PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 4 :		(11) International Publication Number:	WO 85/ 03182
H04L 9/00	A1	(43) International Publication Date:	18 July 1985 (18.07.85)

(21) International Application Number: PCT/US84/02016

(22) International Filing Date: 6 December 1984 (06.12.84)

(31) Priority Application Number: 567,815

(32) Priority Date: 3 January 1984 (03.01.84)

(33) Priority Country: US

(71) Applicant: AMERICAN TELEPHONE & TELEGRAPH COMPANY [US/US]; 550 Madison Avenue, New York, NY 10022 (US).

(72) Inventor: McNAIR, Bruce, Edwin ; 1 Iron Hill Drive, Holmdel, NJ 07733 (US).

(74) Agents: HIRSCH, A., E., Jr. et al.; Post Office Box 901, Princeton, NJ 08540 (US).

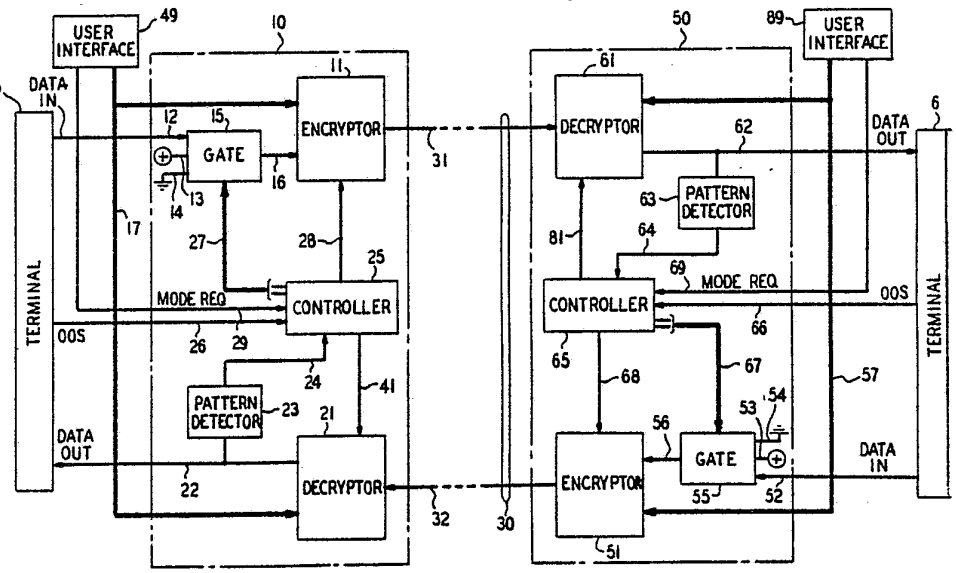
(81) Designated States: AT (European patent), BE (European patent), CH (European patent), DE (European patent), FR (European patent), GB (European patent), JP, KR, LU (European patent), NL (European patent), SE (European patent).

Published
With international search report.

(54) Title: CRYPTOGRAPHIC TRANSMISSION SYSTEM

(57) Abstract

In a cryptographic communication system, a first encryptor (11) transmits to a first decryptor (61) and a second encryptor (51), co-located with the first decryptor (61), transmits to a second decryptor (21), which is co-located with the first encryptor (11). Each encryptor/decryptor pair is adapted to communicate using a selected non-self-synchronizing cryptographic mode. Whenever it is determined that synchronization between, say, the first encryptor and the first decryptor has been lost, both the first decryptor and the co-located, second encryptor are switched from the non-self-synchronizing mode to the self-synchronizing mode. This causes a loss of synchronization between the second encryptor and second decryptor since the latter is still operating in the non-self-synchronizing mode. Upon detection of this loss of synchronization, the second decryptor and the co-located, first encryptor are also switched from the non-self-synchronizing mode to the self-synchronizing mode. In due course, then, synchronization in both transmission directions automatically restores. Return of each encryptor/decryptor pair to operation using the non-self-synchronizing mode is thereafter initiated by having each encryptor transmit a string of '1's followed by a '0'. The encryptor thereupon returns to the non-self-synchronizing mode. The string of '1's is long enough to ensure that synchronization with the encryptor is reestablished and when the '1'-to-'0' transition is detected at the decryptor, it, too, is switched back to the non-self-synchronizing mode.



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			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SN**	Senegal
CH	Switzerland	**LI**	Liechtenstein	**SU**	Soviet Union
CM	Cameroon	**LK**	Sri Lanka	**TD**	Chad
DE	Germany, Federal Republic of	**LU**	Luxembourg	**TG**	Togo
DK	Denmark	**MC**	Monaco	**US**	United States of America
FI	Finland	**MG**	Madagascar		
FR	France	**ML**	Mali		

CRYPTOGRAPHIC TRANSMISSION SYSTEM

Background of the Invention

The present invention relates to the transmission of digital information and has particular application to cryptographic transmission systems.

Techniques for cryptographic transmission of digital information can be categorized as being either self-synchronizing or non-self-synchronizing. Self-synchronizing techniques, such as the cipher text auto key (CTAK) mode of the well-known Data Encryption Standard (DES), have the advantage that the crypto-state vector generators in the encryptor and decryptor will synchronize, i.e., automatically come to store the same crypto-state vector value, without having to be initialized to the same value. Disadvantageously, however, self-synchronizing techniques extend transmission errors, meaning that a single transmission channel error will give rise to an entire burst of errors at the receiver. In high error rate environments, this can render use of encryption impractical.

By contrast, the non-self-synchronizing techniques such as key auto key (KAK) or the state-sequence-driven mode of the DES, do not extend errors. They do, however, require that a synchronization signal be transmitted when the encryptor and decryptor are to be initially synchronized, and, thereafter, whenever they become unsynchronized. This is undesirable from both the cryptanalytic and transmission efficiency points of view.

Summary of the Invention

The present invention provides a way of taking advantage of the desirable aspects of both the self-synchronizing and non-self-synchronizing approaches.

