be decrypted. The scrambling code thereafter would be used by both machines to scramble and unscramble the subsequent communications between the machines.

-5-

Although the use of a public key system would in principle solve the problems of exchanging scrambling codes for use in a time-element scrambling system, the security problems inherent in any system which relies on
5 a list of codes which may be copied remains. Public key codes require a prior list of codes or a computer associated with the device in question. There are strict mathematical requirements for the generation of these codes. As a result, one can not merely make up a
10 code number which is easy to remember. In addition to the security problems of code management, the size of the codes makes the use of these systems awkward. A large number must be entered at the start of the communication. This type of entry process, if done, for
15 example, via a keyboard, has a sufficiently high error rate to make such systems unattractive to a user having the cryptographic expertise of the average telephone user.

Consequently, it is an object of the present
20 invention to provide a time-element scrambling system which can not be compromised by a breach in security at either the sending or receiving end of the communication link.

It is a further object of the present invention
25 to provide a scrambling system which can not be compromised by examining the coding and decoding apparatuses used to scramble and unscramble the voice communications.

It is a still further object of the present
30 invention to provide a scrambling system which is transparent to the user such that someone with no expertise in cryptographic techniques can communicate easily using this system.

These and other objects of the present
35 invention will become evident from the following detailed description of the invention and from the

-6-

accompanying drawings.

SUMMARY OF THE INVENTION

The present invention consists of a novel time-element scrambling system and the component parts thereof for communicating over an non-secure communication link such as a telephone line. An apparatus is provided at each end of the communication link which scrambles and unscrambles the relevant signals using a time-element scrambling system. The scrambling and unscrambling operations are specified by a scrambling code which is exchanged by the two apparatuses in an encrypted form when the communication link is first established. The scrambling code is encrypted using a public key system code which is sent by the apparatus initiating the communication to the other apparatus. The apparatus receiving the encrypting code generates the scrambling code to be used in the communication, encrypts the scrambling code using the public key system encryption code, and returns the encrypted scrambling code to the apparatus which initiated the communication. The initiating apparatus then decrypts the scrambling code using its secret private decryption code. Thereafter, each apparatus uses the scrambling code to scramble its communications with the other apparatus.

The generation of these two codes and their exchange by the two apparatuses is transparent to the users. Each apparatus automatically generates the code for which it is responsible without input from the user of the apparatus. The manner in which the codes are generated guarantees that the next code that will be generated may not be predicted by examining the apparatus in question at any time substantially in advance of the time at which the communication link is established nor can the code be deduced after the communication has ended. The generation of the relevant

-7-

codes and their exchange by the apparatuses in question is automatic. Thus the operation of the system is both transparent to the users and secure against security breaches resulting from the existence of a list of 5 possible codes.

The system includes a calling apparatus and a receiving apparatus. Each of these apparatuses contain means for inputting and outputting the voice signals of the parties using the system, and means for inputting 10 and outputting scrambled electrical signals on the communication link in question. Each apparatus contains means for scrambling the voice signals inputted to it by the user and for unscrambling the scrambled voice signals communicated on said communication link. The 15 scrambling and unscrambling systems each employ a scrambling code which is exchanged by the receiving apparatus and calling apparatus prior to the commencement of the scrambled communication.

The scrambling code is exchanged in an 20 encrypted form to prevent an eavesdropper from using a similar scrambling apparatus to unscramble the communication. In normal operation, the calling apparatus calls the receiving apparatus. First, the two apparatuses exchange messages which serve to verify that 25 a compatible apparatus exists on each end of the communication link. After this verification, the calling apparatus generates an encrypting code according to a public key system and transmits that key to the receiving apparatus. The receiving apparatus then 30 generates a scrambling code, encrypts it using the encrypting code received from the calling apparatus, and then transmits the encrypted scrambling code to the calling apparatus. The calling apparatus decrypts the encrypted scrambling code and stores it for use in 35 scrambling and unscrambling the subsequent communications.

-8-

The voice communications are scrambled by recording the voice signals inputted into the apparatus in question and then replaying said recording in a time sequence different from the sequence in which the recording was made. Each apparatus contains two or more scrambling buffers for recording the voice signals of the user and then replaying the recording in a scrambled form. These buffers alternate functions such that at any given time, one of these scrambling buffers is used to record the voice signals and the other is used to replay the voice signals previously recorded. When the replaying of the previously recorded segment of voice signals is completed, the roles of the two scrambling buffers are reversed. Embodiments using more than two buffers will be apparent to those skilled in the art.

Each scrambling buffer is divided into a plurality of sub-buffers. The voice signals recorded in each sub-buffer are replayed over the communication link. The order in which the various sub-buffers are replayed is substantially different from the order in which the individual sub-buffers were used to record the voice signals; hence the resultant signal on the communication link is unintelligible to an eavesdropper who does not know the order in which the sub-buffers were replayed. The order in which the sub-buffers are replayed is determined by the scrambling code exchanged by the two apparatuses prior to the commencement of the scrambled communication. This code is used to define a pseudo-random playback sequence which is changed after the contents of each scrambling buffer has been completely replayed on the communication link. Hence, even a detailed analysis of the patterns on the communication link will not determine the playback order.

The scrambled signals on the communication link are unscrambled in an analogous manner. Each apparatus

-9-

also contains two unscrambling buffers for recording the scrambled signals received on the communication link and for replaying these signals in unscrambled form. One unscrambling buffer is used to record the incoming
5 signals on the communication link while the other is being used to replay the previously recorded signals in unscrambled form. When the signals in the buffer operating in a playback mode have been completely
10 replayed, the roles of the two unscrambling buffers are reversed, and the signals just recorded in the first unscrambling buffer are replayed. Each of these unscrambling buffers is also divided into a plurality of sub-buffers as were the two scrambling buffers used to
15 scramble the signals. Each sub-buffer in an unscrambling buffer contains the previous contents of one of the sub-buffers of a scrambling buffer contained in the corresponding apparatus at the other end of the communication link. Hence, the signals may be
20 unscrambled by replaying the recorded signals stored in each sub-buffer in the proper order. Since the signals stored in any one sub-buffer are already in the proper order within that sub-buffer, only the order in which the individual sub-buffers are to be replayed is
25 necessary to unscramble the signals. The order in which the sub-buffers are replayed is the same as the order in which they were played into the communication link by the apparatus which performed the scrambling. Since
30 both apparatuses use the same scrambling code to generate the order in which sub-buffers are replayed for any given scrambling buffer, the correct order is known to the unscrambling circuitry.

The scrambling and unscrambling buffers used in the present invention are digital in nature. Each consists of a plurality of contiguous memory slots. The
35 signals to be recorded in a given buffer are first digitized by an analog to digital converter. The output

-10-

of the analog to digital converter is a digital word or bit stream whose value represents the analog signal fed to the converter at a given instant of time. A clock circuit causes the converter to periodically sample this
5 signal. The replaying circuitry contains a digital to analog converter to convert the digital data back to analog form for replaying in analog form on the communication link or on a speaker. The storage operations of the two apparatuses are synchronized by
10 the repeated exchange of synchronization signals on the communication link.

The calling apparatus contains means for generating prime numbers which are used to construct the public key encrypting code sent to the receiving
15 apparatus. The particular prime numbers used to generate the encrypting and corresponding decrypting codes are not predictable from an examination of the calling apparatus at a time significantly prior to the establishment of the communication link. Hence, it is
20 not possible for an eavesdropper to obtain access to the relevant decrypting code by examining the calling apparatus. Furthermore, since the calling apparatus itself generates the encrypting and decrypting code pairs as used in the public key system, neither the user
25 nor an opponent having access to the system's manufacturer can breach the security of the system by obtaining the relevant codes. Finally, since the user does not have to enter the codes, the operation of the apparatus is transparent to the user.

30 After an encrypting and decrypting code pair has been used in a communication, the primes used to generate those codes are replaced by new primes generated by the apparatus. Thus, even an examination of the apparatus after a communication has taken place
35 will not allow an opponent to obtain the codes used to scramble a communication. This prevents an opponent

-11-

from eavesdropping on the communication by recording the scrambled communication and then examining the scrambling apparatus to find the codes used in the scrambling process.

5 The receiving apparatus contains means for generating random numbers which may be used as "seeds" for a pseudo-random number generator. The scrambling code contains such a seed. The next seed to be generated may not be ascertained by an examination of
10 the receiving apparatus at a time significantly prior to the establishment of the communication link, since the receiving apparatus also contains a means for detecting a random event which is used to define the subsequent "seeds" generated by that apparatus. Hence, the
15 security of the system is also protected from breaches in which the eavesdropper obtains a list of the scrambling codes which will be used in future communications, since neither the user nor the system's manufacturer has such a list.

20 BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 illustrates an apparatus according to the present invention.

FIGURE 2 is a flow chart for the calling apparatus initialization steps according to the present
25 invention.

FIGURE 3 is a flow chart for the receiving apparatus initialization steps according to the present invention.

FIGURE 4 is a flow chart for the scrambling
30 steps according to the present invention.

FIGURE 5 is a flow chart for the unscrambling steps according to the present invention.

DETAILED DESCRIPTION OF THE INVENTION

35 An apparatus according to the present invention is shown schematically at 10 in FIGURE 1. It interfaces with a communications link, such as standard telephone

-12-

line, through an output line 40 and an input line 80. It interfaces with its user through a microphone 12 and a speaker 76. The apparatus carries out four functions. First, it establishes a communication link with a
5 compatible apparatus that is also connected to a standard telephone line. Second, it exchanges the code information needed to scramble and unscramble the subsequent phone communication with the compatible apparatus on the other end of the communication link.
10 Third, it scrambles the acoustical voice signals detected by the microphone 12 and transmits the resultant scrambled signals on the output line 40. And fourth, it receives scrambled signals on the input line 80, unscrambles said signals, and then plays back the
15 unscrambled signals on the speaker 76.

The first two functions are carried out by a computer 18 and a modem 19. The apparatus initiating the communication, referred to as the calling apparatus, calls the apparatus which is to receive the
20 communication, referred to as the receiving apparatus. The communication begins with a "hand-shaking" procedure in which the computer in the calling apparatus sends a digital message via the modem 19 to the computer 18 in the receiving apparatus. The computer 18 in the
25 receiving apparatus then responds with a corresponding message which is verified by the calling apparatus. This confirms that a compatible apparatus is connected to both ends of the communication link.

Next, the calling apparatus generates an
30 encrypting code and transmits it to the receiving apparatus in digital form using the modem 19. Upon receiving the encrypting code, the receiving apparatus generates a scrambling code and transforms said scrambling code into an encrypted scrambling code using
35 the encrypting code sent by the calling apparatus. The receiving apparatus then transmits this encrypted

-13-

scrambling code to the calling apparatus. The calling apparatus then decrypts the scrambling code. The scrambling code is then used by both the calling apparatus and receiving apparatus to control the
5 scrambling and unscrambling of the subsequent voice communications between the two apparatuses.

The encrypting code is of the type used in public key systems. It enables the receiving apparatus to encode the scrambling code in a manner such that it
10 cannot be decoded except by the particular calling apparatus which generated the encrypting code.

Public key systems are well known to those skilled in the cryptographic arts. See, e.g., "New directions in Cryptography" 1976, IEEE Transactions on
15 Information Theory, Vol. IT-22, No. 6., and "Cryptography, a Primer" by Allan Konheim, J. Wiley & Sons Publishers, 1981 which are incorporated herein by reference.

In a public key system, a coded "message", X ,
20 is related to an uncoded message, x , by

$$X=f(n,x),$$

where n is an encrypting code. The function, $f(n,x)$, is chosen such that the inverse function is essentially impossible to calculate without knowledge of
25 an additional variable; thus even a knowledge of n will not allow x to be deduced from X . In the present invention,

$$X=x^3 \text{ modulo } n.$$

It can be shown that there exists a value d for
30 which

$$x=X^d \text{ modulo } n.$$

Here d is the decrypting code which must be known in addition to n if one is to decode the message X .

35 In the case in which n is the product of two large prime numbers p and q , it can be shown that

-14-

$$d = [2(p-1)(q-1)+1]/3.$$

Hence, the problem of constructing an encrypting code system for sending the scrambling code over an non-secure communication link is reduced to one of finding large prime numbers. Methods for finding large prime numbers are well known to those skilled in the art of computer science. For example, one can select a large odd number, m , using a pseudo-random number generator and then test it to determine if it is prime. If it is not, 2 is added to it and the test repeated. The testing procedure used in the present invention is to calculate the quantity

$$z = y^{(m-1)} \text{ modulo } m,$$

where y is any number greater than 1 and less than m . This quantity is 1 if m is prime. However, it is not guaranteed that if this quantity is 1, m is prime. Hence, this test is made for several numbers y . If all such numbers produce a $z=1$, then m has a high probability of being prime.

