PCT WORLD INTELLECTU Inter

WO 9604599A1

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, 12/14 | A1

(11) International Publication Number: WO 96/04599

(43) International Publication Date: 15 February 1996 (15.02.96)

(21) International Application Number: PCT/US95/01738

(22) International Filing Date: 9 February 1995 (09.02.95)

(30) Priority Data:
08/286,680 5 August 1994 (05.08.94) US

(71) Applicant: INFOSAFE SYSTEMS, INC. [US/US]; Suite 622, 342 Madison Avenue, New York, NY 10173 (US).

(72) Inventors: SOKOL, Christopher; Apartment 4E, 1443 York Avenue, New York, NY 10021 (US). NAGEL, Robert; Suite 7F, 33 Riverside Drive, New York, NY 10023 (US). LIPSCOMB, Thomas, H.; 145 E. 74th Street, New York, NY 10021 (US).

(74) Agents: MILDE, Karl, F., Jr. et al.; Karl F. Milde, Jr., P.C., Suite 210, 2 Crosfield Avenue, West Nyack, NY 10994 (US).

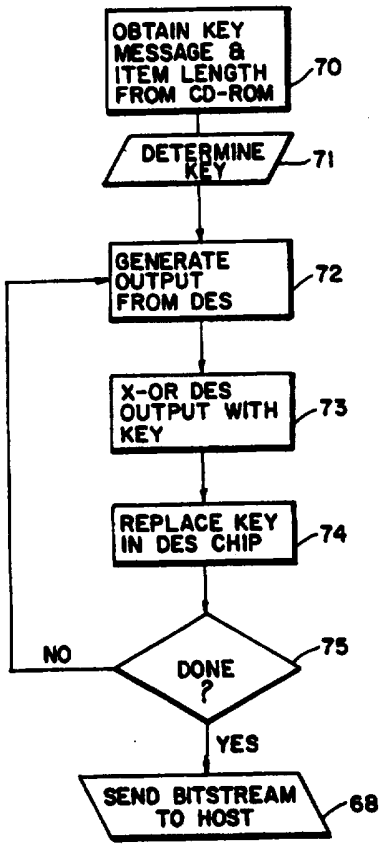
(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, MX, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, UG, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

Published
With international search report.

(54) Title: METHOD AND APPARATUS FOR RETRIEVING SECURE INFORMATION FROM MASS STORAGE MEDIA

(57) Abstract

Apparatus for retrieving information from mass storage media, wherein at least some of the information is in encrypted form and may be decrypted using a decryption algorithm which requires a decryption key. The apparatus comprises a host computer for selecting information to be retrieved from a storage medium; a storage medium reader for reading the selected information from the storage medium and transmitting the same to the host computer; and a decryption device for producing a decryption bitstream and transmitting the same to the host computer. The host computer is operative to receive the selected information from the storage medium reader and the decryption bitstream from the decryption device and to execute a binary exclusive-OR operation between the decryption bitstream and the encrypted information to produce the selected information in decrypted form.



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	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

METHOD AND APPARATUS FOR RETRIEVING SECURE INFORMATION FROM MASS STORAGE MEDIA

BACKGROUND OF THE INVENTION

The present invention relates to a system (method and apparatus) for retrieving secure information from a mass storage medium, such as a CD-ROM, for temporary storage and usage by an information user.

Systems for storage and retrieval of secure information are well known in the art. As used herein, the term "secure information" is intended to mean information (alphanumeric data, graphics and the like) which is either encrypted or otherwise protected to prevent access thereto except by an authorized user. Such systems have been proposed and are employed both for the case where the information source (database) is centralized, and for the case where the information source has been distributed to multiple users. In the latter case, CD-ROMs have been used to export databases to multiple users so that information storage and retrieval takes place at the user site.

In the U.S. Patent No. 5,010,571 to Ron Katznelson and the U.S. Patents Nos. 4,827,508, 4,977,594 and 5,050,213 to Victor Shear, it is proposed to provide encrypted digital information on CD-ROMs at the user site and to monitor and account for each item or "packet" of information which is retrieved and decrypted from a CD-ROM by an authorized user.

This concept of retrieving information on a "pay-as-you-go" basis is also disclosed in the U.S. Patent No.

5,247,575 of Peter J. Sprague and Thomas H. Lipscomb to include individual access to encrypted data which is "broadcast" to multiple user sites from a central source and/or to provide individual access to encrypted data stored at a central source, using conventional time sharing techniques and transmission via telephone dial-up or local area network (LAN) or wide area network (WAN) communication.

All of these prior art systems permit the user's access to the secure information to be monitored and strictly controlled. This is accomplished, in practice, by maintaining a record at each user site of each information packet which is retrieved and the cost thereof to the user, and then "polling" all user sites from a remote central site, on a regular basis, to retrieve the user data and, if necessary, disable the equipment at one or more user sites to prevent further access to the secure information at these sites.

Systems of this type require specialized electronic circuitry at each user site which operates in cooperation with a central computer at a remote site. Particularly when decryption must be effected at each user site, it is difficult to maintain the security and integrity of this electronic equipment.

Furthermore, the provision of an electronic circuit board, or the like, to a personal computer at a user workstation can (actually or apparently) compromise the

integrity of this computer, thus making the system difficult to implement in practice.

SUMMARY OF THE INVENTION

A principal object of the present invention is to provide a method and apparatus for retrieving secure information from a mass storage medium at a user site which is not susceptible to attack or compromise by a user.

It is a further object of the present invention to provide a system for retrieving secure information from a mass storage medium at a user site which does not require a reconfiguration of a personal computer at the user site.

These objects, as well as further objects which will become apparent from the discussion that follows, are achieved, in accordance with the present invention, by providing (1) a personal computer or "host computer"; (2) a storage medium reader, connected to the host computer for reading encrypted information from the storage medium and passing it to the host computer, and (3) a "decryption device", also connected to the host computer, for producing a decryption bitstream and transmitting the same to the host computer. The host computer is operative to receive the selected information from the storage medium reader and the decryption bitstream from the decryption device and to execute a binary exclusive-OR operation between the

decryption bitstream and the encrypted information to produce the selected information in decrypted form.

For a full understanding of the present invention, reference should now be made to the following detailed description of the preferred embodiments of the invention as illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a representative diagram of a workstation comprising a personal computer (PC), a CD-ROM reader and a decryption device all arranged on an SCSI bus.

Fig. 2 is a block diagram of a decryption device for use in the system of Fig. 1.

Fig. 3 is a flow chart showing the general operation of the decryption device of Fig. 2.

Fig. 4 is a flow chart showing the general operation of the decryption device of Fig. 2 in response to an SCSI command from the host computer.

Fig. 5 is a block diagram showing the flow of information in the system of Fig. 1.

Fig. 6 is a flow chart showing the general operation of the decryption device in response to an SCSI command to retrieve an item of information.

Fig. 7 is a flow chart showing the operation of the decryption device in decrypting data.

Fig. 8 is a flow chart showing the operation of the decryption device in creating a decryption key.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The preferred embodiment of the present invention will now be described with reference to Figs. 1-8 of the drawings. Identical elements in the various figures are designated with the same reference numerals.

Fig. 1 illustrates the general nature of the system according to the preferred embodiment of the present invention. As shown here, the system involves a digital computer workstation which is capable of retrieving secure data from a database stored on one or more CD-ROMs.

