OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

(12) (19) (CA) **Brevet-Patent**

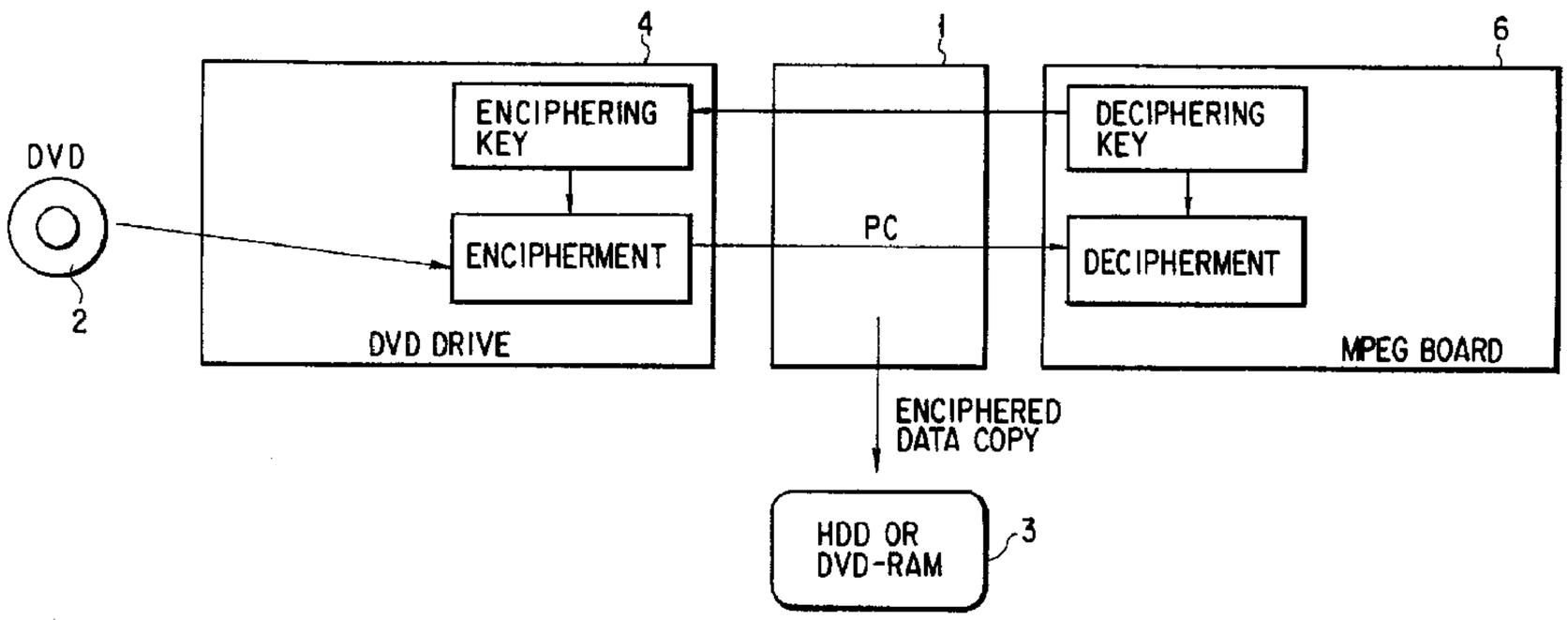
(11) (21) (C) **2,199,241**
(86) 1996/12/11
(87) 1997/07/09
(45) 2001/02/20

(72) NAKAMURA, Seiichi, JP
(73) Kabushiki Kaisha Toshiba, JP

(51) Int.Cl.[6] H04L 9/28, H04N 7/50
(30) 1996/01/08 (8-000985) JP

(54) **PROCEDE ET APPAREIL DE DOUBLAGE DE COMMANDE**

(54) **COPY CONTROL METHOD AND COPY CONTROL APPARATUS**



(57) Une carte MPEG 6 transmet à un lecteur de disque vidéo numérique 4 des données représentant une clé produite par elle-même. Le lecteur 4 produit des données de chiffrement en se basant sur les données reçues, chiffre les données obtenues d'un lecteur de disque vidéo numérique 2 en utilisant les données décrivant la clé et les transmet à la carte MPEG 6. Celle-ci déchiffre les données chiffrées reçues en utilisant les données décrivant la clé produite par elle-même.

(57) An MPEG board 6 issues the key data generated by the board to a DVD drive 4. The DVD drive 4 generates enciphering key data on the basis of the key data, enciphers the provided data read from a DVD 2 on the basis of the key data, and sends it to the MPEG board 6. The MPEG board 6 deciphers the enciphered provided data using the key data generated by the board.

A B S T R A C T

An MPEG board 6 issues the key data generated by the board to a DVD drive 4. The DVD drive 4 generates enciphering key data on the basis of the key data, enciphers the provided data read from a DVD 2 on the basis of the key data, and sends it to the MPEG board 6. The MPEG board 6 deciphers the enciphered provided data using the key data generated by the board.

D E S C R I P T I O N

COPY CONTROL METHOD AND COPY CONTROL APPARATUS

Technical Field

This invention relates to a copy control method and copy control apparatus applied to a data processing system having the function of reproducing and outputting data, such as movies or music, compressed by, for example, the MPEG 2 scheme, (hereinafter, referred to as provided data).

The present invention relates to a copy control method and copy control apparatus which, when recording and reproducing the data recorded on a large capacity recording medium, such as a CD-ROM or a DVD (digital video disk), as copied data, enable the reproduction of the copied data to be controlled by the specific control information recorded on the medium.

The present invention relates to a method of and apparatus for controlling the copying of data supplied through communication which are applied to a computer system having the function of receiving provided data, such as movies or music, via communication means and reproducing and outputting the provided data.

Background Art

For systems that reproduce and output the data, such as movies or music, compressed by, for example, the

MPEG 2 scheme (referred to as provided data) supplied from the film industry or the music industry, copy protection techniques are required to prevent unauthorized copying.

In the case of a system that causes a computer to process the aforementioned high-value added provided data, reproduce the data, and output the resulting data, it is essential to establish highly reliable copy protection techniques capable of preventing unauthorized copying reliably, not such copy protection techniques as would be broken by computer processing.

With conventional copy protection techniques of this type, copy protection data is also recorded on a recording medium, such as a CD-ROM on which the provided data has been recorded, and the copy protection data, together with the provided data, is read and transferred to a copy protection unit, which performs a copy protection process on the provided data, thereby preventing unauthorized copying.

In the case of the conventional copy protection techniques, however, the copy protection process is not carried out until the provided data recorded on the disk has been transferred to the copy protection unit. This permits the intentional unauthorized copying of the provided data in such a system configuration as has a computer unit acting as a transfer unit between the disk reading unit and reproducing unit.

As described above, with a conventional system where the provided data is exchanged via a computer, a highly reliable copy protection technique capable of preventing unauthorized copying reliably has not been established. This leads to the problem of permitting the unauthorized copying of all of the provided data, when a system that enables part of the provided data to be selectively read into the computer and used is constructed.

Disclosure of Invention

It is, accordingly, an object of the present invention to overcome the disadvantages in the prior art by providing a highly reliable copy control method and copy control apparatus which are capable of preventing unauthorized copying reliably even in a system where a computer intervenes in the exchange of data supplied from a large capacity recording medium or the like.

Furthermore, it is an object of the present invention to provide a highly reliable copy control method and copy control apparatus which allow the medium side to control use of copy arbitrarily on a provided data basis without showing the key data used in enciphering and deciphering to the computer unit even in a system where a computer intervenes in the exchange of data supplied from a large capacity recording medium, communication medium, or the like, and which always enable the use of the provided data through authorized

copying.

Since the present invention is such that, in a system where a device capable of copying, such as a computer, intervenes in the exchange of data supplied from a large capacity recording medium, communication medium, or the like, the data read from the medium is in the state enciphered by a specific key on the device capable of copying, such as a computer, it is possible to control the decision as to whether to reproduce the copied data arbitrarily.

Furthermore, according to the present invention, there is provided a highly reliable copy control method and copy control apparatus which allow the medium side to control reproduction of the copied data arbitrarily on a provided data basis without showing the key data used in enciphering and deciphering to a device capable of copying, such as a computer, in a system where the device capable of copying, such as a computer, intervenes in the exchange of data supplied from a large capacity recording medium, communication medium, or the like, and which always enable the use of the provided data through authorized copying. In the present invention, the action of recording the data supplied from the large capacity recording medium, communication medium, or the like in a storage device once, and reading and reproducing the recorded data is referred to as reproduction of the copied data.

