(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: 0 111 381
B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification: 02.11.88

(51) Int. Cl.^{4}: G 07 F 7/10, H 04 L 9/00

(21) Application number: 83304907.5

(22) Date of filing: 25.08.83

(54) Improvements in and relating to autoteller systems.

(30) Priority: 03.12.82 GB 8234568

(43) Date of publication of application:
20.06.84 Bulletin 84/25

(45) Publication of the grant of the patent:
02.11.88 Bulletin 88/44

(84) Designated Contracting States:
BE CH DE FR LI NL SE

(56) References cited:
EP-A-0 002 388
WO-A-81/02655
DE-A-3 023 427
US-A-3 956 615

Federal Information, Processing Standards
Publication No. 46, "Data Encryption Standard"

(73) Proprietor: UNISYS CORPORATION
Burroughs Place
Detroit Michigan 48232 (US)

(72) Inventor: Fernandes, Afonso Manuel Chaves De Almeida
14 St. Paul Road
Richmond Surrey (GB)
Inventor: Abraham, Philip Crum Thomson
26 Hillcrest Road
Biggin Hill Kent (GB)

(74) Representative: Kirby, Harold Douglas Benson et al
G.F. Redfern & Company Marlborough Lodge 14
Farncombe Road
Worthing West Sussex BN11 2BT (GB)

Courier Press, Leamington Spa, England.

Description

The present invention relates to autoteller systems for the automatic dispensation of money to a user upon presentation of a valid card and receipt of correct information from the user validating his right to use. It particularly relates to autoteller systems which employ the technique of encryption for protection of information on the card and further relates to autoteller systems where a remote host contoller communicates with the system.

It is known to employ a card for presentation to an autoteller wherefrom the autoteller reads data for matching against predetermined characteristics to validate the card and for comparison with further data furnished by the user validating the users right to employ the card. It is important to avoid persons of fraudulent intent being able to read the data on a card and understand its meaning. To this end it is known to employ cards having magnetic stripes whereon the data is recorded and to encrypt or "shuffle" the data bits recorded so that even if read no pattern can be perceived.

In prior art autoteller systems the autoteller was substantially an independent unit. Nonetheless, a surprisingly large number of persons had access to the system, including bank staff and system maintainence personnel. Any of these persons was potentially able to discover the manner of encryption and employ that knowledge themselves or through others simply by examination of the system. Thus, although the autoteller was protected against the public, it was not protected against employees of fraudulent intent.

Later prior art autoteller systems included an ability to communicate with a remote host system. The remote host might have been a computer installation some miles away coupled to the autoteller by a serial data telephone link. The host would keep records of unacceptable cards and so on and instruct the autoteller system in what action to take under different circumstances. The same host system might be in supervisory control of many autoteller systems. The existence of the telephone line data link lays the system open to public interference and to access by many more employees, since the amount of equipment is multiplied and the line and the external host system are open to inspection by persons not in the vicinity of the autoteller per se. Further, the ability of the remote host to command the autoteller system creates the possibilty of new methods of fraud where an interloper sends his own commands to the autoteller system instructing it to perform actions it would otherwise not perform under the circumstances it finds.

It is therefore desirable to provide an autoteller system where the manner of encryption of data on a card cannot be discovered by examination of the system itself. It is yet further desirable to provide an autoteller system where communication is possible with a remote host system without the nature of the communication being open to interpretation by persons monitoring the signals passing therebetween.

European Patent Application 0,002,388 (filed 5th December 1978) discloses a system wherein a master key is loaded into a terminal by manual means or under terminal control via an interface adaptor. Both types of operation require that a person or persons know the master key or that the master key is sent via a communication network. Both such systems are risky in that the integrity of the master key can be corrupted and accordingly the present invention consists in a system including an autoteller for dispensing money on presentation of a valid card; said autoteller including a card reader for reading data from a card; a data link for communicating with a remote processor; an encryption module wherein an input word is encrypted in response to a current key word in one out of a plurality of selectable manners of encryption to provide an output word; and a master key word; said system being operative to receive a sub key word from said remote processor, to employ said sub-key word as said input word and said master key word as said current key word and to store said output word as a session key word and thereafter to use said session key word as said current key word; said system being characterised by said encryption module comprising a control processor; by said system comprising a selectably attachable and removeable master key loader containing a non-volatile memory holding a set of instructions for said control processor to perform an algorithm to generate a master key word; and by said system comprising a port on said encryption module for receiving said master key loader to enable said control processor to read instructions therefrom; where said control processor is operative to detect whether or not a master key word is stored in said autoteller and, if no master key word is stored, is operative to perform said algorithm to generate said master key word.

P.C.T. Application W081-02655 discloses a system wherein each message is accompanied by a transmitted key. As messages are passed from node to node in a possible network they are decyphered and then recyphered and sent off again with a new key. This system is also an open system in that the key itself is transmitted from the terminal unit towards the central host computer. It would be far better that, should a key be selected, the identity of that key should be kept secret and accordingly, the present invention is further characterized by comprising a system wherein said sub-key word is one of a plural succession of sub-key words received in succession from said remote controller, wherein said encryption module is operative to generate and store a session key from each of said sub-keys and to allocate a serial number to each session key, the allocated serial number bearing no relationship to the actual value of the associated session key; and wherein the session key actually in use can be changed from time to time by said remote controller calling out a particular selected sub-key by its serial number.

Federal Information Processing Standards Publication No. 46 (data encryption standard) describes various means whereby data can be encrypted. The American National Standard Institute Publication ANSIX3.92-1981 "Data Encryption Algorithm" describes various ways in which encrypted data may be coded and decoded. Each of these documents discloses a process best handled by a controlling encryption processor. This processor will generally be required to interface with another control processor running a terminal or autoteller. It is desirable that both the encryption processor and the controlling processor should be capable of operating using the same software or program so that simplicity and economy of operation and development is achieved. Accordingly the present invention further provides a system wherein said encryption module also comprises an encryption processor operative to perform and control said encryption and operative to receive data and instructions from said control processor and to pass data and status indication back to said control processor, said encryption module including a communication register operative to control communication between said control processor and said encryption processor; said communication register comprising a first interface memory for receiving data from said control processor and for providing data to said encryption processor, and a second interface memory for receiving data from said encryption processor and for providing data to said control processor; said encryption processor deferring access to deposit or recover data in said communication register if said control processor already has access to said communication register; and said control processor deferring access to deposit or receive data in said communication register if said encryption processor already has access to said communication register.

In order further to enhance the commonality of operation between the control processor and the encryption processor the present invention also provides a first address decoder provides activating output whenever and internal adjust bus in the control processor is between first and second address limits and a second address decoder provides activating output whenever the address on the encryption address bus lies between third and fourth predetermined limits, the first and second interface memories ignoring the output from the second address decoder if the first address decoder provides its output. As a further enhancement to the commonality of action between the two processors, each processor in the present invention is designed to deposit a block of words in its appropriate outgoing interface memory and to record therewith indication of the length of the block of words. Each processor is also designed to read the indication of the length of the block of words in that interface memory. from which it derives data and transfer to that memory exactly that number of words.

In a preferred embodiment an autoteller system comprises an internal processor in which case the internal processor preferably provides an internal address bus and an internal data bus for use within the auto teller. The autoteller preferably comprises a serial data interface for providing data communications with a remote host system. The serial data interface preferably communicates with the internal processor via the internal address bus and the internal data bus. The autoteller preferably comprises a card reader preferably communicating with the internal processor via the internal address bus and the internal data bus and operable to read data from a card and communicate that data to the internal processor. The autoteller preferably comprises a keyboard and display coupled to the internal processor via the internal address bus and the internal data bus and operable in the one case to communicate data keyed in by the user to the internal processor and in the other case to provide data to the user from the internal processor. The autoteller preferably comprises a banknote dispenser preferably commanded via the internal data bus and the internal address bus to dispense money to the user. The autoteller preferably comprises an encryption module communicating with the internal processor via the internal address bus and the internal data bus preferably operable to receive data for encryption from the internal processor and to provide encrypted data to the internal processor. The encryption module is preferably selectably operable to decrypt data.

The autoteller preferably comprises a secure case closed behind a secure door. Within the secure case is preferably provided a secure enclosure preferably closed by secure screws unable to be undone without special tools. The enclosure preferably houses the internal processor, the encryption module and the interface circuits to the other elements therein.

The autoteller preferably comprises a key connector outwith the secure enclosure but within the secure case for providing coupling between the encryption module and a key loader.

The encryption module preferably comprises a printed-circuit board. The printed circuit board preferably comprises a first edge connector for plugging into the common backplane of the internal processor and the interface circuits. The printed circuit board preferably comprises a second edge connector for providing connection to a multi-way cable for connecting the encryption module to the key connector.

The key loader preferably comprises a multiway plug for coupling to the key connector. The key loader is preferably housed within a case housing four indicator light-emitting diodes. The key loader preferably comprises a Read-Only-Memory. The Read-Only-Memory is preferably ultra-violet erasable, in which case the key loader preferably comprises an aperture in the case for irradiating the Read-Only Memory and a light-tight grommet affixable therein for the protection of the Read-Only-Memory.

The Read-Only-Memory is preferably coupled, via the key connector, to receive an address bus and a data bus. The encryption module preferably provides a chip-select signal to the Read-Only-Memory in response whereto the Read-Only-Memory preferably provides the data on the data bus in the location addressed by the address bus. The key loader preferably provides a connection to the Read-Only-Memory for programming the Read-Only-Memory when the signal thereon exceeds a predetermined value, under which condition the Read-Only-Memory stores the data on the data bus in the location addressed by the address bus, and which program-inducing signal is preferably not provided by said encryption module.

The encryption module preferably comprises an encryption control processor. The encryption control processor preferably provides an encryption address bus and an encryption data bus for use in the encryption module. The encryption address bus is preferably the address bus supplied to the Read-Only-Memory and the encryption data bus is preferably the data bus provided to the Read-Only-Memory.

The encryption module preferably comprises a communications register for providing communication between the internal data bus of the autoteller and the encryption data bus of the encryption control processor.

The encryption module preferably a resident Read-Only-Memory (ROM) wherein the systems program of the internal processor is stored. The internal processor preferably comprises a volatile Random-Access Memory (RAM) for temporary storage of data during the operation of the encryption module and whose contents are lost if the power is removed from the autoteller. The encryption module preferably comprises a secure random-access memory whose contents cannot be recalled by the remote host and which is sustained in the event of the loss of power to the autoteller, the autoteller preferably comprising a battery backup power supply for supplying power only to the secure sustained RAM in the event of power loss. The backup power supply is preferably situated on the encryption module. The backup power supply is preferably disconnected from the secure, sustained RAM in the event of the printed circuit board housing the encryption module being disconnected from the common back plane of the internal processor of the autoteller, in which case the secure, sustained memory preferably loses its contents. The backup power supply preferably comprises a link on the first edge connector which is broken if the printed circuit board is removed therefrom. The secure, sustained RAM is preferably operable to store encryption key words. The encryption key words are preferably stored in secret locations therein scattered among other data to create uncertainty as to which words stored in the secure, sustained RAM might be encryption key words.

The encryption module preferably comprises an encryption block. The encryption block is preferably operable receive addresses and data respectively from the encryption address bus and the encryption data bus and is preferably operable to provide selectably encrypted or decrypted data back to the encryption data bus.

The encryption module preferably comprises a flag register addressable via the encryption address bus and operable to receive first and second flag characters indicative of the encryption module having received the master key word and a session key word. The flag register preferably comprises comparison means for detecting if the predetermined flag characters have been deposited therein and operable to communicate the fact to a monitor. The monitor preferably monitors the voltage supplied by the battery in the backup power supply and detects if it is low. The monitor preferably provides activating signals to a light-emitting diode drive circuit for driving the light-emitting diodes in the key loader. The light emitting diodes in the key loader preferably provide indication when the keys have been correctly loaded and when the battery is of low voltage.

The encryption block preferably comprises a key register comprising a plurality of eight-bit parallel in parallel out registers individually addressable from an address decoder to accept the data on the encryption data bus when addressed by the encryption control processor via the encryption address bus. The encryption key register is preferably sixty-four bits long. The encryption block preferably comprises an output register preferably comprising a plurality of 8-bit parallel-in-parallel-out registers individually in receipt of data from an encryption circuit itself in receipt of the contents of the key register each operable when individually addressed by the encryption control processor via the address decoder operating on the contents of the encryption address bus to provide their input word onto the encryption data bus. There are preferably eight eight-bit registers in the output register. The encryption block preferably comprises an input register. The input register preferably comprises a direct register for receiving characters for encryption. The direct register preferably comprises a plurality of plural-bit parallel-in-parallel-out registers individually addressable via the address decoder operating on the encryption address bus to accept data from the encryption data bus and provide it as output. The input register preferably comprises a cyphertext register operable in the same manner as the direct register. The encryption control processor preferably is operable to load the cyphertext register with the result of the previous encryption as recovered from the output register. The output of the cyphertext register is preferably provided as the first input to an exclusive-or array in receipt of the output of the direct register as first input and providing output being the parallel-bit exclusive or function of corresponding bits in the two outputs. The output of the exclusive-or array is preferably coupled as the first input to a diplexer and the output of the direct register is preferably provided as the second input to the diplexer which is selectably operable to provide the output of the direct register as output for coupling as input to the encryption circuit if direct operation is required and to provide the output of the exclusive-or array as the input to the encryption circuit if cyphertext chaining of data to and from the remote host system is required.

The communication register preferably comprises a pair of buffer registers each addressable by the internal processor and by the encryption control processor, a first buffer being for the transfer of data from the internal processor for use by the encryption control processor and a second being for the transfer of data from the encryption control processor for use by the internal processor.

In use, the encryption module preferably detects the power-on condition. The encryption control processor then preferably looks to see if the key loader is present. If the key loader is present the encryption module preferably uses the instructions in the keyloader directly to calculate the master key. The algorithm preferably allows access to the encryption block. The calculated master key is preferably stored in a temporary location where its parity is checked. The Master key is then preferably stored in a secure location in the sustained RAM and the contents of the temporary location deleted. The encryption module preferably receives a session sub-key from the remote host via the data link. The session sub-key is preferably encrypted using the master key as the key word to the encryption circuit to create a session key. The session key is preferably stored in the sustained RAM in a secret location. The sustained RAM preferably contains many pieces of data so that it is impossible to discover by inspection which of the pieces of data are keys.