It should be noted that a high probability is all that is needed in practice. If one in million times, m is not prime, than one in a million communications will fail to unscramble. This will be immediately obvious to the communicating parties. The parties can then repeat the communication with a different encrypting code by hanging up and redialing.

The computer 18 generates prime numbers whenever it is not busy supervising a scrambled communication. The prime numbers are generated by testing pseudo-random numbers which may be generated by any of a number of techniques known to those skilled in the computer sciences. For example, a pseudo-random number can be generated using a prime number and the following procedure:

(1) x = current value of seed plus the prime number;

-15-

- (2) $y = 5 * \ln(x)$;
- (3) $z = e^y$
- (4) new seed = $z - \text{trunc}(z)$
- (5) random number = new seed.

5 Here, $\ln(x)$ is the natural logarithm of x , $\text{trunc}(z)$ is the integer part of the number z , and $e = 2.71828$.

Once a prime number is found, it is stored in a table 56. The new prime number replaces a previous prime stored in the table. When a pair of encrypting and decrypting codes are to be generated, the computer 18 selects two prime numbers at random from this table to calculate the codes in question. The prime number table 56 is stored in a non-volatile memory such as an EEPROM so that the table of primes will not be lost if 15 power is removed from the apparatus.

Since the contents of the stored table of primes 56 changes depending upon the history of the particular calling apparatus, it is not possible to predict the encrypting and decrypting codes that will be 20 generated at any given time. To provide further security, a random event generator 50 is used to periodically reset the pseudo-random number generator seed which is used to generate the pseudo-random numbers used for generating prime numbers and scrambling codes. 25 The event chosen may be the difference in phase between the clock 58 and some quantity related to the phase of the AC signal on the power line to which the apparatus of the present invention is connected. Hence even an examination of the apparatus of the present invention 30 will not be sufficient to predict the encrypting and decrypting codes that will be in use at some later time.

It should be noted that the time needed to decode the scrambling code is sufficiently long to introduce a delay in the start of the communication if 35 an encrypting system having sufficiently long codes to assure absolute security is used. The apparatus of the

-16-

present invention is intended for wide spread use, and hence must employ inexpensive computer hardware to perform the various calculations. Such hardware lacks the speed needed to decode a scrambling code using a
5 long encrypting code in a time period of less than a few seconds. It is sufficiently fast, however, to provide a level of security which is sufficient for most communications. For those communications requiring a higher level of security, the apparatus of the present
10 invention provides a second mode of operation which is transparent to the user.

In this second preferred embodiment, two encrypting codes are sent to the receiving apparatus, a short code and a long code. The receiving apparatus
15 returns two scrambling codes, a short scrambling code and a long scrambling code. The short scrambling code is immediately decoded and used to scramble the communication in which it is sent. The long scrambling code is stored along with the identity of the receiving
20 apparatus in a table 57. This long code is decoded and stored after the communication is completed. If the same calling apparatus and receiving apparatus are reconnected in a subsequent communication, the long scrambling codes are used to govern that communication.
25 Hence, a later high security communication can be set up by making a low security communication a few hours in advance of the intended high security communication. If the second communication is commenced before the decoding process is finished and a previously decoded
30 long code is available, that long code is used. If a previously decoded long code is not available, the short scrambling code transmitted at the start of this second communication is used instead of the long scrambling code which has not yet been decoded.

35 The voice signals are scrambled by recording the voice for a predetermined time interval, dividing

-17-

the time interval into a series of sub-intervals, and then replaying the voice recorded during each sub-interval. The order in which the sub-intervals are replayed is substantially different from the order in which the sub-intervals were recorded. This results in an unintelligible pattern. This playback order is determined by the scrambling code passed between the two apparatuses prior to the start of the voice communications.

10 The scrambled signals are unscrambled by applying the process in reverse. The scrambled signals are recorded for the same predetermined time interval which is likewise divided into a series of sub-intervals. The scrambled signals recorded during each sub-interval are then replayed in the order specified by the scrambling code. Since both apparatuses have the same scrambling code, the unscrambling apparatus contains the information needed to properly play back the scrambled signals.

20 The acoustical voice signals of the user are detected by the microphone 12 and converted into digital words by the analog to digital converter 14. Each digital word generated by the analog to digital converter 14 represents the output voltage of microphone 12 at a given sample time. The acoustical voice signal is sampled at a rate determined by a clock 58. The digital words so generated are stored in either a first scrambling buffer 22 or a second scrambling buffer 32 depending on the state of a switch 13 which is under the control of the computer 18. The digital words are stored in the appropriate buffer in the order in which they are generated by the analog to digital converter 14. The two scrambling buffers 22 and 32 are identical. In the preferred embodiment, each contains in excess of 6000 words and the sampling rate is chosen such that each buffer records approximately 3/4 or a second of

-18-

speech from the microphone 12.

The contents of each buffer may be read out through an associated multiplexing circuit. The multiplexing circuit associated with the first scrambling buffer 22 is shown at 20. The multiplexing circuit associated with the second scrambling buffer 32 is shown at 30. The output of the multiplexing circuits 20 and 30 is input to a digital to analog converter 16 which drives the output line 40. The choice of which scrambling buffer is to be read out at a given time is determined by a switch 15 which is also under the control of the computer 18.

In the preferred embodiment, the scrambling buffers 22 and 32 are each divided into a plurality of sub-buffers 24. Each sub-buffer will preferably store 256 digital words of voice data. The associated multiplexing circuits 20 and 30 select which of the sub-buffers is to be read out at a given time. The contents of each sub-buffer are read out one word at a time in the sequence in which they were stored in that sub-buffer. The scrambling of the signal results from scrambling the order in which the sub-buffers are replayed rather than scrambling the contents of each sub-buffer. The order in which the individual sub-buffers are chosen for replaying is determined by the computer using a scrambling table 52 which contains an ordered list of the sub-buffers generated using the scrambling code. In the preferred embodiment, the order in which the sub-buffers are read out is essentially random.

Additional scrambling protocols which provide increased security against cryptanalytical attack may also be used with the apparatus of the present invention. First, one or more of the sub-buffers 24 may be read-out in an order different from that in which the contents of said sub-buffer 24 were stored. For

-19-

example, the contents of said sub-buffer could be read-out in the reverse order. That is, instead of reading out the contents in the order "first in first out", the contents would be read-out in the order "last in first out". The sub-buffers to be read-out in this manner may be specified by including a second seed in the scrambling code. This seed is used to define a second pseudo-random number sequence which in turn specifies the sub-buffers to be read-out in the altered order. Embodiments in which the read-out sequence is varied according to some other ordering procedure will be apparent to those skilled in the art.

Second, the lengths of the various sub-buffers 24 as well as the number of such sub-buffers may be made variable. In this embodiment, the scrambling table 52 would contain the number of sub-buffers, the length of each sub-buffer and the starting location of each sub-buffer in the relevant scrambling buffer, in addition to the order in which the sub-buffers are to be read-out. In this preferred embodiment, the lengths of the sub-buffers are chosen using an independent pseudo-random number sequence generated from an additional seed which is communicated as part of the scrambling code.

To avoid interruptions in the conversation being transmitted by the apparatus of the present invention, the scrambling buffers 22 and 32 are alternatively filled and replayed. While one scrambling buffer is being filled, the other is being replayed. At the end of the read out of a buffer the roles of the two scrambling buffers are reversed by reversing the state of the switches 13 and 15. Hence, one scrambling buffer is always available to record the output of the microphone 12.

In the preferred embodiment, the scrambled conversation is delayed by the time needed to fill a

-20-

buffer and read it out onto the communication link. This time delay may be reduced by employing the "sliding window" technique described by Becker and Piper in Cypher Systems (Wiley Interscience, 1982) which is hereby incorporated by reference. The time delay in question is only necessary if we allow every permutation of the sub-buffers. That is, a two buffer time delay is needed because sufficient time must be allowed to properly decode a transmission in which the last sub-buffer to be filled was the first sub-buffer to be read-out. Thus the sending apparatus must wait for all the sub-buffers to be filled before it can commence reading out the buffer in question onto the communication link. Similarly, the receiving apparatus must wait until all the sub-buffers are filled before it can commence reading out the buffer in question into the speaker. If one limits the possible permutations of the sub-buffers such that any given sub-buffer is not moved more than some maximum number, N, of sub-buffers from its original position, read out may be commenced before the entire buffer is filled. Here, read-out may be commenced as soon as the first N sub-buffers are filled. This maximum number of sub-buffers must be large enough to prevent cryptanalytic attack. However, this number can be substantially less than the entire length of the buffer in question. Thus, substantial reduction in the time delays may be obtained using this technique.

It should be noted that different scrambling buffer lengths may also be used. The buffer length must be sufficiently long to accommodate enough sub-buffers for security, but it must also short enough to assure that long time delays are not introduced into the communication.

The scrambled signals received over the input phone line 80 are unscrambled in an analogous manner. The scrambled signals are converted to digital words by

-21-

an analog to digital converter 62. The output of the analog to digital converter 62 is stored in one of two unscrambling buffers 68 or 70 depending on the state of the switch 63 which is under the control of the computer 18. The unscrambling buffers 68 and 70 are identical to the scrambling buffers 22 and 32 used to store the voice signals prior to scrambling. Each unscrambling buffer is divided into a plurality of sub-buffers 72. The digital values stored in a given sub-buffer may be replayed into a digital to analog converter 74 which drives the speaker 76. The replaying is accomplished with the aid of a multiplexing circuit associated with the unscrambling buffer in question. The multiplexer circuit associated with unscrambling buffer 68 is shown at 64. That associated with unscrambling buffer 70 is shown at 66. Each of the multiplexer circuits is under the control of the computer 18 which has access to an unscrambling table 54 which contains the order in which the unscrambling buffers are to be replayed. The values in each sub-buffer are replayed in the order in which they were received from the analog to digital converter 62, since it is only the order of the sub-buffers that has been scrambled.

As discussed above, other embodiments employing sub-buffers of variable length which are read out in orders different from the order in which the data was recorded are possible. In these embodiments, the computer communicates the starting and ending addresses of each sub-buffer together with the proper read-out order to the relevant multiplexing circuit. This data is contained in scrambling and unscrambling tables 52 and 54. Since both the sending and receiving apparatuses use the same procedures to generate this order starting from the same pseudo-random number seeds, the necessary information is available to both computers.

-22-

While one unscrambling buffer is being replayed, the other is being filled by the analog-to-digital converter 62. At the end of the replaying operation, the roles of the unscrambling
5 buffers are reversed by reversing the positions of the switches 63 and 73.

The scrambling table 52 and the unscrambling table 54 are generated using a pseudo-random number generator which is originally seeded with the scrambling
10 code. Such generators are well known to those skilled in the computer sciences. In the preferred embodiment, each buffer is divided into 32 sub-buffers. Hence the scrambling table 52 contains a list of the numbers from 1 to 32 in an essentially random order. This table may
15 be produced by assigning a pseudo-random number to each of the integers from 1 to 32 and then reordering this list of integers based the psuedo-random number assigned to each. The corresponding unscrambling table 54 contains the inverse of this list. After each table is
20 used, a new table is calculated. The new table replaces the oldest table stored.

To provide further security against cryptanalytic attack, frequence inversion scrambling techniques may be applied to the output of the present
25 invention before said output is placed on the communication link. The addition of frequency inversion scrambling to the output signal results in reduced residual intelligibility of the signal on the communication link. In this alternative embodiment of
30 the present invention, a frequency inversion scrambling circuit 110 is used to transform the output of the digital-to-analog converter 16 before said output is placed on the communication link. An analogous frequency inversion descrambling circuit 104 removes the
35 frequency inversion scrambling before the signal from the communication link is inputted into the

-23-

analog-to-digital converter 62. The protocols used by the frequency inversion scrambling circuit 110 and the frequency inversion descrambling circuit 104 are governed by a separate pseudo-random number seed which is passed as part of the scrambling code exchanged at the beginning of the communication.

In general, a frequency inversion scrambling circuit transforms the frequency spectrum of the signal inputted to it into a different frequency spectrum. The signal to be transformed may be represented mathematically by the equation

$$S(t) = A_i(t)F_i(f_i)$$

where

$S(t)$ is the amplitude of the signal to be transformed at time, t ,

$F_i(f)$ is a function describing the i th frequency band which is centered about a frequency f , and

$A_i(t)$ is the amplitude of the i th frequency component of the signal $S(t)$.