Therefore in accordance with a first aspect of the present invention, there is provided a method of sharing a key for use in copy-protecting data between a data providing device and a data receiving device which respectively provides and receives data therebetween via communication means, the method comprising the steps of:

generating a first random key in the data providing device;

generating a second random key in the data receiving device;

exchanging the first and second random keys between the data providing device and the data receiving device via the communication means; and

generating a shared key using the first and second random keys generated and exchanged in each of the data providing device and the data receiving device.

In accordance with a second broad aspect of the present invention, there is provided a system for sharing a key for use in copy-protecting data between a data providing device and a data receiving device which respectively provides and receives data therebetween via communication means, the system comprising:

means, provided in the data providing device, for generating a first random key and transferring the first random key to the data receiving device via the communication means;

means, provided in the data receiving device, for generating a second random key and transferring the second random key to the data providing device via the communication means; and

means, provided in each of the data providing device and the data receiving device, for generating a shared key using the first and second random keys generated and transferred.

Stated differently, the present invention is characterized in that in the system, the drive and the data reproducing device recognize the copy permission level on the basis of the specific control data recorded on the large capacity recording medium, and when the recognized level is the level permitting the copied data to be reproduced, the data read by the drive is given to the data transfer means without enciphering, and when the recognized level is the level permitting only a specific data reproducing device to reproduce the copied data, the data read by the drive is enciphered using the key data generated by the data reproducing device that is to perform reproduction and the enciphered data is given to the data transfer, and when the recognized level is the level inhibiting the reproduction of the copied data, the drive and the data reproducing device temporarily generate mutually related key data using random numbers, thereby enabling only the data reproducing device having the related key data to reproduce the data read by the drive and disabling all of the data reproducing devices including one having the related key data from reproducing the copied data.

Furthermore, the present invention is characterized in that, in a system including a data providing device for providing data via communication means, a data reproducing device for receiving data from the data providing device via the communication means,

reproducing the received data, and outputting the reproduced data, and means for recording the data provided to the data reproducing device via the communication means as copied data, the data providing device receives key data from the data reproducing device and on the basis of the key data, enciphers the data to be given to the data reproducing device, thereby enabling only the data reproducing device having the key data used in enciphering to reproduce the copied data.

Furthermore, the present invention is characterized in that in the above system, the data providing device and the data reproducing device generate mutually related key data separately using random data, the data providing device enciphers the data to be sent to the data reproducing device using its self-generated enciphering key data, and the data reproducing device deciphers the data received from the data providing device using its self-generated deciphering key data, thereby enabling the data received via the communication means to be reproduced and disabling the copied data from being reproduced.

Furthermore, the present invention is characterized in that in the system, the data providing device sends copy permission data specifying the permission level of copied data to the data reproducing device, and the data reproducing device recognizes the permission level of copy of the provided data on the basis of the copy

permission data received from the data providing device and, when the recognized level is the permission level enabling the copied data to be reproduced, the data to be provided is given without enciphering to the data reproducing device via the communication means, and when the recognized level is the permission level enabling only a specific data reproducing device to reproduce the copied data, the key data is received from the data reproducing device and the provided data enciphered on the basis of the key data is given to the data reproducing device via the communication means, and when the recognized level is the permission level inhibiting the copied data from being reproduced, the data providing device and the data reproducing device temporarily generate mutually related key data using random data, and the provided data enciphered on the basis of the key data is given to the data reproducing device via the communication means.

With the aforementioned copy control mechanisms, even in a system where a device capable of copying, such as a computer, intervenes in the exchange of the data supplied by a large capacity recording medium, a communication medium, or the like, it is possible to construct a highly reliable system which enables the medium side to control the reproduction of the copied data on the provided data basis without showing the key data used in enciphering and deciphering to a device

capable of copying, such as a computer, and which always enables the provided data to be used in the form of authorized copy.

Brief Description of Drawings

FIG. 1 is a block diagram of a basic system configuration according to a first embodiment of the present invention;

FIG. 2 is a block diagram of a system configuration according to a second embodiment of the present invention;

FIG. 3 is a flowchart for the processing sequence in the second embodiment of the present invention;

FIG. 4 is a flowchart for the processing sequence in the second embodiment of the present invention;

FIG. 5 is a flowchart for the processing sequence in the second embodiment of the present invention;

FIG. 6 is a flowchart for the processing sequence in the second embodiment of the present invention;

FIG. 7 shows a data format to help explain the copy permission data (CGMS) in the media file management data block recorded on the data recording medium 20 in the embodiment of the present invention;

FIG. 8 is a conceptual diagram to help explain the way that the drive unit, CPU, and reproducing unit exchange various types of data for encoding and decoding between them in a third embodiment of the present invention;

FIG. 9 is a system block diagram in the third embodiment of the present invention; and

FIG. 10 is a flowchart showing the way that the drive unit, CPU, and reproducing unit exchange various types of data for encoding and decoding between them in the third embodiment of the present invention.

Best Mode of Carrying Out the Invention

Hereinafter, referring to the accompanying drawings, embodiments of the present invention will be explained.

First Embodiment

FIG. 1 is a block diagram showing the basic system configuration according to a first embodiment of the present invention. The figure illustrates an embodiment that permits a first-generation copy in such a manner that, with the provided data, such as movies or music, recorded on a large capacity storage medium (DVD2) being the object of copy protection, only a data reproducing unit (MPEG board 6) having the enciphered key data is allowed to copy and reproduce the data read by a drive (DVD drive 4) by enciphering the provided data supplied from the drive (DVD drive 4) to data transfer means (PC)1, using the key data generated in the data reproducing unit (MPEG board 6).

In FIG. 1, numeral 1 indicates a computer unit (PC) acting as data transfer means that supplies the provided data read by the drive to the data reproducing unit. The computer unit selectively takes in the copy-permitted

provided data read by the drive, stores it in an external storage unit 3, such as an HDD or a DVD-RAM, and enables processes, including editing and correction.

Numeral 2 indicates a DVD disk on which provided data, such as movies or music, the object of copy protection, has been recorded. On the DVD 2, not only the provided data is compressed and recorded by, for example, the MPEG 2 scheme, but also the copy permission data (CGMS) as shown in FIG. 7 is recorded in part of the media file management data block so as to correspond to the provided data.

Numeral 4 indicates a drive unit that reads the data from the DVD 2. The drive unit is referred to as the DVD drive. The DVD drive 4 has the function of receiving the key data generated in the data reproducing unit and enciphering the provided data read by the DVD 2 using the key data. A concrete configuration of the function is shown in FIG. 2.

Numeral 6 indicates a data reproducing unit that receives the provided data read by the DVD drive 4 via the computer unit (PC) 1 and performs a reproducing and outputting processes. The data reproducing unit is referred to as an MPEG board. The MPEG board 6 is provided with a MPEG 2 decoder and obtains the reproduced output data by decoding the provided data compressed by the MPEG 2 scheme received via the computer unit (PC) 1. Moreover, the MPEG board 6 has

the function of not only creating key data and sending the key data to the DVD drive 4 but also deciphering the provided data using the key data. A concrete configuration of the function is shown in FIG. 2.

In the configuration of FIG. 1, the MPEG board 6 not only issues the key data generated at the board 6 to the DVD drive 4 but also holds the key data as a deciphering key.

The DVD drive 4 generates an enciphering key using the key data and enciphers the provided data read by the DVD 2, and thereafter sends the enciphered data to the MPEG board 6 via the computer unit (PC) 1.

The MPEG board 6 receives the provided data enciphered by the DVD drive 4 via the computer unit (PC) 1 and decodes the enciphered data using the deciphering key.

Providing such a copy control mechanism enables only the MPEG board 6 having the key data used in enciphering to record and reproduce the data read by the DVD drive 4 as copied data.

Specifically, when the DVD drive 4 performs one type of enciphering on a type of (or a piece of) provided data, even if a plurality of data reproducing units are connected via a data transfer unit, those except for the data reproducing unit having the key data used in enciphering cannot reproduce the copied data.

In the concrete configuration, the key data sent

from the MPEG board 6 to the DVD drive 4 is enciphered. In addition, in the concrete configuration, exclusive control of copy in the embodiment is selectively effected according to the copy permission data (CGMS). As a concrete example, in FIG. 7, when b0 and b1 in the CGMS are "01," the aforementioned exclusive control of copy is possible.

Second Embodiment

FIG. 2 is a block diagram showing a system configuration in a second embodiment of the present invention. The second embodiment realizes a system having the function of, according to the copy permission data (CGMS) recorded on a large capacity recording medium, selectively switching between the copy permission level of copy free at which all of the data reproducing units are allowed to reproduce the copied data obtained by once recording the provided data read by the drive, the level at which only a specific data reproducing unit is allowed to reproduce the copied data, and the level at which none of the data reproducing units are allowed to reproduce the copied data.

