(54) Title: A SECURITY SYSTEM FOR SSTV ENCRYPTION
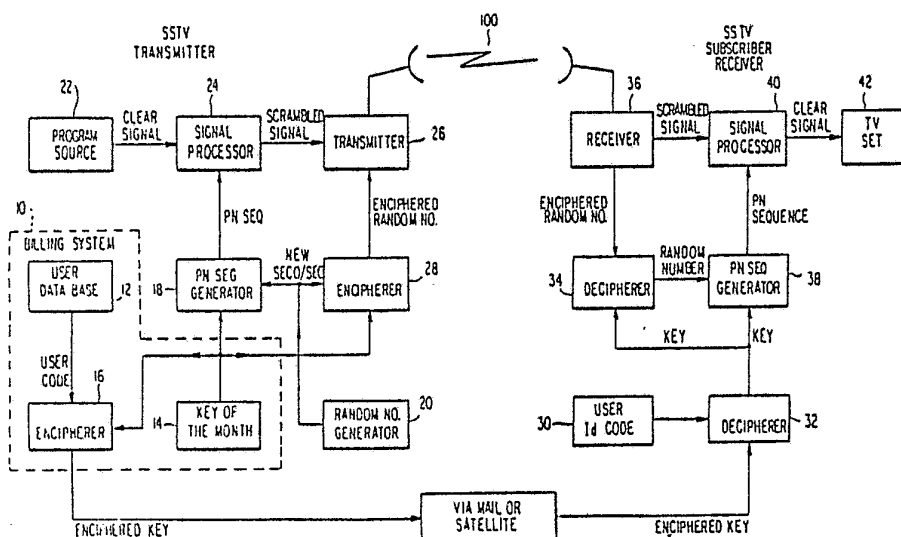
(57) Abstract

In a secure communications system, a key number (14) which is changed periodically, e.g. monthly, and a random number from a random number generator (20) are combined and used as a seed to reset a Pn sequence generator (18), with the output of the generator being used to control encryption of transmission data in a signal processor (24). The key is also provided to a first encipherer (28) to encipher the random number for transmission with the encrypted data. At the receiver, the key is provided in common to a decipherer (34) for deciphering the random number and a Pn sequence generator (38) which is periodically reset by the combination of the key and random number in the same manner as in the transmitter. The Pn sequence is then used to decrypt the information. User identification codes are stored (12) in the transmitter and are used to encipher (16) the key, with each employing its ID code (30) to decipher (32) the key. The user ID codes are known only to the system operator, so that not even a particular user can know the key.

A SECURITY SYSTEM FOR SSTV ENCRYPTION

BACKGROUND OF THE INVENTION

The present invention is related to the confidentiality of television signal transmissions, and more particularly to the protection of TV signal transmissions from unauthorized reception. The environment in which the present invention may be widely applicable, and in the context of which the invention will be described herein, is that of subscriber television and TV program distribution.

Subscriber television systems are becoming increasingly widespread wherein TV signals are sent out via a cable network or over the air and are intended for reception and viewing by only those subscribers who have paid a monthly fee. With the increase in subscriber television systems has also come an increase in the number of people attempting to receive and display the premium television programs without payment. Thus, there is a need for more sophisticated security techniques for preventing such unauthorized reception.

Many existing subscriber television systems utilize directly or indirectly, signals transmitted via satellite, and it is becoming quite common for non-paying individuals to receive and display the premium television programs via television receive only (TVRO) antennas, thus resulting in a substantial loss of revenue for the distributors of the subscription television programs. In addition, various direct satellite broadcast television systems are currently being proposed wherein subscription television programs will be broadcast directly via satellite to

individual subscriber homes. These subscription
satellite television (SSTV) systems will be quite
vulnerable to unauthorized reception, and an effective
security technique is therefore highly desirable.