The transformed signal which is outputted onto the communication link may be represented by an analogous equation

$$S'(t) = B_i F_i(f_i)$$

Where the B_i 's are calculated from the A_i according to a scrambling protocol.

The simplest form of frequency inversion scrambling is one in which the relationship between the A_i 's and the B_i 's is given by

$$B_k(t) = A_{n-k+1}(t) \text{ for } k=1,2,\dots,n.$$

This transformation results in low frequency sounds being converted into high frequency sounds, and high frequency sounds being converted into low frequency sounds.

Other possible relationships between the A_i 's

-24-

and the B_i 's will be apparent to those skilled in the art. For example, the B_i 's could be calculated from the A_i 's by randomizing the order of the A_i 's using a pseudo-random number sequence generator seeded with a
5 seed passed as part of the scrambling code. In this case

$$B_k = A_j$$

where j is chosen at random from a set of values which is initially $1, 2, \dots, n$. Each time a j is so chosen,
10 that j is removed from the set in question. This guarantees that each A_i will be used once and only once.

The frequency inversion unscrambling circuit 104 performs the inverse transformation. The frequency scrambled signals inputted to it from the communication
15 link on line 80 are decomposed into a list of amplitudes representing the amplitude of the said frequency scrambled signals in each of the frequency bands used by the frequency scrambling circuit 110. This list of amplitudes is then reordered using the inverse of the
20 transformation employed by the frequency scrambling circuit 110 to scrambling the signals inputted to it. Since each of the apparatuses at the two ends of the communication link are using the same scrambling code, both apparatuses have the necessary information to
25 construct this inverse transformation. The transformed list of amplitudes is then used to generate an electrical signal which is inputted to the analog-to-digital converter 62.

Means for generating an analog signal from a
30 list of values representing the amplitude of said signal in each of a plurality of predetermined frequency bands are well known to those skilled in the electronic circuit arts. In general, such circuits consist of a number of oscillators. One such oscillator is provided
35 for each frequency band, the frequency of said oscillator being that of the frequency at the center of

-25-

said band. The amplitude of the output of each said oscillator is controlled by an input signal which is proportional to the corresponding value in said list. The outputs of all the oscillators are combined in a summing circuit to produce the signal in question.

Similarly, means for generating a list of values representing the amplitude of an analog signal in each of a plurality of predetermined frequency bands are also well known to those skilled in the electronic circuit arts. Typically, such circuits consist of a series of band pass filters and means for measuring the output amplitude of the signal transmitted by each said filter when the analog signal in question is inputted to said filters. The band of frequencies passed by each said filter corresponds to the band of frequencies in one of said predetermined frequency bands, and the amplitude of the signal passed by said filter corresponds to the said value representing the amplitude of said analog signal in said frequency band.

In addition to specifying the particular transformation used to scramble the frequency spectrum, the scrambling code can also specify the times during the communication at which the transformation in question is changed. For example, the frequency inversion scrambling circuit 110 could alternate between a mode in which simple frequency inversion scrambling as described above is used and no frequency inversion scrambling is used. The times at which the transitions are made could be specified by a pseudo-random number generator using a seed passed as part of the scrambling code.

The frequency inversion scrambling circuit may be placed at other locations in the communication path. For example, the frequency inversion scrambling circuit 110 could be placed between the analog-to-digital converter 16 and the microphone 12. In this embodiment, the corresponding frequency inversion descrambling

-26-

circuit would be placed between the digital to analog converter 74 and the speaker 76. Since the frequency inversion scrambling is independent of the time element scrambling, the order in which the two scrambling techniques are applied to the signal is not important.

It is essential to the operation of the system that both the calling apparatus and receiving apparatus remain synchronized with one another. Although both the calling apparatus and receiving apparatus contain crystal controlled clocks, it is not possible, at reasonable cost, to guarantee this synchronization over a long communication without an additional synchronization means which corrects any slight differences in the clock frequencies. In addition, there is an unknown delay in the communication link itself. This delay may change during the communication in question. Therefore, synchronization signals must be exchanged between the apparatuses during the communication. In the preferred embodiment, a synchronization generator 78 is used to periodically send a signal in the form a pulse at a specified frequency on the communication link. This signal is detected by the apparatus at the other end of the communication link by a synchronization detector 60. During the transmission of this signal, the digital to analog converter 74 is squelched to prevent the signal in question from introducing noise into the communication. The synchronization signal is used to reset the location in the buffer in which the analog-to-digital converter 14 stores its output.

To aid in the detection of the synchronization pulses, a notch filter 96 of conventional design may be included between the digital to analog converter 16 and the communication link to prevent the synchronization detector 60 in the corresponding apparatus at the other end of the communications link from mistaking scrambled

-27-

speech for the synchronization pulse in question. This filter substantially removes the frequency components of the scrambled speech from the narrow band of frequencies corresponding to the synchronization pulses. In addition, the output of the digital to analog converter 16 may be squelched during a short time period which includes the time at which a synchronization pulse is expected. This further limits the possibility of mistaking scrambled speech produced by either apparatus 10 from being mistaken as a synchronization pulse.

In the preferred embodiment, the synchronization pulses are sent out at varying times relative to the times at which the contents of the scrambling buffers are sent. If the synchronization pulses are sent at regular intervals, e.g., after every buffer is read out, an opponent would know how to at least synchronize his device with the scrambler. By varying the times of the synchronization pulses relative to the beginning of the buffer read out, the opponent in question is deprived of this information. Hence, the synchronization pulses are sent out at pseudo-random intervals determined by an independent pseudo-random number generator. Here, the scrambling code exchanged by the apparatuses during the initialization procedure contains a seed for this independent pseudo-random number generator as well as the seed used in the pseudo-random number generator which specifies the sequence in which the various sub-buffers are read out. Each apparatus includes an "offset" table 92 which specifies the time at which the next synchronization pulse is expected relative to the time at which the read out of a particular buffer is to be commenced. Similarly, the synchronization generator 78 in each apparatus has access to a corresponding offset table 94 which specifies the times at which synchronization pulses are sent relative to the times at which the

-28-

contents of the scrambling buffer are sent. The apparatus receiving the synchronization pulse compares its time of arrival to that given in the table and adjusts its timing accordingly. The contents of these
5 tables are loaded by the computer 18 using the pseudo-random number generator which was started from the seed communicated for this purpose during the initialization sequence. Since both apparatuses use the same pseudo-random number generator for this purpose,
10 they remain in synchronization with one another. However, no one else can determine how the synchronization pulses are related to the buffer or sub-buffer read out boundaries. Since the pseudo-random number generator used to specify the offsets is
15 independent of the pseudo-random number generator used to scramble and unscramble the voice signals, an opponent must determine two independent codes to unscramble the communication. This provides a significant increase in the security of the
20 communication in question.

The apparatus of the present invention is intended for use on a communication link consisting of a standard telephone communication system. In such systems, the input line 80 and the output line 40 must
25 share the same communications path.

Such a communications path creates significant difficulties not encountered in non-scrambled communications. Ordinary telephone lines are two-wire circuits in which both directions of speech are combined
30 on a single wire loop to the local switching office. Consider a conversation between two subscribers A and B. At the point at which subscriber A's telephone connects to the loop, electrical currents corresponding to speech from A's microphone are superimposed on electrical
35 currents arriving from the distant subscriber B. If a simple sum of these currents is made to flow in A's

-29-

earphone, he hears his own speech together with the speech from B which is attenuated due to the distance involved. In order to reduce the loudness of A's speech in his own earphone, a portion of the electrical signal produced by A's microphone is electrically subtracted from the sum of the currents present on the loop before those currents are passed through A's earphone. This results in a composite current containing a diminished amount of signal from A while maintaining the magnitude of the signal representing B's speech unaltered. The diminished amount of his own speech which A hears in his earphone is called "sidetone". Although this sidetone is unobjectionable in unscrambled communications, it makes full-duplex operation impractical in a scrambler of the type used in the present invention unless squelching techniques or advanced compensation techniques are employed.

The basic problem inherent in the scrambled communication arises from the time delay which results from the time needed to fill a scrambling buffer and the time needed to accumulate data in the unscrambling buffer. A's sidetone is delayed by two buffer read out times because his speech must be stored in a scrambling buffer prior to being read out onto the line and the speech which is read out into the line is further delayed by the time needed to fill the unscrambling buffer in A's apparatus and to then unscramble it. Thus, A's sidetone appears as an echo in his earphone. Furthermore, A's unscrambling circuits are synchronized to unscrambling signals originating in B's apparatus, not in A's apparatus. Hence, A's sidetone will not be properly unscrambled. The signals leaving B's apparatus arrive at A's apparatus after a delay which depends on the length of the communication link and the various switching circuits employed in said communication link. The synchronization pulses exchanged by the two

-30-

apparatuses keep A's unscrambling buffer synchronized with B's scrambling buffer. Since A's signals "arrive" at his apparatus without the above mentioned delay, they will not be properly synchronized with A's unscrambling
5 buffer. Thus, A will hear his speech scrambled in his earphone delayed by two buffer read out times. In addition to this echo, the local loop modifies the currents generated by A in a manner which is frequency dependent, unpredictable, and which varies with time.
10 Hence, merely subtracting A's output onto the loop from the input to A's unscrambling circuits will not eliminate this scrambled sidetone.

In the preferred embodiment, the sidetone is suppressed by squelching. Simple squelching systems are
15 well known to the art, e.g., push to talk or VOX. These systems are inadequate for scrambled communications. These prior art systems operate by squelching A's earphone during the time he is speaking. However, since A's speech is delayed by the time needed to read out
20 A's scrambling buffer and the time needed to read the contents back into A's unscrambling buffer, this squelching procedure results in A's earphone being squelched at the wrong time. The apparatus of the present invention avoids this problem by squelching the
25 input to A's unscrambling buffer in response to a signal actually being output to the communication link rather than in response to a signal detected at A's microphone as is the case in conventional squelching or VOX systems. When the output of A's digital to analog
30 converter 16 indicates that scrambled signals are being output by A onto the communication link, the output of A's analog-to-digital converter 62, which feeds A's unscrambling buffer, is forced to be zeros by the computer 18. As a result, no signals are output to A's
35 earphone from its unscrambling buffer during this corresponding time.

-31-

Alternative embodiments employing high-speed integrated circuit digital signal processors such as the Texas Instruments TMS 320 configured as an "adaptive echo canceler" will be apparent to those skilled in the art of telephone circuitry. This type of echo canceler periodically measures the parameters of the local loop including time delays and frequency dependencies in the sidetone. This circuit transforms the output of the unscrambling digital to analog converter with appropriate time delays so as to allow said output to be properly subtracted from the input to the unscrambling circuits. It is used as a component of the interface between the apparatus of the present invention and the telephone lines in the above mentioned sidetone subtraction scheme.

It should be noted that neither echo-cancellation nor squelching circuitry are required when the apparatus of the present invention is used on a four-wire circuit, i.e., one in which the two directions of communication are kept distinct from one end of the communication link to the other. Such circuits are commonly found in "private line" installations.

Figure 2 is a flow chart for the initialization sequence programs used by the calling apparatus in establishing a scrambled communication with the receiving apparatus. The communication link is initially established in a conventional manner by the calling apparatus dialing the number of the receiving apparatus and placing the relevant tones on the telephone lines. This software is in the modem 19. Once the communication link has been established, the calling apparatus sends a first message in digital form and waits for a second message from the receiving apparatus. The second message is compared with the text of an expected second message stored in the computer 18 of the calling apparatus. If it does not match, the

-32-

calling apparatus enters a non-secure communication mode in which the calling apparatus does not scramble the conversation. If the second message matches that stored in the calling apparatus, the calling apparatus
5 generates an encrypting code and transmits it to the receiving apparatus.

The encrypting code is generated by selecting two prime numbers from a table 56 of primes stored in the calling apparatus. When the apparatus of the
10 present invention is not busy communicating with another apparatus of the present invention, it generates prime numbers and stores them in table 56. The two prime numbers selected from the table 56 for use in a given communication are selected at random from the stored
15 primes by generating pseudo-random numbers which define which entries in the table are to be used. The encrypting code is the product of the two prime numbers selected. The encrypting code is transmitted to the receiving apparatus in digital form by the modem 19.