In order to prevent unauthorized access to the stored information, at least some of the individual items of information ("information packets") are encrypted prior to storage on a CD-ROM. Some of the information packets may also be stored in decrypted ("cleartext") form on a CD-ROM and can be retrieved by any workstation user by means of a CD-ROM reader. However, only an authorized user with a proper validated code is allowed to decrypt the encrypted information packets.

Upon release of the secure and, if desired, the non-secure information to an authorized user, the user is charged a preset fee set by the information provider (copyright owner or publisher of the information). This

charge is effected automatically by debiting a financial account which has previously been established between the user and the information provider.

To implement this system, there is provided a workstation comprising a personal computer (PC) 10, a CD-ROM reader 12 and a decryption device 14. These three devices, which may be stand-alone devices each arranged in a separate enclosure or combined in one or two enclosures -- e.g., the PC 10 in one enclosure and the CD-ROM reader 12 and decryption device 14 in another -- are connected in a well-known manner to a Small Computer System Interface ("SCSI") bus 16 via a bus interface and controller 18. Alternatively, the devices 12 and 14 may each be connected to the host computer 10 via a bi-directional parallel part or via some other mode of communication.

The personal computer 10 and the CD-ROM reader 12 are conventional devices which are available commercially. The decryption device 14 is a special purpose device which operates to produce a "decryption bitstream" from a key and an input vector and to transport this bitstream to the host computer 10 for storage either in its active memory (RAM) or hard disk drive. This decryption bitstream is identical in length to the information packet which is to be retrieved from the CD-ROM and decrypted.

The decryption device also keeps a running account of the identity of, and charge for each information packet

which is decrypted for later transmission, e.g. by telephone line, to a central billing facility at a remote site. A monitoring facility of this type is known from the aforementioned U.S. Patents Nos. 5,010,571; 4,827,5089 and 5,247,575.

As mentioned above, the decryption device 14 generates a decryption bitstream from a decryption key and an input vector. The decryption key is preferably determined, in the manner fully described below, from a "key message" obtained from the CD-ROM. An input vector, required for key generation, is also obtained from the CD-ROM. Alternatively, either one or both of the decryption key and input vector may be supplied directly to the decryption device 14; e.g., from the host computer or from a remote central billing facility via modem.

According to the invention, both the bitstream, received from the decryption device 14, and the encrypted information packet, received from the CD-ROM reader 12, are combined in the host computer 10 to decrypt the information packet. More particularly, the host computer executes a binary operation between the decryption bitstream and the encrypted information packet to produce the information packet in decrypted form. In the preferred embodiment of the invention, the decryption bitstream is a cypher feedback bitstream and the binary operation is "exclusive-OR". In other words, each bit in the decryption bitstream is

exclusive-ORed with a corresponding bit in the encrypted information packet to produce either a binary "1" or "0" in the corresponding bit position in the decrypted information packet.

Once an information packet is transferred to the host computer 10 and decrypted therein, the workstation user can display it on the computer screen, print out a hard copy and/or transmit a copy by LAN or modem to another workstation.

In accordance with the SCSI standard, the SCSI bus extends up to twenty-six feet in length from end to end and is provided with terminating impedances at each end. Each unit arranged on the bus is provided with a unique address from a maximum of eight addresses (zero to seven). The computer is usually given the address number seven; the addresses of the other devices on the bus may be selected from zero to seven with a manual switch arranged on each device.

In the preferred embodiment of the present invention, the decryption device 14 is disposed in its own enclosure, separate and apart from the personal computer 10 and possibly also the CD-ROM reader 12. To safeguard the firmware and codes which are used by the electronic circuitry, the decryption device may be provided with light-sensitive, erasable memory circuits so that the contents of memory are erased if the enclosure is opened.

Fig. 2 shows the preferred embodiment of the decryption device. This device is connected to the SCSI bus 16 via receptacles 20 and a fifty pin header 22. The SCSI bus controller 18 operates in conjunction with a CPU 24 to receive requests for data from the host computer 10 and initiate requests for key message data from the CD-ROM reader 12.

The device is provided with its own separate power supply 26 so that it operates completely independently of the host computer 10.

The decryption device is also provided with a 2400 baud modem and telephone interface 28 so that it may communicate with a central billing computer at a remote site. This central billing computer routinely calls the decryption device 14 at regular intervals -- for example, each night -- to download the logged information concerning each information packet (IP) that was decrypted, and/or to credit the financial account maintained by the decryption controller when the workstation user makes payment.

The decryption device 14 can also communicate with other devices, such as printers or the like, by means of an RS-232C transceiver 30 and an associated serial port connector 32.

The SCSI address is set from zero to six by a manual ID selector 34. Date and time are provided by a real time clock 36.

Firmware for the decryption device 14 is provided on two 128K flash memory chips 38; intermediate scratch pad storage is provided by a 256K dynamic RAM 40.

Decryption of encrypted data is effected with the aid of a Data Encryption Standard (DES) module 42 which operates in conjunction with a key code scrambler 44. The key code scrambler maintains the keys and the input vector used by the DES module for decryption. Alternatively, the decryption function and/or the key code scrambler function may be implemented in software (firmware) operating in the CPU 24.

All keys utilized by the system are created and maintained in the decryption device 14 so that neither the workstation user nor the PC 10 will have access to these keys.

All of the electronic circuit devices contained in the decryption device of Fig. 2 are standard, commercially available devices. Part numbers are shown in Fig. 2 for the major components.

In a preferred embodiment of the invention, the system of Fig. 1 and, in particular, the decryption device of Fig. 2, operates in the manner shown by the flow charts of Figs. 3, 4 and 6-8.

When first switched on, the CPU 24 executes a self-test routine as is conventional in the art (Block 45 in Fig. 3). Error messages are communicated to the host computer via the

SCSI bus for display to the system user. Thereafter, the CPU enters the idle mode (Block 46) and awaits an interrupt.

If the decryption device receives an SCSI command from the host computer (Block 47) it processes this command (Block 48) as will be described hereinafter in connection with Fig. 4. If the decryption device receives an incoming telephone message (Block 49) from a central billing computer, it processes this message (Block 50) before proceeding. Typical telephone messages are set forth in Table I:

TABLE I

Set Credit (in financial account)
Set Item Price
Set User Password
Clear Financial Account to Zero
Get Financial Account Information
Get User Information
Create User Information
Remove User Information
Send User a Message

Similarly, if an RS232 connection is established (Block 51), permitting communication either to or from the decryption device, the decryption device either transmits information, for example to a printer, or receives a serial message of the type noted above. In this case, the serial message is processed (Block 52) and the device returns to the idle state.

Fig. 4 illustrates how an SCSI command from the host computer is treated by the decryption device. When an SCSI command is received (Block 53) it is analyzed and processed

(Block 54) by the decryption controller. Typical SCSI commands are set forth in Table II:

TABLE II

Get Financial Account Information
Get Purchased Item Information
Assent/Don't Assent to Purchase Item
Log In
Log Out
Poll for an Asynchronous Event (such as an "on sale" notice)
Set User's Default Billing Reference (e.g., last billing reference number used)
Purchase Item
Get Decryption Device Status (i.e., error codes)
Get User Information (i.e., currently logged-in user)
Receive Decrypted Data

Certain PC commands require the decryption device to call the central billing computer via the telephone modem. For example, if the financial account is decremented to zero, the decryption device will automatically call and request additional credit. In this case, the decryption device makes the call (Block 55) and executes the call-out sequence (Block 56). In the call-out protocol, the decryption device dials the number of the central billing facility and transmits both its telephone and identification (ID) numbers. This simple transmission requests an immediate call-back from the central computer during which the financial account is automatically updated.