In FIG. 2, reference symbols 10 and 10A indicate the component parts corresponding to the computer unit (PC) 1 shown in FIG. 1: 10 indicates the CPU of a computer body that supervises control of the entire system, and 10A indicates the system bus for the entire system. Under the control of the CPU 10, the copy

control processing as shown in FIGS. 3 to 6 is executed. The CPU 10 selectively takes in the provided data permitted to copy read by a drive unit 40 from a data recording medium 20, stores it in a storage unit 30, and enables processes, including editing and correction.

Numeral 20 indicates a data recording medium corresponding to a DVD 2. On the data recording medium, not only the provided data is compressed and recorded by the MPEG 2 scheme, but also the copy permission data (CGMS) as shown in FIG. 7 is recorded in part of the media file management data block so as to correspond to the provided data.

Numeral 30 indicates a storage unit corresponding to the external storage unit 3 of FIG. 1. The storage unit is used to store, edit, and correct the copied data.

Numeral 40 indicates a drive unit corresponding to the DVD drive 4 of FIG. 1. The drive unit reads the data from the data recording medium 20. The drive unit comprises cipher generator units 41, 44, registers 42, 43, 45, 48, 51 for storing an enciphering key, a reading unit 46, enciphering units 47, 49, and a deciphering unit 50.

The cipher generator unit 41 generates an enciphering key (1) on the basis of a random value obtained from a random number generator.

The register 42 holds the enciphering key (1) generated by the cipher generator unit 41. The register

43 holds the enciphering key (2) received from a reproducing unit 60 via the system bus 10A.

The cipher generator unit 44 generates an enciphering key (3) using the enciphering key (1) and enciphering key (2). The register 45 holds the enciphering key (3) generated by the cipher generator unit 44.

The reading unit 46 reads the data recorded on the data recording medium 20. Here, the reading unit reads not only the provided data, such as movies or music, the object of copy control, but also the copy permission data (CGMŞ) as shown in FIG. 7, indicating the copy permission level of the provided data.

According to the copy permission data (CGMS), the enciphering unit 47 enciphers the provided data read from the data recording medium 20 using the enciphering key (3) stored in the register 45 or the provided data enciphering key (5) stored in the register 51, or sends the provided data without enciphering it, to the reproducing unit 60 via the system bus 10A.

The register 48 holds the copy permission data (CGMS) read from the data recording medium 20. The enciphering unit 49 enciphers the copy permission data (CGMS) stored in the register 48 and sends the enciphered data to the reproducing unit 60 via the system bus 10A.

The deciphering unit 50 deciphers the enciphered

provided data enciphering key (5) unique to the unit received from the reproducing unit 69. The register 51 holds the enciphering key (5) deciphered by the deciphering unit 50.

Numeral 60 is a unit that reproduces the provided data and corresponds to the MPEG board 6. The reproducing unit includes an MPEG decoder and obtains the reproduced output data by decoding the provided data compressed by the MPEG 2 scheme received via the system bus 10A. Here, the reproducing unit comprises cipher generator units 61, 64, registers 62, 63, 65, 69, 71, 72 for storing enciphering keys, deciphering units 66, 67, an MPEG 2 decoder 68, and an enciphering unit 70.

The cipher generator unit 61 generates an enciphering key (2) on the basis of a random value obtained from a random number generator.

The register 62 holds the enciphering key (1) received from drive unit 40 via the system bus 10A. The register 63 holds the enciphering key (2) generated at the cipher generator unit 61.

The cipher generator unit 64 generates an enciphering key (4) using the enciphering key (1) and enciphering key (2). The register 65 holds the enciphering key (4) generated by the cipher generator unit 64.

The deciphering unit 66 decodes the enciphered copy permission data (CGMS) received from the drive unit 40

via the system bus 10A in the computer body.

According to the copy permission data (CGMS) stored in the register 71, the deciphering unit 67 deciphers the provided data received from the drive unit 40 via the system bus 10A in the computer body, using the enciphering key (4) stored in the register 65 or the provided data deciphering key (6) stored in the register 72, or sends the provided data without deciphering it, to the MPEG 2 decoder 68.

The MPEG 2 decoder 68 decodes the provided data deciphered at the deciphering unit 67 and sends to the controller 80 the provided data that can be reproduced and outputted.

The register 69 holds the provided data enciphering key (5) unique to the unit. The enciphering unit 70 enciphers the provided data enciphering key (5) unique to the unit stored in the register 69 and sends the enciphered data to the drive unit 40.

The register 71 holds the copy permission data (CGMS) deciphered at the deciphering unit 66.

The register 72 holds the provided data deciphering key (6) paired with the provided data enciphering key (5) (e.g., both the keys have values in common) unique to the unit stored in the register 69.

Numeral 80 indicates a display controller that displays the provided data outputted from the MPEG 2 decoder 68 on a display unit 81.

The key values in the registers 45, 65 are cleared once at least at the beginning or end of reproduction and are rewritten. The key values in the registers 69, 72 may be rewritten at the beginning of reproduction, for example, instead of being fixed values.

FIGS. 3 to 6 are flowcharts showing the processing sequence in the second embodiment of the present invention. FIGS. 3 and 4 are flowcharts showing the sequence of setting various types of key data for the enciphering and deciphering processes. FIGS. 5 and 6 are flowcharts showing the copy control processing sequence in reading the provided data.

FIG. 7 illustrates a data format to help explain the copy permission data (CGMS) in the media file management data block recorded on the data recording medium 20. Here, when b0, b1 in the CGMS are "00," all of the reproducing units 60 are allowed to reproduce the copied data; when b0, b1 are "01," only the reproducing unit used in reading the provided data is allowed to reproduce the copied data exclusively; and when b0, b1 is "11," none of the reproducing unit is allowed to reproduce the provided data.

Now, the operation of the second embodiment of the present invention will be described by reference to FIGS. 2 to 7.

First, the process of setting various types of key data for the enciphering and deciphering processes will

be described by reference to the flowcharts shown in FIGS. 3 and 4.

As a result of system start-up by a reproduction instruction, the cipher generator unit 41 in the drive unit 40 generates the enciphering key (1) on the basis of a random value (step 40a in FIG. 3).

The enciphering key (1) generated by the cipher generator unit 41 is not only stored in the register 42 but also set in the register 62 in the reproducing unit 60 under the control of the CPU 10 (step 10a in FIG. 3 and step 60a in FIG. 4).

The cipher generator unit 61 in the reproducing unit 60 generates an enciphering key (2) on the basis of a random value (step 60b in FIG. 4).

The enciphering key (2) generated at the cipher generator unit 61 is not only stored in the register 63 but also set in the register 43 in the drive unit 40 under the control of the CPU 10 (steps 10b and 40b in FIG. 3).

The cipher generator unit 44 in the drive unit 40 generates an enciphering key (3) using the enciphering key (1) stored in the register 42 and the enciphering key (2) stored in the register 43 and then sets it in the register 45 (step 40c in FIG. 3).

The cipher generator unit 64 in the drive unit 60 generates an enciphering key (4) using the enciphering key (1) stored in the register 62 and the enciphering

key (2) stored in the register 63 and then sets it in the register 65 (step 60c in FIG. 4).

The reading unit 46 in the drive unit 40 reads the copy permission data (CGMS) from the data recording medium 20 and sets it in the register 48 (step 40d in FIG. 3).

The enciphering unit 49 enciphers the copy permission data (CGMS) set in the register 48, using the enciphering key (3) stored in the register 45 (step 40e in FIG. 3). The enciphered copy permission data (CGMS) is given to the deciphering unit 66 in the reproducing unit 60 under the control of the CPU 10 (step 10c in FIG. 3).

The deciphering unit 66 deciphers the enciphered copy permission data (CGMS) received from the drive unit 40, using the enciphering key (4) stored in the register 65, and then sets it in the register 71 (step 60d in FIG. 4).

The control unit (not shown) in the reproducing unit 60 determines the contents of the copy permission data (CGMS) stored in the register 71. When determining that b0, b1 in the copy permission data (CGMS) are "01" and therefore recognizing that only the reproducing unit used in reading the provided data is allowed to reproduce the copied data exclusively, the control unit starts up the enciphering unit 70 (step 60e (Yes) in FIG. 4).

Then, the enciphering unit 70 enciphers the provided data enciphering key (5) unique to the unit fixedly stored in the register 69, using the enciphering unit (4) stored in the register 65 (step 60g in FIG. 4).

When b0, b1 in the copy permission data (CGMS) are not "01," dummy data (a null value) is generated in place of the provided data enciphering key (5) (step 60f in FIG. 4).