20 The calling apparatus then waits for an encrypted scrambling code to be received from the receiving apparatus over the modem 19 in digital form. The encrypted scrambling code is then decrypted, using the method described above, and stored in the computer
25 18. The scrambling code is then used as a seed for a pseudo-random number generator used to calculate the values to be entered into the scrambling and unscrambling tables. In the preferred embodiment, each of the buffers used to store the digital values
30 representing the output voltage of the speech input to the microphone 12 of the present invention is divided into 32 sub-buffers 24. The scrambling and unscrambling tables, 52 and 54, each consist of a list of the 32 addresses of the sub-buffers. The 32 addresses are
35 placed in the table in question in a random order. The random order is created by first ordering the addresses

-33-

in ascending order in a scratch table contained in the computer 18 and then assigning a pseudo-random number to each of the addresses. The addresses are then reordered in the scratch table according to the pseudo-random
5 number assigned to each and transferred to the scrambling table 52. The reordered table contains as its first entry the address which was assigned the largest pseudo-random number, as its second entry the address which was assigned the second largest
10 pseudo-random number and so on.

The scrambling table 52 is a mapping of the contents of a scrambling buffer in one apparatus into the unscrambling buffer of the other apparatus. The unscrambling table 54 is the inverse mapping. Its first
15 entry is the address in the unscrambling buffer at which the data which was originally stored in the first sub-buffer of the scrambling buffer in the other apparatus will be stored when that data is received. Its second entry is the address in the unscrambling
20 buffer at which the data which was originally stored in the second sub-buffer of the scrambling buffer of the other apparatus will be stored, and so on.

At any given time, both apparatuses are scrambling data using the same scrambling table 52. The
25 data received by one apparatus from the other is not unscrambled until an unscrambling buffer has been filled and switched to the digital to analog converter 74. It takes the same amount of time to readout a scrambling buffer as to read in the data for the unscrambling
30 buffer. Hence, by the time an unscrambling buffer has been filled, the apparatuses will have generated new scrambling tables. Thus the unscrambling table which is used is the one corresponding to the scrambling table which was used prior to the scrambling table currently
35 being used to scramble the signals. For this reason, the unscrambling table 54, contains space for two

-34-

"unscrambling tables", a first table corresponding to the scrambling table currently being used to scramble data for output to the communication link and a second table corresponding to the scrambling table used prior
5 to said first table.

Figure 3 is a flow chart for the initialization sequence programs used in the receiving apparatus. The receiving apparatus begins by answering the telephone and establishing a communication link using the modem
10 19. It then waits for a first message to be received from the calling apparatus and tests that message against an expected message stored in the computer 18 contained in the receiving apparatus. If the received message does not match the stored message, the receiving
15 apparatus remains in an non-secure mode in which voice communications are not scrambled. If the received message matches the stored message, the receiving apparatus responds by sending a second predetermined message to the calling apparatus. In the preferred
20 embodiment, each message sent by the calling and receiving apparatuses consists of three parts, a character specifying the length of an ASCII string of characters, the ASCII string in question, and two characters specifying a cyclic redundancy check (CRC).
25 The CRC is computed by conventional means. The apparatus which receives the message computes its own CRC check on the message. If it matches the CRC in the message, it sends the ASCII character ACK (hex 06). If it does not match, it sends the ASCII character NAK (hex
30 15) and waits for the sending machine to repeat the message. If the message is not correctly transmitted after a predetermined number of attempts, the apparatuses enter the non-secure mode.

Similarly, when one of the apparatuses sends a
35 message on the communication link to the other, it waits for either an ACK or NAK response indicating whether the

-35-

transmission was successful or not. If unsuccessful, it repeats the message.

Once the predetermined messages have been sent and verified by each apparatus, the receiving apparatus
5 waits for the calling apparatus to send an encrypting code to be used by it in transmitting a scrambling code to the calling apparatus.

The scrambling code is then generated using a pseudo-random number generator. The pseudo-random
10 number is generated using standard pseudo-random number procedures. The procedures typically calculate a pseudo-random number from a "seed" number. A new seed is then calculated and used to calculate the next pseudo-random number. Periodically, the seed used to
15 generate the pseudo-random numbers which will be used to calculate the next prime number and the next scrambling codes, is altered in response to an event which cannot be predicted from the past behavior of the receiving apparatus. For example, when a call is received, the
20 receiving apparatus can change the seed by measuring the time difference between the beginning of the call and the time at which the AC line voltage which provides the power for the receiving apparatus crosses zero volts. Alternatively, each time a call is made from the
25 apparatus of the present invention, the computer can choose a new seed for the pseudo-random number generator used to generate prime numbers and scrambling codes. The new seed value is based on the time interval between the current call and the one preceding it. Since there
30 is no way of predicting the intervals at which calls are made from the apparatus, this guarantees that the next encrypting and decrypting codes as well as the next scrambling code generated by the apparatus may not be predicted from an examination of the apparatus.

35 The scrambling code is stored in the receiving apparatus and then encoded using the encrypting

-36-

procedure described above. The encoded scrambling code is then transmitted to the calling apparatus. The receiving apparatus then resets the various buffers and counters contained therein and waits for a
5 synchronization signal from the calling apparatus. Upon receipt of the synchronization signal, it enters the secure communication mode in which the speech signals input to the receiving apparatus are scrambled and output onto the communications link and the scrambled
10 speech signals received from the communications link are unscrambled and output onto the speaker in the receiving apparatus.

Figure 4 is a flow chart for the scrambling functions in both the calling apparatus and receiving
15 apparatus. As discussed above, the calling apparatus and receiving apparatus each contain buffers 22 and 32 for storing a digital representation of the speech signals inputted into the apparatus of the present invention. These buffers are divided into sub-buffers
20 24 which are read out during the scrambling process. Each sub-buffer 24 is read out in its entirety before reading out the next sub-buffer 24. The order in which the sub-buffers are to be read out is stored in a scrambling table 52 which contains the address of each
25 of the sub-buffers. Initially, a pointer is set to the first entry in this table. The address defined by this pointer is loaded into the appropriate multiplex circuit by the computer. The contents of the sub-buffer so identified are read out of that sub-buffer one slot at a
30 time and then transmitted to the digital to analog converter 16. At the end of each sub-buffer readout operation, the pointer is incremented and the process repeated until the pointer has been incremented past the last entry in the scrambling table.

35 A new scrambling table 52 is then generated using the pseudo-random number generator in the same

-37-

manner as was done in generating the previous table. The buffers used in the scrambling process are then switched in roles. The buffer which was just read out being used to accumulate data from the microphone 12.

- 5 The buffer which had been accumulating data from the microphone is now switched to the digital-to-analog converter 16.

Figure 5 is a flow chart of the unscrambling functions in both the calling and receiving apparatuses.

- 10 As discussed above, the calling and receiving apparatuses each contain buffers 68 and 70 for storing a digital representation of the scrambled voice signals inputted from the communication link. When a buffer has been filled with digital values representing the
- 15 scrambled voice patterns transmitted on the communication link, the buffer is switched to an output mask in which each of the sub-buffers making up this buffer may be connected to the digital-to-analog converter which drives the speaker. Initially, a
- 20 pointer is set to indicate the first entry in the unscrambling table which contains the address of this first sub-buffer to be read out into the speaker 76. The address of sub-buffer so identified is entered in the multiplexer circuit by the computer and the contents
- 25 of that sub-buffer read out to the digital to analog converter, one slot at a time. When the last slot of the sub-buffer is read out, the pointer is incremented, and the next sub-buffer is read out. After the last sub-buffer is read out, the buffer which had been
- 30 accumulating data during the read out of the present buffer is switched to the read out mode, the present buffer being switched to accumulate the incoming voice patterns. A new unscrambling table is then loaded, and the processes repeated.

- 35 Periodically, each apparatus generates a synchronization pulse which is used by the apparatus at

-38-

the other end of the communication link to synchronize its operation. This pulse is generated at the end of every Nth buffer read out. It is detected by corresponding apparatus and used to reset the location in the input buffers at which digital values are being accumulated. When a synchronization pulse is detected by the synchronization detector 60, the computer is interrupted. It then resets the buffer being used to accumulate digital representation of the voice pattern such that the next digital value will be stored at the first location in this buffer.

In the preferred embodiment, both the calling and receiving functions are contained in the same apparatus. However, embodiments in which these functions are contained in separate machines will be obvious to those skilled in the art. Separately the functions would provide an added degree of security in specialized systems such as those used for carrying out banking operations. In addition, a system in which the calling apparatus has significantly more computing capability than the receiving apparatus would allow use of longer encrypting codes and have a higher degree of security.

Various modifications will be apparent to those skilled in the art without departing from the present invention as claimed.

-39-

WHAT IS CLAIMED IS :

1. A scrambling system for communicating over an non-secure communication link comprising a calling apparatus and a receiving apparatus, wherein each of said calling apparatus and receiving apparatus
5 comprises: acoustical input means for generating analog voice signals corresponding to spoken transmissions of the user of said calling apparatus or receiving apparatus; acoustical output means for outputting acoustical signals corresponding to analog signals
10 coupled thereto; electrical input means for detecting analog signals on said communication link; electrical output means for outputting analog signals onto said communication link; means for storing a scrambling code; means responsive to said stored scrambling code for
15 scrambling analog signals generated by said acoustical input means and for coupling said scrambled signals to said electrical output means; means responsive to said stored scrambling code for unscrambling analog signals detected by said electrical input means and for coupling
20 said unscrambled analog signals to said acoustical output means; said calling apparatus further comprising: calling means for establishing a communication link with a said receiving apparatus, including means for verifying that said receiving apparatus is compatible
25 with said calling apparatus; means for generating an encrypting code; means for transmitting said encrypting code over said communications link to said receiving apparatus; means for detecting on said communications link a scrambling code encrypted using said encrypting
30 code transmitted by said receiving apparatus; and means for decrypting said scrambling code; said receiving apparatus further comprising: receiving means for establishing a communication with a calling apparatus over said communication link, including means for

-40-

verifying that said calling apparatus is compatible with said receiving apparatus; means for detecting on said communication link said encrypting code transmitted by said calling apparatus; means for generating a
5 scrambling code; means for encrypting said scrambling code using said encrypting code; and means for transmitting said encrypted scrambling code over said communication link to said calling apparatus.

2. The scrambling system of Claim 1 wherein a
10 receiving apparatus and a calling apparatus are contained in the same apparatus.

3. The scrambling system of Claim 1 wherein said calling means for verifying that said receiving apparatus is compatible with said calling apparatus
15 comprises: means for sending a first predetermined message to said receiving apparatus; means for receiving a second predetermined message from said receiving apparatus; and means for verifying said second predetermined message.

20 4. The scrambling system of Claim 3 wherein said receiving means for verifying that said calling apparatus is compatible with said receiving apparatus comprises: means for receiving said first predetermined message; means for verifying said first predetermined
25 message; and means for sending said second predetermined message to said calling apparatus.

5. The scrambling system of Claim 3 or Claim 4 wherein said first and second predetermined messages comprise strings of ASCII characters.

30 6. The scrambling system of Claim 1 wherein said encrypting code is the product of first and second prime numbers.

7. The scrambling system of Claim 6 further comprising: means for computing said first and second
35 prime numbers.

8. The scrambling system of Claim 7 wherein

-41-

said means for computing said first and second prime numbers comprises: means for generating a pseudo-random number; means for determining if said pseudo-random number has a high probability of being a prime number; and means for periodically resetting said pseudo-random number generating means in response to a substantially random event.

9. The scrambling system of Claim 1 further comprising: means responsive to said scrambling code for generating a pseudo-random number.

10. The scrambling system of Claim 1 wherein said means for scrambling analog signals comprises: means for recording analog signals representative of acoustical signals inputted on said acoustical input means during a predetermined time interval, said predetermined time interval being divided into a plurality of sub-intervals; and means for replaying said recorded analog signals and for coupling said analog signals to said electrical output means, wherein the analog signals recorded in each sub-interval are replayed in their entirety before replaying the analog signals recorded in another sub-interval, and wherein the order in which the sub-intervals are chosen to be replayed is determined by said scrambling code.

11. The scrambling system of Claim 10 wherein said means for recording said analog signals comprises: means for generating a digital value corresponding to said analog signal at successive points in time; clock means for specifying the times at which each said digital value is generated; first and second scrambling buffer means for storing said generated digital values, each said buffer means comprising: a plurality of contiguous memory slots, one said digital value being stored in each said memory slot, the order of said digital values in said scrambling buffer means being the same as the order in which said digital values were

-42-

generated, each said scrambling buffer means being further divided into a plurality of sub-buffers, each said sub-buffer comprising: a contiguous block of memory slots, one such sub-buffer corresponding to each of said sub-intervals; means for alternately routing said generated digital values into said first and said second scrambling buffer means, including means for causing said digital values to be initially routed into said first scrambling buffer means and means for causing said digital values to be routed into the other of said first or second scrambling buffer means when the buffer means into which said digital values are currently being routed is filled.