Each telephone transaction, initiated by the central billing computer, preferably comprises three steps:

(1) A download to the central billing facility of the current financial account status, all billing transactions

completed since the previous download, and the user information stored in the decryption device;

(2) A transmission from the central billing facility to the decryption device of any updates, such as changes in pricing information and the like; and

(3) A communication of all error codes from the decryption device to the central billing facility which indicate that the decryption device is not functioning properly.

In addition, the financial account balance in the decryption device can be updated by the central billing facility. It can be credited, if payment was made to the central billing facility by the user, or debited, for example if a check was returned from the bank marked "insufficient funds".

Each billing transaction provided to the central billing facility preferably contains, at a minimum, the following information:

Time and Date of Decryption
Identification No. of Information Packet (IP)
Volume No. of CD-ROM
Information Owner or Distributor of IP
Type of IP (Classification)
Price Paid for IP
Billing Reference, if inserted by the User

When an item (IP) is purchased by a user, and the decryption device 14 is able to complete this transaction by decrementing the financial account and decrypting the item, this transaction is logged into the flash memory 38 of the

device 14. In this case, the logging operation is flagged (Block 57) and carried out (Block 58) at the completion of the transaction. Thereafter, the decryption device returns to the idle mode (Block 59).

Fig. 5 illustrates the flow of data in the decryption of an information packet. As shown therein, the DES module 42 in the decryption device 14 is supplied an initial key for the key register and an initial input vector for the input register. Both the key register and input register are 64 bits (8 bytes) in length. The DES module generates a 64 bit bitstream which is transmitted to the host computer 10. This bitstream is also fed back and combined with the key in the key register with a binary exclusive-OR operation. This procedure is known in the art as "cypher feedback".

The DES module repeats the process of producing a 64 bit output with each new key that is entered into the key register. This procedure continues until the bitstream generated is equal in length to the encrypted information packet retrieved by the CD-ROM reader 12.

The decryption bitstream and the encrypted information packet, received by the host computer 10, are combined, bit by respective bit, with a binary exclusive-OR operation to produce the information packet in cleartext.

Referring to Fig. 6, the retrieval of an item (IP) commences with a request by the host computer 10 (Block 60).

The host computer sends this request to both the CD-ROM reader 12 and the decryption device 14 via the SCSI bus.

The decryption device 14 initially queries the file directory of the CD-ROM to determine whether or not the item of information is encrypted (Block 61). If not, the decryption device initiates a data transmission to the host computer indicating that cleartext will be forthcoming and then remains idle for the duration of the data retrieved transmission. Thereafter, the data item is transferred to the host computer (Block 62) from the CD-ROM reader 12.

If the file directory indicates that the desired item is encrypted, the decryption device checks the user's financial account to determine if there is a sufficient positive balance to pay for the item (Block 64). If not, the decryption device informs the host computer of the insufficient credit (Block 65).

If credit is sufficient, the decryption device transmits the cost of the item to the host computer and asks the host to confirm the purchase (Block 66) by displaying the cost to the user and requesting a user response. If the user fails to accept the purchase, the transaction is terminated (Block 67).

If the host computer confirms the purchase of the item at the price indicated, the decryption device initiates a data request to the CD-ROM reader. The item is thus caused to be read by the CD-ROM reader and it is transferred to the

host computer, where it is combined with the decryption bitstream from the decryption device 14 to produce the item in cleartext. Once the item of information has been supplied to the host computer and decrypted therein, it is available for storage, both temporary and archival storage, and may be read and copied by the user, as desired.

Fig. 7 illustrates the role of the decryption device of Fig. 2 in decrypting an item of information. As such, Fig. 7 represents the operation of Block 68 in Fig. 6.

As an initial step, the decryption device 14 obtains a key message and the length of the item to be retrieved from the CD-ROM (Block 70). Thereafter, the device determines the decryption key (Block 71) for this item from key rules and key data which are available (e.g., stored) locally. Preferably, each separate item of information has a unique decryption key. The method of determining the key will be described in detail hereinafter in connection with Fig. 8.

The DES module 42 of the decryption device processes only eight bytes of data at a time. Accordingly, the decryption device enters a "loop" wherein the DES module repeatedly produces eight bytes of data until the total length of the bitstream is equal to or greater than the length of the item to be retrieved.

Initially, a key and an input vector are supplied to the DES and an eight byte output is produced (Block 72). Thereafter, the DES output is combined with the key in a

binary exclusive-OR operation to produce a new key (Block 73). This key is then placed in the key register of the DES module (Block 74) and the process is repeated until a bitstream of sufficient length is generated (Block 75). Finally, this bitstream is transmitted to the host computer (Block 68).

Fig. 8 illustrates how the decryption key is determined from the key rules and the key data which are available locally for each separate item of information stored on the CD-ROM. In order to determine the key, it is necessary to obtain both the key rules and the key data for the specific item of information, and then to apply the rules to this data. Examples of both rules and data are given below.

The key rules and the key data are preferably obtained from one or more of the following five sources:

(1) Non-volatile storage of a "system message" within the decryption controller (flash memory);

(2) A "communication message" received from either the host computer, via the SCSI bus or RS232C interface, or the central billing facility via the telephone modem;

(3) A "media message" contained on the CD-ROM header which is generic to all the files stored thereon (for example, the volume number of the CD-ROM);

(4) A "file message" constructed from information on the file directory associated with the specific item of information (IP) to be decrypted (for example, the identity,

length, location and date of the respective file) and/or the header portion of the IP itself; and

(5) A "current status message" obtained from some element of the decryption controller (for example, the real time clock) or the host computer.

Referring to Fig. 8, it is seen that a "key message" -- that is, the key rules and key data for generating a key -- is obtained by retrieving a stored system message (Block 80), by retrieving a stored communication message (Block 81), by reading the media message from the CD-ROM (Block 82), by reading the file directory and header of the selected IP from the CD-ROM (Block 83), and by obtaining the current status of the decryption controller (Block 84). With this information, all of which is available locally at the user site, the key rules and key data are selected (Block 85). Thereafter, the key data is applied to the key rules (Block 86) to produce the decryption key.

By way of example and not limitation, the following key rules are suggested:

(1) Add the CD-ROM volume number from the media message to the length of the IP from the file message.

(2) Add the date from the media message to the date from the file message.

(3) Add the most recent communication message (initial vector) to the file location in the file message.

(4) Subtract the date found in the file message (date of creation of the IP) from the current status (present date). If the result is positive and less than one year, proceed to decrypt. If the result is negative or more than one year, do not generate a key (do not generate a bitstream).

Other combinations of key rules and key data will readily occur to those skilled in the art.

There has thus been shown and described a novel system for retrieving secure information from a mass storage medium which fulfills all the objects and advantages sought therefor. Many changes, modifications, variations and other uses and applications of the subject invention will, however, become apparent to those skilled in the art after considering this specification and the accompanying drawings which disclose the preferred embodiment thereof. All such changes, modifications, variations and other uses and applications which do not depart from the spirit and scope of the invention are deemed to be covered by the invention, which is to be limited only by the claims which follow.