The purpose of a security subsystem for an SSTV
system is to protect the distributor's business
interest and, accordingly, the following objectives
should be achieved:

(1) To prevent a non-subscriber from receiving
intelligible video and audio signals by
using a regular home television set;

(2) To prevent a delinquent subscriber from
receiving intelligible video and audio
signals by using the SSTV decoder;

(3) To prevent a legitimate subscriber from
receiving intelligible video and audio
signals of unsubscribed SSTV channels or
programs;

(4) To discourage an average technician from
building his own receiver capable of
obtaining acceptable quality video and audio
signals;

(5) To discourage a small unauthorized business
concern from manufacturing and marketing
devices which are capable of receiving and
displaying acceptable quality video and
audio signals from the SSTV channels; and

(6) To allow a legitimate subscriber to receive
and display high quality video and audio
signals from the subscribed channels or
programs.

It would also be highly desirable to achieve the above
objectives at a reasonable cost.

A number of security systems for CATV exist, most
of which involve the suppression or removal of the

horizontal sync pulses from the video signal before transmission, and the recovery of the sync pulses at the receive end. These techniques will prevent people without the sync recovery circuits from receiving and displaying the programs and may therefore achieve objectives (1) and (6) above, but these security systems do not achieve objectives (2) and (3) and, since sync recovery circuits are relatively easily designed and manufactured, also do not satisfy objectives (4) and (5).

More sophisticated techniques may include additional intelligence in the subscriber's decoder box, including the capability of receiving commands from a control center which are specifically addressed to an individual subscriber and are used to turn on or off some or all of the channels. These more sophisticated security techniques may succeed in achieving objectives (1)-(3) and (6), but still do not satisfy objectives (4) and (5). For example, most of these techniques involve the checking of a password, and a particular channel is turned on only if the password is matched. This could be relatively easily by-passed by modifying the subscriber's decoder box or building a separate box with all of the necessary features except the on/off switch. Further, subscribers may also be able to tamper with the decoder box to receive more programs than are actually paid for.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a security subsystem for a subscription television system wherein all of the above-mentioned objectives (1)-(6) are achieved.

It is a further object of this invention to provide such a security subsystem of minimal cost and complexity.

These and other objects are achieved according to
the present invention by using a cryptographic tech-
nique for scrambling and descrambling of the video
signals. The scrambling and descrambling techniques
5   utilize a "key" which is changed on a regular basis
and is sent only to paid subscribers, and even this
"key" is sent in a different encrypted form to each
subscriber so that delinquent subscribers cannnot
learn the current key from others.

10   A record is kept of unique user ID codes corres-
ponding to each subscriber, and in a transmitter
according to the preferred embodiment of this inven-
tion, the key is ciphered with each subscriber's
unique ID code prior to sending the key to that
15 subscriber. A random number generator in the trans-
mitter generates a new random number at regular inter-
vals, for example, every second, and this number is
combined with the key, and the combined number is then
used as a seed to reset a PN sequence generator every
20 second. This PN sequence generator will thus generate
a PN sequence with a random seed in one-second seg-
ments, and the segmented PN sequence is supplied to a
signal processor where it is used to scramble the
audio and video program signals. The random number
25 generator is also ciphered with the key and the en-
ciphered random number is continually transmitted with
the scrambled video signal.

At the receiver, the enciphered key, which has
been sent either via satellite or mail, is deciphered
30 in the receiver utilizing the particular subscriber's
unique ID code, which ID code is internal to the
receiver and is unknown to the subscriber. The de-
ciphered key is then in turn used to decipher the
enciphered random number received with the scrambled
35 program signal. The deciphered key and random number
are then combined as in the transmitter, and the

combined signal is used to continually reset a PN
sequence generator identical to that in the trans-
mitter so that a segmented PN sequence will be gener-
ated in the receiver which is identical to that
generated in the transmitter, and this segmented PN
sequence can then be used to descramble the received
signal. The descrambled signal will then be supplied
to the subscriber television set.

BRIEF DESCRIPTION OF THE DRAWING

The invention will be more clearly understood
with reference to the following description in con-
junction with the accompanying drawing wherein the
single figure is a block diagram of the essential
components of the SSTV security system according to
the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The drawing illustrates a functional block dia-
gram of the SSTV security system according to this
invention. The SSTV transmitter will typically in-
clude or have access to a billing system computer 10
which will store subscriber information including a
list of paid subscribers and their corresponding
unique user ID codes. This information may typically
be stored in a user data base 12 within the computer.
Also within the computer will be a register 14 or the
like containing a key which will be changed on a
regular basis, e.g. monthly. In preparation for
sending this "key of the month" to each current sub-
scriber, the key is enciphered in an encipherer 16
with the user ID code unique to that particular cur-
rent subscriber, and the enciphered key is then sent
to the subscriber.