12. The scrambling system of Claim 11 wherein said means for replaying said recorded analog signals comprises: means for generating an analog signal corresponding to a digital value stored in a selected memory slot in said first or said second scrambling buffer means at a time specified by said clock means; means for specifying an ordered sequence of sub-buffers responsive to said scrambling code; slot ordering means for specifying an ordered sequence of memory slots in each said sub-buffer; and sub-interval playback means for replaying the analog digital signals stored in each sub-buffer in the order specified by said order sequence specifying means, said sub-interval playback means including means for selectively coupling each of the digital values stored in a specified sub-buffer to said analog signal generating means to successively generate an analog signal therefrom, the order of said analog signal generation being specified by said slot ordering means.

13. The scrambling system of Claim 1 wherein said means for unscrambling analog signals comprises: means for recording said analog signals detected by said electrical input means during a predetermined time

-43-

interval, said predetermined time interval being divided into a plurality of sub-intervals; and means for replaying said recorded analog signals and for coupling said replayed analog signals to said acoustical output means, wherein the analog signals recorded in each sub-interval are replayed in their entirety before the analog signals recorded in another sub-interval are replayed, and wherein the order in which the sub-intervals are selected to be replayed is determined by said scrambling code.

14. The scrambling system of Claim 13 wherein said means for recording said analog signals comprises: means for generating a digital value corresponding to said analog signals at successive points in time; clock means for specifying the times at which each said value is generated; first and second unscrambling buffer means for storing the digital values so generated, each said unscrambling buffer means comprising: a plurality of contiguous memory slots, one said digital value being stored in each said memory slot the order of said digital values in said unscrambling buffer means being the same as the order in which said digital values were generated; each said unscrambling buffer means being further divided into a plurality of sub-buffers, each said sub-buffer comprising: a contiguous block of memory slots, one such sub-buffer corresponding to each of said sub-intervals; means for alternately routing said generated digital values into said first or second unscrambling buffer means, including means for causing said digital values to be initially routed into said first unscrambling buffer means and means for causing said digital values to be routed into the other of said first or second unscrambling buffer means when the unscrambling buffer means into which said digital values are currently being routed is filled.

15. The scrambling system of Claim 14 wherein

-44-

said means for replaying said recorded analog signals comprises: means for generating an analog signal corresponding to a digital value stored in a selected memory slot in said first or said second scrambling
5 buffer means at a time specified by said clock means; means for specifying an ordered sequence of sub-buffers responsive to said scrambling code; slot ordering means for specifying an ordered sequence of memory slots in each said sub-buffer; and sub-interval playback means
10 for replaying the recorded digitized analog signals stored in each sub-buffer in the order specified by said order sequence specifying means, said sub-interval playback means including means for selectively coupling each of the digital values stored in a specified
15 sub-buffer to said analog signal generating means to successively generate an analog signal therefrom, the order of said analog signal generation being specified by said slot ordering means.

16. The scrambling system of Claim 12 wherein
20 said means for specifying an ordered sequence of sub-buffers comprises: means for storing a list of numbers representing the order in which said sub-buffers are to be replayed, said order being responsive to said scrambling code and being substantially random; and
25 means responsive to said scrambling code for regenerating said list of numbers after each of said first and second buffers is replayed.

17. The scrambling system of Claim 16 wherein
said means for generating said list of numbers comprises
30 a pseudo-random number generator.

18. The scrambling system of Claim 1 further comprising: means coupled to said electrical output means for sending a synchronization pulse; means coupled to said electrical input means for receiving a
35 synchronization pulse; and means for specifying the times at which said sending means sends said

-45-

synchronization pulse and for determining the times at which said means for receiving said synchronization pulse expects to receive said synchronization pulse.

19. The scrambling system of Claim 1 wherein
5 each of said calling apparatus and said receiving apparatus further comprises: means for storing a long scrambling code; means for specifying that said long scrambling code is to be used in scrambling and
10 unscrambling said analog signals by said scrambling and unscrambling means; means for storing the identity of the other of said calling apparatus or receiving apparatus with which a communication had previously taken place and for relating said identity to said long scrambling code; said calling apparatus further
15 comprising: means for generating a long encrypting code; means for transmitting said long encrypting code over said communication link to said receiving apparatus; means for detecting on said communication link a long scrambling code transmitted by said receiving apparatus
20 encrypted using said encryption code; means for decrypting said long scrambling code; said receiving apparatus further comprises: means for detecting on said communication link said long encrypting code transmitted by said calling apparatus; means for generating a long
25 scrambling code; means for encrypting said long scrambling code using said long encrypting code; and means for transmitting said encrypted long scrambling code over said communication link to said calling apparatus.

30 20. A scrambling apparatus for communicating over an non-secure communication link with a compatible scrambling apparatus comprising: acoustical input means for generating analog voice signals corresponding to spoken transmissions of the user of said scrambling
35 apparatus; acoustical output means for outputting acoustical signals corresponding to analog signals

-46-

coupled thereto; electrical input means for detecting analog signals on said communication link; electrical output means for outputting analog signals to said communication link; means for storing a scrambling code; means responsive to said stored scrambling code for scrambling analog signals generated by said acoustical input means and for coupling said scrambled signals to said electrical output means; means responsive to said stored scrambling code for unscrambling analog signals detected by said electrical input means and for coupling said unscrambled analog signals to said acoustical output means; calling means for establishing a communication over said communication link with a compatible scrambling apparatus, including means for verifying that said compatible scrambling apparatus is compatible with said scrambling apparatus; means for generating an encrypting code; means for transmitting said encrypting code over said communication link to said compatible scrambling apparatus; means for detecting on said communication link a scrambling code encrypted using said encrypting code transmitted by said compatible scrambling apparatus; and means for decrypting said scrambling code.

21. The scrambling apparatus of Claim 20 further comprising: means for detecting that a compatible calling scrambling apparatus is attempting to communicate with said apparatus over said communication link; means for verifying that said calling scrambling apparatus is compatible with said scrambling apparatus; means for detecting on said communication link and encrypting code transmitted by said calling scrambling apparatus; means for generating a scrambling code; means for encrypting said scrambling code using said encrypting code; and means for transmitting said encrypted scrambling code over said communication link to said calling scrambling apparatus.

-47-

22. The scrambling apparatus of Claim 20 wherein said means for verifying that said compatible scrambling apparatus is compatible with said scrambling apparatus comprises: means for sending a first
5 predetermined message to said compatible scrambling apparatus; means for receiving a second predetermined message from said compatible scrambling apparatus; and means for verifying said second predetermined message.

23. The scrambling apparatus of Claim 22
10 wherein said first and second predetermined messages comprise strings of ASCII characters.

24. The scrambling apparatus of Claim 20 wherein said encrypting code is the product of first and second prime numbers.

15 25. The scrambling apparatus of Claim 20 further comprising: means for responsive to said scrambling code for generating a pseudo-random number.

26. The scrambling apparatus of Claim 20 wherein said means for scrambling analog signals
20 comprises: means for recording analog signals representative of acoustical signals inputted on said acoustical input means during a predetermined time interval, said predetermined time interval being divided into a plurality of sub-intervals; and means for
25 replaying said recorded analog signals and for coupling said replayed analog signals to said electrical output means, wherein the analog signals recorded in each sub-interval are replayed in their entirety before
30 replaying the analog signals recorded in another sub-interval, and wherein the order in which the sub-intervals are chosen to be replayed is determined by said scrambling code.

27. The scrambling apparatus of Claim 26 wherein said means for recording said analog signals
35 comprises: means for generating a digital value corresponding to said analog signal at successive points

-48-

in time; clock means for specifying the times at which each said digital value is generated; first and second scrambling buffer means for storing said generated digital values, each said buffer means comprising: a
5 plurality of contiguous memory slots, one said digital value being stored in each said memory slot, the order of said digital values in said scrambling buffer means being the same as the order in which said digital values were generated, each said scrambling buffer means being
10 further divided into a plurality of sub-buffers, each said sub-buffer comprising: a contiguous block of memory slots, one such sub-buffer corresponding to each of said sub-intervals; means for alternately routing said digital values into said first and said second
15 scrambling buffer means, including means for causing said digital values to be initially routed into said first scrambling buffer means and means for causing said digital values to be routed into the other of said first or second scrambling buffer means when the buffer means
20 into which said digital values are currently being routed is filled.

28. The scrambling apparatus of Claim 27 wherein said means for replaying said recorded analog signals comprises: means for generating an analog signal
25 corresponding to a digital value stored in a selected memory slot in said first or said second scrambling buffer means at a time specified by said clock means; means for specifying an ordered sequence of sub-buffers responsive to said scrambling code; slot ordering means
30 for specifying an ordered sequence of memory slots in each said sub-buffer; and sub-interval playback means for replaying the analog signals stored in each sub-buffer digitized in the order specified by said order sequence specifying means, said sub-interval
35 playback means including means for selectively coupling each of the digital values stored in a specified

-49-

sub-buffer to said analog signal generating means to successively generate an analog signal therefrom, the order of said analog signal generation being specified by said slot ordering means.

5 29. The scrambling apparatus of Claim 20 wherein said means for unscrambling analog signals comprises: means for recording said analog signals detected by said electrical input means during a predetermined time interval, said predetermined time
10 interval being divided into a plurality of sub-intervals; and means for replaying said recorded analog signals and for coupling said replayed analog signals to said acoustical output means, wherein the analog signals recorded in each sub-interval are
15 replayed in their entirety before the analog signals recorded in another sub-interval are replayed, and wherein the order in which the sub-intervals are selected to be replayed is determined by said scrambling code.

20 30. The scrambling apparatus of Claim 29 wherein said means for recording said analog signals comprises: means for generating a digital value corresponding to said analog signals at successive points in time; clock means for specifying the time at
25 which each said value is generated; first and second unscrambling buffer means for storing the digital values so generated, each said unscrambling buffer means comprising: a plurality of contiguous memory slots, one said digital value being stored in each said memory slot
30 the order of said digital values in said unscrambling buffer means being the same as the order in which said digital values were generated; each said unscrambling buffer means being further divided into a plurality of sub-buffers, each said sub-buffer comprising: a
35 contiguous block of memory slots, one such sub-buffer corresponding to each of said sub-intervals; means for

-50-

alternately routing said generated digital values into said first or said second unscrambling; buffer means, including means for causing said digital values to be initially routed into said first unscrambling buffer
5 means and means for causing said digital values to be routed into the other of said first or second unscrambling; buffer means when the unscrambling buffer means into which said digital values are currently being routed is filled.

10 31. The scrambling apparatus of Claim 30 wherein said means for replaying said recorded analog signals comprises: means for generating an analog signal corresponding to a digital value stored in a selected memory slot in said first or said second scrambling
15 buffer means at a time specified by said clock means; means for specifying an ordered sequence of sub-buffers responsive to said scrambling code; slot ordering means for specifying an ordered sequence of memory slots in each said sub-buffer; and sub-interval playback means
20 for replaying the digitized recorded analog signals stored in each sub-buffer in the order specified by said order sequence specifying means said sub-interval playback means including means for electrically coupling each of the digital values stored in a specified
25 sub-buffer to said analog signal generating means to successively generate an analog signal therefrom, the order of said generation being specified by said slot ordering means.

30 32. The scrambling apparatus of Claim 28 wherein said means for specifying an ordered sequence of sub-buffers comprises: means for storing a list of numbers representing the order in which said sub-buffers are to be replayed, said order being responsive to said scrambling code and being substantially random; and
35 means responsive to said scrambling code for regenerating said list of numbers after each of said

-51-

first and second buffers is replayed.

33. The scrambling apparatus of Claim 32 wherein said means for generating said list of numbers comprises: a pseudo-random number generator.

5 34. The scrambling apparatus of Claim 20 further comprising: means coupled to said electrical output means for sending a synchronization pulse; means coupled to said electrical input means for receiving a synchronization pulse; and means for specifying the
10 times at which said sending means sends said synchronization pulse and for determining the times at which said means for receiving said synchronization pulse effects to receive said synchronization pulse.

 35. The scrambling apparatus of Claim 20
15 further comprising: means for storing a long scrambling code; means for specifying that said long scrambling code is to be used in scrambling and unscrambling said analog signals by said scrambling and unscrambling means; means for storing the identity of a compatible
20 scrambling apparatus with which a communication had previously taken place; said scrambling apparatus further comprising: means for generating a long encrypting code; means for transmitting said long encrypting code over said communication link to said
25 compatible scrambling apparatus; means for detecting on said communication link a long scrambling code encrypted using said encrypting code transmitted by said compatible scrambling apparatus; and means for decrypting said long scrambling code.