In particular, in a cryptographic transmission system embodying the principles of the invention, an encryptor and decryptor are adapted to communicate using a non-self-synchronizing cryptographic mode. However,

whenever the decryptor's cryptographic synchronization with the encryptor has been lost--as would be manifested, for example, by the bit error rate at the decryptor output becoming very large--action is initiated at the decryptor to cause both the decryptor and the encryptor to switch to a self-synchronizing mode. Once synchronization has been re-established, the encryptor and decryptor are returned to the original, non-self-synchronizing mode.

In preferred embodiments, the invention is implemented in a two-way transmission system in which a first encryptor transmits to a first decryptor and a second encryptor, co-located with the first decryptor, transmits to a second decryptor, which is co-located with the first encryptor. In accordance with a feature of the invention, which is applicable not only to cryptographic transmission systems, but also to other types of two-way transmission systems, there is provided an advantageous way for it to be communicated from, say, the local end of the channel to the remote end thereof that there are abnormalities in the received data signal and/or the recovered data stream as, for example, would result in a cryptographic transmission system, from a loss of cryptographic synchronization. In particular, whenever such abnormalities are detected at the local end, abnormalities are caused to occur in the signal being transmitted in the opposite direction, i.e., from the local end to the remote end. Such abnormalities might be, for example, violations of a source coding format, irregularities in the channel coding format, etc. The occurrence of these abnormalities, when detected at the remote end, is interpreted thereat to mean that, indeed, there is a problem at the local end. Appropriate corrective action can then be taken.

Thus, in a cryptographic transmission system embodying the principles of the invention and, in particular, embodying the feature thereof just described, whenever it is determined at, for example, the first decryptor in response to the detection of format violations

in the decrypted data that synchronization between the first decryptor and the first encryptor--which have theretofore been operating in a non-self-synchronizing mode--has been lost, both the first decryptor and the co-located, second encryptor are switched from the non-self-synchronizing mode to the self-synchronizing mode. This causes a loss of synchronization between the second encryptor and second decryptor since the latter is still operating in the non-self-synchronizing mode and thus gives rise to format violations in the data decrypted by the second decryptor. When these violations are detected, the second decryptor and the co-located, first encryptor are also switched from the non-self-synchronizing mode to the self-synchronizing mode. In due course, then, synchronization in both transmission directions automatically is restored.

Also in preferred embodiments, return of the system to the non-self-synchronizing mode is thereafter initiated by having each encryptor transmit a synchronization pattern comprised of first and second portions, the latter being uniquely distinguishable from any portion of the former. Illustratively, the synchronization pattern is comprised of a string of bits having a first clear text value, e.g., "1", followed by at least one bit having the other value, e.g., "0". The encryptor is thereupon returned to the non-self-synchronizing mode. The string of bits is long enough to ensure that synchronization with the decryptor is re-established, and when the bit value transition is detected at the decryptor it, too, is switched back to the non-self-synchronizing mode. The re-synchronization is thus complete.

A particular advantage of the above-described preferred implementation is that an interloper cannot tell when transitions from one encryption mode to the other occur, thereby maintaining high resistance to cryptanalysis.

Brief Description of the Drawing

FIG. 1 is a block diagram of an illustrative cryptographic digital communication system embodying the principles of the present invention;

FIG. 2 is a state diagram helpful in explaining the operation of the system of FIG. 1; and

FIG. 3 is a block diagram of an illustrative encryptor used in the system of FIG. 1.

Detailed Description

The system of FIG. 1 comprises a pair of substantially identical digital cryptographic transceivers 10 and 50 embodying the principles of the invention. This system operates to securely communicate data, digital information, e.g., between respective associated terminals 5 and 6 (each which may be a CRT terminal, computer, etc.) via a two-way, full-duplex communication channel 30 illustrating a pair of one-way communication lines 31 and 32.

Data desired to be communicated from terminal 5 to terminal 6 is applied by the former to the transmission section of transceiver 10 via data input lead 12. That lead comprises a first input lead for a 3-input gate 15. During normal data communications, which will be assumed to be ongoing, a controller 25 within transceiver 10 applies to gate 15 via lead pair 27 a signal indicating that gate 15 is to apply to its output lead 16 the signal on lead 12. From lead 16, the data is applied to an encryptor 11. The latter encrypts the data on lead 16 in response to a 56-bit key variable supplied in parallel from a user interface 49 on cable 17. User interface 49, in turn, (as well as user interface 89 discussed hereinbelow) can receive the key variable from an external source in conventional fashion in accordance with any of the numerous key distribution techniques known in the art. The key variable is illustratively changed once per communication session, or "call".

The mode of encryption used by encryptor 11 is

selected to be either the cipher text auto key (CTAK) mode of the Data Encryption Standard (DES), which is a self-synchronizing mode of encryption, or the state-sequence-driven (SSD) mode thereof, which is a non-self-synchronizing mode of encryption, the selection being specified from within transceiver 10 by a controller 25 via a transmit mode lead 28. Encryptor 11 applies the encrypted data to line 31, from which the encrypted data is received, or recovered, by the reception portion of transceiver 50, that portion including a decryptor 61.

Transceiver 50, more particularly, further includes a controller 65. As is described below, controller 65 has information as to whether the received data was CTAK- or SSD-encrypted in transceiver 10 and controller 65 provides that information to decryptor 61 via a receive mode lead 81. This allows decryptor 61, which receives the same aforementioned encryption key from user interface 89 on cable 57, to appropriately decrypt the received data using a CTAK or SSD decryption mode that corresponds to the CTAK or SSD encryption mode used by encryptor 11. The decrypted data is then provided to terminal 6 on lead 62.