The transmitter includes a pseudo-random number
(PN) sequence generator 18 and a random number gener-
ator 20. The random number generator 20 periodically
generates a new random number, e.g. once every second,

and the outputs of the random number generator 20 and
key register 14 are combined and loaded into the PN
sequence generator 18 to periodically reset or "seed"
the PN sequence generator 18 in a manner well known in
the art. Each seeding of the sequence generator 18
will begin a new segment of the PN sequence. The
program signal from source 22 is supplied to a signal
processor 24 where it is encrypted with the segmented
PN sequence from generator 18. The encryption tech-
nique used may be any one of a variety of well known
techniques and need not be discussed in detail herein.
The encrypted, or scrambled, signal is then provided
to a transmitter 26 for transmission over link 100 to
the various subscriber receivers.

The random number from generator 20 is enciphered
with the key of the month in an encipherer 28, and the
enciphered random number is transmitted with the
scrambled video signal over the link 100.

At the receiver, a register 30 or the like
internal to the subscriber TV receiver contains a
subscriber-specific secret user ID code which is set
prior to installation and is stored in the user data
base 12 of the billing computer at the transmitter.
Thus, when the subscriber receiver receives the en-
ciphered key or when the user receives the enciphered
key by mail and enters the enciphered key into the
receiver, a decipherer 32 in the receiver deciphers
the enciphered key with the secret user ID code
specific to that particular subscriber, and the
deciphered key is provided to a decipherer 34. A
receiver 36 separates the scrambled signal from the
enciphered random number received over link 100 and
provides the enciphered random number to the de-
cipherer 34 where it is deciphered with the key
received from the decipherer 32. The deciphered

random number and key are then combined and loaded
into the PN sequence generator 38 to reset or "seed"
the sequence generator in the same manner as in the
transmitter, to thereby result in the same segmented
PN sequence as was used for scrambling in the SSTV
transmitter signal processor 24. This segmented PN
sequence is then provided to signal processor 40 where
it is used to descramble the received program signal.
The descrambled signal is then provided to the
subscriber television set 42.

The above-described security system provides a
novel technique for generating and synchronizing a
segmented pseudo-random number (PN) sequence, and a
secure key distribution method. The segmented PN
sequence generated is used to control the video and
audio signal processors that scramble and descramble
the program signals. Since a different segmented PN
sequence will be generated by each distinct key, the
scrambling sequence is different for each key, and by
periodically changing the key the scrambling and
descrambling sequences will change. Thus, it is not
possible for anyone without exact knowledge of the
current key to descramble the received program signal
with or without a descrambling device.

For each given duration of time, a particular
channel is scrambled by a PN sequence that is
generated by a randomly selected number and the key of
the month. To prevent subscribers of different
channels from exchanging the keys among themselves, it
is essential that the key for a given channel distri-
buted to each subscriber look different, and this
accomplished by enciphering the key with each
subscriber's unique user ID code. In this way,
although a single key is provided by the register 14
at any one time, a different key is required by each
subscriber. It is only when the subscriber-specific

key is entered into the receiver that the true key of
the month contained in register 14 can be provided to
the decipherer 34 and sequence generator 38, and the
deciphering of this true key of the month in the
5   decipherer 32 is performed internally of the
subscriber receiver and without the subscriber's
knowledge.

An important feature of any security system is
that a legitimate subscriber must be capable of
10   obtaining synchronization within a short period of
time. In the system according to the present
invention, the PN sequence used for scrambling and
unscrambling the signal in signal processors 24 and
40, respectively, is separated into short segments
15   each of which is seeded by the combination of the key
of the month and a random number which changes, for
example, once every second. Thus, assuming that a
legitimate subscriber does have his appropriate key,
the time required to acquire synchronization will be
20   substantially equal to the duration of each random
number so that synchronization can be acquired rapidly
in case of loss of sync due to power outages,
rainstorms, changing of channels, etc.