30 36. A scrambling apparatus for communicating over an non-secure communication link with a compatible scrambling apparatus comprising: acoustical input means for generating analog voice signals corresponding to spoken transmissions of the user of said scrambling
35 apparatus; acoustical output means for outputting acoustical signals corresponding to analog signals

-52-

coupled thereto; electrical input means for detecting analog signals on said communication link; electrical output means for outputting analog signals on to said communication link; means for storing a scrambling code; means responsive to said stored scrambling code for scrambling analog signals generated by said acoustical input means and for coupling said scrambled signals to said electrical output means; means responsive to said stored scrambling code for unscrambling analog signals detected by said electrical input means and for coupling said unscrambling analog signals to said acoustical output means; receiving means for establishing a communication with said compatible scrambling apparatus over said communication link, including means for verifying that said compatible scrambling apparatus is compatible with said scrambling apparatus; means for detecting on said communication link an encrypting code transmitted by said compatible scrambling apparatus; means for generating a scrambling code; means for encrypting said scrambling code using said encrypting code; and means for transmitting said encrypted scrambling code over said communication link to said compatible scrambling apparatus.

37. The scrambling apparatus of Claim 36 wherein said receiving means for verifying that said compatible apparatus is compatible with said scrambling apparatus comprises: means for receiving a first predetermined message from said compatible scrambling apparatus; means for verifying said first predetermined message; and means for sending a second predetermined message to said compatible scrambling apparatus.

38. The scrambling apparatus of Claim 37 wherein said first and second predetermined messages comprise strings of ASCII characters.

39. The scrambling apparatus of Claim 36 wherein said encrypting code is the product of first and

-53-

second prime numbers.

40. The scrambling apparatus of Claim 36 further comprising: means for responsive to said scrambling code for generating a pseudo-random number.

5 41. The scrambling apparatus of Claim 36 wherein said means for scrambling analog signals comprises: means for recording analog signals representative of acoustical signals inputted on said acoustical input means during a predetermined time
10 interval, said predetermined time interval being divided into a plurality of sub-intervals; and means for replaying said recorded analog signals and for coupling said analog signals to said electrical output means, wherein the analog signals recorded in each sub-interval
15 are replayed in their entirety before replaying the analog signals recorded in another sub-interval, and wherein the order in which the sub-intervals are chosen to be replayed is determined by said scrambling code.

20 42. The scrambling apparatus of Claim 41 wherein said means for recording said analog signals comprises: means for generating a digital value corresponding to said analog signal at successive points in time; clock means for specifying the times at which
25 each said digital value is generated; first and second scrambling buffer means for storing the digital values so generated, each said buffer means comprising: a plurality of contiguous memory slots, one said digital value being stored in each said memory slot, the order of said digital values in said scrambling buffer means
30 being the same as the order in which said digital values were generated, each said scrambling buffer means being further divided into a plurality of sub-buffers, each said sub-buffer comprising: a contiguous block of memory slots, one such sub-buffer corresponding to each of said
35 sub-intervals; means for alternately routing said generated digital values into one of said first and said

-54-

second scrambling buffer means, including means for causing said digital values to be initially routed into said first scrambling buffer means and means for causing said digital values to be routed into the other of said first or second scrambling buffer means when the buffer means into which said digital values are currently being routed is filled.

43. The scrambling apparatus of Claim 42 wherein said means for replaying said recorded analog signals comprises: means for generating an analog signal corresponding to a digital value stored in a selected memory slot in said first or said second scrambling buffer means at a time specified by said clock means; means for specifying an ordered sequence of sub-buffers responsive to said scrambling code; slot ordering means for specifying an ordered sequence of memory slots in each said sub-buffer; and sub-interval playback means for replaying the digitized analog signals stored in each sub-buffer the order specified by said order sequence specifying means, said sub-interval playback means including means for selectively coupling each of the digital values stored in a specified sub-buffer to said analog signal generating means to successively generate an analog signal therefrom, the order of said analog signal generation being specified by said slot ordering means.

44. The scrambling apparatus of Claim 36 wherein said means for unscrambling analog signals comprises: means for recording said analog signals detected by said electrical input means during a predetermined time interval, said predetermined time interval being divided into a plurality of sub-intervals; and means for replaying said recorded analog signals and for coupling said replayed analog signals to said acoustical output means, wherein the analog signals recorded in each sub-interval are

-55-

replayed in their entirety before the analog signals recorded in another sub-interval are replayed, and wherein the order in which the sub-intervals are selected to be replayed is determined by said scrambling
5 code.

45. The scrambling apparatus of Claim 44 wherein said means for recording said analog signals comprises: means for generating a digital value corresponding to said analog signals at successive
10 points in time; clock means for specifying the time at which each said digital value is generated; first and second unscrambling buffer means for storing the digital values so generated, each said unscrambling buffer means comprising: a plurality of contiguous memory slots, one
15 said digital value being stored in each said memory slot, the order of said digital values in said unscrambling buffer means being the same as the order in which said digital values were generated; each said unscrambling buffer means being further divided into a
20 plurality of sub-buffers, each said sub-buffer comprising: a contiguous block of memory slots, one such sub-buffer corresponding to each of said sub-intervals; means for alternately routing said generated digital values into said first or said second unscrambling
25 buffer means, including means for causing said digital values to be initially routed into said first unscrambling buffer means and means for causing said digital values to be routed into the other of said first or second unscrambling buffer means when the
30 unscrambling buffer means into which said digital values are currently being routed is filled.

46. The scrambling apparatus of Claim 45 wherein said means for replaying said recorded analog signals comprises: means for generating an analog signal
35 corresponding to a digital value stored in a selected memory slot in said first or said second scrambling

-56-

buffer means at a time specified by said clock means;
means for specifying an ordered sequence of sub-buffers
responsive to said scrambling code; slot ordering means
for specifying an ordered sequence of memory slots in
5 each said sub-buffer; and sub-interval playback means
for replaying the digitized recorded analog signals
stored in each sub-buffer in the order specified by said
order sequence specifying means, said sub-interval
playback means including means for selectively coupling
10 each of the digital values stored in a specified
sub-buffer to said analog signal generating means to
successively generate an analog signal therefrom, the
order of said analog signal generation being specified
by said slot ordering means.

15 47. The scrambling apparatus of Claim 43
wherein said means for specifying an ordered sequence of
sub-buffers comprises: means for storing a list of
numbers representing the order in which said sub-buffers
are to be replayed, said order being responsive to said
20 scrambling code and being substantially random; and
means responsive to said scrambling code for
regenerating said list of numbers after each of said
first and second buffers is replayed.

25 48. The scrambling apparatus of Claim 47
wherein said means for generating said list of numbers
comprises a pseudo-random number generator.

49. The scrambling apparatus of Claim 36
further comprising: means coupled to said electrical
output means for sending a synchronization pulse; means
30 coupled to said electrical input means for receiving a
synchronization pulse; and means for specifying the
times at which said sending means sends said
synchronization pulse and for determining the times at
which said means for receiving said synchronization
35 pulse effects to receive said synchronization pulse.

50. The scrambling apparatus of Claim 36

-57-

further comprising: means for storing a long scrambling code; means for specifying that said long scrambling code is to be used in scrambling and unscrambling said analog signals by said scrambling and unscrambling means; means for storing the identity of a compatible scrambling apparatus with which a communication had previously taken place; means for detecting on said communication link a long encrypting code transmitted by said compatible scrambling apparatus; means for generating a long scrambling code; means for encrypting said long scrambling code using said long encrypting code; and means for transmitting said encrypted long scrambling code to said compatible scrambling apparatus over said communications link.

51. The scrambling system of Claim 1 or the scrambling apparatus of Claim 20 or Claim 36 further comprising means for inhibiting said unscrambling means when said scrambling means is outputting non-zero scrambled signals on said electrical output means.

52. The scrambling system of Claim 5 or the scrambling apparatus of Claim 27 or Claim 38 wherein each said means for receiving a predetermined message comprises: means for determining if said message was properly transmitted on said communication link; means coupled to said communication link for indicating that said message was received correctly; and means coupled to said communication link for indicating that said message was not received correctly and should be retransmitted; each said means for sending a predetermined message comprises means for determining if said predetermined message was properly received including means for repeating said predetermined message if it was not properly received.

53. The scrambling system of Claim 52 wherein each of said first and second predetermined message comprises a variable length string of ASCII characters

-58-

preceded by a character which specifies the length of said ASCII string of characters and followed by two characters which specify a cyclic redundancy check test value; wherein said first predetermined message includes
5 the character "H" as the last character of said ASCII string and the second predetermined message includes the character "A" as the last character of said ASCII string; wherein said means for determining if a said predetermined message was properly transmitted on said
10 communication link comprises means for computing a cyclic redundancy check value and means for comparing said value with the cyclic redundancy check test value in said predetermined message; wherein said means for indicating that said predetermined message was not
15 correctly received comprises sending the ASCII character NAK (hex 15) on said communication link; and wherein said means for indicating that said predetermined message was correctly received comprises sending the ASCII character ACK (hex 06) on said communication link.

20 54. The scrambling system of Claim 18 or the scrambling apparatus of Claims 34 or 49 wherein said synchronization pulse comprises a pulse of electrical energy in a predetermined frequency band and wherein said electrical output means includes notch filtering
25 means for substantially removing electrical energy in said predetermined frequency band from said scrambled signals.

 55. The scrambling system of Claim 18 or the scrambling apparatus of Claims 34 or 49 wherein said
30 specifying means is responsive to said scrambling code, said system or said apparatus further comprising means for squelching the acoustical output means during the sending of said synchronization pulse.

 56. The scrambling system of Claim 1 or the
35 scrambling apparatus of Claim 20 or Claim 36 wherein said scrambling means for coupling said scrambled

-59-

signals to said electrical output means further
comprise: frequency scrambling output means for
generating an output electrical signal from a list of
output amplitude values, each said output amplitude
5 value specifying the amplitude of said output electrical
signal one of a plurality of predetermined frequency
bands and for coupling said output electrical signal to
said electrical output means; frequency scrambling input
means for computing a list of input amplitudes values,
10 each said input amplitude value representing the
amplitude of said scrambled signals in each of said
plurality of predetermined frequency bands; and
frequency scrambling amplitude reordering means for
transforming said list of input amplitude values into a
15 list of output amplitude values, said amplitude
reordering means being responsive to said scrambling
code, wherein said scrambled signals are inputted to
said frequency scrambling input means and the list of
input amplitude values computed by said frequency
20 scrambling input means is then transformed by said
frequency scrambling amplitude reordering means into an
output list which is then coupled to said frequency
scrambling output means; and wherein said electrical
input means further comprising frequency unscrambling
25 input means for computing a list of input amplitudes
values from the analog signals detected on said
communication link, each said input amplitude value
representing the amplitude of said analog signals in
each of said plurality of predetermined frequency bands;
30 frequency unscrambling amplitude reordering means for
transforming said list of input amplitude values into a
list of output amplitude values, the transformation
being performed by said frequency unscrambling amplitude
reordering means being the inverse of the transformation
35 performed by said frequency scrambling amplitude
reordering means, and frequency unscrambling output

-60-

means for generating an output electrical signal from
said list of output amplitude values and for coupling
said output electrical signal to said unscrambling
means, wherein the analog signals detected on said
5 communication link are inputted to said frequency
unscrambling input means, the list of input amplitudes
so generated being transformed by said frequency
unscrambling amplitude reordering means, said
transformed amplitude values being then inputted to said
10 frequency unscrambling output means.