At the same time, data from terminal 6 desired to be communicated to terminal 5 is applied to data input lead 52. During normal data communications, controller 65 applies to gate 55 via lead pair 67 a signal indicating that gate 55 is to apply to its output lead 56 the signal on lead 52. From lead 56, the data is applied to an encryptor 51. The latter encrypts the data in response to the encryption key provided on cable 57 using either CTAK encryption or SSD encryption, as specified by controller 65 via transmit mode lead 68. Encryptor 51 applies the encrypted data to line 32, from which the encrypted data is received within transceiver 10 by decryptor 21. As described below, controller 25 within transceiver 10 has information as to whether the data was CTAK- or SSD-encrypted within transceiver 50 and controller 25 provides

that information to decryptor 21 via a receive mode lead 41. This allows decryptor 21, which also receives the encryption key on cable 17, to appropriately decrypt the received data. The decrypted data is then provided to terminal 5 on lead 22.

Also extending to transceivers 10 and 50 from user interfaces 49 and 89 are user mode request lead 29 and 69, respectively. These leads supply to controllers 25 and 65 signals which indicate whether a CTAK or SSD mode of operation--both for encryption and decryption--is desired. Obviously, the signals on these leads must be coordinated, lest the two transceivers be given inconsistent mode requests, i.e., one CTAK and one SSD. Such coordination is the responsibility of the user and, as is well known, may be achieved, for example, via the action of human operators communicating by telephone, who control the mode request signal via a switch (not shown) on their respective user interfaces.

The other elements of the system shown in FIG. 1 will be discussed at appropriate points in the following description of FIG. 2.

Specifically, FIG. 2 depicts the various possible logical states for each transceiver and the various possible paths among those states. Thus, as indicated by path 201, each transceiver, when started up, enters state 200 wherein encryptors 11 and 51 operate in CTAK mode to encrypt the data on leads 12 and 52, and decryptors 21 and 61 operate in CTAK mode to decrypt the encrypted data received from lines 32 and 31, respectively. If the signal on the transceivers' user mode request leads 29 and 69, respectively, indicate that CTAK is the requested operating mode, the transceivers simply remain in normal operation in state 200, as indicated by path 202. Since CTAK is a self-synchronizing cryptographic mode, the system automatically becomes synchronized after a short transmission period, by which is meant that the crypto-state vector generated within each encryptor (as described below) becomes

identical to the crypto-state vector generated within the decryptor with which it communicates. (Typically, the data desired to be communicated will be prefixed by a preamble of "don't care" data which is loaded into each encryptor and decryptor for synchronization purposes.) From that point on, the data transmitted by the encryptor in each transceiver will be accurately recovered by the decryptor in the other.

If, however, the signals on leads 29 and 69 indicate that SSD is the requested operating mode, steps must be taken to first obtain cryptographic synchronization between each encryptor and the decryptor with which it communicates, since SSD is a non-self-synchronizing mode of encryption. To this end, the transceivers immediately enter state 205 via path 203.

Once, for example, transceiver 10 is in state 205, its controller 25 causes encryptor 11, which is still operating in CTAK mode, to begin to transmit over line 31 a synchronization pattern comprised of two portions, the second being uniquely distinguishable from any part of the first. The synchronization pattern, more particularly, is illustratively comprised of a string of clear text "1"s followed by a single clear text "0", the term "clear text" meaning the value of the bits as they are applied to the encryptor. The number of "1"s in the string is sufficient to ensure that cryptographic synchronization is established between encryptor 11 and decryptor 61, that number being at least 64 in this embodiment. Controller 35 causes the synchronization pattern to be applied to encryptor 11 changing the signal on lead pair 27 so as to first indicate to gate 15 that it should provide on lead 16 the signal on lead 13, which is tied to a constant positive voltage, representing binary "1", and to then indicate to gate 15 that it should provide on lead 16 the signal on lead 14, which is tied to ground, representing binary "0".

Similarly, once transceiver 50 enters state 205, controller 65 thereof causes encyptor 51, which is also

still operating in CTAK mode, to begin to transmit the aforementioned synchronization pattern, in CTAK mode, to decryptor 21 of transceiver 10 over line 32. Controller 65 achieves this by providing appropriate signals to gate 55 via lead pair 67, thereby causing gate 55 to provide as its output first the signal on lead 53, on which a constant "1" is carried, and then the signal on lead 54, on which a constant "0" is carried.

At the same time that encryptor 11 begins to transmit the aforementioned synchronization pattern, a pattern detector 23 within transceiver 10 begins to look on lead 22 for a 64-bit run of clear text "1"s followed by a clear text "1"-to-"0" transition. Moreover, at the same time that encryptor 51 begins to transmit the synchronization pattern, a pattern detector 63 within transceiver 50 begins to look for the run of clear text "1"s and the "1"-to-"0" transition on lead 62. When pattern detector 23 (63) detects such a transition, it signals controller 25 (65) on lead 24 (64), thereby indicating (assuming no transmission errors or other irregularities) that cryptographic synchronization between encryptor 51 (11) and decryptor 21 (61) has been established.

Paths 206 and 207 in FIG. 2 respectively indicate that each transceiver remains in state 205 as long as a) the transceiver is waiting for completion of the transmission of the synchronization pattern, which event is referred to in the drawing as "TX sync timeout," and b) the "1"-to-"0" transition, referred to in the drawing as the "RX sync transition," has not yet been detected.

Looking now specifically, for example, at transceiver 10, assume that RX sync is detected by pattern detector 23 before encryptor 11 has completed transmission of the synchronization pattern. In this case, transceiver 10 enters state 210 via path 208. Decryptor 21 has now been switched from CTAK to SSD operation and is thus able to begin decryption of SSD-encrypted data from

encryptor 51. At the same time, encryptor 11 continues transmitting the synchronization pattern in the CTAK mode, the latter action being indicated by path 211. When encryptor 11 thereafter completes transmission of the synchronization pattern, transceiver 10 enters state 220 via path 212. Encryptor 11 is thus also switched to the SSD mode and is able to begin to transmit SSD-encrypted data to decryptor 61.