The CPU 10 transfers the enciphered provided data enciphering key (5) unique to the unit or the dummy data substituting for that key to the deciphering unit 50 in the drive unit 40 (step 10d in FIG. 3).

The deciphering unit 50 deciphers the enciphered provided data enciphering key (5) unique to the unit received from the reproducing unit 60 and then sets the deciphered data in the register 51.

The above process completes the process of setting various types of key data for the enciphering and deciphering processes.

Next, the copy control process in reading the provided data will be described by reference to the flowcharts in FIGS. 5 and 6.

The CPU 10 gives the drive unit 40 an instruction to read the provided data (step S1 in FIG. 5).

Receiving a read instruction from the CPU 10, the control unit (not shown) in the drive unit 40 starts up the reading unit 46. The reading unit 46 provides drive

control of the data recording medium 20 and reads the provided data (MPEG 2 data) and the copy permission data (CGMS) from the data recording medium 20 (step S2 in FIG. 5).

The copy permission data (CGMS) read from the data recording medium 20 is stored in the register 48 and then is supplied to the enciphering unit 47.

The enciphering unit 47 determines the contents of the copy permission data (CGMS) stored in the register 48. When determining that b0, b1 in the CGMS are "00," the enciphering unit outputs (passes) the provided data directly without enciphering the provided data. When they are "01," the enciphering unit enciphers the provided data using the provided data enciphering key (5) unique to the unit stored in the register 51. When they are "11," the enciphering unit enciphers the provided data using the enciphering key (3) stored in the register 45 (steps S3 to S7 in FIG. 5).

The provided data (MPEG 2 data) outputted from the enciphering unit 47 is transferred to the deciphering unit 67 in the reproducing unit 60 via the system bus 10A (step S8 in FIG. 5).

When receiving the provided data (MPEG 2 data) from the enciphering unit 47 in the drive unit 40, the deciphering unit 67 in the reproducing unit 60 determines the contents of the copy permission data (CGMS) stored in the register 71. When determining that b0, b1

in the CGMS are "00," the deciphering unit outputs (passes) the provided data directly without deciphering the provided data. When they are "01," the deciphering unit deciphers the provided data using the provided data enciphering key (6) unique to the unit stored in the register 72. When they are "11," the deciphering unit deciphers the provided data using the enciphering key (4) stored in the register 65 (steps S11 to S16 in FIG. 5).

The provided data (MPEG 2 data) outputted from the deciphering unit 67 is decoded by the MPEG 2 decoder 68. Then, the decoded data is sent to the display controller 80 and is displayed on the display unit 81 (step S17 in FIG. 5).

In this case, when b0, b1 in the copy permission data (CGMS) are "00," the CPU 10 can reproduce and output the copied data arbitrarily without specifying a reproducing unit, by loading the provided data (MPEG 2 data) into the storage unit 30.

When b0, b1 in the copy permission data (CGMS) are "01," loading the provided data (MPEG 2 data) into the storage unit 30 enables only the reproducing unit 60 having the provided data enciphering key (6) unique to the unit paired with the provided data enciphering key (5) unique to the unit used in the enciphering process to reproduce the copied data.

In this case, when the copied data, together with

the enciphering key (6) stored in the register 72, is stored in the storage unit 30, the corresponding copied data can be reproduced by reading the stored key data and resetting it in the register 72, even if the key value in the register 72 is rewritten in a later reproducing process.

When b0, b1 in the copy permission data (CGMS) is "11," the copied data cannot be deciphered because the value of the enciphering key (4) has already changed at the time of reproduction, even if the provided data (MPEG 2 data) is loaded as the copied data into the storage unit 30. As a result, none of the reproducing units can reproduce the copied data.

By setting new key values in the registers 69, 72 or the registers 45, 65 each time the contents of the copy permission data (CGMS) are changed, a highly reliable copy protection mechanism enabling accurate permission control on a given data amount basis can be implemented.

As described above, with the configuration that enables each item of the provided data (each title of the movies or music) to be enciphered and prevents a computer or the like from reading the data easily, highly reliable copy control of provided data most suitable for computer processing is established.

Since only the data reproducing unit used in reading is allowed to reproduce a copy of the data read

by a computer or the like, this enables authorized use of the copied data and prevents unauthorized use of the copied data.

Third Embodiment

Hereinafter, a third embodiment of the present invention will be explained by reference to FIGS. 8 to 10.

First, a CPU 10 sends "START AUTHENTICATION" command to a drive unit 90 (step S41). In response to the START AUTHENTICATION" command, the RANID generator unit in the drive unit 90 causes a random generator to generate a random number and sends the generated random number as RANID to the CPU 10 (steps S21, S23). The RANID is an ID for identifying one MPEG board, when there are a plurality of MPEG boards acting as reproducing units, for example. The CPU 10 acquires the RANID from the drive unit 90 and sends it to the reproducing unit 120. The reproducing unit 120 causes a CHKEY 1 generator unit 121 to encipher the RANID using algorithm A, generate CHKEY 1, hold it, and send it to the CPU 10 (steps S71, S73). The CHKEY 1 is a key for identifying an MPEG board or a disk drive unit. The CPU 10 acquires the CHKEY 1 from the reproducing unit 120 and transfers it to the drive unit 90 (step S43). The drive unit 90 causes an enciphering unit 95 to encipher the CHKEY 1 using algorithm B, generate KEY 1, hold it, and send it to the CPU 10 (steps S25, 27). The CPU 10

acquires the KEY 1 from the drive unit 90 and transfers it to the reproducing unit 120. The reproducing unit 120 causes a cipher generator unit 123 to encipher the held CHKEY 1 using algorithm B, generate KEY 1, and compare it with the KEY 1 acquired from the CPU. If the comparison result shows that they coincide with each other, this means that the authentication of the drive unit by the reproducing unit has finished correctly.

Furthermore, the drive unit 90 causes the cipher generator unit 99 to encipher the held KEY 1 using algorithm C, generate KEY 2, hold it, and send it to the CPU (step S29). The CPU 10 acquires the CHKEY 2 from the drive unit 90 and transfers it to the reproducing unit 120. If the comparison result at step S75 shows that they coincide with each other, the reproducing unit 120 causes the cipher generator unit 129 to encipher the CHKEY 2 sent from the CPU using algorithm D, generate KEY 2, hold the KEY 2, and send it to the CPU 10. The CPU 10 acquires the KEY 2 from the reproducing unit 120 and transfers it to the drive unit (step S49). The drive unit causes the cipher generator unit 101 to encipher the held KEY 2 using algorithm D and generate KEY 2 and causes a comparison circuit 105 to compare the KEY 2 with the KEY 2 acquired from the CPU (steps S29, S31). If the comparison result shows that they coincide with each other, this means that the drive unit has authenticated the reproducing unit properly. As a

result, the mutual authentication between the drive unit and the reproducing unit has been completed. Then, the drive unit causes the enciphering unit 113 to encipher the DISK KEY and the TITLE KEY using the KEY 1, KEY 2, and algorithm and send the enciphered data to the CPU (step S33). The CPU acquires the enciphered DISK KEY and TITLE KEY from the drive unit and sends it to the reproducing unit (step S51). The reproducing unit causes the deciphering unit 137 to decipher the enciphered DISK KEY and TITLE KEY using the KEY 1, KEY 2, and algorithm E. Explanation of the copy permission data will not be given, because it is the same as in the second embodiment.

As described above, with the embodiment of the present invention, it is possible to construct a highly reliable system which allows the medium side to control use of copy arbitrarily on a provide data basis without showing the key data used in enciphering and deciphering to a computer unit even in a system where the computer unit intervenes in the exchange of data supplied from a large capacity recording medium or the like, and which always enables use of the provided data through authorized copying.

While in the embodiment, a large capacity disk, such as a DVD or a CD-ROM, requiring a drive unit has been taken as an example of a data providing medium, the present invention may be applied to a system

configuration where a data providing medium is provided externally via, for example, a communication channel, in the same manner as in the above embodiment. This configuration can be implemented easily by providing an external data providing unit that makes communication with the individual component parts of the drive unit 40 except for the reading unit in FIG. 2 and by replacing the signal paths represented by broken lines in FIG. 2 with communication paths.

While in the embodiment, the copy permission data (CGMS) and the provided data enciphering key (5) unique to the unit are enciphered and then transferred, they are not necessarily enciphered. They may not be enciphered, depending on the degree of reliability required.

While in the second embodiment, the drive unit 40 and reproducing unit 60 each generate the primary key data on the basis of random data, the present invention is not restricted this. For instance, at least either the drive unit 40 or the reproducing unit 60 may generate the primary key data on the basis of random data, and on the basis of the primary key data, the drive unit 40 and reproducing unit 60 each generate temporary secondary key data by themselves. The essential thing is that the drive unit and data reproducing unit have only to temporarily generate the mutually related key data using random data.