C L A I M S

What is claimed is:

1. Apparatus for retrieving information from mass storage media, wherein at least some of said information is in the form of information packets which are stored on said media in encrypted form and which may be decrypted using a decryption algorithm, said apparatus comprising in combination:

(a) a storage medium for storing information including said encrypted information packets;

(b) a host computer for selecting information to be retrieved from said storage medium and issuing commands for reading said selected information;

(c) a storage medium reader connected to said host computer for reading said selected information from said storage medium and transmitting the same to said host computer in response to said reading commands, at least some of said selected information being said encrypted information packets; and

(d) a decryption device connected to said host computer for producing, for each selected encrypted information packet, an associated decryption bitstream and transmitting the same to said host computer for decrypting said selected encrypted information packet;

wherein the host computer is operative to receive each said selected encrypted information packet from said storage

medium reader and said associated decryption bitstream from said decryption device and to execute a binary operation between said selected encrypted information packet and said associated decryption bitstream to produce said selected information packet in decrypted form.

2. The apparatus defined in claim 1, wherein said decryption bitstream is a cypher feedback bitstream and said binary operation is exclusive-OR.

3. The apparatus defined in claim 1, wherein at least one decryption algorithm is associated with said storage medium for decryption of said encrypted information packets, wherein said decryption algorithm is defined, at least in part, by data stored on said storage medium, and wherein said decryption device is connected to said storage medium reader to receive said data and is operative to generate said decryption bitstream from said data.

4. The apparatus defined in claim 3, wherein said decryption algorithm is defined by rules and by data applied to said rules, wherein a decryption message comprising at least one of said rules and said data is stored on said storage medium, and wherein said decryption device is operative to receive said message and to generate said decryption bitstream from said message.

5. The apparatus defined in claim 4, wherein said information stored on said storage medium is divided into segments; wherein each segment has associated therewith a different and unique decryption message.

6. The apparatus defined in claim 5, wherein said storage medium has stored thereon a plurality of separate, content-defined files of information and wherein said segments of information are said files of information.

7. The apparatus defined in claim 6, wherein said storage medium is a CD-ROM having a plurality of storage blocks and wherein said files of information are the information stored in said separate storage blocks on said CD-ROM.

8. The apparatus defined in claim 6, wherein said files of information are said encrypted information packets.

9. The apparatus defined in claim 8, wherein said storage medium has stored thereon a file directory containing the identity, length, location and date of each file, and wherein the decryption message for each file is defined at least in part, by information contained in said file directory.

10. The apparatus defined in claim 9, wherein said decryption message for a particular file is defined by data selected from the group consisting of the identity, length, location and date of the respective file contained in said file directory.

11. The apparatus defined in claim 8, wherein said storage medium has stored thereon a media message containing information unique to the storage medium, and wherein the decryption message for each file is defined, at least in part, by information contained in said media message.

12. The apparatus defined in claim 8, further comprising a real time clock for providing the current date and time, and wherein said decryption message is defined, at least in part, by said current date and time.

13. The apparatus defined in claim 8, further comprising an input device for providing a communication message, and wherein said decryption message is defined, at least in part, by said communication message.

14. The apparatus defined in claim 5, wherein said decryption message for each segment is defined, at least in part, by data stored in the respective segment on said storage medium.

15. The apparatus defined in claim 1, further comprising a telephone modem for receiving telephone messages via the telephone network from a remote source and disabling means, coupled to said telephone modem, for disabling said decryption device from producing a decryption bitstream at a prescribed moment of time unless reset by the receipt of a telephone message.

16. The apparatus defined in claim 15, wherein said disabling means is operative to disable said decryption device upon expiration of a given length of time after receipt of a prior telephone message.

17. The apparatus defined in claim 16, wherein said given length of time is included in said prior telephone message.

18. The apparatus defined in claim 1, wherein said decryption device has an enclosure to inhibit access thereto by unauthorized personnel and disabling means for disabling said decryption device from producing a decrypting bitstream when said enclosure is removed.

19. The apparatus defined in claim 18, wherein said disabling means includes a light-sensitive programmable element for storing a program, said programmable element

being operative to erase the stored program upon the receipt of light.