Assume, on the other hand, that, from state 205, transmission of the synchronization pattern by encryptor 11 completes before pattern detector 23 detects the RX sync transition. In this case, transceiver 10 leaves state 205 for state 215 via path 209. Encryptor 11 has now been switched to the SSD operation and can begin to transmit SSD-encrypted data, while pattern detector 23 continues to wait for the RX sync transition, as indicated by path 216. When that transition is ultimately detected, transceiver 10 enters state 220 via path 218 and decryptor 21 is also switched to the SSD mode.

Since transceivers 10 and 50 are substantially identical, the state transition sequence described in the previous paragraph applies with equal validity to the operation of transceiver 50. The ultimate result, then, is that both transceivers are established in state 220, with data being communicated over both lines 31 and 32 in the SSD mode.

A further possibility to be accounted for is that the RX sync transition awaited in state 215 will not have been detected by the pattern detector within a particular transceiver within a predetermined receiver synchronization timeout period. If this is so, it cannot be safely assumed that synchronization has been restored. Accordingly, that transceiver is returned to state 205.

More specifically, assume for example, that pattern detector 63 within transceiver 50 does not detect RX sync transition within the aforementioned received synchronization timeout period. Accordingly, transceiver

50 returns from state 215 to state 205 via path 217. Encryptor 51 is switched back to CTAK operation and again initiates transmission of the synchronization pattern. Pattern detector 61, meanwhile, continues to wait for the RX sync transition on lead 62.

At this point, transceiver 10 will also return to state 205, no matter what state it was in. This can be understood as follows: If transceiver 10 is in state 215 when transceiver 50 re-enters state 205, this means that the RX sync transition has not yet been detected by pattern detector 23. Accordingly, the re-initiation of the transmission synchronization pattern by encryptor 51 will cause the synchronization timeout period waited for by transceiver 10 on path 216 to elapse before the RX sync transition in the newly-transmitted synchronization pattern will occur. This causes transceiver 10 to return to state 205 via path 217 just as transceiver 50 did.

Assume, on the other hand, that transceiver 10 is in either state 210 or state 220 when transceiver 50 returns from state 215 to state 205. Assume, further, that the data provided by each one of terminals 5 and 6 on leads 12 and 52, respectively, is formatted using a selected format violations of which are detectable within the other terminal. Such a format may be, for example, framed PCM, HDLC, etc. Consider, now, the data stream generated by decryptor 21 on lead 22 in response to the stream of "1"s initiated within transceiver 50. This data stream will not conform to the selected format since it was generated by decryptor 21 in response to a data stream that was not generated within terminal 6. (Indeed, since decryptor 21 is operating in SSD mode while encryptor 51 is operating in CTAK mode, the data stream on lead 22 will not even be a string of "1"s but, rather, some random bit pattern.) With format violations thus being detected within terminal 5, the latter provides an out-of-synchronization (OOS) indication to controller 25 on lead 26. Controller 25 responds by returning transceiver 10 to state 205 via path

213, if transceiver 10 was in state 210, thereby switching decryptor 21 from SSD operation back to CTAK operation, or via path 223 if transceiver 10 was in state 220, thereby switching both encryptor 11 and decryptor 21 from SSD to CTAK operation. With both transceivers thus in state 205, system operation proceeds as already described.

A similar sequence of events would obtain if it were pattern detector 23, rather than pattern detector 63, that did not detect the transition awaited in state 215 within the receiver synchronization timeout period. Accordingly, this eventuality need not be discussed in further detail except to point out the existence of an out-of-synchronization lead 66 extending to controller 65 from terminal 6.

Once both transceivers are concurrently in state 220, they remain in that state--encrypting and decrypting data in SSD mode operation, as indicated by path 221--until one of two things happens. One possibility is that the signals on user mode request leads 29 and 69 may change, indicating that the user desires a CTAK mode of operation. In this case, each transceiver simply returns to state 200, via path 222.

The other possibility is that cryptographic synchronization between one or both encryptor/decryptor pairs is lost. Assume, by way of example, that the loss of synchronization is between encryptor 51 and decryptor 21. In accordance with a feature of the invention, this fact is made known at encryptor 51 as follows: The fact that cryptographic synchronization between encryptor 51 and decryptor 21 has been lost means that there will be a very high bit error rate and accompanying format violations in the data provided on lead 22. Terminal 5 then generates an out-of-synchronization indication to controller 25 on lead 26. This causes transceiver 10 to return to state 205 via path 223, thereby switching both encryptor 11 and decryptor 21 from SSD to CTAK operation. The thus-initiated transmission of CTAK-encrypted "1"s over path 31 by

encryptor 11 causes a very high bit error rate in the data provided on lead 62 because transceiver 50 is still in state 220 and thus decryptor 61 is operating in SSD mode. Upon detecting this very high bit error rate, terminal 6 generates an out-of-synchronization indication to controller 65 on lead 66. This causes transceiver 50 to also leave state 220 and enter state 205 via path 223, thereby switching both encryptor 51 and decryptor 61 from SSD to CTAK operation. From this point, system operation proceeds as already described, resulting, ultimately, in a return by both transceivers to state 220, with both encryptors and both decryptors being switched back to SSD operation.

One further point to be addressed in conjunction with FIG. 2 relates to the fact that if transceivers 10 and 50 have been in state 200, and thus have been operating in CTAK mode, for any period of time, they are assumed to be cryptographically synchronized. Thus, if it were desired to switch to SSD operation at a subsequent point in time, it would not, in theory, be necessary for each transceiver to proceed to state 205 for the purpose of establishing synchronization. Rather, it might be possible for each transceiver to proceed directly to state 220. As a practical matter, however, it would still be necessary for each decryptor to be able to identify the precise point in the received data stream at which the data becomes SSD-encrypted, as opposed to CTAK-encrypted. That point is, of course, identified by the "1"-to-"0" transition in the synchronization pattern. Thus, in this embodiment, even if a transceiver has been operating for a period of time in CTAK mode in state 200, a subsequent request to change to SSD mode causes the transceiver to enter state 205 as shown in the drawing.