The individual components in the security system
25   according to the present invention are known in the
art and need not be described in detail herein since
the internal details of these components do not
constitute a part of the present invention. The
encipherers used to encipher the key of the month and
30   the random number can be two different encipherers,
but for the sake of hardware simplicity at the receive
side, and consequent cost savings in mass production
of the subscriber receivers, it is preferable that the
same encipherers be used. The encipherer may employ
35   any enciphering method as long as it has a suffi-
ciently high level of security.

The PN sequence generator can be any general PN sequence generator as long as it also has sufficient security strength, e.g. a properly selected non-linear feedback shift register may suffice.

The random number generator in the transmitter may be a well known thermal noise generator which generates "true" random numbers, or it may be a pseudo-random number generator similar to the sequence generator 18, implemented in a well known manner with digital electronics or computer software. Similarly, the technique for combining the key of the month and the random number generator to produce the "seed" for the PN sequence generators 18 and 38 is not critical, with the simplest technique being a bit-by-bit modulo-2 addition of the two numbers.

In general, each of the functional blocks in the drawing can be implemented with existing techniques, with system complexity and cost and security strength depending on the particular implementation of each of the functional blocks.

The transformation of the simple cipherer is specified by a variable which is different for each channel or special program, and is changed every month.

The user ID code 30 within each subscriber set may be a set of binary switches or a bit pattern programmed into a read-only memory in a sealed box to prevent the subscriber from seeing or changing the number.

The use of a simple cipherer in addition to the non-linear feedback shift-register may seem to increase the system complexity unnecesarily. However, since only a small amount of data, namely the "seed", need be handled each time, and since the statistical properties of the cipherer do not impact to the output of the PN sequence generator, the cipherer can be very

simple. One possible approach, for example, is a ROM table of random bits with or without cipher feedback. The use of this simple cipherer greatly simplifies the problem of cryptosynchronization and key distribution,

5 and therefore reduces the overall system complexity.

Suitable alternatives for the scrambling of the program signals include conventional scrambling techniques such as on-off switching, randomly inverting lines, fields or frames, and delaying horizontal

10 lines or fields by certain randomly fixed steps. In any case, the technique used will require the generation of a PN sequence which must be synchronized at both the transmit and receive sides.

11

WHAT IS CLAIMED IS:

1. In a communications system including a transmitter and a receiver, said transmitter including a program source for providing a program signal representing program information, a transmit signal processor for encrypting said program signal in accordance with a transmit control signal and transmit means for transmitting said encrypted signal, said receiver including receive means for receiving said encrypted signal, a receiver signal processor for decrypting said encrypted signal in accordance with a receive control signal and means for receiving said decrypted signal and providing said program information, the improvement comprising:

first generator means at said transmitter for generating a first sequence of signals representing a first sequence of numbers;

key number means at said transmitter for providing a key number signal representing a key number;

second generator means at said transmitter for generating a second sequence of signals representing a second sequence of numbers, said second generator means being periodically reset by a reset signal comprising the output of said first generator means to thereby generate a plurality of sequence segments each beginning with a reset signal, the output of said second generator means comprising said transmit control signal;

means at said transmitter for enciphering said first sequence of signals with said key number signal and for providing said enciphered first signal sequence to said transmit means for transmission with said encrypted program signal;

means at said receiver for providing said key number signal;

receive deciphering means at said receiver for receiving said enciphered first signal sequence and said key number, deciphering said first signal sequence in accordance with said key number and providing said deciphered first signal sequence as an output; and

receive generating means for generating a sequence of signals representing said first sequence of numbers, said receive generating means being periodically reset by a reset signal comprising the output of said receive deciphering means to thereby generate said plurality of sequence segments, said plurality of sequence segments being provided by said receive generating means to said receive signal processor as said receive control signal.

2.   A commications system as defined in claim 1, further comprising:

means for providing an identification number signal uniquely identifying said receiver;

means for enciphering said key number signal with said identification signal;

means at said receiver for providing said identification number signal; and

means at said receiver for receiving said identification number signal and said enciphered key number signal and for deciphering said key number signal, said deciphered key number signal being provided to said receive deciphering means.