Furthermore, while in the embodiment, the provided data enciphering key (5) unique to the unit and the provided data deciphering key (6) unique to the unit are provided independently in the reproducing unit 60 and are stored in the registers 69 and 79 separately, the present invention is not limited to this. For instance, common key data may be used for both of the provided data enciphering key (5) and deciphering key (6) unique to the unit. The essential thing is that the reproducing unit 60 has only to grasp the enciphering scheme of the inputted provided data and the contents of the enciphering key in order to decipher the inputted provided data.

Still furthermore, while in the second embodiment, the copy control mechanism which permits a first-generation copy in such a manner that only the reproducing unit 60 having the provided data enciphering key (6) unique to the unit paired with the provided data enciphering key (5) unique to the unit used in enciphering is allowed to reproduce the copy, and the copy control mechanism which prevents all of the reproducing units from reproducing the copy are used selectively, the present invention is not limited to this. For instance, the copy permission modes may be combined arbitrarily as follows: the copy permission mode of free copy and the copy permission mode that prevents all of the reproducing units from reproducing

the copy may be combined; or the copy permission mode of free copy and the copy permission mode of first-generation copy may be combined.

Still furthermore, while in the embodiments, the system where a computer intervenes in the exchange of the data provided from a large capacity recording medium, communication medium, or the like has been used, the present invention is not restricted to this, but may be applied to a system configuration where a computer does not intervene directly in the exchange of the provided data. For instance, the copy control mechanism may be applied to the interface section between units capable of reproducing the provided data between a drive that reads the provided data from an MD, a CD-ROM, or a DVD, or a communication medium having the function of transmitting the provided data, and a unit that reproduces the read-out data.

Still furthermore, while in the embodiments, the provided data, such as movies or music, compressed by the MPEG 2 scheme has been used, the present invention is not limited to this. For instance, the present invention may be applied to a system configuration capable of reproducing the data compressed by the MPEG 1 or MPEG 4 scheme.

While in the embodiments, the provided data recorded on the recording medium has been raw data, all of the provided data may be enciphered and recorded on

a recording medium or only part of the provided data may be enciphered and recorded on a recording medium.

Industrial Applicability

It is possible to provide a highly reliable copy control method and copy control apparatus which allow the medium side to control use of copy arbitrarily on a provided data basis without showing the key data used in enciphering and deciphering to a device capable of copying, such as a computer, in a system where a device capable of copying, such as a computer, intervenes in the exchange of data supplied from a large capacity recording medium, communication medium, or the like, and which always enable use of the provided data through authorized copying.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of sharing a key for use in copy-protecting data between a data providing device and a data receiving device which respectively provides and receives data therebetween via communication means, the method comprising the steps of:

generating a first random key in the data providing device;

generating a second random key in the data receiving device;

exchanging the first and second random keys between the data providing device and the data receiving device via the communication means; and

generating a shared key using the first and second random keys generated and exchanged in each of the data providing device and the data receiving device.

2. The method according to claim 1, further comprising the step of transferring data which is enciphered using at least the shared key from the data providing device to the data receiving device via the communication means.

3. The method according to claim 1, further comprising the step of transferring copy permission data from the data providing device to the data receiving device via the communication means.

4. The method according to claim 3, wherein the copy permission data indicates one of conditions that:

any device is allowed to reproduce a copy;

only the data receiving device is allowed to reproduce a copy; and

no device is allowed to reproduce a copy.

5. The method according to claim 1, wherein the data providing device is a DVD-ROM drive.

6. The method according to claim 1, wherein the data receiving device is a MPEG decoder.

7. The method according to claim 1, wherein the first random key is generated in response to a request from the data receiving device.

8. A method of sharing a key for use in copy-protecting data between a data providing device and a data receiving device which respectively provides and receives data there between via communication means, the method comprising the steps of:

generating a first random key in the data providing device;

generating a second random key in the data receiving device;

exchanging the first and second random keys between the data providing device and the data receiving device via the communication means;

generating a shared key using the first and second random keys generated and exchanged in each of the data providing device and the data receiving device;

generating an exchanged key for use in handling copy-protected contents data to be transferred between the data providing device and the data receiving device via the communication means;

transforming the exchanged key at one of said data receiving device and data providing device, using the shared key and transferring the transformed exchanged key via the communication means to the other of said data receiving device and data providing device; and

reverse-transforming the transformed exchanged key using the shared key in the other of said data receiving device and data providing device.

9. The method according to claim 8, wherein said transforming step includes a step of enciphering the exchanged key using the shared key, and said reverse-transforming step includes a step of deciphering the transformed exchanged key using the shared key.

10. The method according to claim 8, wherein the exchanged key includes a unique key, which is generated in

the data receiving device, for enciphering/deciphering the copy-protected contents data.

11. The method according to claim 8, further comprising the step of transferring data which is enciphered using at least the shared key from the data providing device to the data receiving device via the communication means.

12. The method according to claim 8, wherein the exchanged key includes copy permission data to be transferred from the data providing device to the data receiving device via the communication means.

13. The method according to claim 12, wherein the copy permission data indicates one of conditions that:

any device is allowed to reproduce a copy;

only the data receiving device is allowed to reproduce a copy; and

no device is allowed to reproduce a copy.

14. The method according to claim 8, wherein the data providing device is a DVD-ROM drive.

15. The method according to claim 8, wherein the data receiving device is an MPEG decoder.

16. The method according to claim 8, wherein the first random key is generated in response to a request from the data receiving device.

17. A system for sharing a key for use in copy-protecting data between a data providing device and a data receiving device which respectively provides and receives data therebetween via communication mean, the system comprising:

means, provided in the data providing device, for generating a first random key and transferring the first random key to the data receiving device via the communication means;

means, provided in the data receiving device, for generating a second random key and transferring the second random key to the data providing device via the communication means; and

means, provided in each of the data providing device and the data receiving device, for generating a shared key using the first and second random keys generated and transferred.

18. The system according to claim 17, further comprising means for transferring data which is enciphered using at least the shared key from the data providing device to the data receiving device via the communication means.

19. The system according to claim 17, further comprising means for transferring copy permission data from

the data providing device to the data receiving device via the communication means.

20. The system according to claim 19, wherein the copy permission data indicates one of conditions that:

any device is allowed to reproduce a copy;

only the data receiving device is allowed to reproduce a copy; and

no device is allowed to reproduce a copy.

21. The system according to claim 17, wherein the data providing device is a DVD-ROM drive.

22. The system according to claim 17, wherein the data receiving device is an MPEG decoder.

23. The system according to claim 17, wherein the first random key is generated in response to a request from the data receiving device.

24. A system for sharing a key for use in copy-protecting data between a data providing device and a data receiving device which respectively provides and receives data therebetween via communication means, the system comprising:

means, provided in the data providing device, for generating a first random key and transferring the first random key to the data receiving device via the communication means;

means, provided in the data receiving device, for generating a second random key and transferring the second random key to the data providing device via the communication means;

means, provided in each of the data providing device and the data receiving device, for generating a shared key using the first and second random keys generated and transferred;

means for generating an exchanged key for use in handling copy-protected contents data to be transferred between the data providing device and the data receiving device via the communication means;

means for transforming the exchanged key at one of said data receiving device and data providing device, using the shared key and transferring the transformed exchanged key via the communication means to the other of said data receiving device and data providing device; and

means for reverse-transforming the transformed exchanged key using the shared key in the other of said data receiving device and data providing device.

25. The system according to claim 24, wherein said transforming means includes means for enciphering the exchanged key using the shared key, and said reverse-transforming means includes means for deciphering the transformed exchanged key using the shared key.

26. The system according to claim 24, wherein the exchanged key includes a unique key, which is generated in the data receiving device, for enciphering/deciphering the copy-protected contents data.

27. The system according to claim 24, further comprising means for transferring data which is enciphered using at least the shared key from the data providing device to the data receiving device via the communication means.

28. The system according to claim 24, wherein the exchanged key includes copy permission data to be transferred from the data providing device to the data receiving device via the communication means.

29. The system according to claim 28, wherein the copy permission data indicates one of conditions that:

any device is allowed to reproduce a copy;

only the data receiving device is allowed to reproduce a copy; and

no device is allowed to reproduce a copy.

30. The system according to claim 24, wherein the data providing device is a DVD-ROM drive.

31. The system according to claim 24, wherein the data receiving device is an MPEG decoder.

32. The system according to claim 24, wherein the first random key is generated in response to a request from the data receiving device.