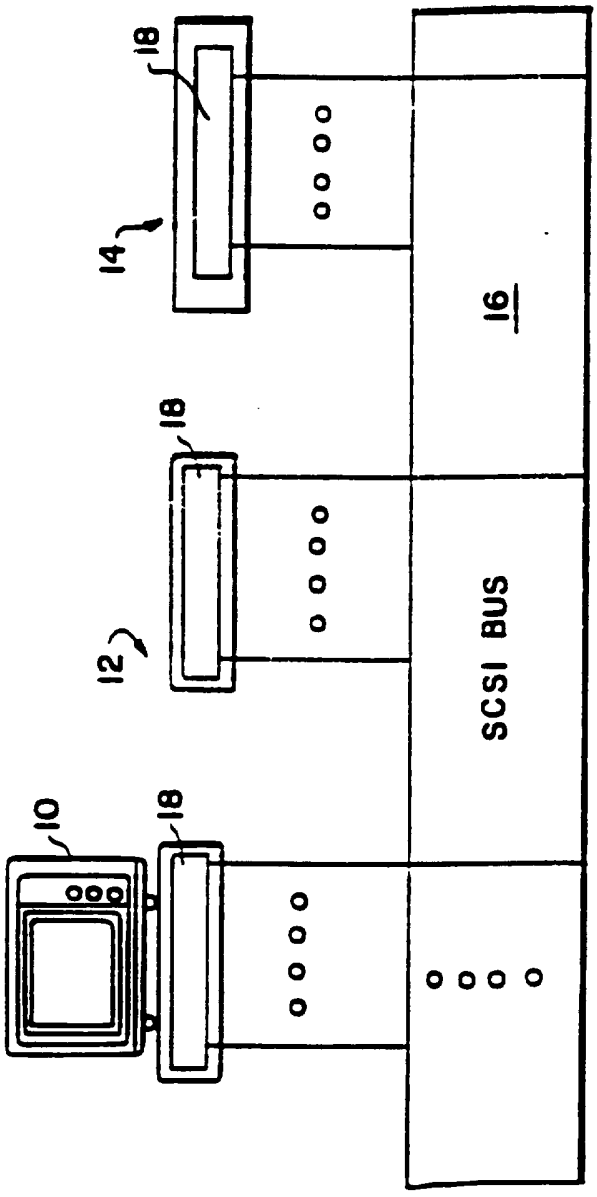


FIG.1

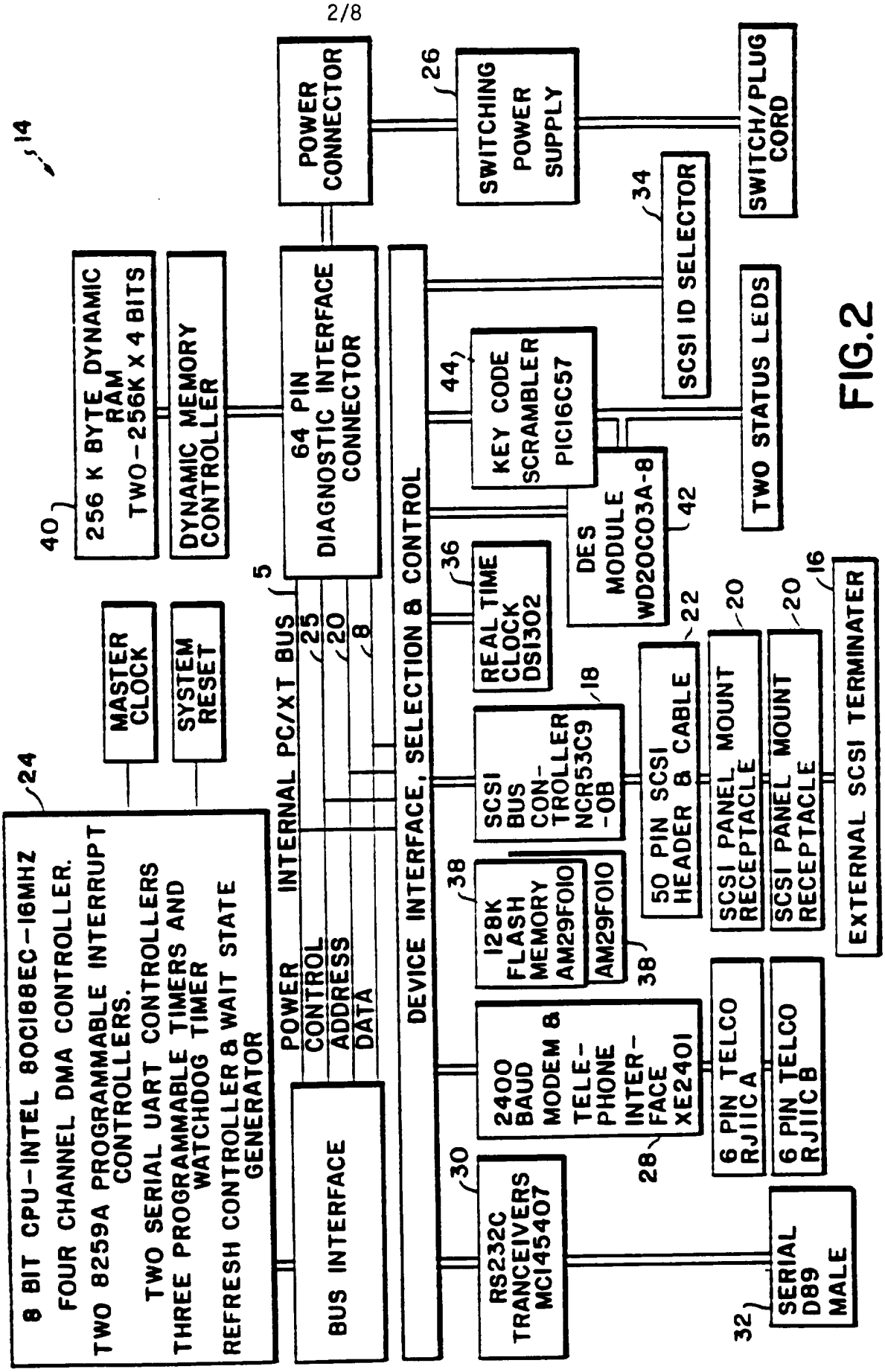

14
8 BIT CPU-INTEL 80C188EC-16MHZ
FOUR CHANNEL DMA CONTROLLER.
TWO 8259A PROGRAMMABLE INTERRUPT CONTROLLERS.
TWO SERIAL UART CONTROLLERS
THREE PROGRAMMABLE TIMERS AND WATCHDOG TIMER
REFRESH CONTROLLER & WAIT STATE GENERATOR
24
MASTER CLOCK
SYSTEM RESET
40
256 K BYTE DYNAMIC RAM TWO-256K X 4 BITS
DYNAMIC MEMORY CONTROLLER
POWER CONNECTOR
26
SWITCHING POWER SUPPLY
SWITCH/PLUG CORD
34
SCSI ID SELECTOR
TWO STATUS LEDS
64 PIN DIAGNOSTIC INTERFACE CONNECTOR
5
44
KEY CODE SCRAMBLER PIC16C57
DES MODULE WD2OC03A-8
42
22
POWER
CONTROL
ADDRESS
DATA
25
20
8
INTERNAL PC/XT BUS
DEVICE INTERFACE, SELECTION & CONTROL
36
REAL TIME CLOCK DS1302
SCSI BUS CON-TROLLER NCR53C9-0B
18
50 PIN SCSI HEADER & CABLE
20
SCSI PANEL MOUNT RECEPTACLE
20
SCSI PANEL MOUNT RECEPTACLE
16
EXTERNAL SCSI TERMINATER
38
128K FLASH MEMORY AM29F010
AM29F010
38
BUS INTERFACE
30
2400 BAUD MODEM & TELE-PHONE INTER-FACE XE2401
28
6 PIN TELCO RJ11C A
6 PIN TELCO RJ11C B
RS232C TRANCEIVERS MC145407
32
SERIAL D89 MALE