An exemplary embodiment of encryptor 11 is shown in FIG. 3. Encryptor 51 is, illustratively, identical to encryptor 11 and need not be discussed in further detail.

At the heart of encryptor 11 is an encryption

circuit 150. This circuit is illustratively a commerically available integrated circuit which implements the Data Encryption Standard (DES). Circuit 150 has two principal inputs. One of these is the aforementioned key variable on cable 17. The value of this key variable defines which of the 2^{56} possible instances of the DES encryption algorithm the circuit is to use.

The other input to circuit 150 is the so-called crypto-state vector, which is generated internally within encryptor 11 and provided on cable 152. The crypto-state vector is a binary word having, in this example, 64 bits, whose value changes for each bit of the lead 16 input data. For each value of the crypto-state vector, encryption circuit 150 generates on lead 151 a single encrypted bit in accordance with the selected encryption algorithm. That bit is then applied to one input of an exclusive-OR gate 155. The other input for gate 155 is the current "clear text" data bit on lead 16, which lead is denoted internally within the encryptor as lead 158. The stream of bits at the output of gate 155 comprises the encryptor's "cipher text" output on line 31, which lead is denoted internally within the encryptor as lead 156.

The remainder of the circuitry of encryptor 11 generates the crypto-state vector on cable 152. In particular, that circuitry includes 33-stage crypto-state shift register 110, 32-stage crypto-state shift register 125, exclusive-OR gates 115 and mode 130 and selectors 120 and 135. At any given point in time, the crypto-stage vector on cable 152 comprises the 32 bits then stored in register 125, which are provided on cable 128, and the first 32 bits stored in register 110, which are provided on cable 113. When the next crypto-state vector is needed, a new bit is shifted into register 110 from selector 120 output lead 121 and, concurrently, a new bit is shifted into register 125 from selector 135 output lead 136.

The source of the bits that each one of selectors 120 and 135 puts on its respective output lead depends on

whether the encryptor is operating in CTAK mode or SSD mode, as specified by the signal on transmit mode lead 28. In particular, when the encryptor is to operate in CTAK mode, the signal on lead 28 causes selector 120 to provide on its output lead 121 the bits on register 125 output lead 129--which derive from the last stage of register 125--and it causes selector 135 to provide on its output lead 136 the bits on cipher text output lead 31, the latter bits being extended to selector 135 via lead 159.

On the other hand, when the encryptor is to operate in SSD mode, the signal on lead 28 causes selector 120 (135) to provide on its output lead the bits on the output lead 116 (131) of exclusive-OR gate 115 (130). Exclusive-OR gate 115, in particular, is a 2-input gate which, illustratively, receives its inputs from the 14th and 33rd stages of register 110 via a cable 112. Exclusive-OR gate 130 is a 4-input gate which, illustratively, receives its inputs from the 10th, 30th, 31st and 32nd stages of register 125 via as cable 121.

Decryptors 21 and 61 are not only substantially identical to one another, but also are very similar in structure to encryptors 11 and 61. In fact, the structure shown in FIG. 3 can be used as a decryptor by applying the received cipher text on lead 158, taking the signal on lead 156 as the decryptor output, and taking the signal for lead 159 from lead 158 rather than from lead 156.

Although not the case in the illustrative embodiment of FIG. 3, the encryptors and decryptors shown in FIG. 1 may include conventional modulation, demodulation and other data transmission circuitry to facilitate transmission and recovery of the encrypted bits.

Controllers 25 and 65 are, illustratively, respective microprocessors programmed in straightforward fashion to perform the functions described herein.

As previously noted, the above-described feature of the invention--wherein the existence of an abnormality in the signal received at (say) a local end of the

transmission channel is communicated to the remote end by causing there to be abnormalities in the signal transmitted in the other direction--is applicable not only to cryptographic transmission systems, but also to other types of two-way transmission systems. Thus, for example, consider a system in which two-way communication is carried on between two modems at some first data rate. Assume that, as the result of a subsequent channel degradation, the bit error rate in the data transmitted to the local end becomes abnormally high. Assume further that the appropriate corrective action is for data to be transmitted from the remote end to the local end at a lower bit rate. The fact that such corrective action needs to be taken can be communicated from the local end to the remote end by causing the data that is transmitted to the remote end from the local end to be transmitted using, for example, signal constellation points, many or all of which are intentionally dispersed from the "ideal" points. The abnormally high dispersion in the received signal points serves as notice at the remote end that, in fact, a lower bit rate should be gone to.

It will thus be appreciated that the foregoing merely illustrates the principles of the invention. It is anticipated that those skilled in the art will be able to devise numerous arrangements which, although not explicitly shown or described herein, embody the principles of the invention.

Claims

1. A cryptographic transceiver including

local encryption means (11) operative for encrypting data applied thereto using a seclected non-self-synchronizing encryption mode,

transmission means (15) for initiating transmission of the encrypted data to a remote decryption means (61), and

local decryption means (21) operative for decrypting received data that was encrypted by a remote encryption means (51) using a selected non-self-synchronizing encryption mode,

CHARACTERIZED IN THAT

said local encryption means (11) is further operative to encrypt said data using a selected self-synchronizing encryption mode,

said local decryption means (21) is further operative to decrypt received data that was encrypted by said remote encryption means (51) using a selected self-synchronizing encryption mode, and

said transceiver includes controller means (25) operative in response to an indication that said remote encryption means (51) and said local decryption means (21) are not cryptographically synchronized for switching the operation of said local encryption means (11) to a self-synchronizing encryption mode and for switching the operation of said local decryption means (21) to a self-synchronizing decryption mode.

2. The transceiver of claim 1 is further

CHARACTERIZED IN THAT

interface means (49) operative upon the switching of the operation of said local encryption means to said self-synchronizing encryption mode applies to said local encryption means a data stream having first and second portions, said second portion being uniquely distinguishable from any part of said first portion and said first portion being of sufficient length to ensure

that said local encryption means and said remote decryption means are cryptographically synchronized by the time that said second portion is decrypted by said remote decryption means, said controller means is further operative subsequent to the encryption of said second portion by said local encryption means for switching the operation of said local encryption means back to said non-self-synchronizing encryption mode.