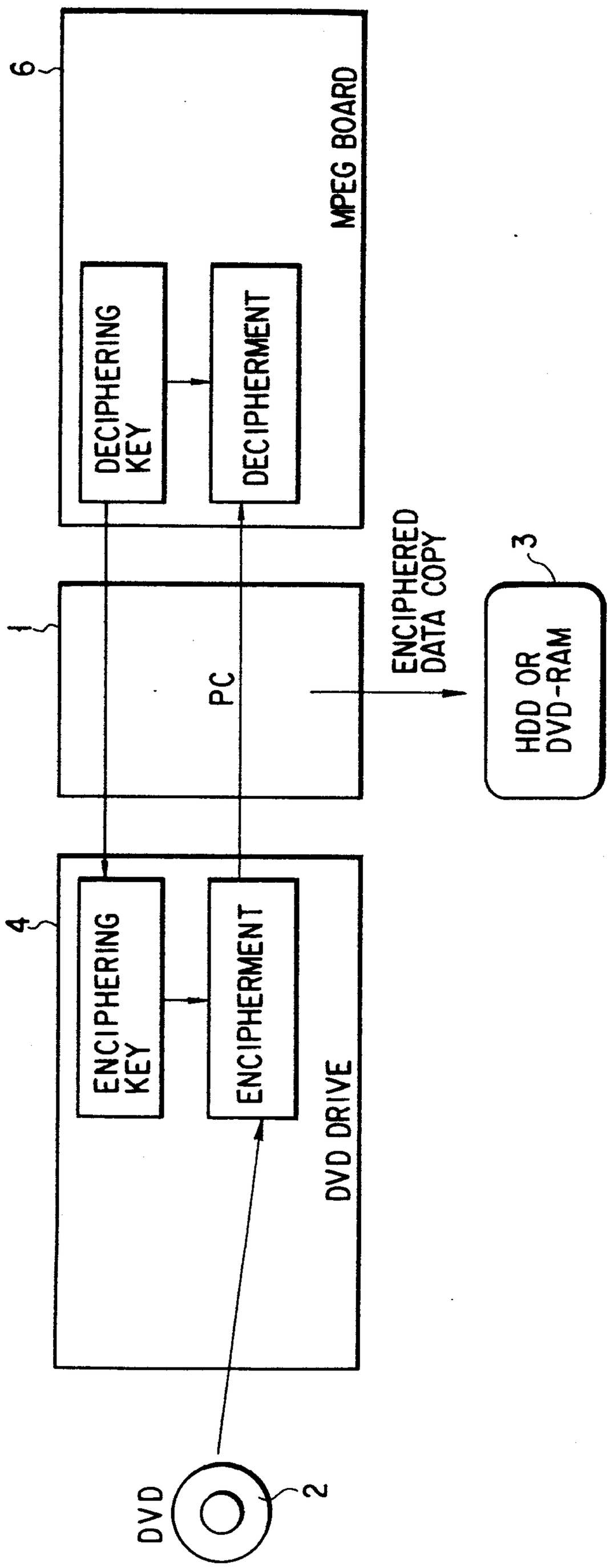


FIG. 1

Marks & Clerk

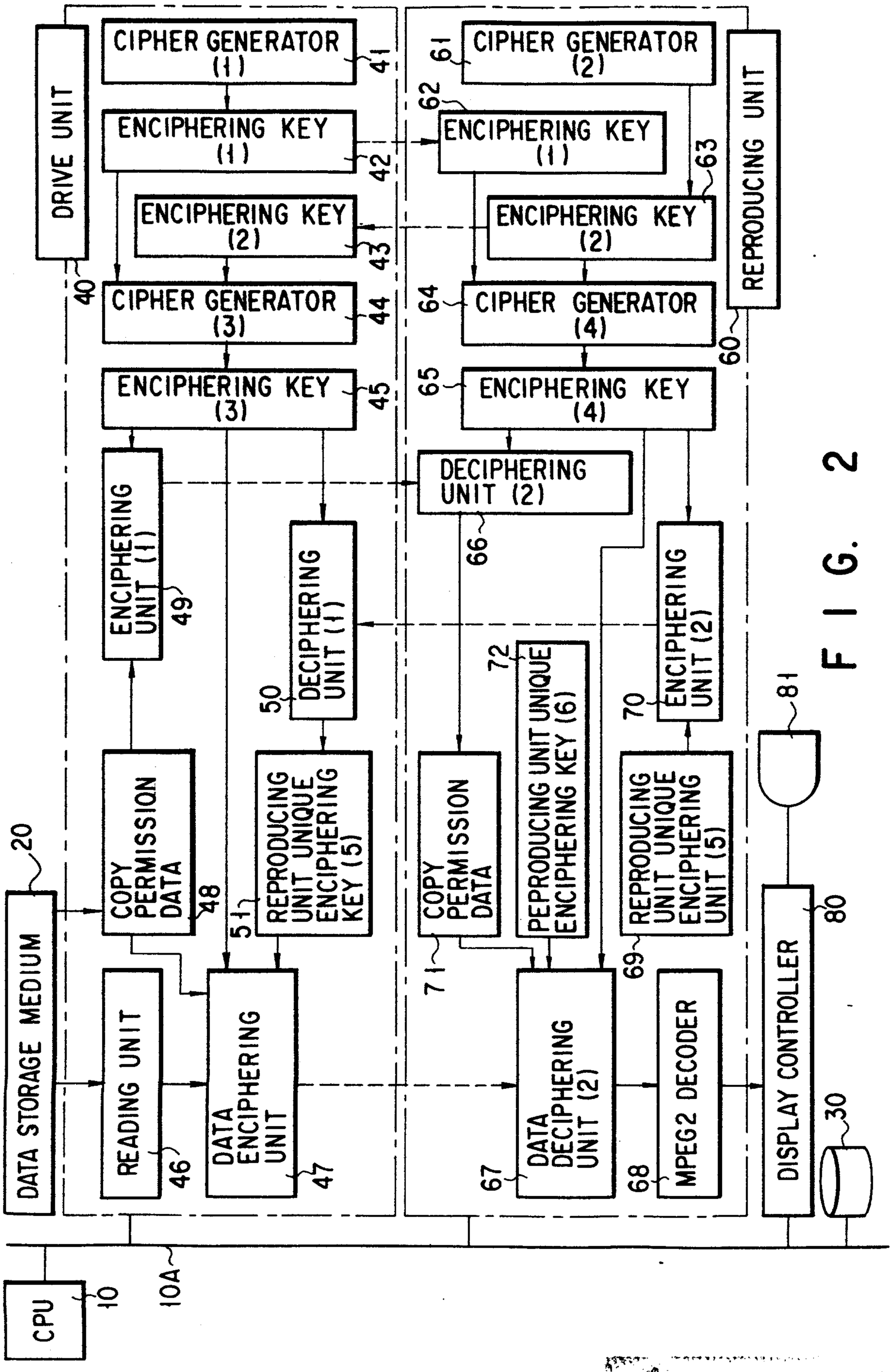

CIPHER GENERATOR (1)
41
CIPHER GENERATOR (2)
61
62
ENCIPHERING KEY (1)
42
ENCIPHERING KEY (1)
63
ENCIPHERING KEY (2)
43
ENCIPHERING KEY (2)
40
CIPHER GENERATOR (3)
44
CIPHER GENERATOR (4)
64
60
ENCIPHERING KEY (3)
45
ENCIPHERING KEY (4)
65
DECIPHERING UNIT (2)
66
ENCIPHERING UNIT (1)
49
DECIPHERING UNIT (1)
50
72
PEPRODUCING UNIT UNIQUE ENCIPHERING KEY (6)
70
ENCIPHERING UNIT (2)
81
20
COPY PERMISSION DATA
48
REPRODUCING UNIT UNIQUE ENCIPHERING KEY (5)
51
COPY PERMISSION DATA
71
REPRODUCING UNIT UNIQUE ENCIPHERING UNIT (5)
69
80
DATA STORAGE MEDIUM
READING UNIT
46
DATA ENCIPHERING UNIT
47
DATA DECIPHERING UNIT (2)
67
MPEG2 DECODER
68
DISPLAY CONTROLLER
30
CPU
10
10A