FIG.2

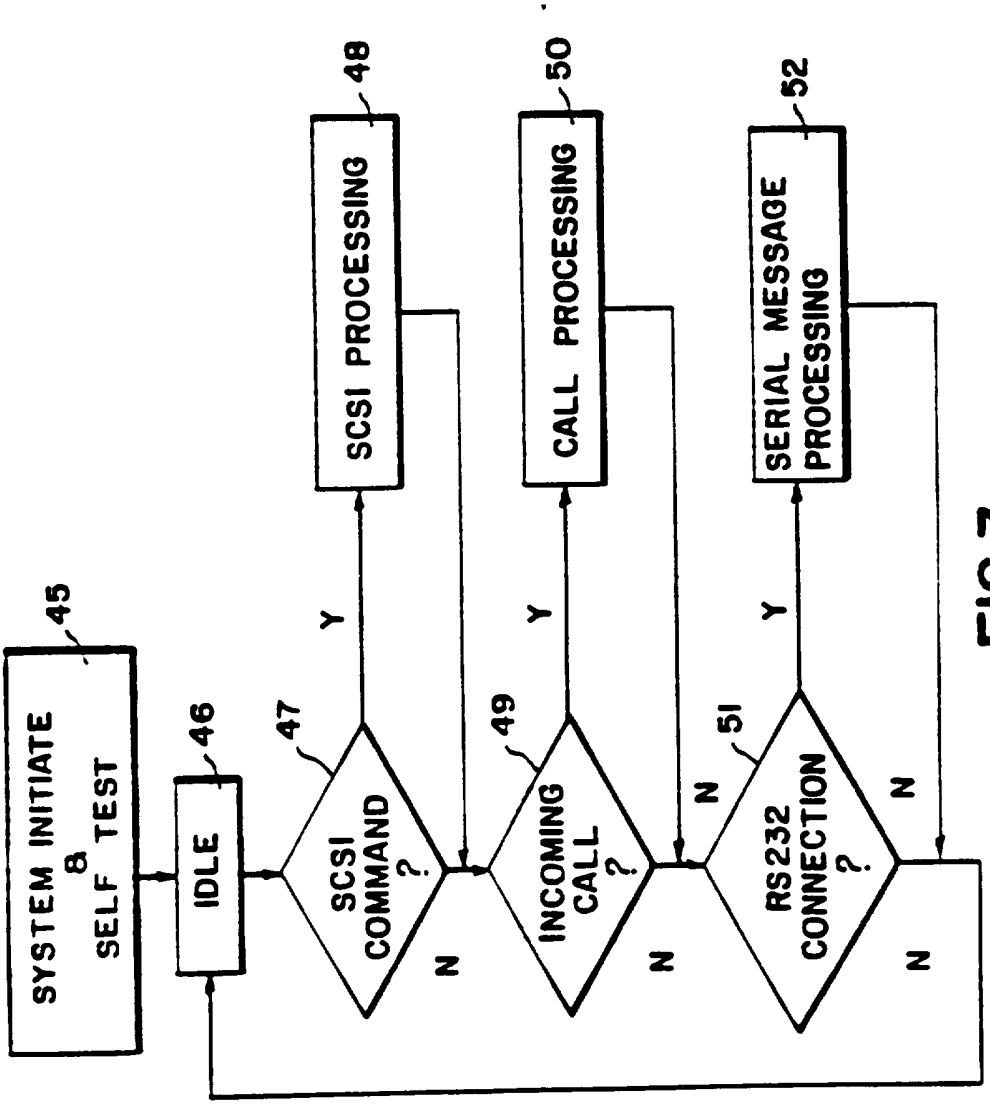

SYSTEM INITIATE & SELF TEST
45
IDLE
46
SCSI COMMAND ?
47
Y
N
SCSI PROCESSING
48
INCOMING CALL ?
49
Y
N
CALL PROCESSING
50
RS232 CONNECTION ?
51
Y
N
SERIAL MESSAGE PROCESSING
52

FIG.3

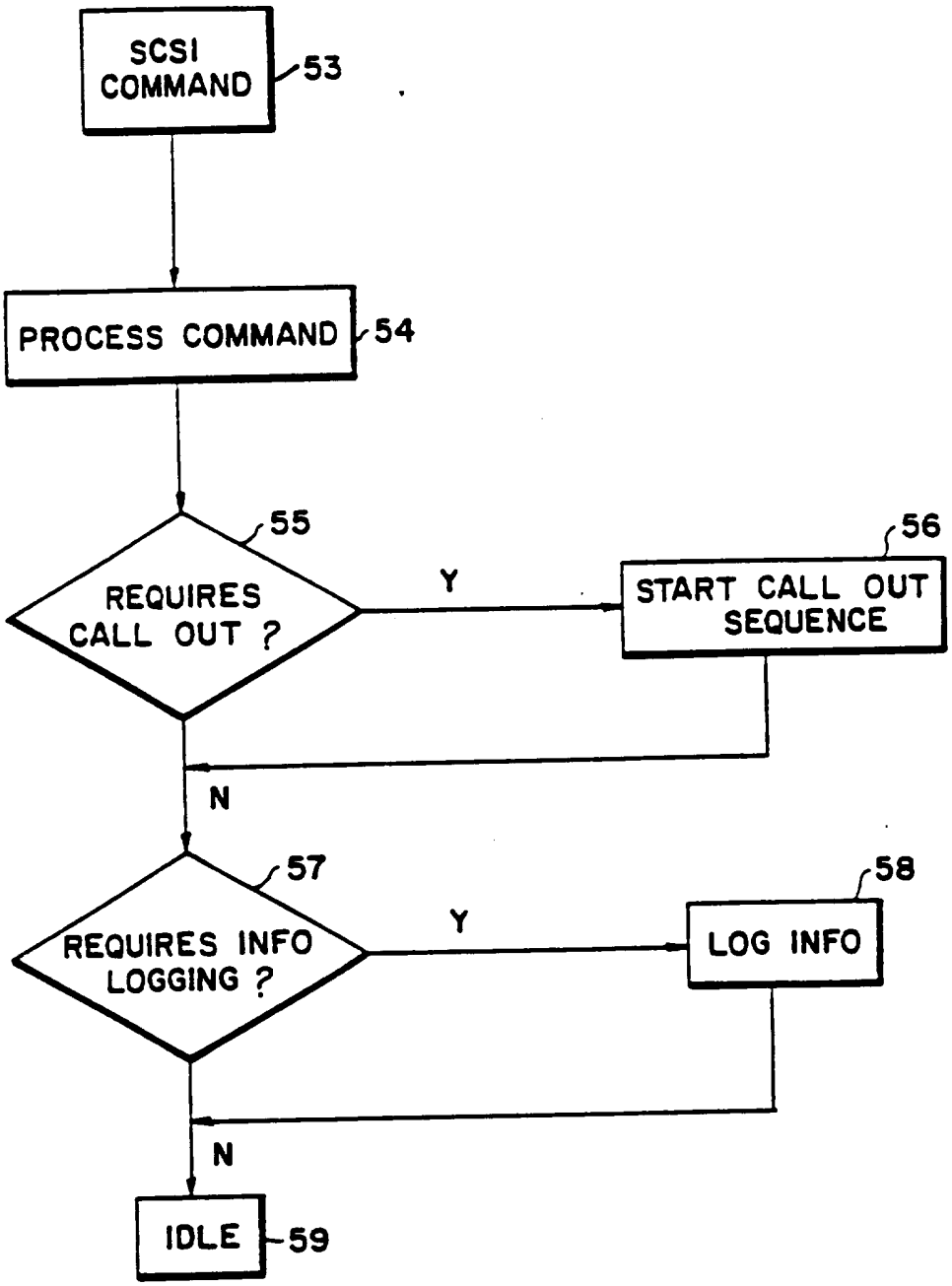

SCSI COMMAND
53
PROCESS COMMAND
54
55
REQUIRES CALL OUT ?
Y
56
START CALL OUT SEQUENCE
N
57
REQUIRES INFO LOGGING ?
Y
58
LOG INFO
N
IDLE
59