The encryption module is preferably operable to receive a succession of communication sub-keys from the remote host system. The communication sub-keys are preferably encrypted using the master key as the key word to the encryption circuit to create a corresponding succession of communication keys. The communication keys are preferably stored in the secure RAM in the same manner as the master and session keys.

The remote host is preferably in a position to indicate to the encryption module which one of the communication keys it wishes to use. Thereafter the encryption module is preferably operable to use the indicated communication key to encrypt data. The encryption module is preferably selectably operable to operate in the cyphertext manner when instructed to do so via the remote host. The cyphertext manner preferably consists in the encryption of current data after it has undergone an exclusive-or combination with the result of the previous encryption.

The invention is further described, by way of an example, by the following description taken in conjunction with the appended drawings, in which:

Figure 1 is a schematic representation of the various elements present in and associated with the autoteller system.

Figure 2 shows details of the mechanical construction of the autoteller.

Figure 3 shows the mechanical layout of the ercryption module of figure 1.

Figure 4 shows mechanical detail of the key loader.

Figure 5 shows a schematic circuit diagram of the key loader.

Figure 6 shows a schematic circuit diagram of the encryption module printed circuit board of figure 3.

Figure 7 shows a schematic circuit diagram of the communication register of figure 6.

Figure 8 shows a schematic circuit diagram of the encryption block of figure 6.

Figure 9 shows a schematic circuit diagram of the input register of figure 8.

Figure 1 shows a schematic circuit diagram generally indicating the elements in the autoteller of the preferred embodiment and the functional relationships therebetween.

The autoteller 10 comprises an autoteller internal processor 12 for controlling the immediate actions of the autoteller 10. The internal processor 12 provides an internal data bus 14 for providing data to and receiving data from the various other elements in the autoteller 10. The internal processor 12 also provides an internal address bus 16 whereby each of the various elements in the autoteller 10 can be addressed for data deposition or data retrieval therefrom. The autoteller internal controller 12 is, for preference, a minicomputer. However, it will be apparent that the function of the internal controller 12 can be accomplished using any other type of state-sequence machine ranging from the programmable to the hard-wired.

The autoteller 10 comprises a serial data interface 18 for providing data communication via a serial data link 20 with a remote host system 22. The interface 18 converts parallel data received from the internal data bus 14 when addressed by the internal address bus 16 into a serial stream of binary digits. The serial data link 20 is, for preference, a three-wire system comprising a data wire for receiving the series of binary digits, a clock wire for carrying a clock signal for clocking the series of binary digits, and a ground wire. This is not restrictive, and the serial data link 20 could equally comprise a telephone line and a pair of modems. Equally, any other type of data communication link can be used with the present invention.

The autoteller 10 also comprises a card reader 24. The card reader 24 accepts a card from the autoteller user and, when addressed by the internal processor 12, informs the processor 12 that a card is present. The internal processor 12 then commands the card reader 24 to read data from the card and transfer it via the internal data bus 14 to the internal processor 12.

The autoteller 10 further comprises a keyboard and display 26. The internal processor 12 instructs the display 26 to request the user to type out his personal number on the keyboard 26. If the personal number, received via the data bus 14 by the internal processor 12, does not match up with predetermined information recovered from the card by the card reader 24 according to a predetermined relationship after a predetermined number of attempts at entry of the personal number, the internal processor 12 instructs the card reader 24 to swallow the card and deposit it a bin on the assumption that the would-be user had no right to use the card, being ignorant of the personal number.

The autoteller 10 further comprises a banknote dispenser 28. If the user successfully enters his personal number within the predetermined number of attempts the internal processor 12 instructs the display 26 to ask the user how much money he wishes to withdraw. The user then responds by typing out the amount on the keyboard 26 which information is communicated to the internal processor 12. In response the internal processor 12 then instructs the banknote dispenser 28 to dispense the required number and types of banknotes to the user.

The remote host system 22 can be used to control many more than just one autoteller 10. The remote host 22 maintains records of bad cards and instructs the internal processor 12 to retain any card in the card reader 24 which is suspect. It is to be appreciated that the remote host system 22 can address a plurality of autotellers 10 via the same serial data link 20 and it is preferred that this be so. It is however possible to address each autoteller 10 via its own, unique serial data link 20. The function of the remote host processor 22 is one of supervision and general control. The autoteller 10 communicates its transactions to the remote host system 22 and the remote host 22 communicates operating instructions to the autoteller 10. It is not strictly part of the present invention what those instructions might be and what data is passed between the host system 22 and the autoteller 10, save as hereinafter described in connection with the use and loading of encryption keys. By way of example, the autoteller 10 might inform the host 22 of identification information on the card, bank account number, and time of last use, all derived from the card reader 24. In response the remote host system 22 might instruct the autoteller 10 to withold or not to withold payment, or tell the autoteller 10 the upper limit of payment. Similarly the autoteller 10 may be instructed to retain the card or be informed as to what new information to record on the card using a recording facility on the card reader 24.

The autoteller 10 lastly comprises an encryption module 30. The encryption module 30 is operable to receive blocks of data from the internal processor 12 via the internal data bus 14 when addressed by the internal address bus 16 and to render up blocks of encrypted or decrypted data to the internal processor 12 onto the internal data bus 14 when addressed to do so via the internal address bus 16. The manner of encryption or decryption is selectable in response to the encryption module responding to commands to use a selectable key. In a first mode of operation the internal processor 12 provides data recovered by the card reader 24 from the presented card to the encryption module 30 for selectable encryption or decryption and receives the selectably encrypted or decrypted data back from the encryption module 30, the manner of encryption or decryption being predetermined by the loading of a key, the key being variable from time to time. In a second manner of operation one out of a plurality of communication keys is selected by the remote host system 22 and data provided to the encryption module 30 from the internal processor 12 for selectable encryption or decryption and communication back to the internal processor 12. The data may have been received from the remote host system 22 by the internal processor 12 via the serial data link 20 and the serial data interface 18, or may be a message originated by the internal processor 12 for communication to the remote host system 22 in a similar manner. In a third manner of operation, the encryption module 30 performs a cyphertext operation using a host 22 selectable encryption key whereby received data from the host 22 or data to be sent to the host 22 is divided into blocks and combined in an exclusive-or operation with the result of encryption or decryption of the previous block before itself being encrypted or decrypted.

The term encryption is herein defined as the altering of the order of the binary digits in a plural binary digit data word according to a predetermined pattern. The term decryption is herein defined as the altering back of the order of the binary digits in an encrypted plural binary digit word to their original order. A key is herein defined as the plural binary digit word defining the pattern of encryption or decryption, whereby alteration of the key alters the pattern of encryption or decryption.

It is to be appreciated that decryption is merely a special case of encryption, the pattern causing the decryption of a previously-encrypted message being, in absense of previous encryption, just another encryption pattern. While there is no mathematical distinction therebetween, for the purposes of the present invention and the description thereof encryption and decryption are treated as if they were separate operations.

Figure 2 shows the mechanical construction of the autoteller 10 of figure 1.

The autoteller 10 is housed within a secure steel case 32 closed by a secure steel door 34 which can be locked. Within the secure case 32 is a secure enclosure 36, also made from steel and closed by a steel panel 38 held by special screws 40 which can only be undone using a special tool. The enclosure 36 houses the internal processor 12, the encryption module 30 and interface circuits for the other elements of the autoteller 10. The autoteller 10 comprises a key connector 42 affixed within the secure case 32 but outwith the secure enclosure 36 for loading encryption keys in a manner to be described hereunder. The key connector 42 is therefore accessible to bank personnel whenever the case 32 is opened. The autoteller 10 further comprises a banknote dispenser enclosure 44 shown in phantom outline for housing a safe for money and a dispenser mechanism and a user facia protrusion 46 protruding through the wall of the bank and presenting to the user the keyboard and display 26 and the dispensing end of the banknote dispenser.

Figure 3 shows mechanical details of the construction of the encryption module 30.

The encryption module 30 comprises a printed-circuit board 48 with a first edge connector 50 for connecting the printed circuit board 48 into the common backplane of the internal processor 12 through which all power and communication with the common processor 12 is derived. The encryption module 30 comprises a second edge connector 52 on the edge of the printed circuit board 48 remote from the first edge connector 50. The second edge connector 52 is used to load a secure key into the encryption module 30. A plug 54 mates with the second edge connector 52, coupling it to a multi-way flat cable 56 which in turn couples the second edge connector 52 to the key connector 42 shown in figure 2.

Figure 4 shows mechanical detail of the key loader in conjunction with the key connector 42.

The key loader 58 is a pocketable outboard Read-Only-Memory (ROM) for the encryption module 30. The key loader 58 is housed in a shatterproof resin case 60 at the extreme and flared end of which is provided a key loader connector 62 for mating with the key connector 42 to provide multiple connections to the encryption module 30. The key loader 58 comprises an ultra-violet erasable ROM 66 housed beneath an aperture 64 in the case 60 wherethrough the ROM 66 can be irradiated if required to destroy its contents prior to loading fresh contents. The aperture 64 is closed by a light-tight grommet 68 to prevent the accidental irradiation of the ROM 66 and to prevent the slow attrition of its contents by daylight.

First, second, third and fourth light-emitting diodes (LED's) 70, 72, 74, 76 are provided in the sloping front of the case 60, directly driven via the key connector 42, for indicating key loading status in the encryption module 30.

Figure 5 shows a schematic circuit diagram of the key loader 58.

The key loader connector 62 provides a ground line 78 providing a common power return for the key loader 58. A first LED driving line 80 supplies illuminating power to the first LED 70, a second LED driving line 82 provides illuminating power to the second LED 72, a third LED driving line 84 provides illuminating power to the third LED 74, and a fourth LED driving line 86 provides illuminating power to the fourth LED 76, the first, second, third and fourth LED's 70, 72, 74, 76 each being coupled to the ground line 78 as the common return for the illuminating power.

The key loader 58 comprises an erasable Read-Only Memory 88 corresponding to the ROM 66 of figure 4. The ROM 88 receives operational power via a power line 90. The ROM 88 receives a chip selecting input via a chip select line 92 in response whereto the ROM 88 is rendered operational either to receive or render up data. The ROM 88 receives a programming input signal via a programme line 94. If the voltage on the program line 94 exceeds a predetermined threshold value for longer than a predetermined time and the signal is provided on the chip select line 92 the ROM 88 stores the data presented to it in the location addressed. If the ROM 88 is in receipt of the signal on the chip select line 92 alone, it renders up data stored in the location addressed. The ROM 88 is provide data on and renders up data to an 8-bit wide data bus 96 provided by the encryption module 30 and its locations are addressed via an 11-bit wide address bus 98. The ROM 88 comprises 2048 locations at each one of which an 8-bit parallel word can be stored. The encryption module 30 does not programme the ROM, and consequently the programme line 94 is not provided by the encryption module 30. The ROM 88 is pre--programmed at another, dedicated installation and it will be apparent to those skilled in the art how this can be done. The ROM 88 need not necessarily be ultra-violet erasable, but can be of the once-programmed variety where fuse links are blown and the like, in which case there is no need for the aperture 64 and the grommet 68. Similarly, the ROM 88 can be mask-programmed before assembly into the key loader 58, in which case there is no need for providing programming facilities via the key loader connector 62. As another alternative, the ROM 88 can be of the electrically-alterable variety in which case there is no need for the aperture 64 or the grommet 68 but there is a requirement for a line for cancelling the information in an addressed location. These and other variations on the nature of the ROM 88 and the differing requirements thereof under each circumstance will become apparent to those skilled in the art in consequence of the following description.

Figure 6 shows a schematic circuit diagram of the encryption module 30.

The encryption module 30 comprises a communication register 100 for providing communication with the internal processor 12 of the autoteller 10. The encryption module 30 further comprises an encryption control processor 102 which provides an encryption data bus 96 and an encryption address bus 98 for use as will later be described in the encryption module and for use as has already been described via the key connector 42 as the data bus 96 and the address bus 98 in the key loader 58. The communication register 100 is in receipt of the internal data bus 14 and of the internal address bus 16 from the internal processor 12 of the autoteller 10 and is also in receipt of the encryption data bus 96 and of the encryption address bus 98. The internal processor 12 can address the communication register 100 to deposit a block of data therein for later retrieval by the encryption control processor 102 and can address the communication register 100 to retrieve therefrom a block of data previously deposited therein by the encryption control processor 102.

In association with the encryption control processor 102 and in receipt of the encryption data bus 96 and of the encryption address bus 98 there is provided a resident ROM 104, a volatile RAM 106 and a sustained secure RAM 108. The resident ROM 104 is pre-loaded with the operating instructions for the encryption control processor and its contents cannot be changed. The volatile RAM 106 is a random-access memory used as a temporary store by the encryption control processor 102. The control processor 102 can write data therein or retrieve data therefrom. When power is removed from the encryption module 30 the contents of the volatile RAM 106 are lost. The secure sustained RAM 108 is operated in conjunction with a backup battery power supply 110 providing power thereto via a battery power line 112. When power is available to the encryption module in the normal manner, the energy on the power line 112 is derived from the general source, not shown, provided via the first edge connector 50 which source also charges up a battery in the backup power supply 110. When power is removed from the autoteller 10 the backup power supply 110 provides battery potential on the power line 112 which can sustain the sustained secure RAM 108 for up to ten days. The ground return line 114 of the backup power supply 110 is seperately externalised on the first edge connector 50 and is coupled via an external link 116 on the first edge connector 50 to the main power supply ground 118 to the encryption module 30 also provided on the first edge connector 50. Thus, whilst the printed circuit board 48 is plugged in via its first edge connector 50, the ground return line 114 of the battery backup power supply 110 is coupled via the external link 116 to the supply ground 118 so that if power is removed from the autoteller 10 the battery will sustain the sustained RAM 108, since one side of the supply to the sustained RAM 108 is provided via the supply ground 118. However, if power is removed from the autoteller 10 and the printed circuit board 48 is unplugged the link 116 between the ground return line 114 and the power supply ground 118 is broken so that the battery backup power supply 110 is unable to sustain the secure sustained RAM 108 and its contents are lost. The same result ensues if the printed circuit board 48 is unplugged whilst power is still supplied to the autoteller 10. The encryption control processor 102 can write data into and retrieve data from the secure RAM 108. The secure RAM 108 is used to store data, such as encryption keys, which it is not for interlopers to discover, or subsequently use. Thus, if the encryption module 30 is removed, it is not possible upon subsequent investigation to discover secret information nor is it possible to employ the encryption module 30 elsewhere since all of the secret information necessary for the operation of the autoteller 10 is lost as soon as the encryption module 30 is unplugged.