FIG. 2

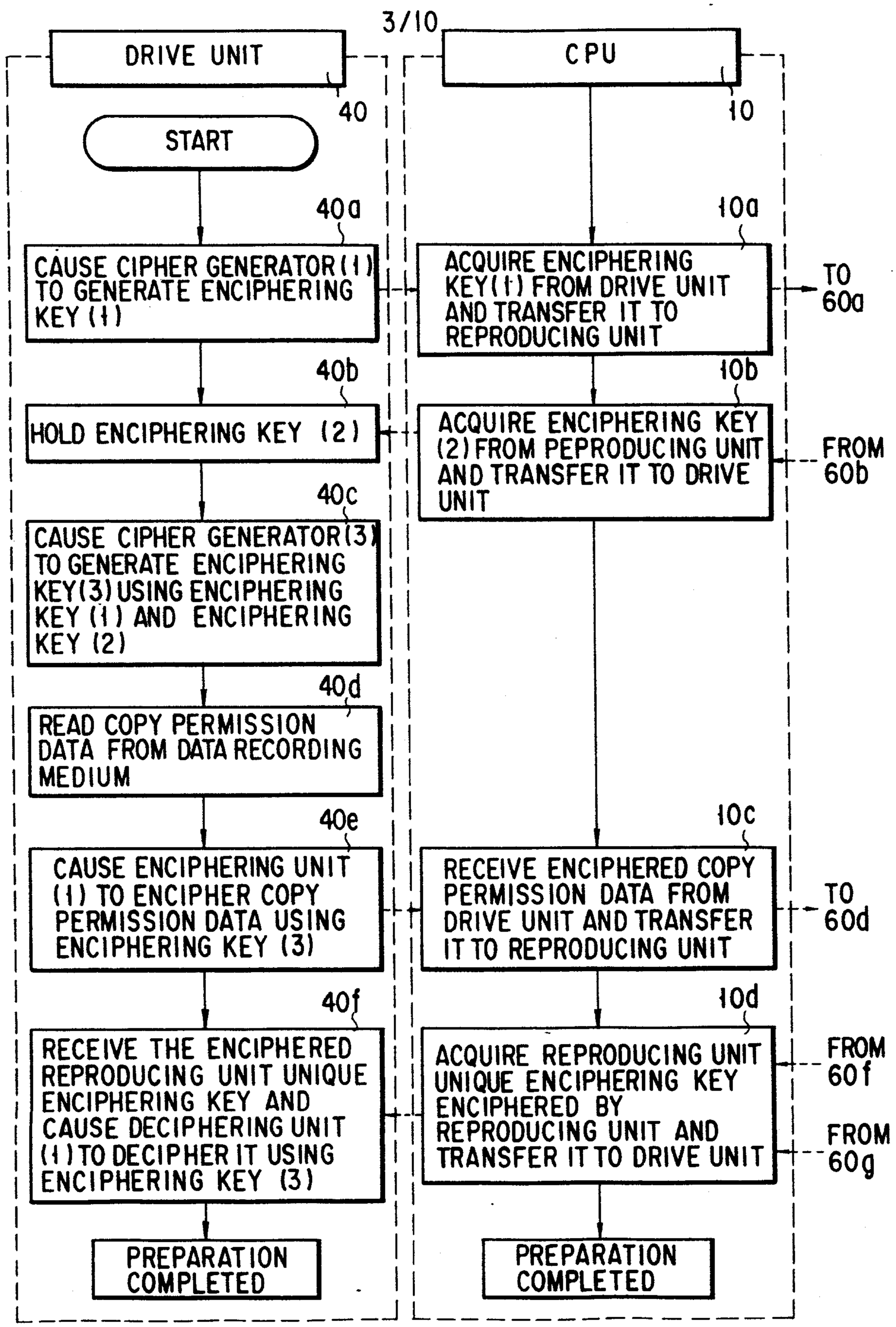
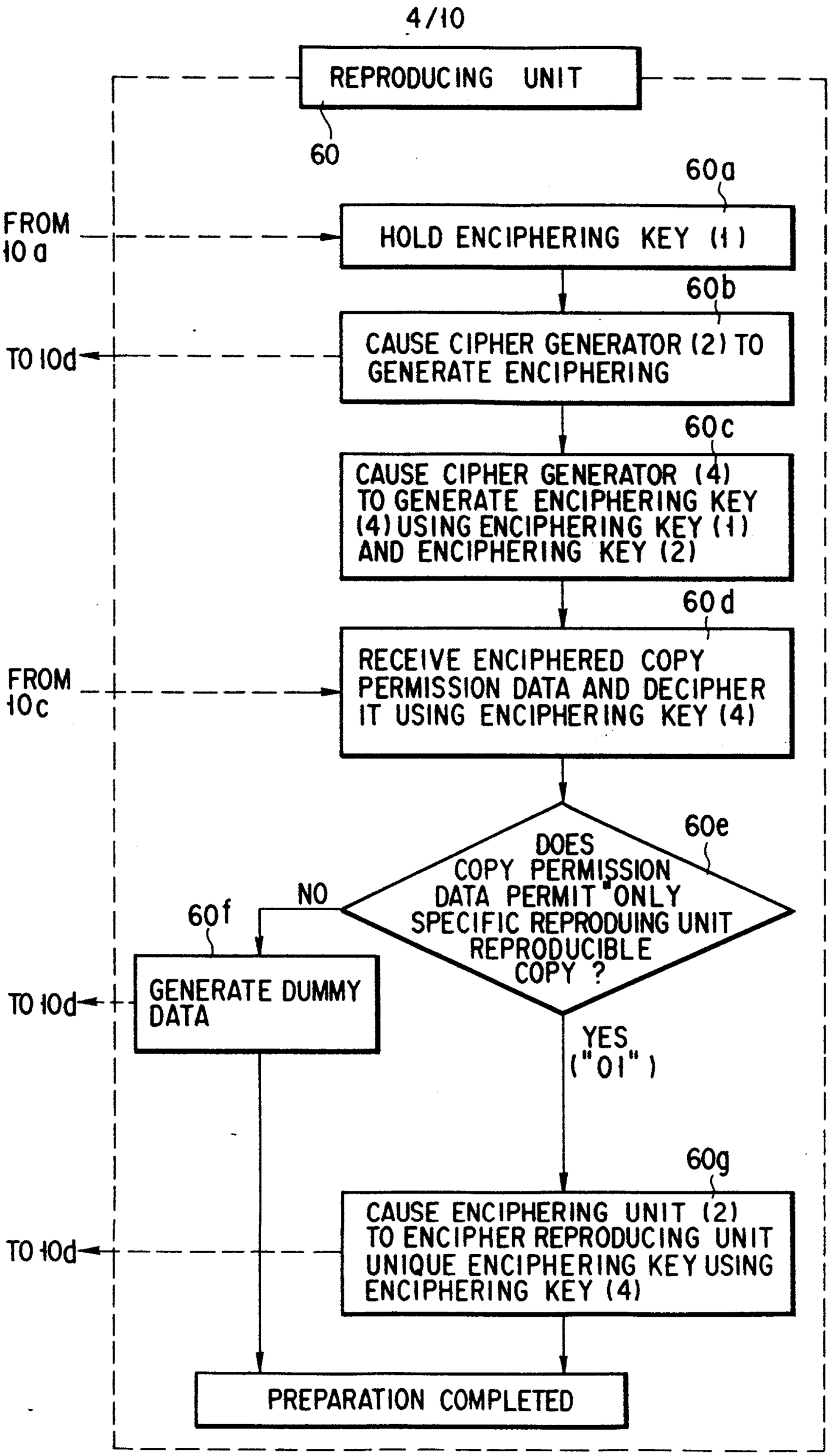