3. The transceiver of claim 2 further CHARACTERIZED IN THAT

said first portion is a sequence of bits of a first bit value and

said second portion has at least one bit of a second bit value.

4. A method for controlling a cryptographic transceiver which comprises local encryption means (11) operative to encrypt data applied thereto using a selected non-self-synchronizing encryption mode, transmission means (15) for initiating transmission of the encrypted data to a remote decryption means (61), and local decryption means (21) operative to decrypt received data that was encrypted by a remote encryption means (51) using a selected non-self-synchronizing encryption mode, said local encryption means (21) being further operative to encrypt said data using a selected self-synchronizing encryption mode, and said local decryption means (21) being further operative to decrypt received data that was encrypted by said remote encryption means (51) using a selected self-synchronizing encryption mode,

CHARACTERIZED BY

the step of

switching the operation of said local encryption means to a self-synchronizing encryption mode and the operation of said local decryption means to a self-synchronizing decryption mode in response to an indication that said remote encryption means and said local decryption means are not cryptographically synchronized.

5. The invention of claim 4
CHARACTERIZED BY
the further steps of:
1) applying to said local encryption means upon the switching of the operation of said local encryption means to said self-synchronizing encryption mode a data stream having first and second portions, said second portion being uniquely distinguishable from any part of said first portion and said first portion being of sufficient length to ensure that said local encryption means and said remote decryption means are cryptographically synchronized by the time that said second portion is decrypted by said remote decryption means, and
2) switching the operation of said local encryption means back to said non-self-synchronizing encryption mode subsequent to the encryption of said second portion by said local encryption means.
6. The method of claim 5 further
CHARACTERIZED IN THAT
said first portion is a sequence of bits of a first bit value and
said second portion has at least one bit of a second bit value.

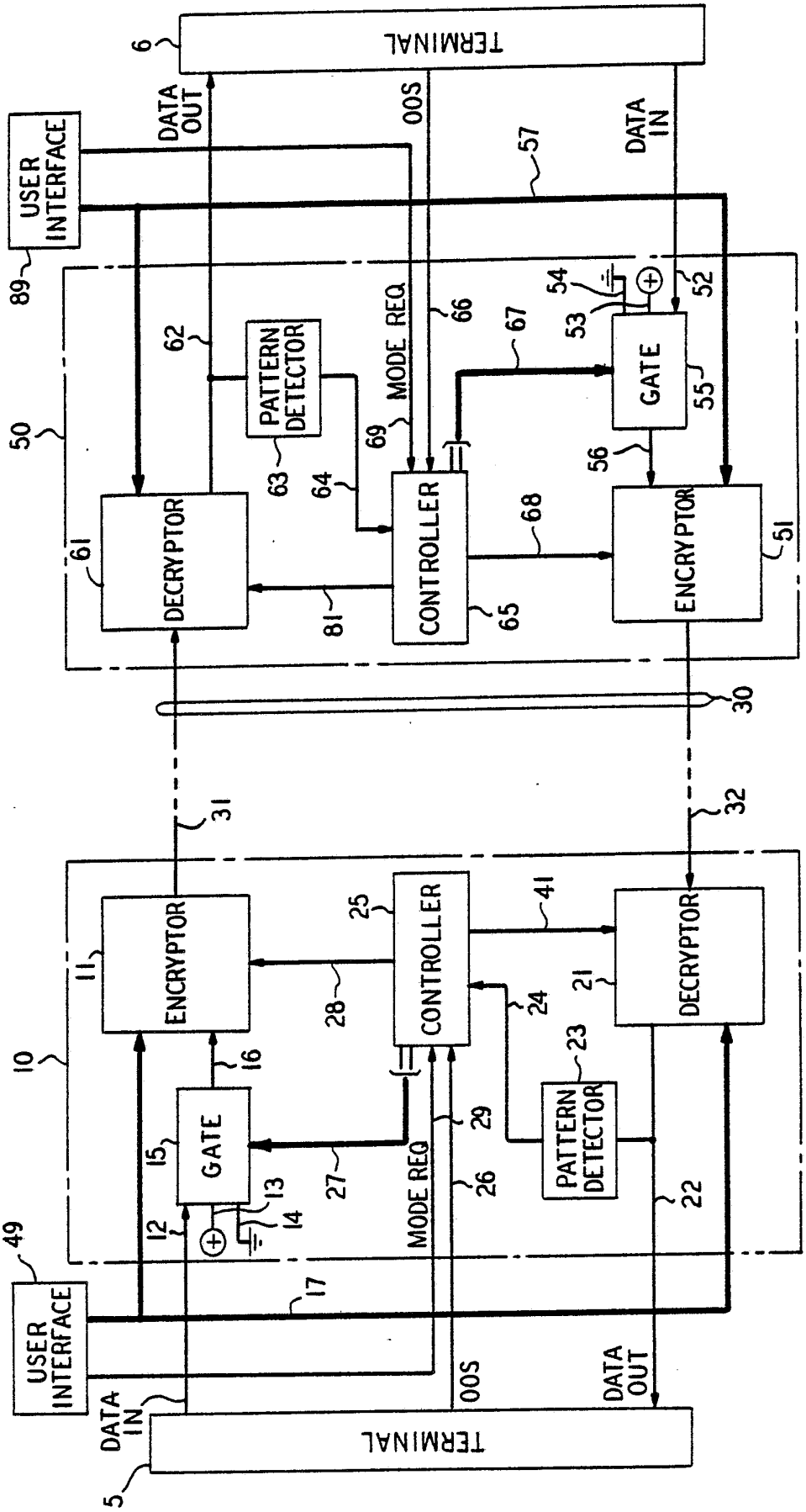

TERMINAL
DATA OUT
OOS
DATA IN
USER INTERFACE
57
89
50
62
PATTERN DETECTOR
MODE REQ
66
67
54
53
52
GATE
55
56
69
63
64
DECRYPTOR
61
CONTROLLER
68
ENCRYPTOR
51
81
65
30
31
32
ENCRYPTOR
11
25
CONTROLLER
41
DECRYPTOR
21
28
24
10
16
23
PATTERN DETECTOR
GATE
15
29
27
MODE REQ
26
22
13
14
12
49
17
USER INTERFACE
DATA IN
OOS
DATA OUT
TERMINAL
5
6