The encryption module 30 further comprises an encryption block 120 coupled to receive the encryption data bus 96 and the encryption address bus 98. The encryption control processor 102 is operable to provide the encryption block 120, by a process of addressing and data supply, with a key for encryption, a data character to be encrypted and is operable to address the encryption block 120 to recover the encrypted or selectably decrypted data.

The encryption module 30 comprises a flag comparator 122 once again coupled to receive the encryption data bus 96 and the encryption address bus 98 from the encryption control processor 102. At the end of key loading, to be described, the encryption control processor 102 deposits first and second predetermined flag characters in the flag comparator 122 and the flag comparator 122 provides indication on first and second 124 126 flag lines to a monitor circuit 128 of the presence of the flags. The monitor 128 also checks the battery potential in the backup power supply 110 and detects when it falls below a predetermined value. The monitor circuit 128 provides activating signals to a LED driving circuit 130 operable to respond thereto to provide the illuminating energy to the first, second, third and fourth LED's 70, 72, 74, 76 via the first, second, third and fourth LED driving lines 80, 82, 84, 86 respectively.

Figure 7 shows a schematic circuit diagram of the communication register 100 of figure 6.

The communication register 100 comprises a first interface RAM 132 for the temporary storage of data to be transferred from the internal processor 12 to the encryption control processor 102 and a second interface RAM 133 for the temporary storage of data to be transferred from the encryption control processor 102 to the internal processor 12. The communication register is in receipt of the internal address bus 16 of the autoteller 10 and receives it as an input to a first address decoder 134. The communication register 100 is also in receipt of the encryption address bus 98, receiving it as an input on a second address decoder 136. The first address decoder 134 examines the address on the internal address bus 16 and, if it lies within first and second numerical limits, these limits indicating the boundaries of the address field used by the internal processor 12 for accessing the communication register 100, the first address decoder 134 provides output indicative thereof. The second address decoder 136 examines the address on the encryption address bus 98 and, if it lies between third and fourth numerical values, being the upper and lower limits of the address field used by the encryption control processor 102 to access the communication register 100, it provides output indicative thereof.

The communication register 100 comprises a first address diplexer 138 in receipt of the internal address bus 16 as a first input and in receipt of the encryption address bus 98 as a second input. The output indication of the first address decoder 134 is coupled as a first controlling input to the first address diplexer 138 and the output indication of the second address decoder 136 is coupled as a second controlling input to the first address diplexer 138. When the first address decoder 134 provides its output indication the first address diplexer 138 provides, as its output, on the first interface RAM address bus 139, as the address input to the first interface RAM 132, the address on the internal address bus 16 of the internal processor 12, regardlessly of the indication provided by the second address decoder 136. When the second address decoder 136 provides its output indication, and the first address decoder 134 does not provide its output indication, the first address diplexer 138 provides, as output on the first interface address bus 139, the address provided on the encryption address bus 98. When neither the first address decoder 134 nor the second address decoder 136 provides output indication, the first address diplexer 138 provides no output.

The communication register 100 comprises a second address diplexer 140 in receipt of the internal address bus 16 as a first input and in receipt of the encryption address bus 98 as a second input. The output indication of the first address decoder 134 is provided as a first controlling input to the second address diplexer 140 and the output of the second address decoder 136 is provided as a second controlling input to the second address diplexer 140. When the second address decoder 136 provides its output indication, the second address diplexer 140 provides, as its output, regardlessly as to whether or not the first address decoder 134 is providing its output indication, on the second interface RAM address bus 141, the address supplied on the encryption address bus 98, as the address input to the second interface RAM 133. When the first address decoder 134 provides its output indication and the second address decoder 136 does not provide its output indication, the second address diplexer 140 provides, as the address input to the second interface RAM 133 via the second interface RAM address bus 141, the address supplied by the internal address bus 16 of the autoteller 10 internal processor 12. When neither the first address decoder 134 nor the second address decoder 136 provides its output indication the second address diplexer 140 provides no output.

The communication register 100 comprises a first bidirectional data diplexer 142, in receipt of the contents of the internal data bus 14 and selectably operable to couple the contents of the internal data bus 14 as data input onto a first interface RAM data bus 144. The first data diplexer 142 is also selectably operable to couple data provided by the first interface RAM 132 on the first interface RAM data bus 148 as input data onto the encryption data bus 14. The first data diplexer 142 receives the output of the first address decoder 134 as a first controlling input and receives the output of the second address decoder 136 as a second controlling input. When the first address decoder 134 provides its output indication, regardlessly as to whether or not the second address decoder 136 provides its output indication, the first data diplexer 142 couples the data on the internal data bus 14 as data input to the first interface RAM 132 via the first data interface RAM data bus 144. When the second address decoder 136 provides its output indication and the first address decoder 134 does not provide its output indication, the first data diplexer 142 couples output data, provided by the first interface RAM 132 via the first interface RAM data bus 144, onto the encryption data bus 96. When neither the first address decoder 134 nor the second address decoder 136 provides an output indication, the first data diplexer 142 neither accepts nor receives data.

The communication register 100 further comprises a second data diplexer 146 coupled to the second interface RAM via a second interface RAM data bus 148, coupled to selectably receive data from the encryption data bus 96 onto the second interface RAM data bus 148, coupled to selectably provide data from the second interface RAM data bus 148 onto the internal data bus 14, coupled to receive the output of the first address decoder 134 as a first controlling input and coupled to receive the output of the second address decoder 136 as a second controlling input.

When the second address decoder 136 provides its output indication, regardlessly as to whether the first address decoder 134 provides its output indication or not, the second data diplexer 146 couples the data presented on the encryption data bus 96 as input data to be stored by the second interface RAM 133 to the second interface RAM 133 via the second interface RAM data bus 148. When the first address decoder 134 provides its output indication and the second address decoder 136 does not provide its output indication, the second data diplexer 146 couples output data from the second interface RAM 133 provided thereby on the second interface RAM data bus 148 as input to the internal data bus 14. When neither the first address decoder 134 provides its output indication nor the second address decoder 136 provides its output indication the second data diplexer 146 neither accepts nor receives data.

The arrangement of address decoders 134, 136, address diplexers 138, 140, data diplexers 142, 146 and RAMs 132, 133 described allows the internal processor 12 to have a pre-emptive access to the first interface RAM 132 for the deposition of data therein and a secondary right to access to the second interface RAM 133 for the retrieval of data therefrom and allows the encryption control processor 102 to have a pre-emptive right of access to the second interface RAM 133 for the deposition of data therein and a secondary right of access to the first interface RAM 132 for the retrieval of data therefrom.

In operation, if the internal processor 12 wishes to pass data or instruction words to the encryption control processor 102, it first checks to see if the second address decoder 136 is providing its output indication. This is achieved by means of an interrogatable status register, not shown for reasons of simplicity, whose operation will be apparent to those skilled in the art. If the second address decoder 136 is providing its output indication the internal processor 12 waits until it ceases to do so. If there is no such indication the internal processor 12 proceeds immediately with data transfer. The internal processor 12 calls up the address of the first location in both the first and second interface RAMs. However, contained within the address is an indication as to whether the internal processor 12 wishes to read or write data in the communication register 100. If the internal processor 12 wishes to write data only the first interface RAM 132 is activated and if the internal processor 12 wishes to read data only the second interface RAM 133 is activated. The internal processor 12 addresses each of the locations in turn, either reading or writing data, in the RAMs 132, 133. In the first location, if writing, the internal processor 12 deposits an instruction word indicating the nature of the following message, for example, indicating that the following data is to be encrypted in a certain manner. In a second location in the first interface RAM 132, if writing, the internal processor 12 deposits a length word indicating the number of data words following. Similarly, if reading, the internal processor 12 retreives the word in the first location of the second interface RAM 133 earlier deposited therein by the encryption control processor I02 indicative of the nature of the data following, e.g. data encrypted with a particular key, and then retreives the word in the second location of the second interface RAM 133 indicative of the number of data words following. If writing the internal processor 12 goes on to deposit the number of data words indicated and if reading the internal processor 12 goes on to retreive the number of data words indicated, in each case by incrementing the address on the internal address bus 16 through the appropriate sequence of addresses.

The first and second interface RAMs 132, 133 are each capable of storing 1024 8-bit data words. The encryption processor 102, when wishing to operate through the communication register 100, looks to see if the first address decoder 134 is providing its output indication in the same way that the internal processor 12 looks to see if the second address decoder 136 is providing its output indication, waiting in the same manner until it alone wishes to access the communication register 100. The only difference between the manner of operation of the encryption control processor 102 and the manner of operation of the internal processor 12 lies in that the internal processor 12 deposits data in the first interface RAM 132 and retrieves data from the second interface RAM 133 whereas the encryption control processor 102 deposits data in the second interface RAM 133 and retrieves data from the first interface RAM 132. In this way the internal processor 12 and the encryption control processor 102 can pass plural-word data messages and identifying instructions between one another.

It is not important to the understanding of the present invention how the internal processor 12 deals with received messages, save as later described. In the case of the encryption control processor 102, data words are retrieved one by one from locations in the volatile RAM 106 and transferred one by one to the appropriate locations in the second interface RAM 133. It is not possible for the encryption control processor 102 to recover data from the secure RAM 108 since to be able to access the data therein would mean access to secret information. Thus the encryption control processor 102 is not provided with an instruction it can obey for transferring data from the secure RAM 108 to the communication register 100. However, the encryption control processor 102 can receive information, notably keys, for storage in the secure RAM 108. This is explained below.

Those skilled in the art will appreciate that means for transferring clock control to the RAMs 132, 133 between processors 12, 102 must be provided for the loading and unloading thereof as described. Those skilled in the art will also appreciate that other methods of transferring data between the two processors 12, 102 can equally be applied to the present invention employing modifications thereto which will be apparent and, as will become clear from the following description, the only requirement is that indication be provided along with the associated data as to the nature of the processing required to be performed on or having been performed on the data.

Figure 8 shows a schematic block diagram of the encryption block 120 of figure 6.

The encryption block 120 comprises an input register 150 operable to receive a series of eight 8-bit data words from the encryption data bus 96 and present them as an input to an encryption circuit 152 via the encryption circuit input bus 154. The exact construction and manner of operation of the input register 150 is to be described below. At this stage it is enough to say that a 64-bit input word is assembled for parallel presentation to the encryption circuit 150.

The encryption block 120 further comprises a key register 156. The key register 156 comprises eight 8-bit registers each coupled to receive an 8-bit word from the encryption data bus 96 to present a parallel 64-bit key word to the encryption circuit 152 via the key bus 158.

The encryption block 120 further comprises an output register 160 coupled to receive a 64-bit parallel encrypted or decrypted word from the encryption circuit 152 in eight 8-bit registers each individually addressable thereafter to render up their contents onto the encryption data bus 96.

The encryption block 120 yet further comprises an encryption address decoder 164 coupled to receive the encryption address bus 98 and operable to provide an addressing signal to each of the 8-bit registers in the input register 150, the key register 158 and the output register 160. Each of the 8-bit registers constitutes a seperate address to the encryption control processor 102. The encryption address decoder 164 decodes the addresses on the encryption address bus 98 and provides a separate activating signal to the selected one of the 8-bit registers whenever one of the 8-bit registers is addressed. Each of the 8-bit registers receives its own individual activating signal via its own individual addressing line, symbolised in figure 8 by an input register address bus 166 being representative of the collection of addressing lines going to the 8-bit registers in the input register 150, an output register address bus 168 being representative of the collection of address lines going to the output register 160, and a key register address bus 170 being representative of the collection of address lines going to the 8-bit registers in the key register 156.

Not shown in figure 8 for simplicity, is a 1-bit control register separately addressable via the encryption data bus 96 and the encryption address bus 98 decoded by the encryption address decoder 164 to accept one of the binary digits provided by the encryption databus 96, in just the same way as the 8-bit registers accept their inputs in, for example, the key register 156. The contents of the control register are coupled as a further input to the encryption circuit 152. The encryption circuit 152 responds to the content of the control register by encrypting the data provided by the input register 150 if the content of the control register is logically true and by decrypting the data provided by the input register 150 if the content of the control register is logically false.

The encryption circuit 152 accepts a 64-bit input word from the input register 150, accepts a 64-bit key word from the key register 158, and provides a 64-bit encrypted or decrypted version of the input word to the output register 160. The encryption circuit 152 employed as part of the present invention in its preferred embodiment is characterised by the use of Integrated Circuit type WD 2001 made by Western Digital Corporation and supporting an encryption algorithm defined in the United States National Bureau of Standards Data Encryption Standard (DES). Each of the 2^{64} different possible key words provided to the key register 156 elicits a different one of 2^{64} different scrambling patterns for the order of the 64 binary digits provided by the input register 150 to be altered before presentation to the output register 160. If the encryption circuit 152 is ordered to encrypt the input register 150 data it applies the selected scrambling pattern, and if ordered to decrypt, it applies the complementary "unscrambling" pattern of binary digit positions to undo the selected scrambling pattern.

It will become clear from the following description that the particular embodiment of encryption circuit 152 chosen by way of example to describe the action of the preferred embodiment of the present invention is not restrictive in its type. Systems encrypting and decrypting word lengths other than 64-bits are equally applicable, as are systems where input and key data can be supplied time-sequentially rather than in parallel. Those skilled in the art will be aware of the modifications to the preferred embodiment which would be required for the use of such alternative systems.

In use, the encryption control processor 102 loads the key word into the key register 156 8-bit word by 8-bit word until the key register 156 is full and the whole of the key word is therein. The encryption control processor 102, subject to the constraints to be described in connection with the construction and operation of the input register 150, then loads the input register 150 8-bit word by 8-bit word until the whole of the input word lies therein and the input register 150 is full. After an appropriate period of waiting for the encryption circuit 152 to perform its function, the encryption control processor 102 withdraws the resulting encrypted or decrypted result 8-bit word by 8-bit word from the output register 160.