1 / 5

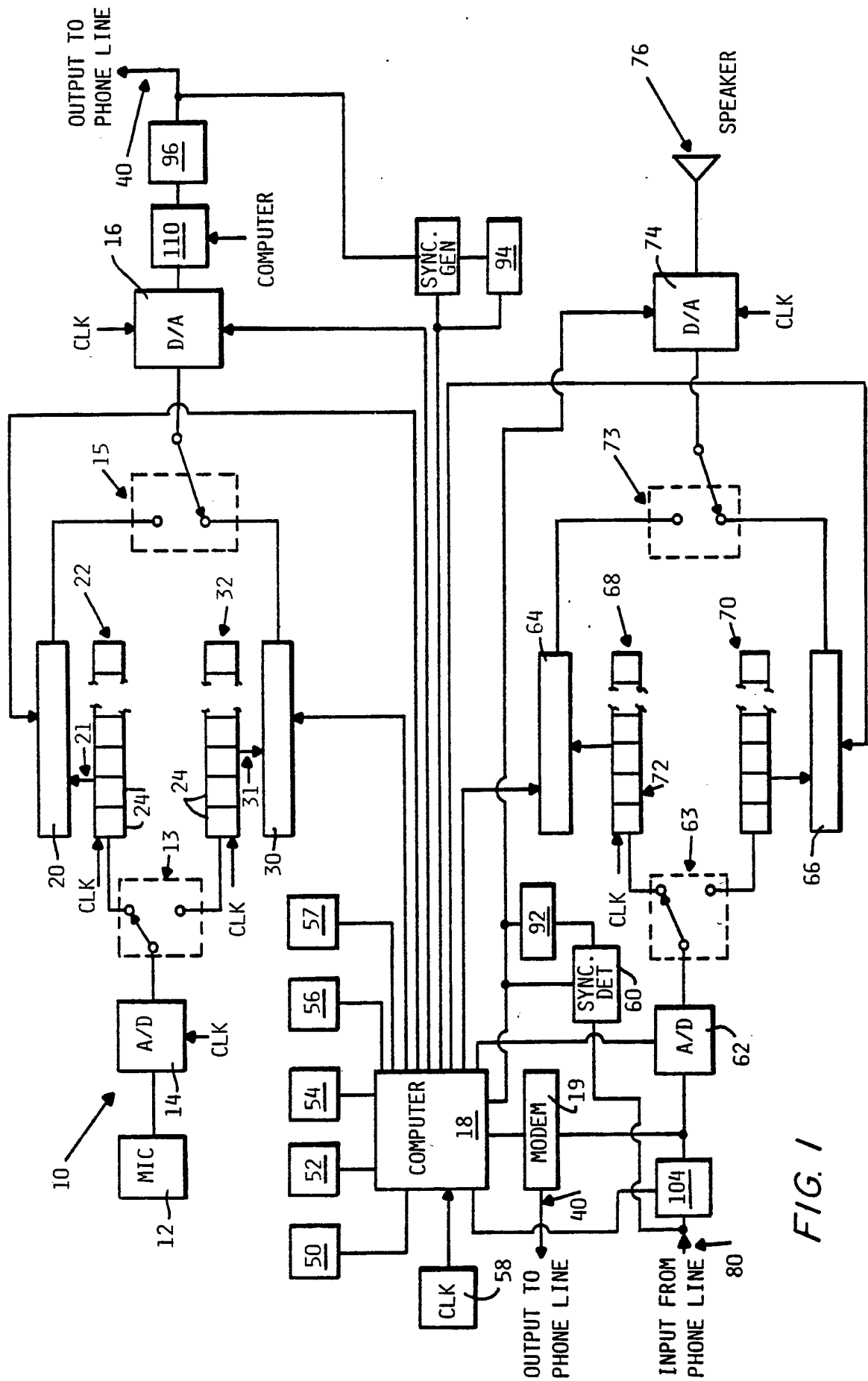
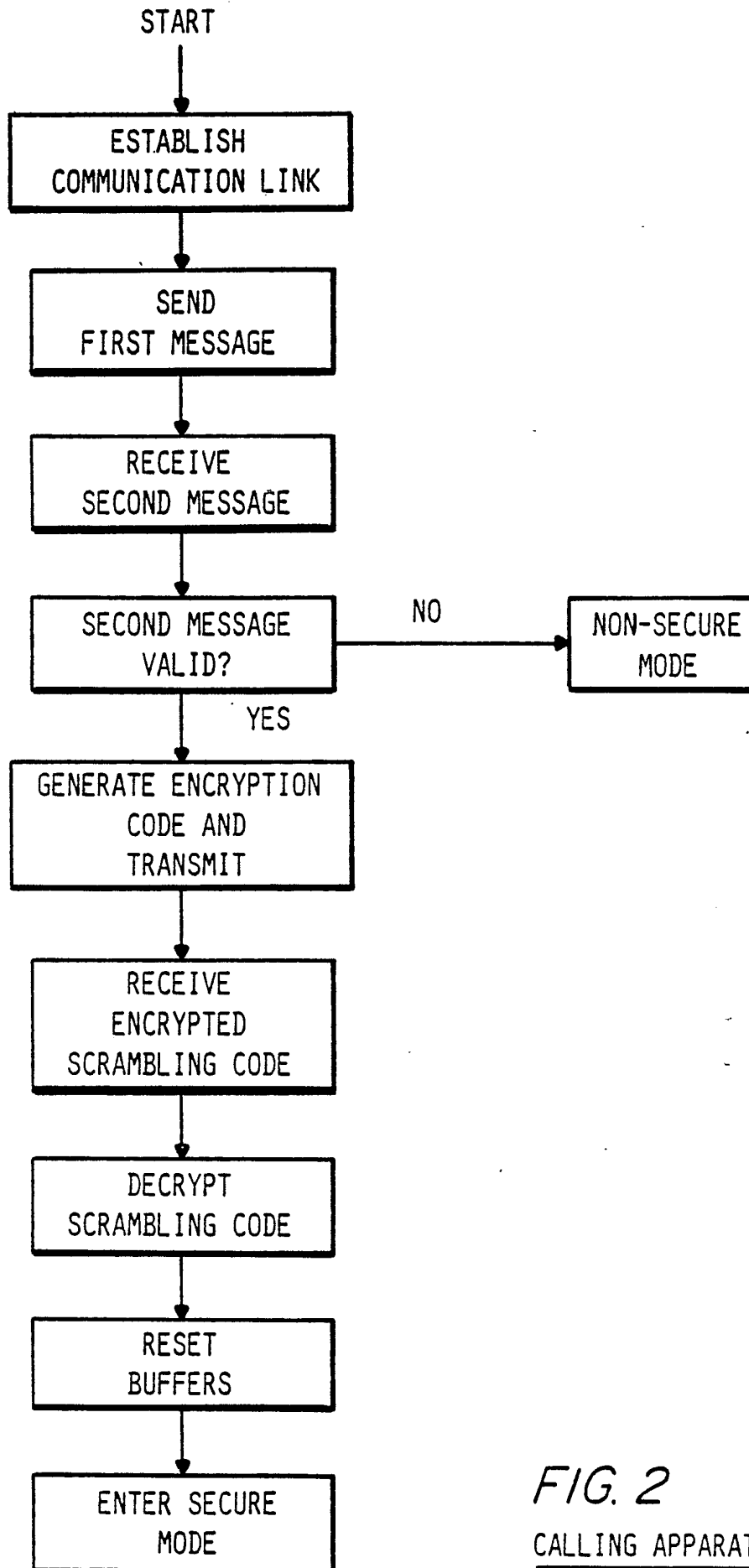
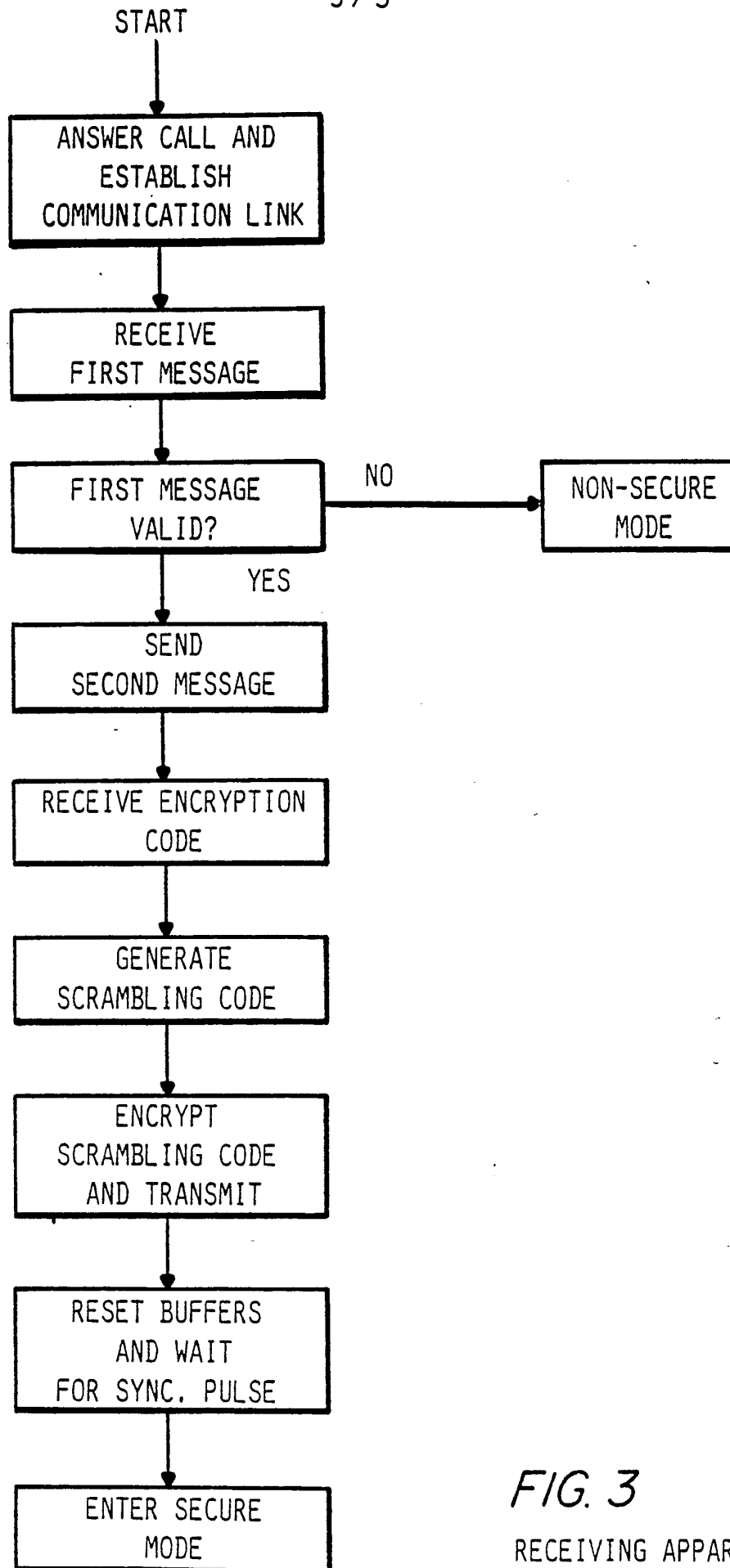