FIG. 1

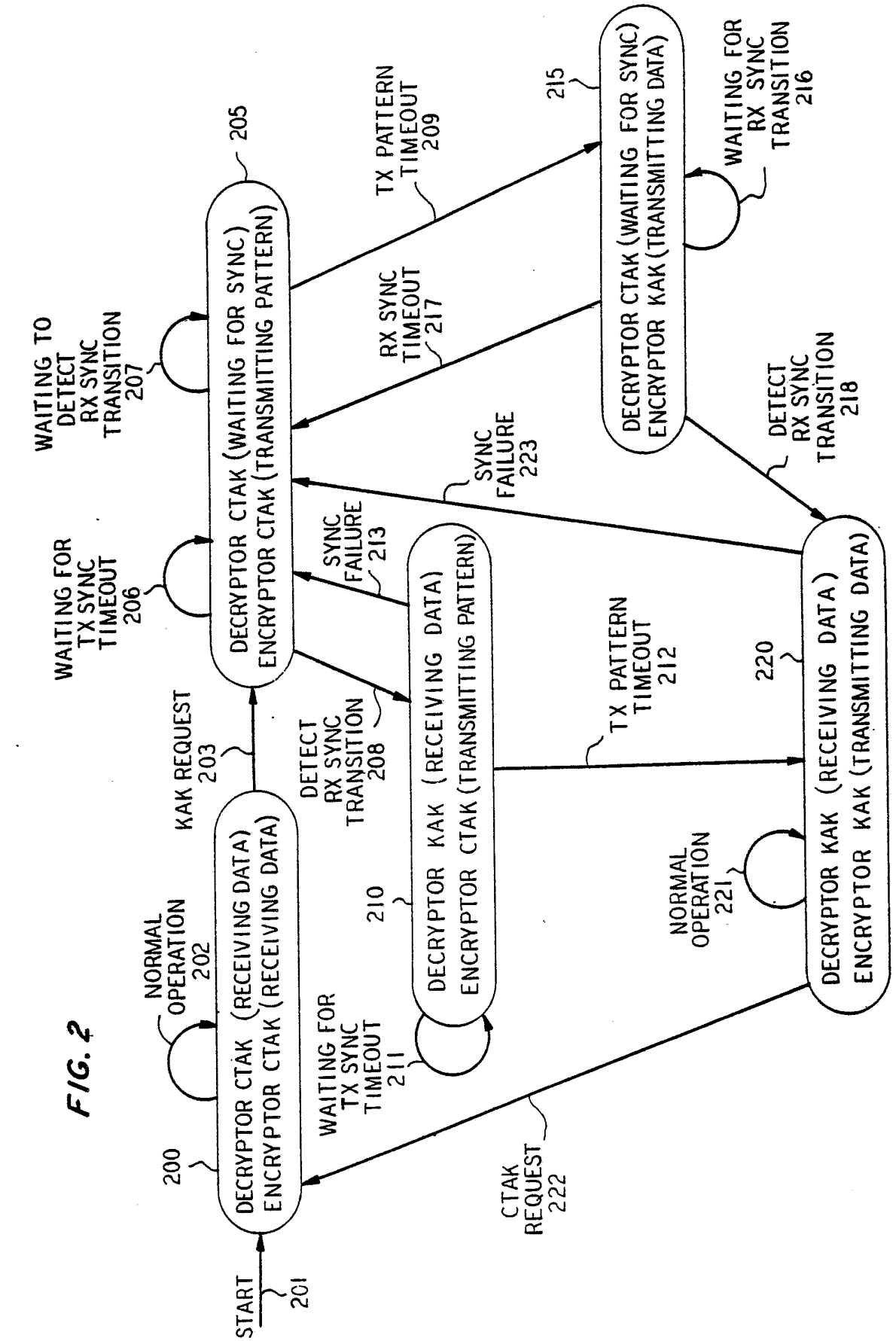
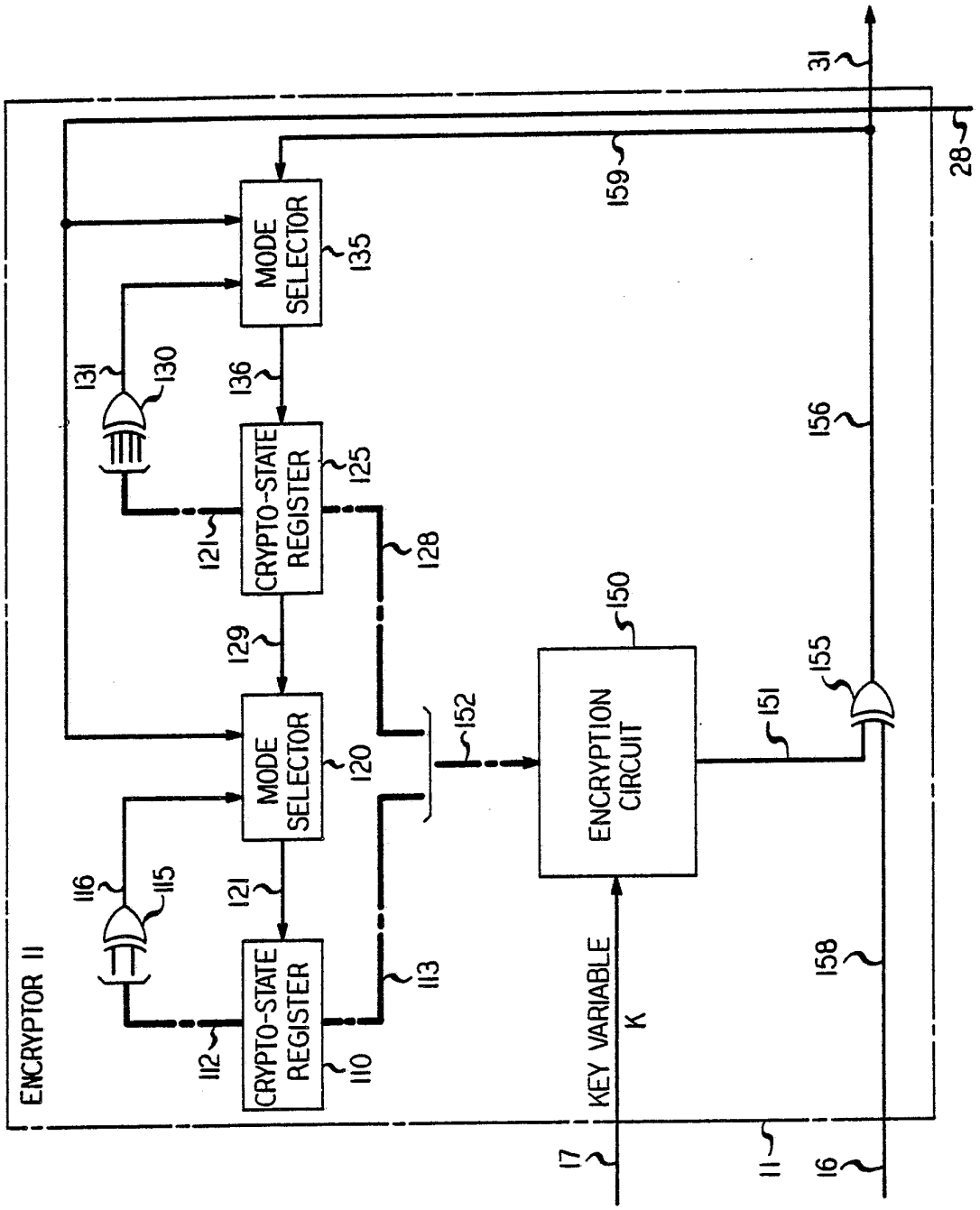