Figure 9 shows a schematic circuit diagram of the input register 150 of figure 8.

The input register 150 comprises a direct register 172 coupled to receive the encryption data bus 96 and eight addressing lines from the input register address bus 166 one for addressing each of eight 8-bit registers therein, the direct register 172 thereby being loadable with a 64 bit direct data word. The contents of the direct register 172 are provided as a 64-bit parallel word on a direct register output bus 174.

The input register 150 further comprises a 64-bit cyphertext register 176 coupled to receive the encryption data bus 96 and a further eight addressing lines from the input register address bus, one for addressing each of eight 8-bit registers therein, the cyphertext register 176 thereby being loadable with a 64-bit cyphertext data word in the manner earlier described. The contents of the cyphertext register 176 are provided as a 64-bit parallel output on a cyphertext output bus 178.

The input register 150 further comprises an exclusive-or array 180, in receipt of the 64-bit parallel direct data word as a first input, in receipt of the 64-bit parallel cyphertext data word as a second input, and operable to provide a 64-bit parallel exclusive-or output word on an exclusive-or output bus 182, where each binary digit in the exclusive-or output word represents the exclusive-or function of the pair of binary digits in the corresponding positions in the direct data word and the cyphertext data word, the exclusive or function being logically true if one or the other but not both of the corresponding binary digits is true and otherwise logically false, the relationship being clarified by the Boolean Equation

$$E = D.\overline{C} + C.\overline{D}$$

where E is the binary digit in the Exclusive-or output word, D is the binary digit in the direct data word and C is the binary digit in the cyphertext data word.

The input register 150 further comprises a cypher flip-flop register 184 in receipt of a single bit from the encryption data bus 96 via a single bit input line 186 and in receipt of a single address line 188 from the input register address bus 166 being decoded from the encryption address bus 98 by the encryption address decoder 164. The encryption control processor 102 is thereby able to cause the contents of the cypher flip-flop register 184 to assume a logically true or a logically false condition. The condition of the contents of the cypher flip-flop register 184 is coupled as a cypher output signal on a cypher output line 190.

The input register 150 lastly comprises an encryption diplexer 192 in receipt of the 64-bit parallel direct data word as a first input, in receipt of the 64-bit parallel exclusive-or output word as a second input, in receipt of of the cypher output signal as a controlling input, operable in response to the contents of the cypher flip-flop register 184 being logically false to provide as output, on the 64-bit wide encryption circuit input bus 154, the direct data word on the direct data output bus 174 and operable in response to the contents of the cypher flip-flop register 184 being logically true to provide, as output onto the encryption circuit input bus 154, the exclusive-or output word on the exclusive-or output bus 182.

In operation the encryption control processor 102 elects whether a straight encryption is required or a cyphertext operation. If straight encryption is required the encryption control processor 102 addresses the cypher flip-flop register 184 and sets its contents to logically false, having the effect of causing the encryption diplexer 192 to provide, as the input to the encryption circuit 152 on the encryption circuit input bus 154, the contents of the direct register 172. The encryption control processor 102 then loads the direct register 174 with a 64-bit direct data word as described, waits, and accepts the encrypted word from the output register 160.

If cyphertext operation is required, the encryption control processor 102 addresses the cypher flip-flop register 184 and sets its content to being logically true. This has the effect of causing the encryption diplexer 192 to provide as the encryption circuit 152 input signal on the encryption circuit input bus 154 the exclusive-or output word provided on the exclusive-or output bus 182 by the exclusive-or array 180. The input register 150 is then ready to commence a cyphertext operation for the cypher-encryption of data messages to and from the remote-host 22.

In order to start the cyphertext operation the encyption control processor 102 must first load the cyphertext register 176 with a start word. It achieves this by loading, 8-bit word by 8-bit word, a 64-bit string of all ones into the eight 8-bit registers making up the cyphertext register 176. The start word chosen for preference in this instance is an all-zeros word, but this is by no means restrictive and those skilled in the art will be aware of many other start words which can be used. The encryption control processor 102 then loads the first eight 8-bit bytes of the message to be cyphertext encrypted into the direct register 172. The exclusive or array 180 provides the encryption circuit 152 input bus 154 with the described exclusive-or function generated between the contents of the cyphertext register 176 and the direct register 172. The encryption control processor 102 waits and receives the output of the encryption circuit 152 from the output register 160, and this output is used as the first eight bytes of the cyphertext message. The encryption control processor 102 takes the first eight bytes of the cyphertext message and places it into temporay storage in the volatile RAM 106. The encryption control processor 102 then retrieves the first eight bytes from the RAM 106 and loads them into the cyphertext register 176. The encryption control processor 102 then loads the next eight bytes of the message to be cyphertext encrypted into the direct register 172, waits for the encryption circuit 152 to work and stores the result in the volatile RAM 106 as before, once again retrieving the result therefrom and placing it into the cyphertext register 176 and loading the direct register 172 with the next eight bytes, of the message to be cyphertext encrypted. In this way the encryption control processor 102 takes the message to be cyphertext encrypted from its store in the RAM 106 by eight byte (64 bit) blocks and loads each block into the direct register 172, loading the cyphertext register 176 with the result of the previous encryption. The encryption circuit 152 then encrypts the result of forming the exclusive-or function between the contents of the direct register 172, namely the eight byte block of the data to be cyphertext encrypted and the previously cyphertext-encrypted eight byte block, being the contents of the cyphertext register 176. In this way the encryption control processor 102 carries on until the whole of the message to be cyphertext encrypted is complete. The message is required to be an integral number of 64 bits long.

In the overall operation of the autoteller 10, when the autoteller 10 is switched on, after an initial power-on and confidence check, the encryption control processor 102 looks to see if the key-loader 58 is present. It does so by calling up address 3000 hexadecimal. This is the address of the first location in the Read-Only memory 88 and contains a predetermined flag character. In this instance the predetermined flag character is hexadecimal A, but it can any non-zero character desired. If the encryption control processor 102 sees data A at address 3000 hexadecimal it knows that the key loader 58 is plugged onto the key connector 42. In response the encryption control processor 102 jumps to execute the program starting at address 3001, this being the next address in the ROM 88. The programme in the ROM 88 is any programme that the autoteller owner wishes to employ to generate a master key word 64 bits long. The program has access to use of the encryption block, and to cyphertext encryption. In addition it can use any encryption alogithm of its own style that it pleases. It can start with any data that is chosen, and use any function available through the encryption control processor 102. The master key generation program is secret, and known only to the owner of the autoteller. In fact, the program does not even have to be known to the owner, since it is contained on the key loader 58. The key loader 58 when not in use is kept by a single bank official who does not need to know what is stored thereon.

Having completed the algorithm defined by the contents of the ROM 88, the encryption control processor 88 stores the 8-byte master key it has generated in a temporary location in the volatile RAM 106. It then places a predetermined flag character in the flag comparator 122 indicative of the master key having been loaded. Thereafter it signals to the internal processor 12 that it is ready to receive a session sub-key from the remote host 22. The internal processor 12 signals the host 22 to supply it with a session sub-key via the data link 20 and the serial data interface 18. The remote host 22 then supplies a 64-bit session sub-key to the internal processor 12 which passes it in turn to the encryption control processor 102. The encryption control processor 102 loads the master key from its temporary location in the volatile RAM 106 into the key register 156 of the encyption block 120, loads the received session sub-key into the direct register 172, commands the cypher flip-flop register 184 to produce straight encryption, and accepts the output from the output register 160 as the session key. The encryption control processor 102 then destroys the contents of the temorary storage location in the volatile RAM 106 for the master key, storing the master key in the secure RAM 108 in a first predetermined location and storing the session key in the secure RAM 108 in a second predetermined location, scattering other data throughout the secure RAM so that it is not possible to determine what data in the secure RAM 108 represents keys.

If, on inspection of memory location 3000 hexadecimal the encryption control processor 102 does not see A as stored data, then it knows that the key loader 58 is not present on the key connector 42. Accordingly, it retrieves the master key from the predetermined location in the secure, sustained RAM 108 and sets the predetermined flag character in the flag comparator 122 if the master key passes its parity check. The encryption control processor 102 then continues as before as if the master key had been loaded by the key loader 58. In either case, as soon as the session key has been successfully loaded from the remote host 22 and encrypted using the master key, the encryption control processor 102 sets a second predetermined flag character in the flag comparator 122 indicative of the successful loading of the session key.

The session key is used thereafter for the encryption and decryption of data recorded on the card presented to the autoteller 10 by the prospective user. The manner of use is not restrictive, but, purely by way of example, the autoteller 10 can read a card, the internal processor 12 commanding the card reader 24. The card reader 24 transfers the data it obtains into temporary storage in the internal processor 12. Thereafter the internal processor 12 sends the data, or some selected part of the data from the card, in a block via the communication register 100, together with an instruction as to whether the data is to be encrypted or decrypted. to the encryption module 30. The encryption module 30 obeys the instruction, as will become clear from later description, within a predetermined range of operations. Having performed the required operation, as earlier described, the encryption module 30 returns the operated-upon data back to the internal processor 12. The internal processor 12 can, if it is so desired, command the keyboard 26 to render up its entered number and transfer that number to the encryption module 30 for encryption or decryption, the encryption module 30 returning the result to the internal processor 12.

The internal processor 12 can then operate in any desired manner according to any desired algorithm chosen by the owner of the autoteller upon the data derived from the card reader 24 and from the keyboard 26 to determine whether a desired correspondence exists between the number entered on the keyboard 26 and the data from the card reader 24, validating the user's right to employ the card. Thereafter the autoteller 10 can dispense money to the user or not dependently upon whether the correspondence exists and upon whether the host system 22 allows such an action after authorisation communication therewith.

The description so far has indicated the master key being loaded soley via the key loader 58. It is to be appreciated that, at the discretion of the owner of the autoteller 10, the master key can be loaded from the remote host system 22. This permits the owner to employ any measure of security that he so desires.

On the understanding that, where a piece of data such as a key is indicated, that piece of data was obtained by the internal processor 12 from the host system 22 and where other data such as card data and keyboard data is indicated, the internal processor 12 obtains it from its peripheral parts 24, 26, the internal processor 12 sends commands and data to encryption module 30 via the communication register 100 as described and receives data and indication of the operation performed back from the encryption module 30.

If the first word in a block provided via the communication register 100 by the internal processor 12 for the encryption control processor 102 is hexadecimal 00, the internal processor 12 commands the encryption module 30 merely to echo back the message it receives for the encryption module 30 to act as a temporary store and as a possible confidence test upon the encryption module 30. The encryption control processor 102 takes the subsequent data words into temporary storage in the volatile RAM 106. The encryption control processor 102 returns the temporarily stored data to the communication register 100 for provision back to the internal processor 12, causing the first character in the second interface RAM 133 to be hexadecimal 50, indicatively of the following data being echoed data.

If the first word in a block in the first interface RAM 132 is hexadecimal 31, the internal processor 12 is commanding the encryption module 30 to encrypt the following block of data by blocks of 64 bits using the session key. The session key is recovered from its secure location in the sustained RAM 108 and loaded into the key register 156. Straight encryption is then performed as earlier described. At the end of encryption, the encryption control processor 102 loads the result thereof from the volatile RAM 106 into the second interface RAM 133, causing the first character therein to be hexadecimal 51 to indicate to the internal processor 12 that the following block of data has been encrypted using the session key. Such an instruction and response can be used on data read from a user's card.

If the first word in a block in the first interface RAM 132 is hexadecimal 32, the internal processor 12 is commanding the encryption module 30 to decrypt the following block of data using the session key by blocks of 64 bits. The session key is recovered from its secure location and loaded into the key register 156. Straight decryption is then performed as earlier described. At the end of decryption the encryption control processor 102 loads the result thereof from the volatile RAM 106 into the second interface RAM 133 causing the first character therein to be hexadecimal 52 indicative to the internal processor 12 of the following block of data having been decrypted using the session key.

If the first character in a block of data in the first interface RAM 132 is hexadecimal 33, the internal processor 12 is commanding the encryption control processor 102 to accept the following eight bytes of data as the session key. The encryption control processor 102 loads the eight bytes directly into the secure locations earlier described in the secure RAM 108. The encryption module 30 then signals back to the internal processor 12 that the session key has been loaded by setting a binary digit in a device status register, not shown, whose operation will be apparent to those skilled in the art and which can be interrogated by the internal processor 12.

If the first character in a block of data in the first interface RAM 132 is hexadecimal 34 the internal processor 12 is commanding the encryption control processor 102 to accept the following eight bytes of data as a session sub-key and to encrypt them using the master key before storage in the secure RAM 108 as the session key. The encryption control processor 102 responds thereto as indicated, and, as before, sets the binary digit in the status register indicative of the session key having been loaded.

If the first character in a block of data in the first interface RAM 132 is hexadecimal 35 the internal processor 12 is commanding the encryption control processor 102 to accept the following eight bytes of data as a session sub-key and to decrypt them using the master key before storage in the secure RAM 108 as the session key. The encryption control processor 102 responds thereto as indicated and, as before, sets the binary digit in the status register indicatively of the the session key having been loaded.

If the first and only character in the first interface RAM 132 is hexadecimal 36 the internal processor 12 is commanding the encryption control processor 102 to clear the session key. The encryption control processor 102 responds by clearing the secure location in the secure RAM 108 whereat the eight 8-bit bytes of the session key are stored and by resetting the binary digit in the status register now indicatively of the session key no longer being loaded. As a further action the encryption control processor 102 also unloads the predetermined flag character from the flag comparator 122 so that it no longer provides indication of the session key being loaded.

If the first and only character in the first interface RAM 132 is hexadecimal 37 the internal processor 12 is commanding the encryption control processor to clear all flags. The encryption control processor 102 responds by resetting all status flags, resetting all indications to the flag comparator 122 so that it no longer provides indication of the session or master keys being loaded and by clearing the entire contents of the secure RAM 108, inclusively of the master key, so that fresh keys must be loaded before operation can continue. As will become clear from later description, this can include a plurality of communications keys stored therein.