FIG.4

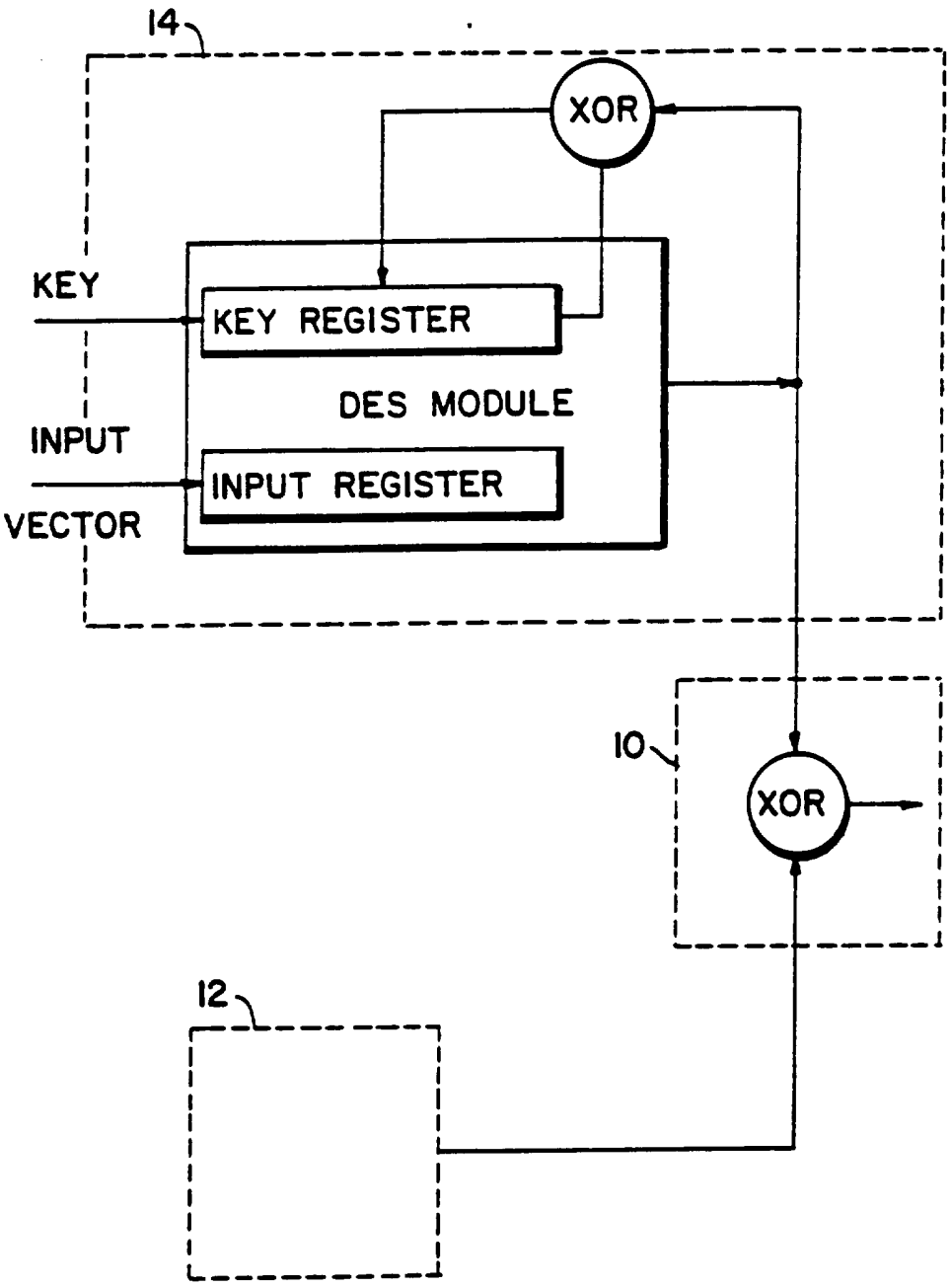

14
XOR
KEY
KEY REGISTER
DES MODULE
INPUT
INPUT REGISTER
VECTOR
10
XOR
12

FIG.5

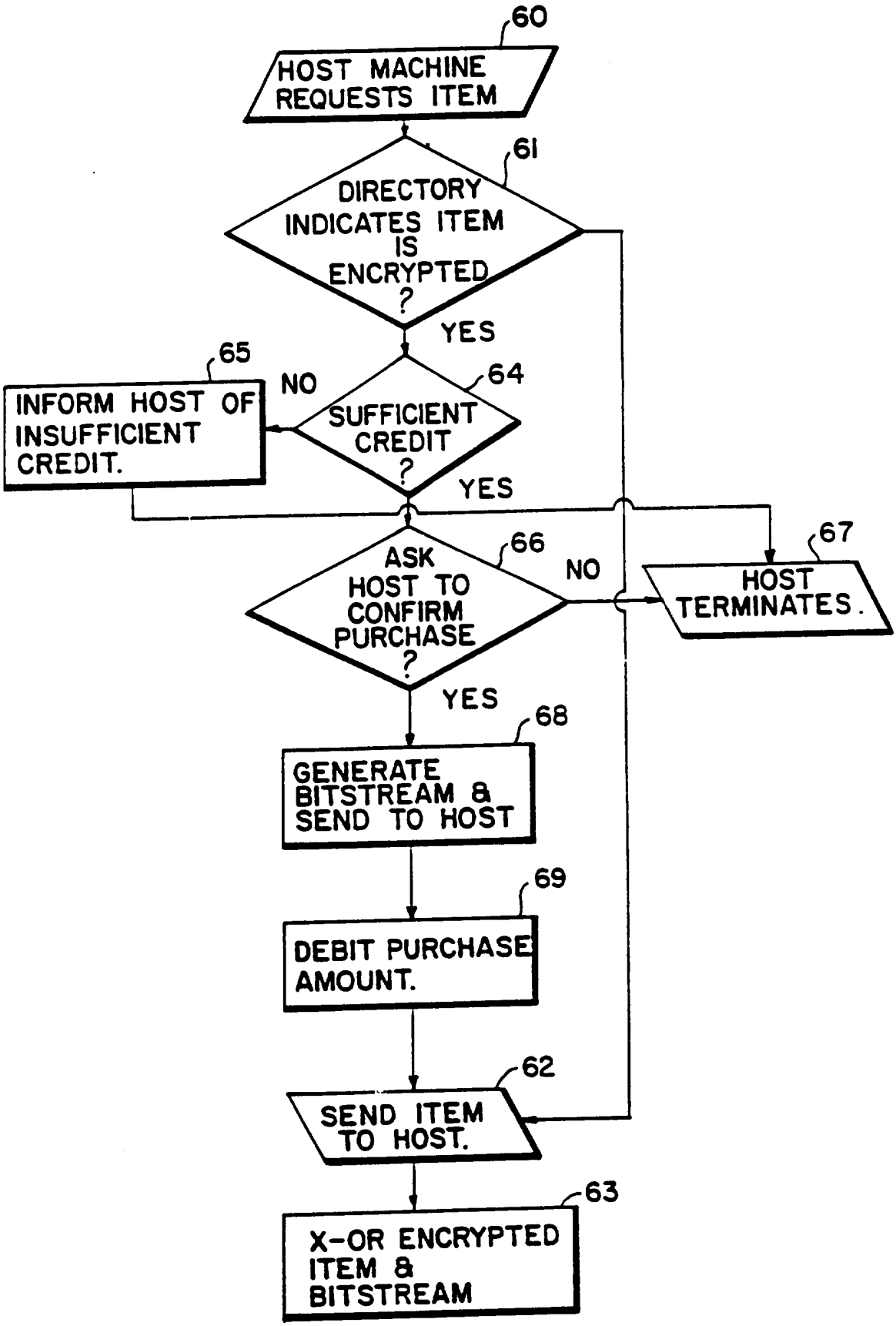

60
HOST MACHINE REQUESTS ITEM
61
DIRECTORY INDICATES ITEM IS ENCRYPTED ?
YES
NO
64
SUFFICIENT CREDIT ?
65
INFORM HOST OF INSUFFICIENT CREDIT.
YES
66
ASK HOST TO CONFIRM PURCHASE ?
NO
67
HOST TERMINATES.
YES
68
GENERATE BITSTREAM & SEND TO HOST
69
DEBIT PURCHASE AMOUNT.
62
SEND ITEM TO HOST.
63
X-OR ENCRYPTED ITEM & BITSTREAM