3.   A communications system as defined in either one of claims 1 or 2, wherein each of said reset signals provided to said second generator means comprises a combination of said key number signal and a signal of said first signal sequence, and wherein each of said reset signals provided to said receive

generator means comprises a combination of said key number signal and a signal of said deciphered first signal sequence.

4. A communications system as defined in claim 3, wherein said key number signal is changed at predetermined time intervals.

5. A communications system as defined in claim 4, wherein said second generator means is a non-linear pseudorandom sequence generator.

6. A communications system as defined in claim 3, wherein a plurality of receivers receive the encrypted signal transmitted by said transmitter, each of said receivers having a corresponding unique identification number and said enciphered key number received at each receiver being enciphered with the user identification number unique to said each receiver.

7. The communications system as defined in claim 6, wherein said first signal sequence represents a substantially random number sequence.

8. In a method of providing security in a signal transmission system, said method including the steps of encrypting in accordance with an encryption control signal a program signal representing information, transmitting said encrypted signal, receiving said encrypted signal, decrypting said received encrypted signal in accordance with a decryption control signal and providing said information represented by said decrypted signal, the improvement comprising:

generating a key number signal representing a key number;

generating a first signal sequence representing a first sequence of numbers;

generating a second signal sequence representing a second sequence of numbers, said second

signal sequence being periodically reset by a reset
signal comprising a signal of said first signal
sequence to thereby generate a plurality of second
20 sequence segments;

        providing said second sequence segments to
said transmit signal processor as said encryption
control signal;

        enciphering said first signal sequence with
25 said key number and providing said enciphered first
sequence to said transmitter for transmission with
said encrypted signal;

        decrypting said enciphered first sequence at
said receiver in accordance with said key number
30 signal;

        generating said second sequence segments at
said receiver by resetting a receive number signal
generator with a reset signal comprising said
deciphered first signal sequence; and

35   providing said second sequence segments to
said receive signal processor as said decryption
control signal.

        9.   A method as defined in claim 8, further
comprising:

        enciphering said key number signal at said
transmitter with a user identification number signal
5   uniquely identifying said receiver;

        transmitting said enciphered key number
signal to said receiver;

        deciphering said enciphered key number
signal at said receiver in accordance with said user
10 identification number signal uniquely identifying said
receiver; and

        providing said deciphered key number signal
to said deciphering means.