If the first word stored in the first interface RAM 132 is hexadecimal 38 the internal processor 12 is commanding the encryption control processor 102 to load the following eight 8-bit characters as the master key, this time supplied by the remote host system 22, directly into the secure RAM 108 location reserved for it and to provide the predetermined character to the flag comparator 122 for it to provide output indication of the master key having been loaded, and to set an appropriate flag in the device status register (not shown).

If the first word stored in the first interface RAM 132 is hexadecimal 39 the internal processor 12 is commanding the encryption control processor 102 to provide cyphertext encryption, using the session key, in the manner already described, for the data following. The encryption control processor 102 responds by taking the cyphertext encrypted data from temporary storage in the volatile RAM 106 and loading it into the second interface RAM 133, making the first character therein hexadecimal 59 indicatively of the following data having been cyphertext encrypted.

If the first character stored in the first interface RAM 132 is hexadecimal 3A the internal processor 12 is commanding the encryption control processor 102 to cyphertext decrypt the following block of data in the same manner as the already described cyphertext encryption save that the decryption facility of the encryption circuit 152 is selected. After the cyphertext decryption, just as for cyphertext encryption, having used the session key, the encryption control processor 102 takes the cyphertext decrypted message from temporary storage in the volatile RAM 106 and places it into the second interface RAM 133 making the first word therein hexadecimal 5A indicatively to the internal processor 12 of the following block of data having been cyphertext decrypted.

In addition to the features already described, the autoteller system 10 also comprises means for the transmission and reception of secure messages between the external host system 22 and the internal processor 12 using a selectable one out of a plurality of communication keys.

After the master key and the session keys have been loaded into the encryption module 30, the internal processor 12 examines the status register, already described but not shown in the drawings, whereby the encryption control processor 102 signals to the internal processor 12 that all has been carried out successfully, and, if all is in order, signals to the external host system 22 that it is ready to receive communications keys or communication sub-keys.

The internal processor 12 receives an indication from the external host system 22 that the following stream of binary digits represents a serialisation of an ordered succession of one hundred 64-bit communication keys or communication sub-keys. The external host 22 also indicates if the following binary digits are actual keys or are sub-keys. The internal processor 12 assembles the stream of binary digits into a succession of 8-bit bytes for provision to the encryption control processor 102.

If the first word stored in the first interface RAM 132 is hexadecimal 3B the internal processor 12 is commanding the encryption control processor 102 to accept the following eight hundred ordered bytes of data as communications keys. The encryption control processor 102 strips out the data in eight-byte blocks i.e. 64 bit blocks and stores each block in a predetermined location in the secure RAM 108 such that each block can be located by the calling up of its serial number. That is to say, by calling up the first block, the block first presented to the first interface RAM 132 is obtained, by calling up the fifteenth block the fifteenth block stored in the first interface RAM is obtained, and so on so that each block can be accessed merely by calling up its number lying between 1 and 100. It is to be appreciated that more blocks or fewer blocks than 100 can be used in the present invention. Each stored block of 64 bits becomes a communication key. The encryption control processor 102 thereafter sets a binary digit in the device status register, (already mentioned but not shown) indicatively to the internal processor 12 of the communication keys having been loaded.

If the first word stored in the first interface RAM 132 is hexadecimal 3C the internal processor 12 is commanding the encryption control processor 102 to accept the following succession of eight hundred ordered 8-bit bytes of data as communication sub-keys. The encryption control processor 102 strips out the data in eight-byte blocks and encrypts them using the master key, once again storing the result of the encryption as a succession of communication keys in the secure RAM 108, each one being individually recallable by the provision of the number 1 to 100 indicative of the serial order of its receipt among the other communication keys.

If the first word stored in the first interface RAM 132 is hexadecimal 3D, the internal processor 12 is internal processor 12 is commanding the encryption control processor 102 to accept the following succession of eight hundred ordered 8-bit bytes of data as communication sub-keys, to be operated upon in just the same manner as if the first word stored had been hexadecimal 3C, save that the decryption function of the encryption circuit 152 is selected as opposed to the encryption function.

If the first word stored in the first location of the first interface RAM 132 is hexadecimal 40, the internal processor 12 is commanding the encryption control processor 102 to encrypt the following message using an elected communication key. As stated before, the second word stored in the first interface RAM 132 indicates how many data words follow. If the first word is 40 the encryption control processor 102 interprets the third word stored therein as indicating which of the hundred communication keys is to be used. The third word is therefore a number elected by the internal processor 12 via the external host system 12 from 1 to 100 for data communication purposes. The elected communication key is loaded into the key register 156 and encryption of the remaining contents of the first interface RAM proceeds as before described. The encryption control processor 102 deposits the result of the encryption from temporary storage in the volatile RAM 106 into the second interface register 133 making the first word therein 60 to indicate to the internal processor 12 that encryption using a communication key has taken place on the following data, making the second word indicative of the serial number of the communication key employed, and indicating in the third word the number of following data words.

If the first word stored in the first location of the first interface RAM 132 is hexadecimal 41 the internal processor 12 is commanding the encryption control processor 102 to decrypt the following message using an elected communication key. All takes place as before as if the first word had been hexadecimal 40, save that the decryption function of the encryption circuit 152 is selected and the encryption control processor 102 makes the first word in the second interface RAM 133 hexadecimal 61 as opposed to hexadecimal 60, indicating to the internal processor 12 that the following data stored therein has been decrypted using the communication key elected in the third word therein.

If the first word stored in the first location of the first interface RAM 132 is hexadecimal 43 the internal processor 12 is commanding the encryption control processor 102 to cyphertext encrypt the following data using the communication key elected in the third word stored therein. Cypheretext encryption takes place as before described with the elected communication key loaded into the key register 156 from the secure RAM 108. The encryption control processor 102 deposites the result of the cyphertext encryption into the second interface RAM 133 making the first word therein hexadecimal 63 indicating to internal processor 12 that the following data has been cyphertext encrypted using the communication key indicated by the number stored in the third location therein.

If the first word stored in the first location of the first interface RAM 132 is hexadecimal 44 the internal processor 12 is commanding the encryption control processor 102 to cyphertext decrypt the following data using the communication key elected in the third word stored therein. All takes place as if the first word were hexadecimal 43 save that the decryption facility of the encryption circuit 152 is selected and that the encryption control processor 102 makes the first word stored in the second interface RAM 133 hexadecimal 64 to indicate to the internal processor 102 that the following data has been cyphertext decrypted using the communication key elected in the third word stored therein.

In this manner, by passing keys which are selectably encryptable or decryptable using the master key, or are directly usable without encryption or decryption but are referred to ever after transmission from the host 22 in either of the two cases by a serial number unrelated to their value so that an interloper cannot discover which key is being used for data communications between the host 22 and the autoteller system 10, the communication of data therebetween is rendered secure. The host 22 indicates with each message which of the keys is to be used in what manner, and the internal processor 12 responds by causing the encryption control processor 102 to operate upon the received data in the selected manner to generate the communication text, the internal processor 12 applying the inverse command to the encryption control processor 102 for the rendering unintelligible of data for transmission from the internal processor 12 to the host 22.

Returning briefly to the monitor circuit 128 of figure 6, the monitor 128 causes the first LED 70 to be lit if the master key has not been loaded, causes the second LED 72 to be lit if the master key has not been loaded and the encryption control processor 102 does not detect the presence of the key loader 58, causes the third and fourth LEDS 76, 78 to be lit if the master key has been loaded but the battery terminal voltage is low, and causes the fourth LED 78 alone to be lit if the master key has been successfully loaded and the unit in operational. In this manner, the security personnel in charge of the key loader 58 can chart the course of the loading of the master key and are provided in some small part with a diagnosis of at least the symptom if not the cause of malfunction in the event of the autoteller system 10 failing to operate.

While the monitoring operation employed to light the LEDs 72, 74, 76, 78 in response to internal conditions in the encryption module 30 has heretofore been described using a monitor circuit 128, it is to be appreciated that the function of the monitor circuit 128 could be absorbed into the overall operation of the encryption control processor 102 which can set and reset latches and the like in response to its internal states to drive the LEDs 72, 70, 74, 76.

Claims

1. A system including an autoteller (10) for dispensing money on presentation of a valid card; said autoteller including a card reader (24) for reading data from a card; a data link (20) for communicating with a remote processor (22); an encryption module (30) wherein an input word is encrypted in response to a current key word in one out of a plurality of selectable manners of encryption to provide an output word; and a master key word; said system being operative to receive a sub key word from said remote processor (22),to employ said sub-key word as said input word and said master key word as said current key word and to store said output word as a session key word and thereafter to use said session key word as said current key word; said system being characterised by said encryption module (30) comprising a control processor (12); by said system comprising a selectably attachable and removeable master key loader (58) containing a non-volatile memory (66, 88) holding a set of instructions for said control processor (12) to perform an algorithm to generate a master key word; and by said system comprising a port (52) on said encryption module (30) for receiving said master key loader (58) to enable said control processor (12) to read instructions therefrom; where said control processor (12) is operative to detect whether or not a master key word is stored in said autoteller (10) and, if no master key word is stored, is operative to perform said algorithm to generate said master key word.

2. A system according to Claim 1 wherein said sub-key word is one of a plural succession of sub-key words received in succession from said remote processor (22) wherein said encryption module (30) is operative to generate and store a session key from each of said sub-keys and to allocate a serial number to each session key, the allocated serial number bearing no relationship to the actual value of the associated session key; and wherein the session key actually in use can be changed from time to time by said remote controller calling out a particular selected sub-key by its serial number.

3. A system according to Claim 1 or Claim 2

wherein said encryption module (30) also comprises an encryption processor (102) operative to perform and control said encryption and operative to receive data and instructions from said control processor (12) and to pass data and status indication back to said control processor (12), said encryption module (30) including a communication register (100) operative to control communication between said control processor (12) and said encryption processor (102); said communication register (100) comprising a first interface memory (132) for receiving data from said control processor (12) and for providing data to said encryption processor (102), and a second interface memory (133) for receiving data from said encryption processor (102) and for providing data to said control processor (12); said encryption processor (102) deferring access to deposit or recover data in said communication register if said control processor (12) already has access to said communication register (100); and said control processor (12) deferring access to deposit or recover data in said communication register (100) if said encryption processor (102) already has access to said communication register (100).

4. A system according to Claim 3 wherein said control processor (12) comprises an internal address bus (16); wherein said encryption processor (102) comprises an encryption address bus (98); wherein said communication register (100) comprises a first address decoder (134) coupled to receive said internal address bus (98) and operative to provide a first activating signal to said first and second interface memories (132, 133) if an address on said internal address bus (16) lies between first and second predetermined limits; wherein said communication register (100) comprises a second address decoder (134) coupled to receive said encryption address bus (98) and operative to provide a second activating signal to said first and second interface memories (132, 133) if an address on said encryption address bus (98) lies between third and fourth predetermined limits; and wherein said first and second interface memories (132, 133) are operative to ignore said second activating signal if said first activating signal is provided.

5. A system according to claim 3 or 4 wherein said control processor (12) is operative to deposit a block of words in said first interface memory (132) and to record therewith, indication of the number of words in the block, and wherein said encryption processor (102) is operative to read said indication of the number of words in a block and to transfer that number of words from said first interface memory (132) and wherein said encryption processor (102) is operative to deposit a block of words in said second interface memory (133) and to record therewith, indication of the number of words in the block, and wherein said control processor (12) is operative to read said indication of the number of words in a block and to transfer that number of words from said second interface memory (133).

Patentansprüche

1. Automatisches Bankschaltersystem (10) zur Ausgabe von Geld bei Vorlage einer gültigen Karte;

mit einem Kartenleser (24) zum Lesen von Kartendaten;

mit einer Datenverbindung (20) zu einem entfernten Prozessor (22);

mit einem Verschlüsselungsmodul (30), mit dem ein Eingabewort abhängig von einem aktuellen Schlüsselwort in einer aus einer Mehrzahl von auswählbaren Verschlüsselungsarten verschlüsselt wird, um ein Ausgangswort zu erzeugen; und

mit einem Haupt-Schlüsselwort;

wobei dem System ein Unter-Schlüsselwort von einem Unter-Prozessor (22) zuführbar ist, um dieses Unter-Schlüsselwort als Eingabewort und das Haupt-Schlüsselwort als aktuelles Schlüsselwort zu benutzen, das Ausgangswort als Vorgangs-Schlüsselwort zu speichern und danach das Vorgangs-Schlüsselwort als aktuelles Schlüsselwort zu benutzen;

dadurch gekennzeichnet, daß das Verschlüsselungsmodul (30) einen Steuerprozessor (12) aufweist;

daß das System einen wahlweise anschaltbaren und entfernbaren Hauptschlüsseleinsatz (58) enthält, der einen nicht-flüchtigen Speicher (66, 88) zum Halten eines Instruktionssatzes für den Steuerprozessor (12) enthält, damit dieser nach einem Algorithmus ein Haupt-Schlüsselwort erzeugt;

daß das System einen Anschluß (52) an dem Verschlüsselungsmodul (30) zum Empfang dieses Hauptschlüsseleinsatzes (58) enthält, um es dem Steuerprozessor (12) zu ermöglichen, daraus Instruktionen zu lesen; und

daß der Steuerprozessor (12) dazu ausgebildet ist, festzustellen, ob ein Haupt-Schlüsselwort in dem Bankschaltersystem (10) gespeichert ist oder nicht, wobei der Steuerprozessor entsprechend dem Algorithmus das Hauptschlüsselwort erzeugt, wenn kein solches gespeichert ist.

2. System nach Anspruch 1, dadurch gekennzeichnet, daß das Unter-Schlüsselwort eines aus einer Folge von Unter-Schlüsselworten ist, die in einer Folge von dem entfernten Prozessor (22) empfangen werden;

daß das Verschlüsselungsmodul (30) dazu ausgebildet ist, ein Vorgangs-Schlüsselwort aus jedem der Unter-Schlüsselworte abzuleiten und zu speichern sowie jedem Vorgangs-Schlüsselwort eine Seriennummer zuzuordnen, wobei die zugeordnete Seriennummer keine Beziehung zu dem tatsächlichen Wert des zugeordneten Vorgangs-Schlüsselwortes hat; und

daß das gerade in Benutzung befindliche Vorgangs-Schlüsselwort von Zeit zu Zeit durch den entfernten Prozessor geändert werden kann, indem ein besonders ausgewähltes Unter-Schlüsselwort durch seine Seriennummer aufgerufen wird.