FIG.6

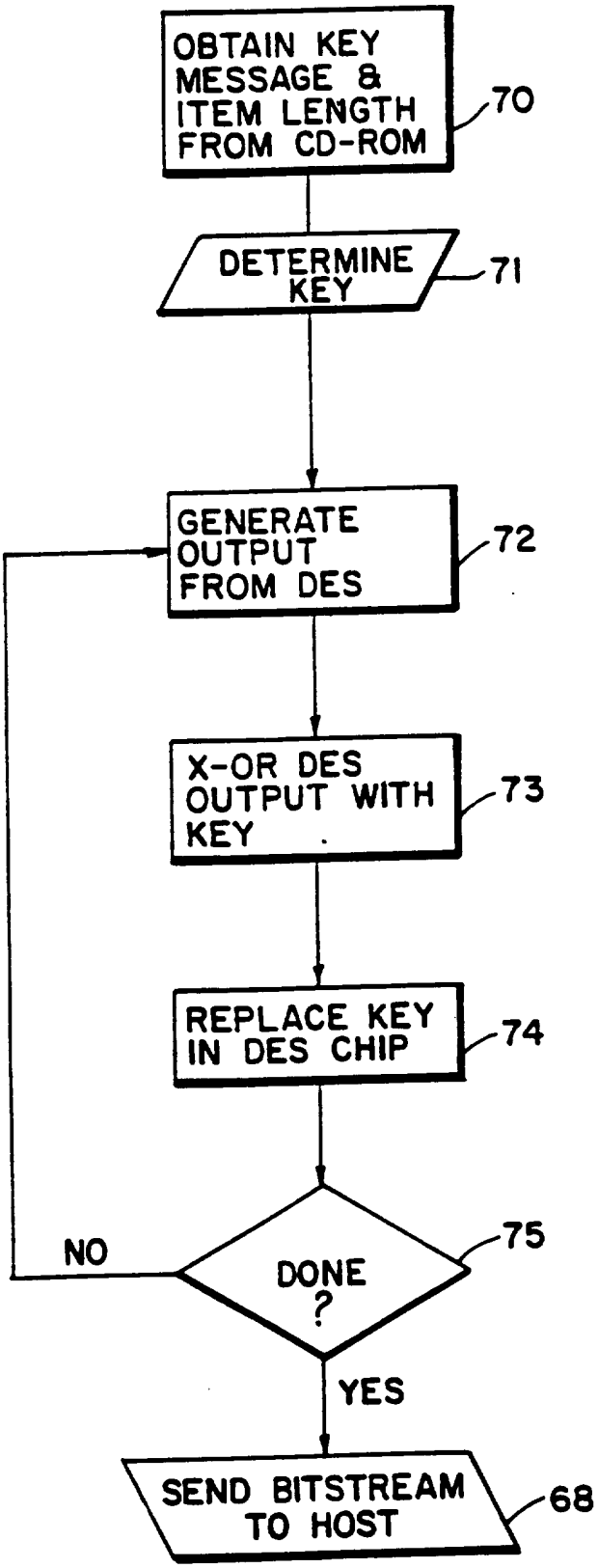

OBTAIN KEY MESSAGE & ITEM LENGTH FROM CD-ROM
70
DETERMINE KEY
71
GENERATE OUTPUT FROM DES
72
X-OR DES OUTPUT WITH KEY
73
REPLACE KEY IN DES CHIP
74
DONE ?
75
NO
YES
SEND BITSTREAM TO HOST
68

FIG.7

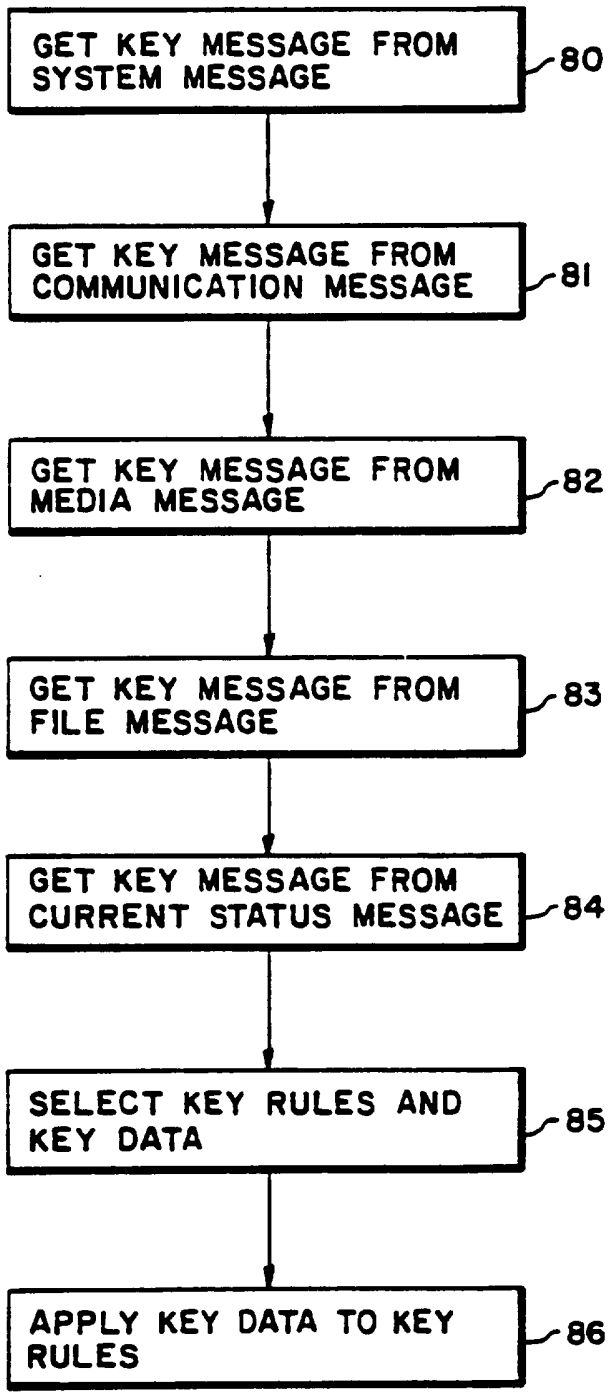

GET KEY MESSAGE FROM SYSTEM MESSAGE
80
GET KEY MESSAGE FROM COMMUNICATION MESSAGE
81
GET KEY MESSAGE FROM MEDIA MESSAGE
82
GET KEY MESSAGE FROM FILE MESSAGE
83
GET KEY MESSAGE FROM CURRENT STATUS MESSAGE
84
SELECT KEY RULES AND KEY DATA
85
APPLY KEY DATA TO KEY RULES
86

FIG.8

INTERNATIONAL SEARCH REPORT

Inter...onal Application No
PCT/US 95/01738

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00 G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO,A,88 02960 (PERSONAL LIBRARY SOFTWARE INC) 21 April 1988 see the whole document ---	1-17
A	WO,A,90 02382 (INDATA CORP) 8 March 1990 see page 30, paragraph 3 - page 43, paragraph 2; figures 5-13 -----	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"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 when the document is taken alone

"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

1

Date of the actual completion of the international search	Date of mailing of the international search report
27 June 1995	04.07.95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Moens, R

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter. ..onal Application No
PCT/US 95/01738

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A-8802960	21-04-88	EP-A-	0329681	30-08-89
		US-A-	4977594	11-12-90
		US-A-	5410598	25-04-95
		US-A-	5050213	17-09-91
		US-A-	4827508	02-05-89
		US-A-	5272750	21-12-93
WO-A-9002382	08-03-90	AU-A-	4188289	23-03-90
		EP-A-	0472521	04-03-92
		US-A-	5247575	21-09-93