START
201
DECRYPTOR CTAK (RECEIVING DATA)
ENCRYPTOR CTAK (RECEIVING DATA)
200
NORMAL OPERATION 202
KAK REQUEST 203
DECRYPTOR CTAK (WAITING FOR SYNC)
ENCRYPTOR CTAK (TRANSMITTING PATTERN)
205
WAITING TO DETECT RX SYNC TRANSITION 207
WAITING FOR TX SYNC TIMEOUT 206
TX PATTERN TIMEOUT 209
RX SYNC TIMEOUT 217
SYNC FAILURE 213
DETECT RX SYNC TRANSITION 208
DECRYPTOR KAK (RECEIVING DATA)
ENCRYPTOR CTAK (TRANSMITTING PATTERN)
210
WAITING FOR TX SYNC TIMEOUT 211
TX PATTERN TIMEOUT 212
SYNC FAILURE 223
DECRYPTOR CTAK (WAITING FOR SYNC)
ENCRYPTOR KAK (TRANSMITTING DATA)
215
WAITING FOR RX SYNC TRANSITION 216
DETECT RX SYNC TRANSITION 218
DECRYPTOR KAK (RECEIVING DATA)
ENCRYPTOR KAK (TRANSMITTING DATA)
220
NORMAL OPERATION 221
CTAK REQUEST 222

FIG. 2

FIG. 3


ENCRYPTOR 11
MODE SELECTOR
135
CRYPTO-STATE REGISTER
125
MODE SELECTOR
120
CRYPTO-STATE REGISTER
110
ENCRYPTION CIRCUIT
150
KEY VARIABLE
K
131
130
136
121
129
116
115
121
112
113
152
128
159
156
155
151
158
31
28
17
11
16

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 84/02016

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

IPC[4]: H 04 L 9/00

II. FIELDS SEARCHED

Minimum Documentation Searched [7]

Classification System	Classification Symbols
IPC[4]	H 04 L

Documentation Searched other than Minimum Documentation to the Extent that such Documents are included in the Fields Searched [8]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [9]

Category [10]	Citation of Document, [11] with indication, where appropriate, of the relevant passages [12]	Relevant to Claim No. [13]
A	US, A, 4274085 (MARINO) 16 June 1981 see column 6, lines 53-59 --	1
A	DE, A1, 2827615 (LICENTIA) 10 January 1980 see page 19, line 16 - page 20, last line --	1
A	Electrical Communication, vol. 58, no. 1, 25 October 1983 (Harlow, GB) Baroncini et al.: "Inexpensive digital encryption systems for cordless telephone secrecy", pages 141-142, see page 141, right-hand column, paragraph 2 - page 142, right-hand column, last line --	1
A	1982 Carnahan Conference on Security Technology, Lexington, US, Published May 12-14, 1982 Pietrasiewicz: "Federal standards for telecommunications privacy and security - recent progress", pages 19-30, see page 29, line 10 - page	1 ./.

* Special categories of cited documents: [10]

"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

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
26th March 1985	22 AVR. 1985
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	G.L.M. Kruydenberg

Form PCT/ISA/210 (second sheet) (January 1985)

III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET)

Category *	Citation of Document, with indication, where appropriate, of the relevant passages	Relevant to Claim No
	30, line 15	

ANNEX TO THE INTERNATIONAL SEARCH REPORT ON

INTERNATIONAL APPLICATION NO. PCT/US 8402016 (SA 8455)

This Annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report. The members are as contained in the European Patent Office EDP file on 16/04/85

The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A- 4274085	16/06/81	None	
DE-A- 2827615	10/01/80	None	