FIG. 1

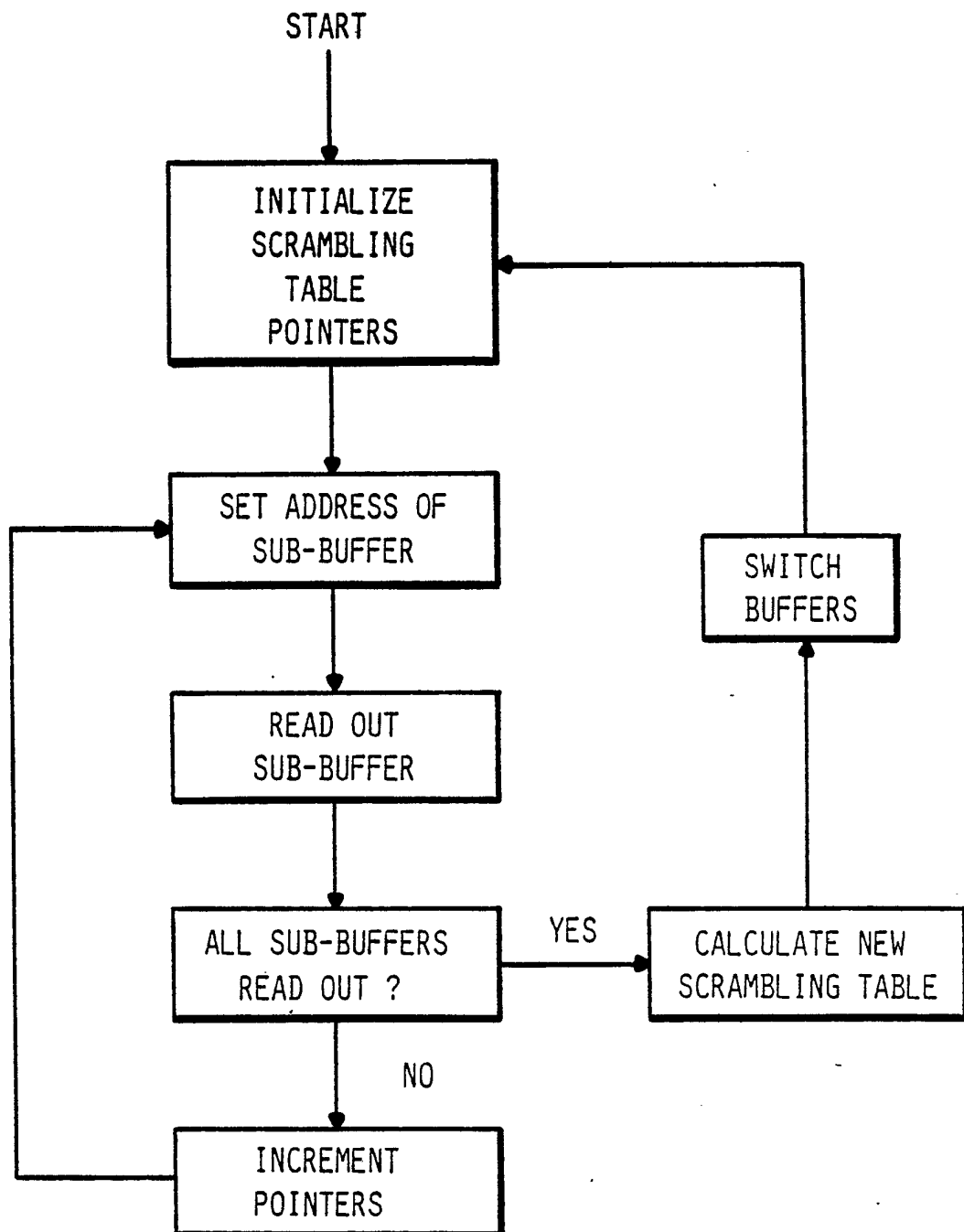
2 / 5

*FIG. 2*CALLING APPARATUS

3 / 5

*FIG. 3*RECEIVING APPARATUS

4 / 5

*FIG. 4*SCRAMBLING FUNCTION

5 / 5

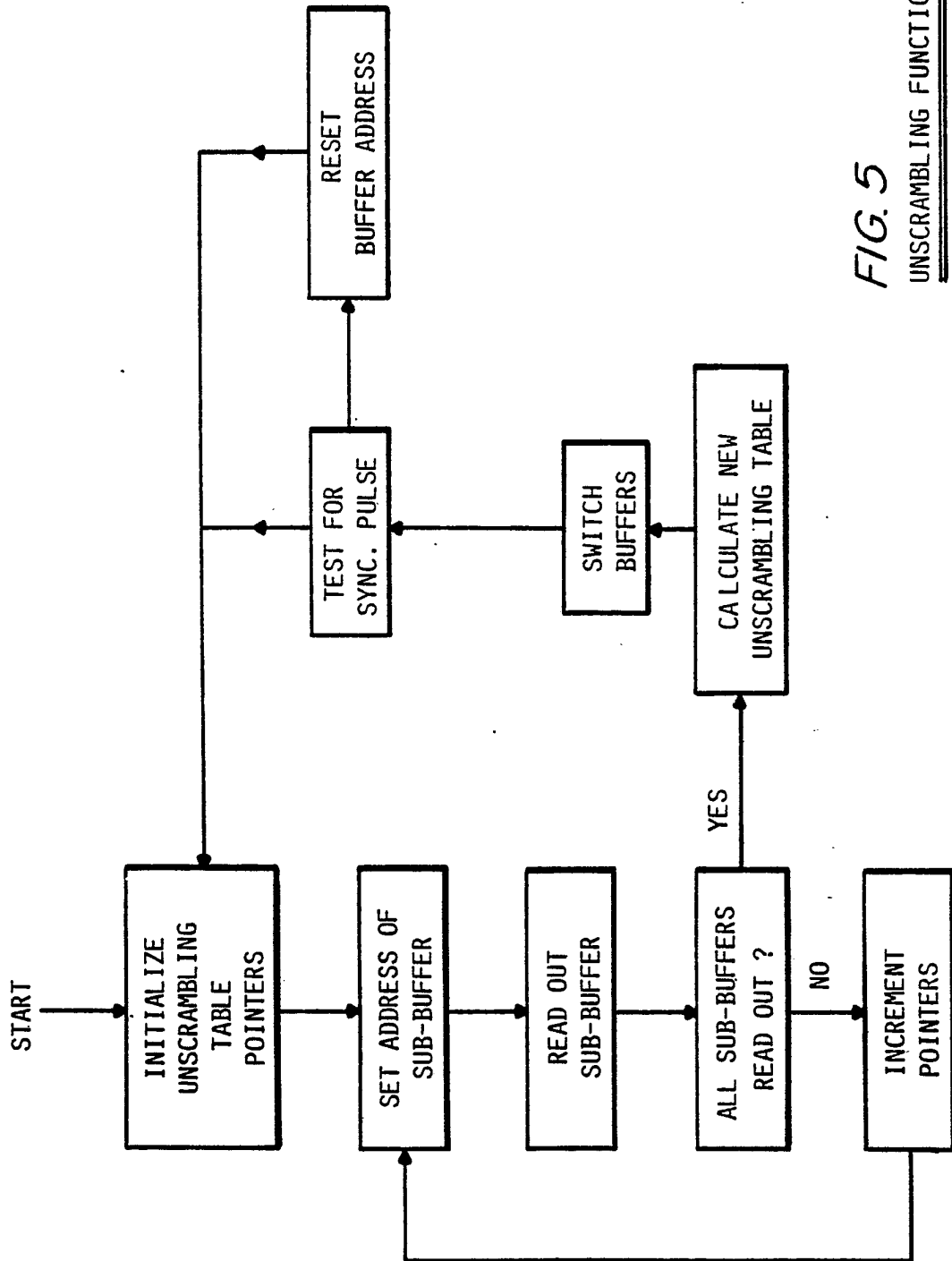


FIG. 5
UNSCRAMBLING FUNCTIONS

INTERNATIONAL SEARCH REPORT

International Application No. **PCT/US86/01364**

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) ³ According to International Patent Classification (IPC) or to both National Classifications: INT. CL. ⁴ H04M 1/70, 3/16; H04L 9/00; H04L 1/14; H04K1/00, 1/04 U.S. CL. 179/1.5R, 1.55; 178/22.11, 22.13; 455/26; 371/32,33,34 1/06																							
II. FIELDS SEARCHED Minimum Documentation Searched ⁴ <table style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 20%; border-bottom: 1px solid black;">Classification System</th> <th style="border-bottom: 1px solid black;">Classification Symbols</th> </tr> <tr> <td style="border-right: 1px solid black; padding: 5px; vertical-align: top;">US. CL.</td> <td style="padding: 5px; vertical-align: top;">179/1.5R, 1.55; 178/22.11, 22.13; 455/26; 371/34</td> </tr> </table> Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched ⁵			Classification System	Classification Symbols	US. CL.	179/1.5R, 1.55; 178/22.11, 22.13; 455/26; 371/34																	
Classification System	Classification Symbols																						
US. CL.	179/1.5R, 1.55; 178/22.11, 22.13; 455/26; 371/34																						
III. DOCUMENTS CONSIDERED TO BE RELEVANT ¹⁴ <table style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 10%; border-bottom: 1px solid black;">Category ⁶</th> <th style="border-bottom: 1px solid black;">Citation of Document, ¹⁵ with indication, where appropriate, of the relevant passages ¹⁷</th> <th style="border-bottom: 1px solid black;">Relevant to Claim No. ¹⁸</th> </tr> <tr> <td style="text-align: center; vertical-align: top; padding: 5px;">A</td> <td style="padding: 5px;">US, A, 4,020,285 Published 26 April 1977 Branscome et al.</td> <td style="text-align: center; vertical-align: top; padding: 5px;">1-56</td> </tr> <tr> <td style="text-align: center; vertical-align: top; padding: 5px;">Y</td> <td style="padding: 5px;">US, A, 4,200,770 Published 29 April 1980 Hellman et al. (Column 4 line 44- column 5 line 48)</td> <td style="text-align: center; vertical-align: top; padding: 5px;">1,20,36</td> </tr> <tr> <td style="text-align: center; vertical-align: top; padding: 5px;">Y</td> <td style="padding: 5px;">US, A, 4,280,193 Published 21 July 1981 Baun et al. (column 58 line 41-49)</td> <td style="text-align: center; vertical-align: top; padding: 5px;">11,12,14,15, 16,27,28,30, 31,42,43,45, and 46</td> </tr> <tr> <td style="text-align: center; vertical-align: top; padding: 5px;">Y</td> <td style="padding: 5px;">US, A, 4,351,059 Published 21 September 1982 Gregoire et al. (Abstract and Fig. #2)</td> <td style="text-align: center; vertical-align: top; padding: 5px;">1,3,4,5,20- 23, 36-38,52, 53</td> </tr> <tr> <td style="text-align: center; vertical-align: top; padding: 5px;">Y</td> <td style="padding: 5px;">US, A, 4,377,862 Published 22 March 1983 Koford et al. (Abstract and Fig. #2)</td> <td style="text-align: center; vertical-align: top; padding: 5px;">1,3-5, 20-23, 36-38,52,53</td> </tr> <tr> <td style="text-align: center; vertical-align: top; padding: 5px;">Y</td> <td style="padding: 5px;">US, A, 4,433,211 Published 21 February 1984 McCalmont et al. (See Fig. #1)</td> <td style="text-align: center; vertical-align: top; padding: 5px;">1,2,6-20,24- 36,39-51,54- 56</td> </tr> </table>			Category ⁶	Citation of Document, ¹⁵ with indication, where appropriate, of the relevant passages ¹⁷	Relevant to Claim No. ¹⁸	A	US, A, 4,020,285 Published 26 April 1977 Branscome et al.	1-56	Y	US, A, 4,200,770 Published 29 April 1980 Hellman et al. (Column 4 line 44- column 5 line 48)	1,20,36	Y	US, A, 4,280,193 Published 21 July 1981 Baun et al. (column 58 line 41-49)	11,12,14,15, 16,27,28,30, 31,42,43,45, and 46	Y	US, A, 4,351,059 Published 21 September 1982 Gregoire et al. (Abstract and Fig. #2)	1,3,4,5,20- 23, 36-38,52, 53	Y	US, A, 4,377,862 Published 22 March 1983 Koford et al. (Abstract and Fig. #2)	1,3-5, 20-23, 36-38,52,53	Y	US, A, 4,433,211 Published 21 February 1984 McCalmont et al. (See Fig. #1)	1,2,6-20,24- 36,39-51,54- 56
Category ⁶	Citation of Document, ¹⁵ with indication, where appropriate, of the relevant passages ¹⁷	Relevant to Claim No. ¹⁸																					
A	US, A, 4,020,285 Published 26 April 1977 Branscome et al.	1-56																					
Y	US, A, 4,200,770 Published 29 April 1980 Hellman et al. (Column 4 line 44- column 5 line 48)	1,20,36																					
Y	US, A, 4,280,193 Published 21 July 1981 Baun et al. (column 58 line 41-49)	11,12,14,15, 16,27,28,30, 31,42,43,45, and 46																					
Y	US, A, 4,351,059 Published 21 September 1982 Gregoire et al. (Abstract and Fig. #2)	1,3,4,5,20- 23, 36-38,52, 53																					
Y	US, A, 4,377,862 Published 22 March 1983 Koford et al. (Abstract and Fig. #2)	1,3-5, 20-23, 36-38,52,53																					
Y	US, A, 4,433,211 Published 21 February 1984 McCalmont et al. (See Fig. #1)	1,2,6-20,24- 36,39-51,54- 56																					
[*] Special categories of cited documents: ¹⁵ "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. "&" document member of the same patent family																							
IV. CERTIFICATION <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; border-bottom: 1px solid black; padding: 5px;">Date of the Actual Completion of the International Search ²</td> <td style="width: 50%; border-bottom: 1px solid black; padding: 5px;">Date of Mailing of this International Search Report ²</td> </tr> <tr> <td style="border-bottom: 1px solid black; padding: 5px;">2 August 1986</td> <td style="border-bottom: 1px solid black; padding: 5px; text-align: center;">19 AUG 1986</td> </tr> <tr> <td style="border-bottom: 1px solid black; padding: 5px;">International Searching Authority ¹</td> <td style="border-bottom: 1px solid black; padding: 5px;">Signature of Authorized Officer ²⁰</td> </tr> <tr> <td style="padding: 5px;">ISA/US</td> <td style="padding: 5px; text-align: center;"> Aaron J. Lewis </td> </tr> </table>			Date of the Actual Completion of the International Search ²	Date of Mailing of this International Search Report ²	2 August 1986	19 AUG 1986	International Searching Authority ¹	Signature of Authorized Officer ²⁰	ISA/US	 Aaron J. Lewis													
Date of the Actual Completion of the International Search ²	Date of Mailing of this International Search Report ²																						
2 August 1986	19 AUG 1986																						
International Searching Authority ¹	Signature of Authorized Officer ²⁰																						
ISA/US	 Aaron J. Lewis																						