        10. The method as defined in claim 9, further
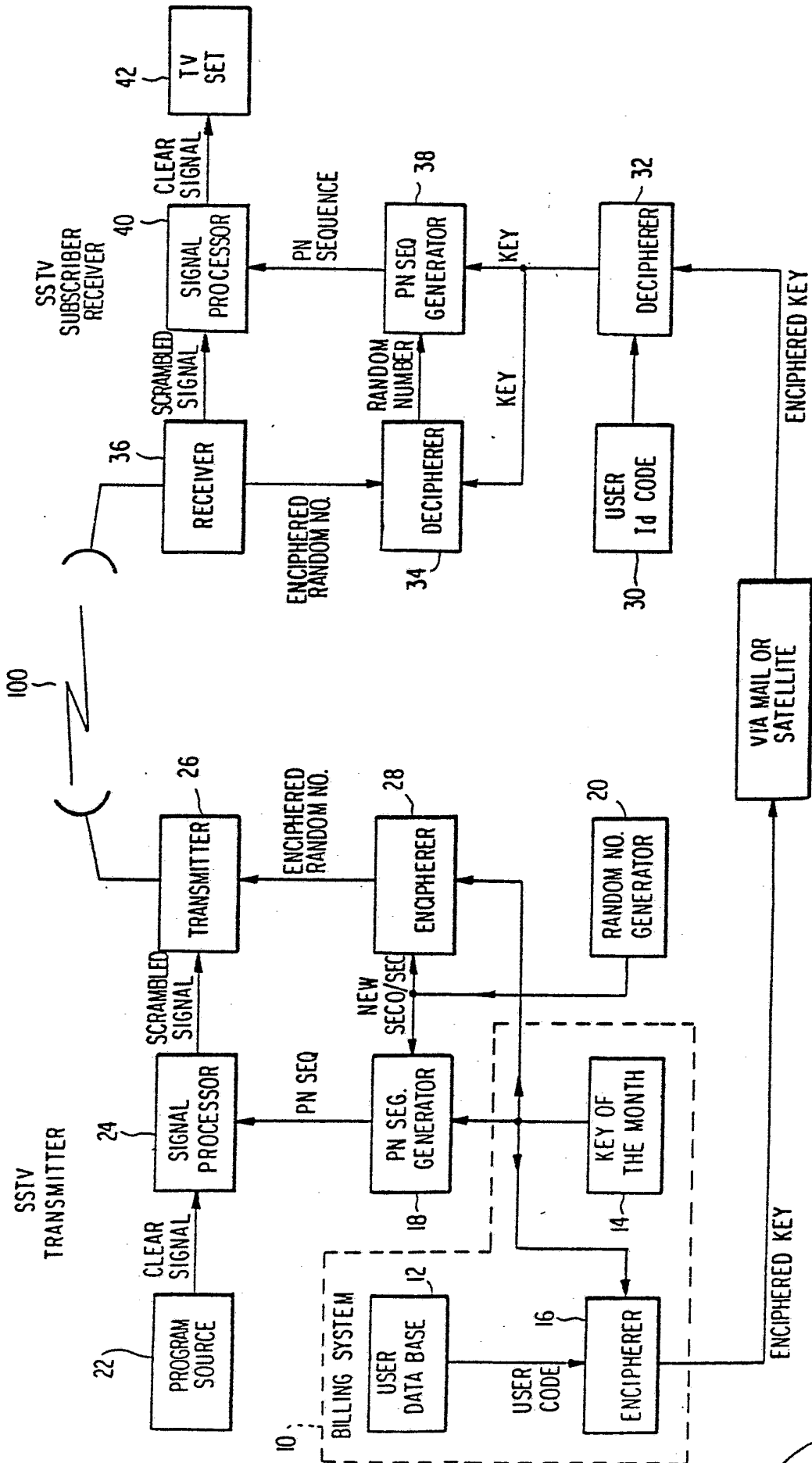comprising the steps of:

combining said key number signal and a signal in said first sequence to obtain said reset signal in said transmitter; and

combining said key number signal and a signal in said deciphered first sequence in order to obtain said reset signal in said receiver.

11. The method as defined in any one of claims 8-10, further comprising the step of periodically changing said key number signal.

12. The method as defined in claim 11, wherein said second generator means in said transmitter and said generator means in said receiver each generate non-linear pseudo-random signal sequences.

13. The method as defined in claim 12, wherein said first signal sequence represents a substantially random number sequence.

1 / 1

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 8-2 / 0 1 6 3 1

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [6]

According to International Patent Classification (IPC) or to both National Classification and IPC

INT. Cl. HO4M 1/32, HO4L 9/00, HO4N 7/16
US. Cl. 178/22.08, 22.09, 22.15, 358/224, 122

II. FIELDS SEARCHED

Minimum Documentation Searched [4]	
Classification System	Classification Symbols
US	178/22.08, 22.09, 22.15 358/114, 122

Documentation Searched other than Minimum Documentation
to the Extent that such Documents are Included in the Fields Searched [6]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [14]

Category [*]	Citation of Document, [16] with indication, where appropriate, of the relevant passages [17]	Relevant to Claim No. [18]
X,P	US, A, 4,323,921, Published 6 April 1982, Guillou.	1-13
X,P	US, A, 4,337,483, Published 29 June 1982, Guillou.	1-13
X,P	US, A, 4,354,201, Published 12 October 1982, Sechet et al.	1-13
Y	US, A, 4,292,650 Published 29 September 1981, Hendrickson.	1-13
Y	US, A, 4,115,662, Published 19 September 1978, Guinet et al.	1-13

* Special categories of cited documents: [16]

"A" document defining the general state of the art

"E" earlier document but published on or after the International filing date

"L" document cited for special reason other than those referred to in the other categories

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the International filing date but on or after the priority date claimed

"T" later document published on or 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

IV. CERTIFICATION

Date of the Actual Completion of the International Search [3]	Date of Mailing of this International Search Report [3]
25 January 1983	27 JAN 1983
International Searching Authority [1]	Signature of Authorized Officer [10]
ISA/US	S.A. Cangialosi