3. System nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß das Verschlüsselungsmodul

(30) auch einen Verschlüsselungsprozessor (102) aufweist, mit dem die Verschlüsselung durchgeführt und gesteuert wird und der Daten und Instruktionen von dem Steuerprozessor (12) empfängt und Daten und Statusanzeigen an den Steuerprozessor (12) zurückliefert.

daß das Verschlüsselungsmodul (30) ein Kommunikationsregister (100) aufweist, das die Kommunikation zwischen dem Steuerprozessor (12) und dem Verschlüsselungsprozessor (102) steuert;

daß das Kommunikationsregister (100) einen ersten Interface-Speicher (132) zum Empfangen von Daten von dem Steuerprozessor (12) und liefern von Daten an den Verschlüsselungsprozessor (102) sowie einen zweiten Interface-Speicher (133) zum Empfang von Daten von dem Verschlüsselungsprozessor (102) und zum Liefern von Daten an den Steuerprozessor (12) enthält;

daß der Verschlüsselungsprozessor (102) den Zugriff zum Eingeben und Ausgeben von Daten in den bzw. aus dem Kommunikationsregister verzögert, wenn der Steuerprozessor (12) bereits Zugriff zu dem Kommunikationsregister (100) hat; und daß der Steuerprozessor (12) den Zugriff zum Eingeben und Ausgeben von Daten in den bzw. aus dem Kommunikationsregister (100) verzögert, wenn der Verschlüsselungsprozessor (102) bereits Zugriff zu dem Kommunikationsregister (100) hat.

4. System nach Anspruch 3, dadurch gekennzeichnet, daß der Steuerprozessor (12) einen internen Adressbus (16) aufweist;

daß der Verschlüsselungsprozessor (102) einen Verschlüsselungs-Adressbus (98) aufweist;

daß das Kommunikationsregister (100) einen ersten Adressdecoder (134) aufweist, der zum Empfang an den internen Adressbus (98) angeschlossen ist und ein erstes Aktivierungssignal an den ersten und den zweiten Interface-Speicher (132, 133) liefert, wenn eine Adresse auf dem internen Adressbus zwischen einer ersten und einer zweiten vorgegebenen Grenze liegt;

daß das Kommunikationsregister (100) einen zweiten Adressdecoder (134) aufweist, der zum Empfang an den Verschlüsselungs-Adressbus angeschlossen ist und ein zweites Aktivierungssignal an den ersten und den zweiten Interface-Speicher (132, 133) liefert, wenn eine Adresse auf dem Verschlüsselungs-Adressbus (98) zwischen einer dritten und einer vierten vorgegebenen Grenze liegt; und

daß der erste und der zweite Interface-Speicher (132, 133) das zweite Aktivierungssignal ignoriert, wenn das erste Aktivierungssignal vorhanden ist.

5. System nach Anspruch 3 oder 4, dadurch gekennzeichnet, daß der Steuerprozessor (12) einen Block von Worten in den ersten Interface-Speicher (132) eingibt und damit zusammen eine Angabe der Anzahl der Worte in dem Block aufzeichnet;

daß der Verschlüsselungsprozessor (102) diese Angabe der Anzahl der Worte in dem Block liest und diese Anzahl von Worten aus dem ersten Interface-Speicher (132) überträgt;

daß der Verschlüsselungsprozessor (102) einen Block von Worten in dem zweiten Interface-Speicher (133) ablegt und damit zusammen eine Angabe der Anzahl der Worte in dem Block aufzeichnet; und

daß der Steuerprozessor (12) diese Angabe der Anzahl der Worte in dem Block liest und diese Anzahl von Worten aus dem zweiten Interface-Speicher (133) überträgt.

Revendications

1. Système comprenant un guichet (10) pour distribuer des billets de banque sur présentation d'une carte validée, ce guichet comportant un lecteur de carte (24) pour lire les données inscrites sur une carte, une liaison de données (20) pour communiquer avec un processeur à distance (22), un module de cryptage (30) dans lequel on crypte un mot d'entrée en réponse à un mot de clé courant suivant l'une des différentes façons possibles de cryptage pour donner un mot de sortie ainsi qu'un mot-clé principal, ce système recevant un mot-clé secondaire du processeur éloigné (22) pour utiliser ce mot-clé secondaire comme mot d'entrée et le mot-clé principal comme mot-clé courant pour enregistrer le mot de sortie comme un mot-clé de session, puis utiliser le mot-clé de session comme mot-clé courant, système caractérisé en ce que le module de cryptage (30 comporte un processeur de commande (12), le système comporte un chargeur de clé principal (58) susceptible d'être fixé et enlevé sélectivement, chargeur contenant une mémoire morte (66, 88) contenant un ensemble d'instructions pour le processeur de commande (12), pour effectuer un algorithme générant un mot-clé principal et un port (52) sur le module de cryptage (30) pour recevoir le chargeur de clé principal (58) pour autoriser le processeur de commande (12) d'y lire des instructions, le processeur de commande (12) détectant si un mot-clé principal est ou non inscrit dans le guichet (10) et si aucun mot-clé principal n'y est inscrit, il exécute l'algorithme pour générer le mot-clé principal.

2. Système selon la revendication 1, caractérisé en ce que le mot-clé secondaire est l'un des mots-clés secondaires de la suite reçus successivement du processeur à distance (22), le module de cryptage (30) générant et inscrivant une clé de session à partir de chaque clé secondaire et attribuant un numéro d'ordre à chaque clé secondaire, le numéro attribué ne traduisant aucune relation entre la valeur réelle et la clé de session correspondante, la clé de session effectuant utilisée pouvant changer de temps à autre en étant modifiée par le contrôleur à distance appelant une clé secondaire choisie, particulière par son numéro d'ordre.

3. Système selon la revendication 1 ou la revendication 2, caractérisé en ce que le module de cryptage (30) comporte également un processeur de cryptage (102) qui exécute et commande le cryptage et reçoit des données et des instructions du processeur de commande (12) et fait

passer les données et les indications d'état en retour vers le processeur de commande (12), ce module de cryptage (30) comportant un registre de communications (100) commandant les communications entre le processeur de commande (12) et le processeur de cryptage (102), le registre de communications (100) comportant une première mémoire d'interface (132) recevant les données du processeur de commande (12) et fournissant les données au processeur de cryptage (102) ainsi qu'une seconde mémoire d'interface (133) recevant les données du processeur de cryptage (102) et fournissant les données au processeur de commande (12), le processeur de cryptage (102) interdisant l'accès pour le dépôt ou la récupération de données dans le registre de communications si le processeur de commande (12) a déjà accédé au registre de communications (100) et le processeur de commande (12) interdisant l'accès au dépôt ou à la récupération de données dans le registre de communications (100) si le processeur de cryptage (102) a déjà accédé à ce registre de communications (100).

4. Système selon la revendication 3, caractérisé en ce que le processeur de commande (12) comporte un bus d'adresses interne (16), le processeur de cryptage (102) comporte un bus d'adresses de cryptage (98), le registre de communications (100) comporte un premier décodeur d'adresses (134) recevant le bus d'adresses interne (98) et fournissant un premier signal d'activation à la première et à la seconde mémoires d'interface (132, 133) si une adresse du bus d'adresses interne (16) est comprise entre une première et une seconde limites prédéterminées, le registre de communications (100) comportant un second décodeur d'adresses (134) recevant le bus d'adresses de cryptage (98) et fournissant un second signal d'activation à la première et à la seconde mémoires d'interface (132, 133) si une adresse du bus d'adresses de cryptage (98) est comprise entre une troisième et une quatrième limites prédéterminées, et la première et la seconde mémoires d'interface (132, 133) ignorent le second signal d'activation si le premier signal d'activation est présent.

5. Système selon la revendication 3 ou 4, caractérisé en ce que le processeur de commande (12) dépose un bloc de mots dans la première mémoire d'interface (132) et enregistre en même temps l'indication du nombre de mots contenus dans le bloc, le processeur de cryptage (105) lisant l'indication du nombre de mots dans un bloc et transférant ce nombre de mots de la première mémoire d'interface (132), le processeur de cryptage (102) déposant un bloc de mots dans la seconde mémoire d'interface (133) et pour y enregistrer en même l'indication du nombre de mots contenus dans le bloc et le processeur de commande (12) lit cette indication du nombre de mots dans un bloc et transfère ce nombre de mots de la seconde mémoire d'interface.

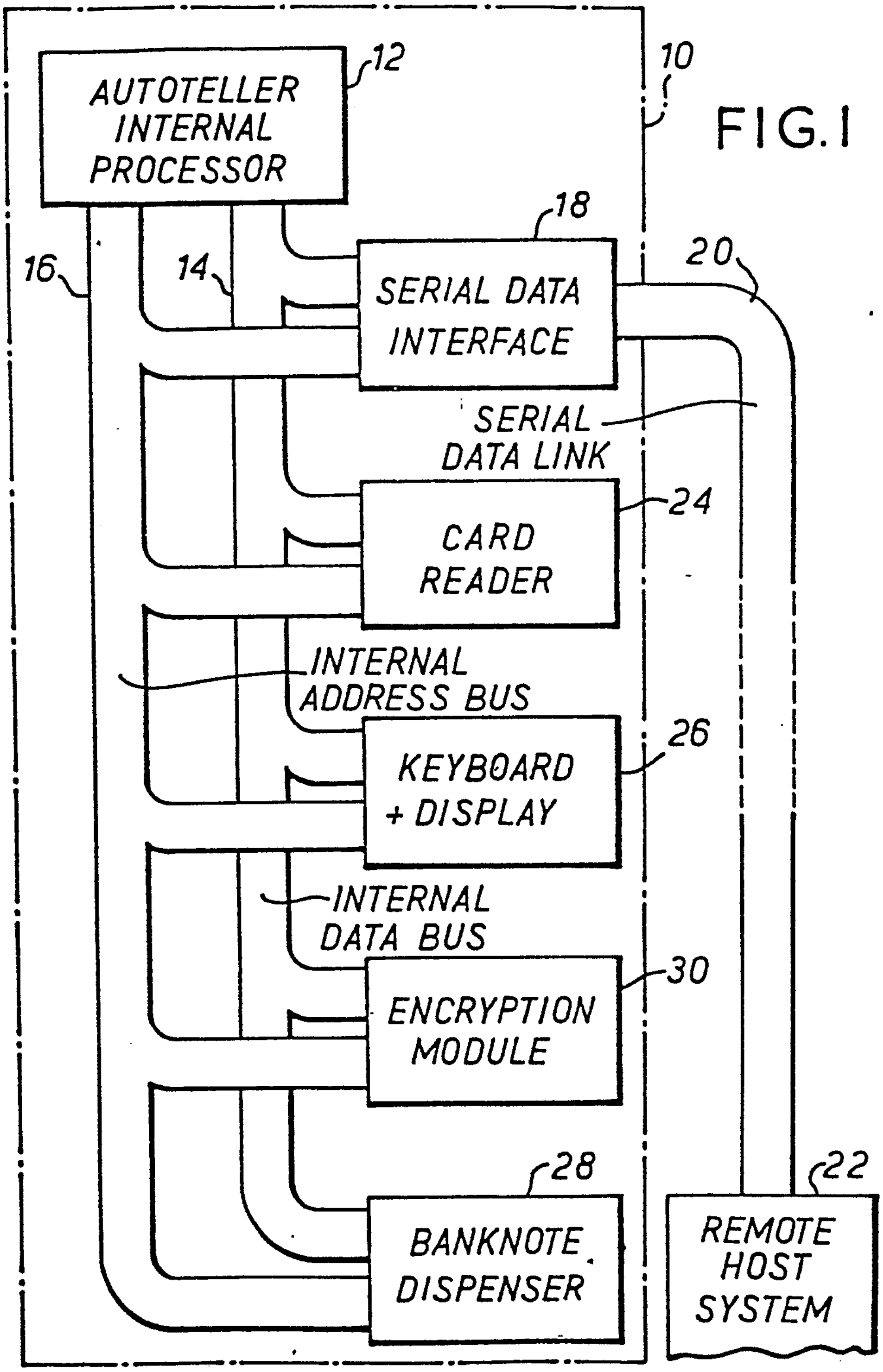
AUTOTELLER INTERNAL PROCESSOR
12
10
16
14
18
SERIAL DATA INTERFACE
20
SERIAL DATA LINK
CARD READER
24
INTERNAL ADDRESS BUS
KEYBOARD + DISPLAY
26
INTERNAL DATA BUS
ENCRYPTION MODULE
30
BANKNOTE DISPENSER
28
REMOTE HOST SYSTEM
22

FIG.1

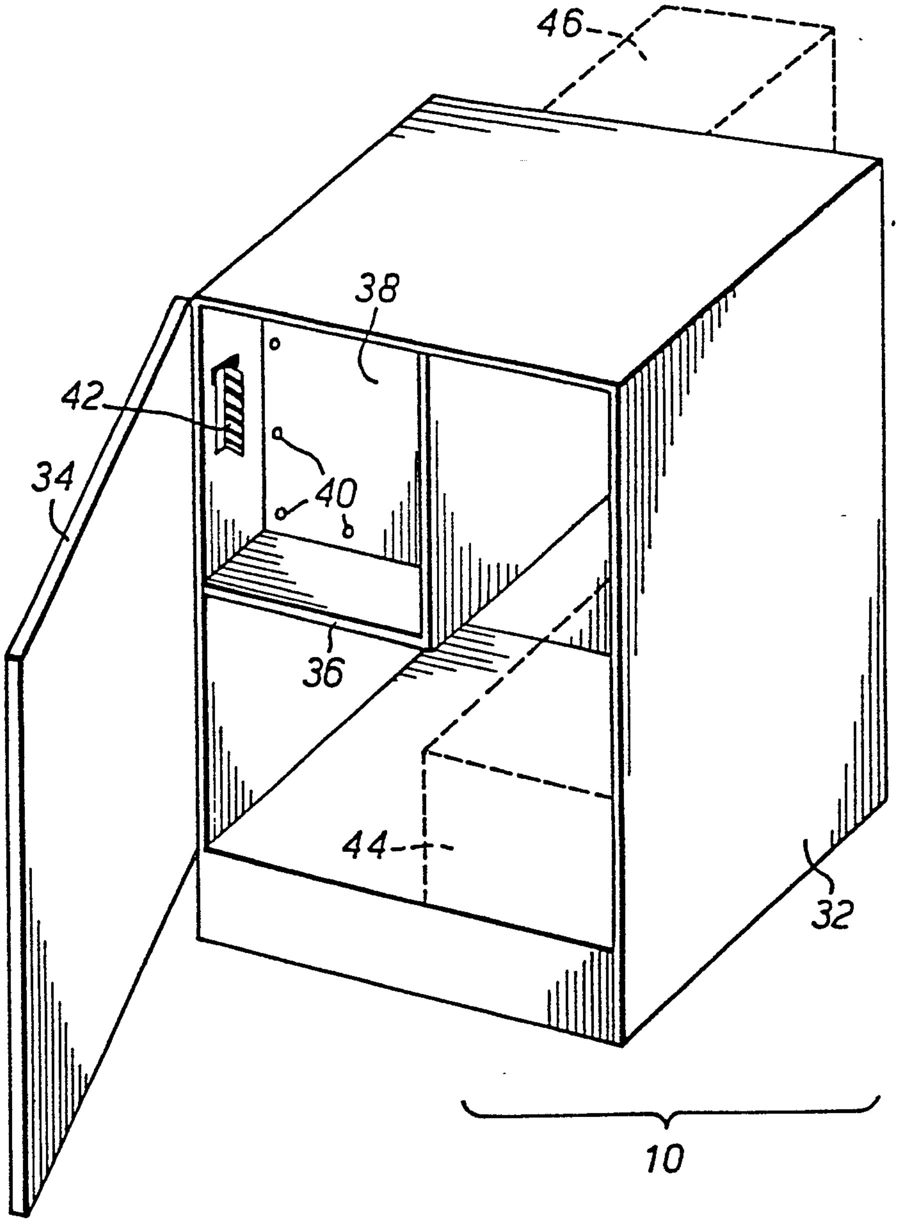

FIG. 2

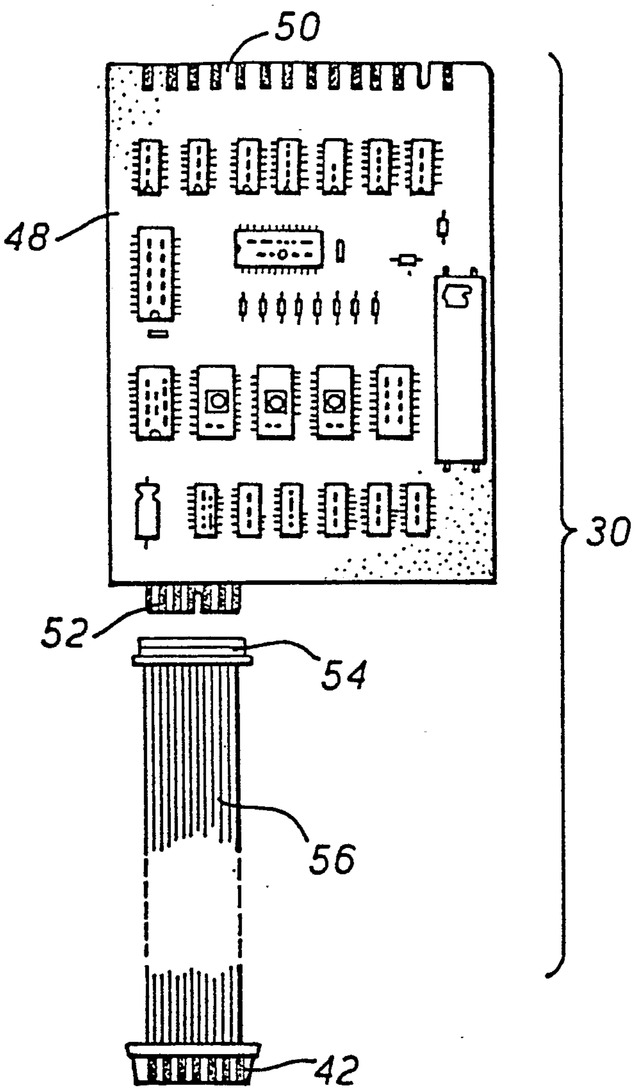

FIG. 3

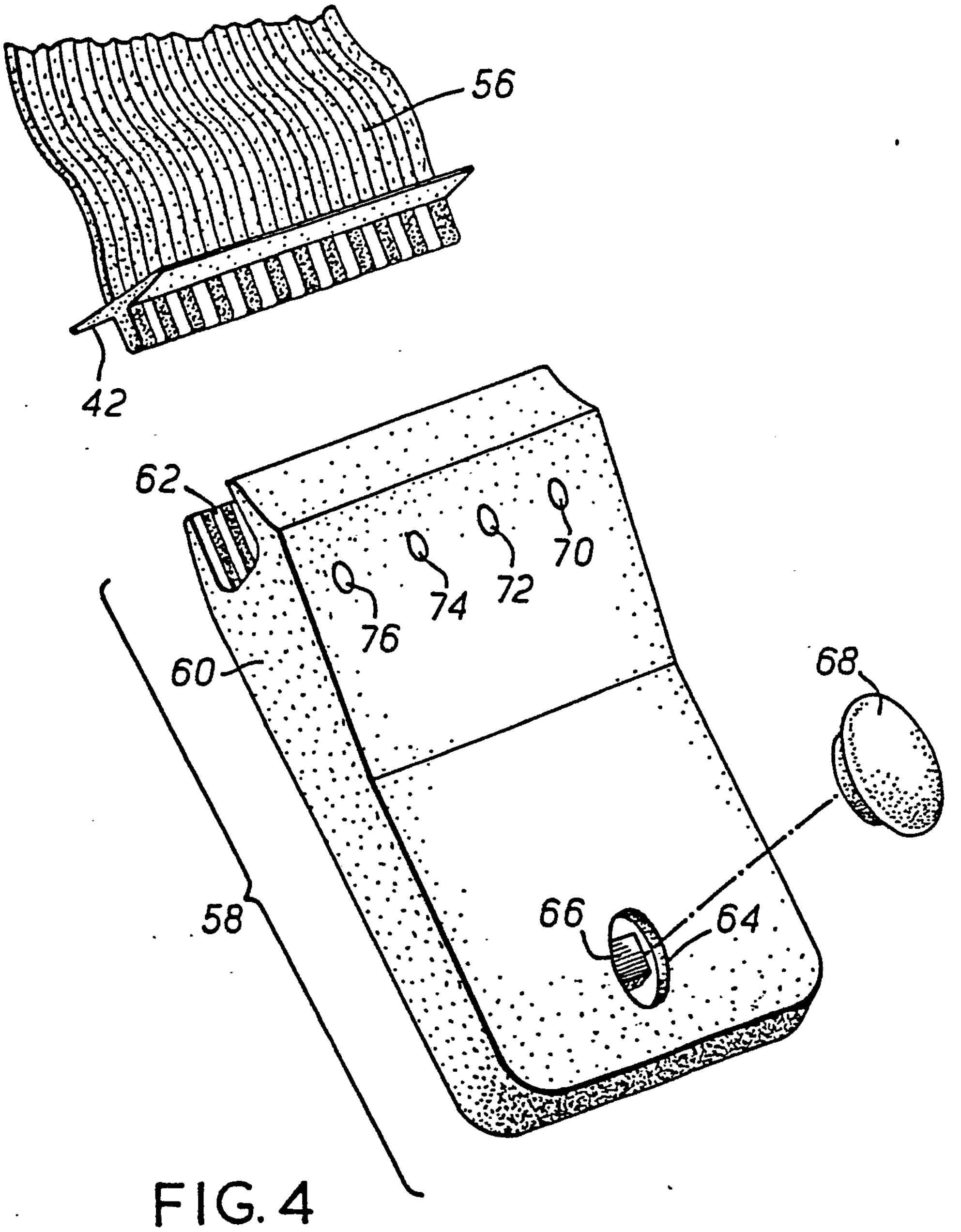

FIG. 4

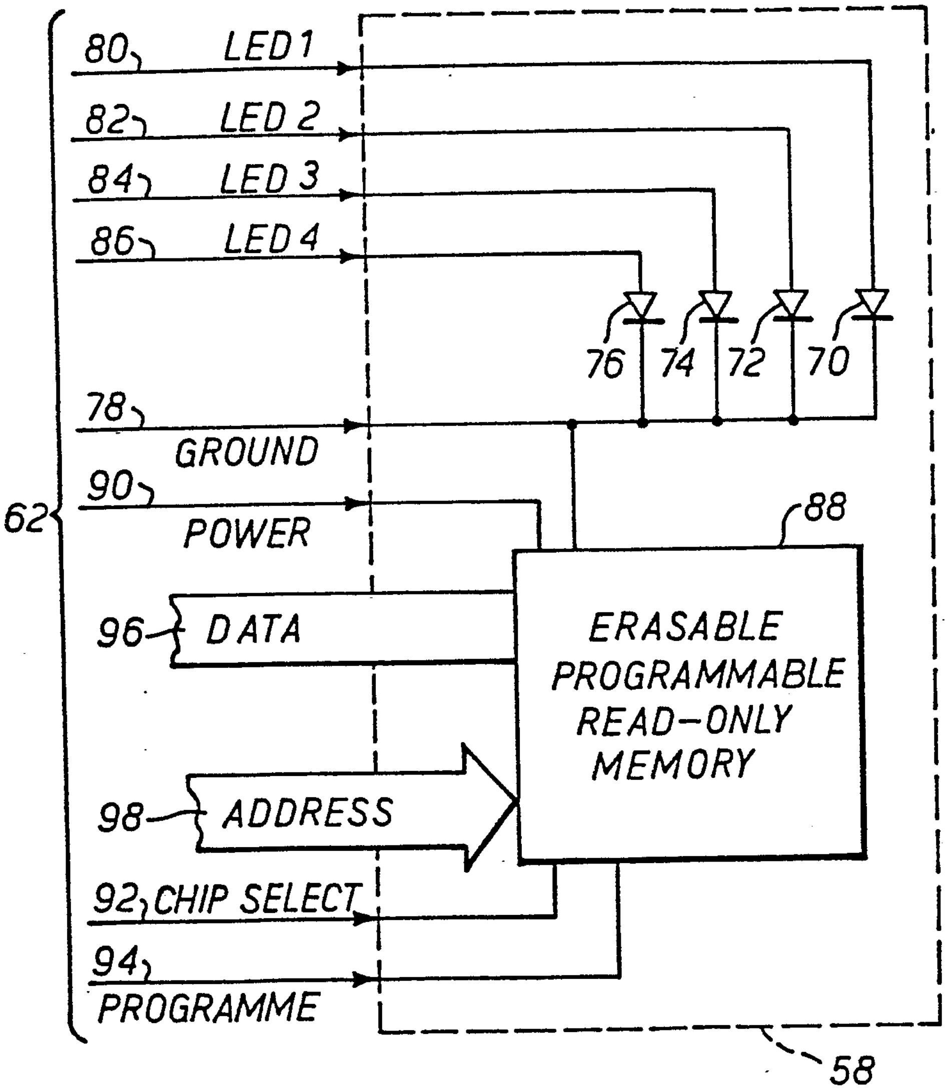
80
LED 1
82
LED 2
84
LED 3
86
LED 4
76
74
72
70
78
GROUND
90
POWER
62
88
96
DATA
ERASABLE PROGRAMMABLE READ-ONLY MEMORY
98
ADDRESS
92
CHIP SELECT
94
PROGRAMME
58

FIG. 5

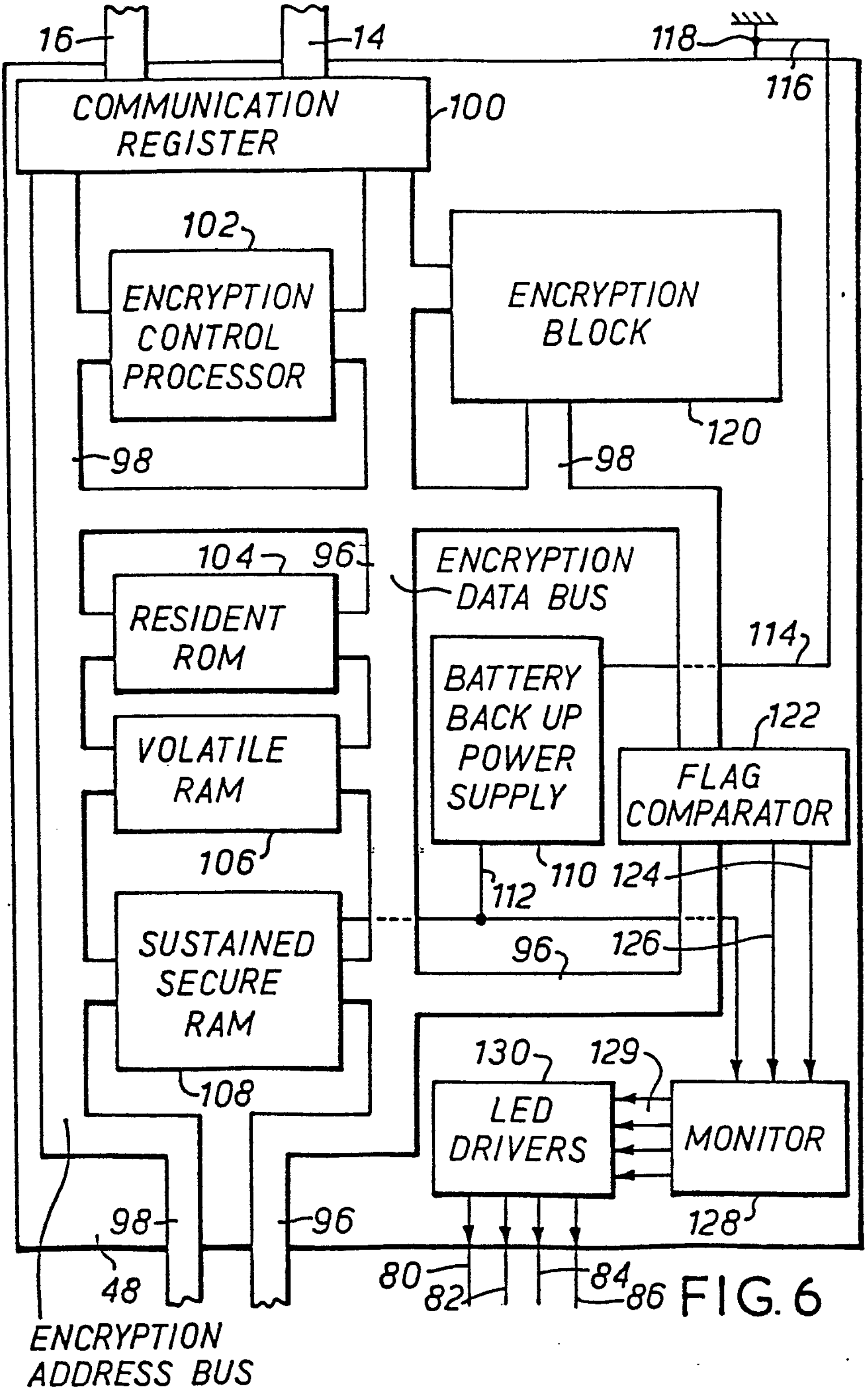
16
14
118
116
COMMUNICATION REGISTER
100
102
ENCRYPTION CONTROL PROCESSOR
ENCRYPTION BLOCK
98
120
98
104
96
RESIDENT ROM
ENCRYPTION DATA BUS
114
BATTERY BACK UP POWER SUPPLY
122
FLAG COMPARATOR
VOLATILE RAM
106
112
110
124
SUSTAINED SECURE RAM
96
126
130
129
108
LED DRIVERS
MONITOR
98
96
128
48
80
82
84
86
ENCRYPTION ADDRESS BUS

FIG. 6

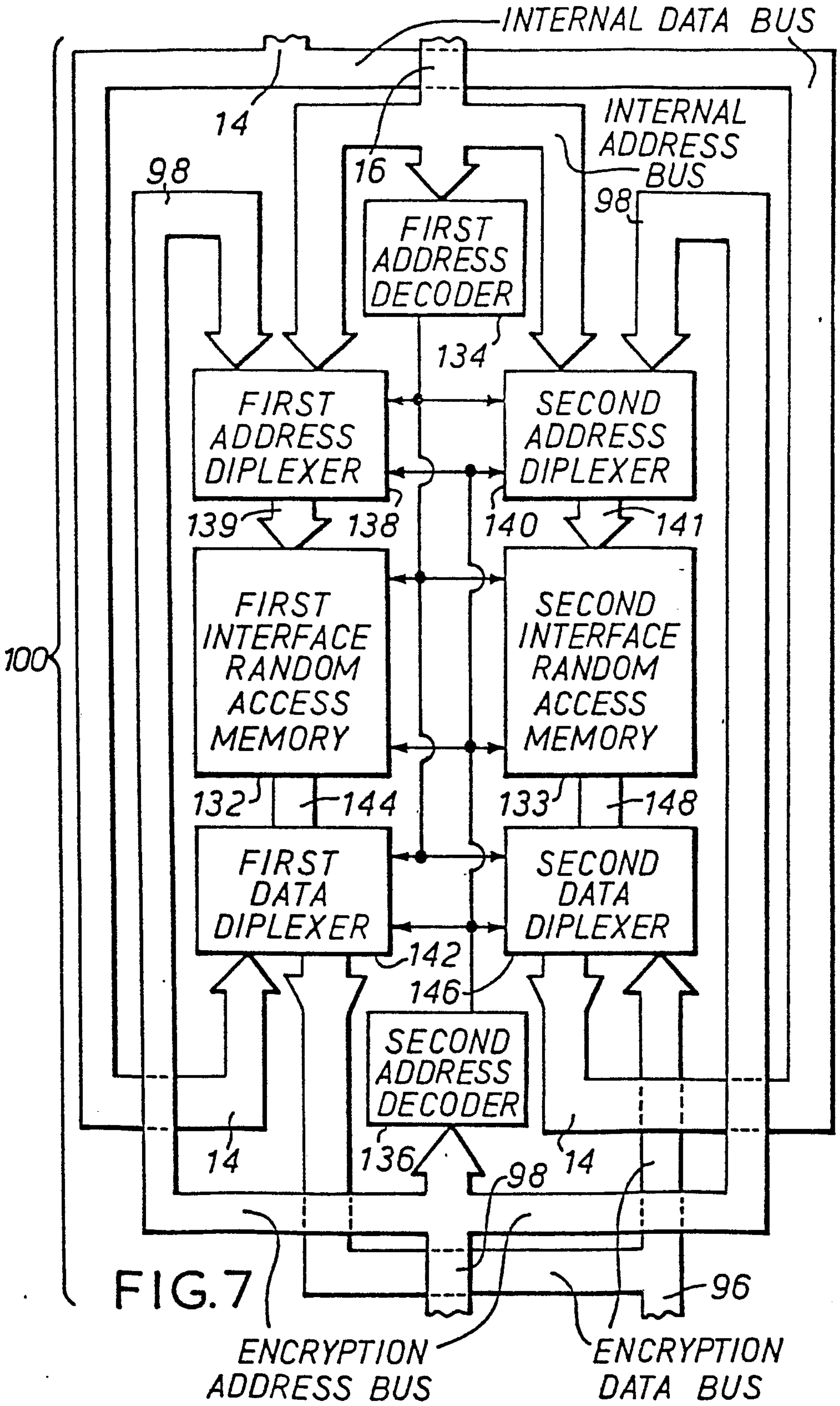
INTERNAL DATA BUS
14
INTERNAL ADDRESS BUS
16
98
98
FIRST ADDRESS DECODER
134
FIRST ADDRESS DIPLEXER
SECOND ADDRESS DIPLEXER
139
138
140
141
FIRST INTERFACE RANDOM ACCESS MEMORY
SECOND INTERFACE RANDOM ACCESS MEMORY
100
132
144
133
148
FIRST DATA DIPLEXER
SECOND DATA DIPLEXER
142
146
SECOND ADDRESS DECODER
136
14
14
98
96
ENCRYPTION ADDRESS BUS
ENCRYPTION DATA BUS

FIG.7

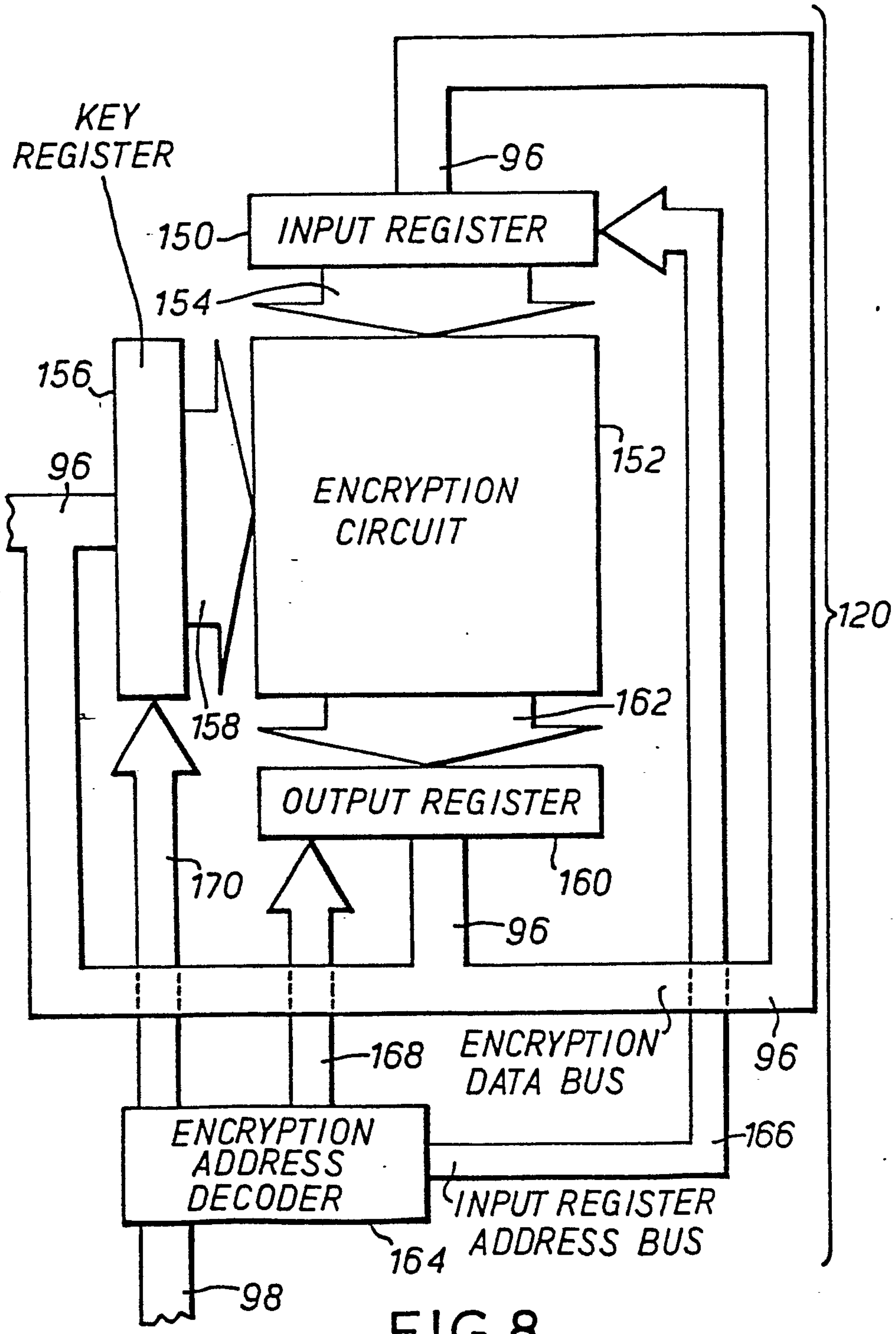
KEY REGISTER
INPUT REGISTER
150
96
154
156
96
ENCRYPTION CIRCUIT
152
120
158
162
OUTPUT REGISTER
160
170
96
168
ENCRYPTION DATA BUS
96
ENCRYPTION ADDRESS DECODER
166
INPUT REGISTER ADDRESS BUS
164
98

FIG. 8

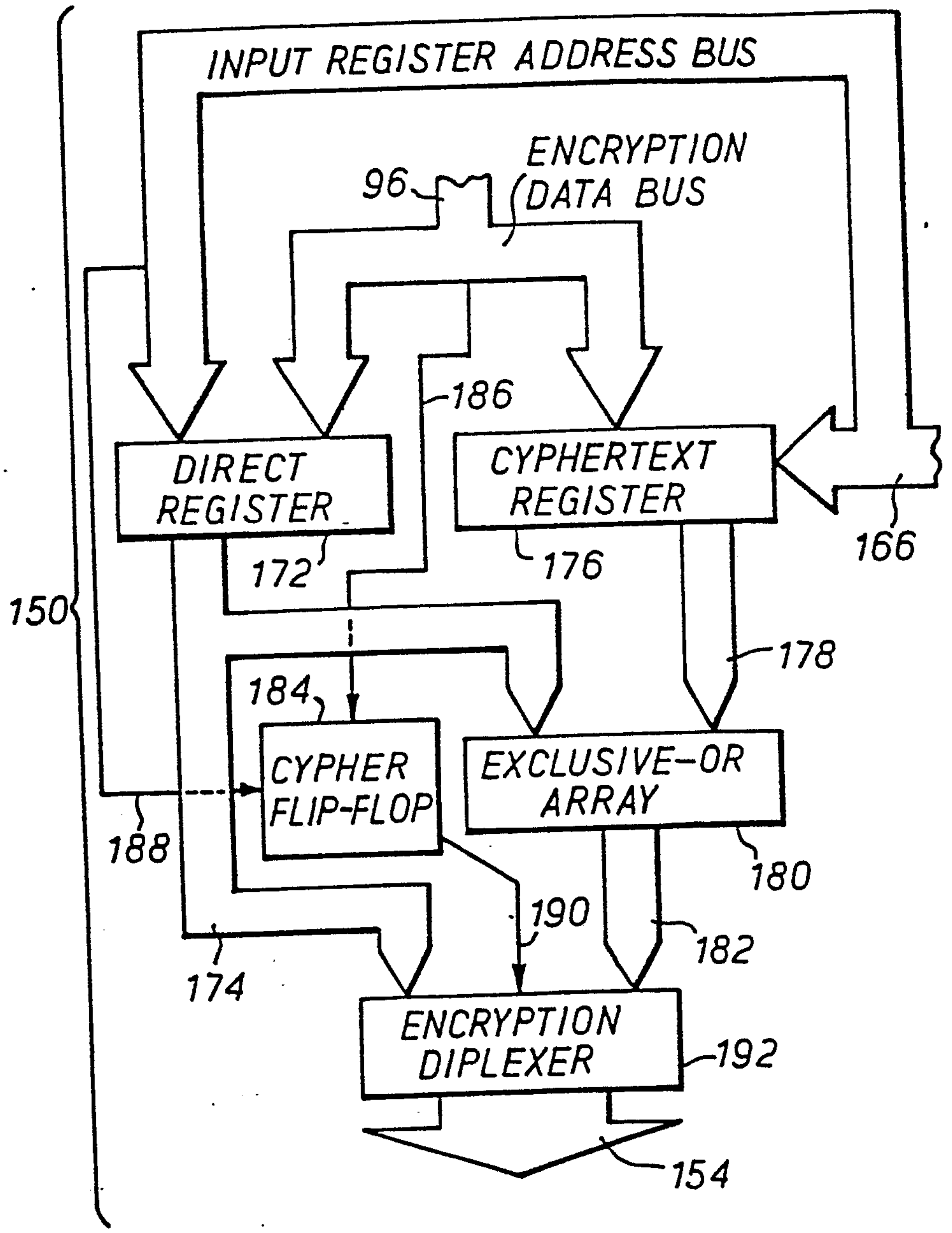
INPUT REGISTER ADDRESS BUS
ENCRYPTION DATA BUS
96
186
DIRECT REGISTER
CYPHERTEXT REGISTER
166
172
176
150
178
184
CYPHER FLIP-FLOP
EXCLUSIVE-OR ARRAY
188
180
190
182
174
ENCRYPTION DIPLEXER
192
154

FIG.9