FIG. 3

Marks & Clerk



F I G. 4

Marks & Clerk

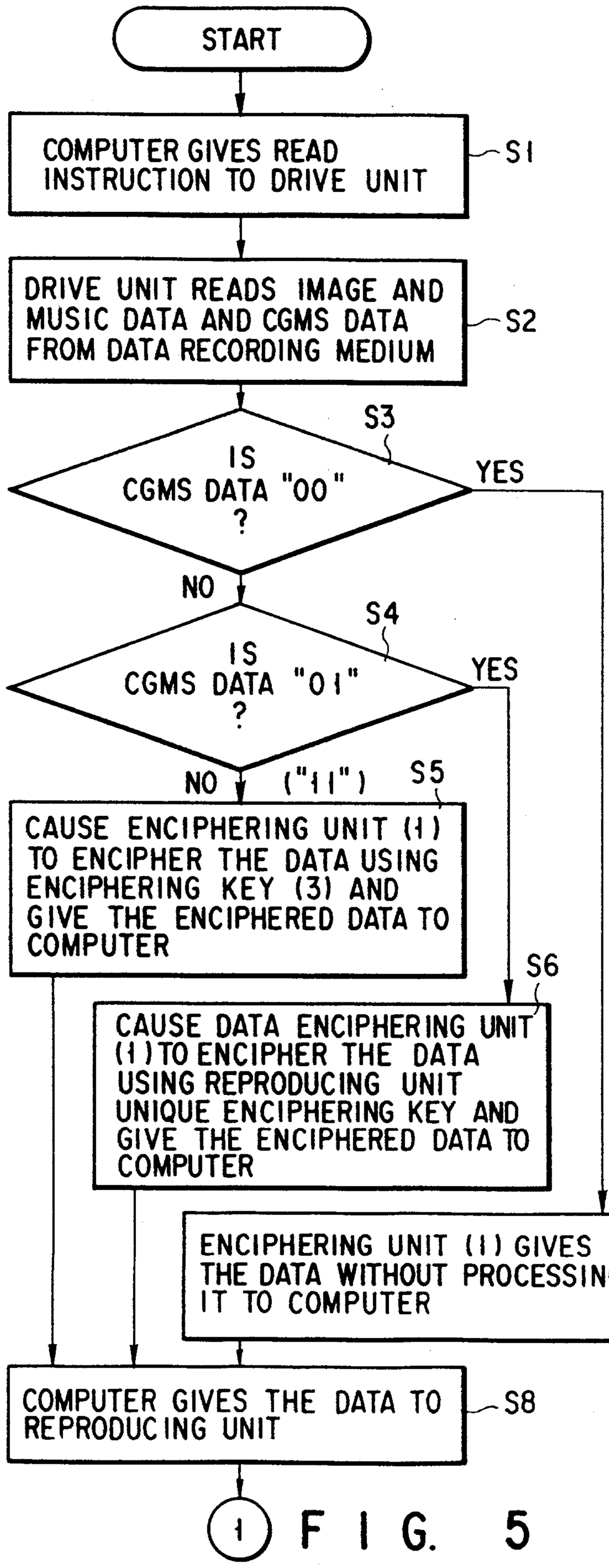


FIG. 5

Naiks & Clerk

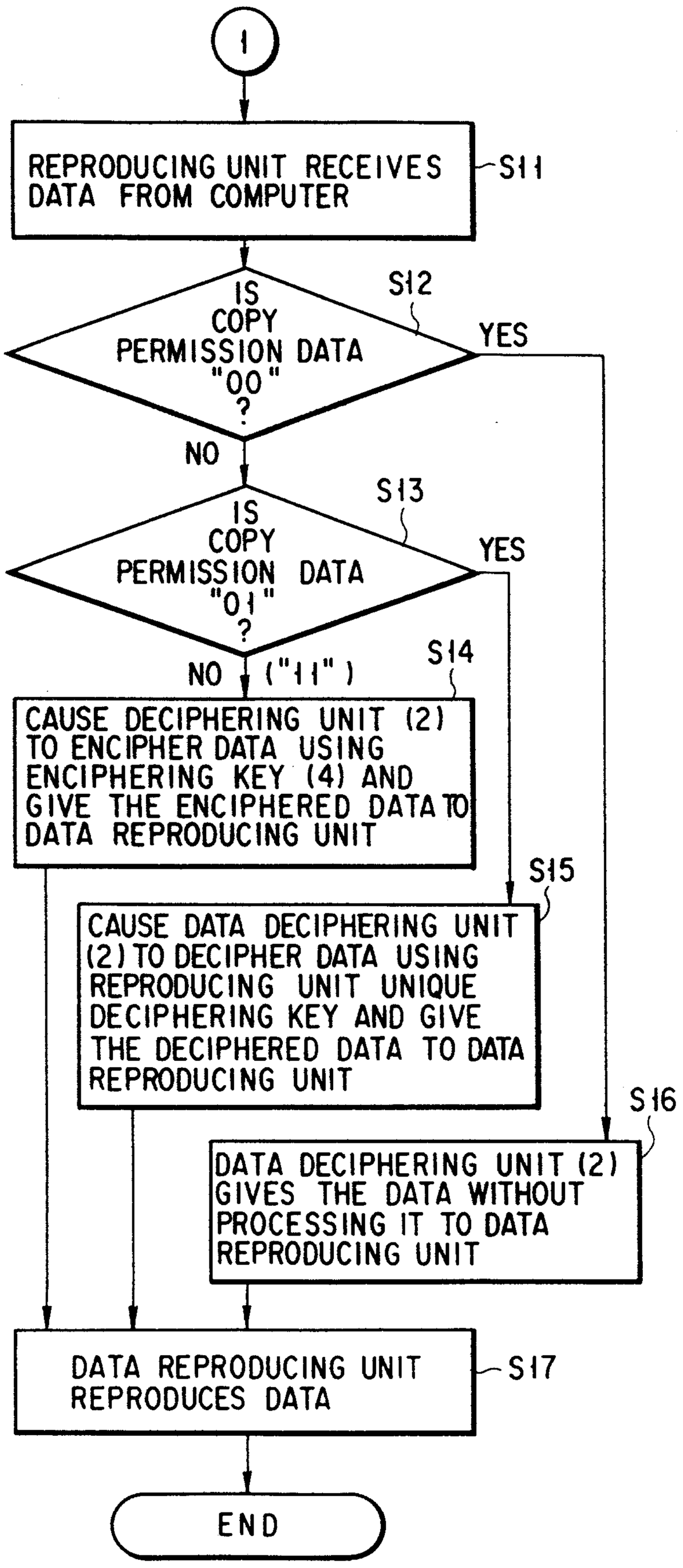
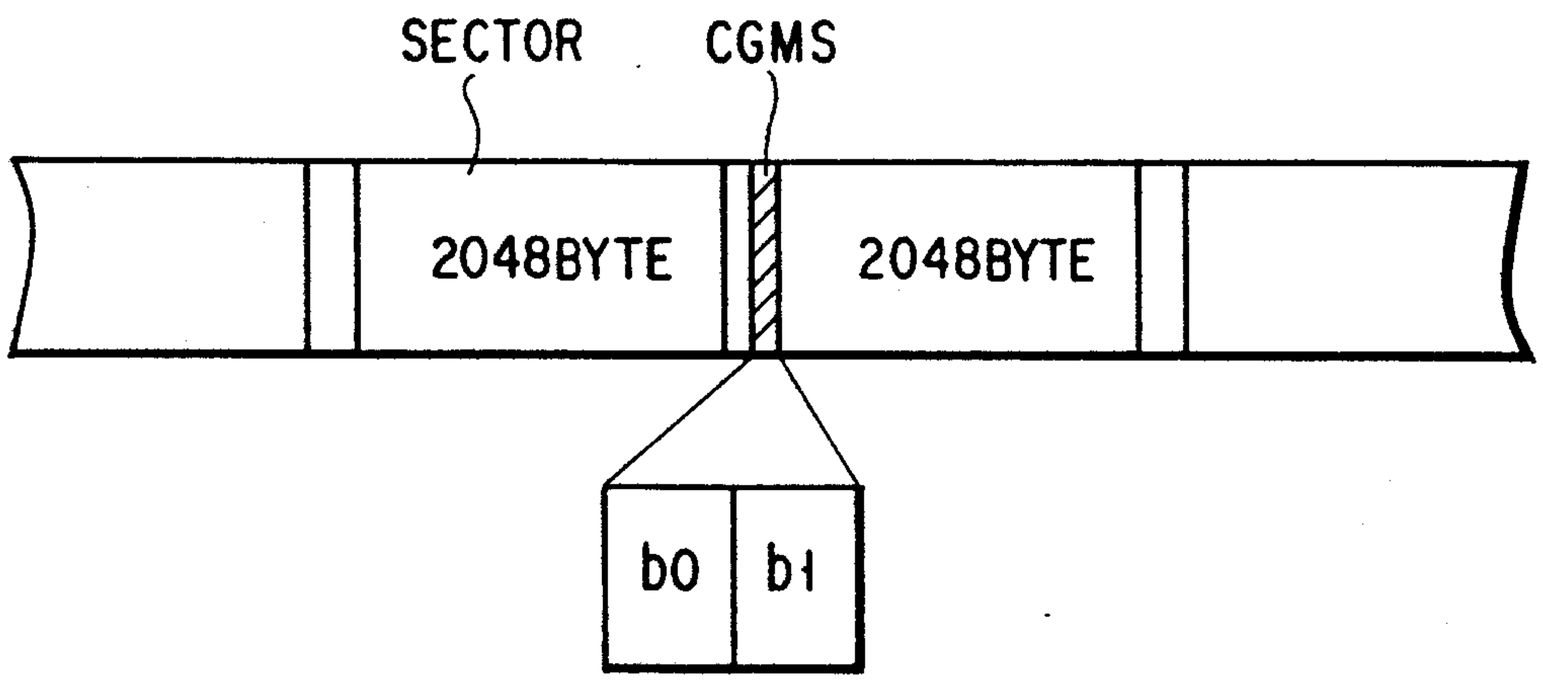


FIG. 6

Marks & Clerk



(CGMS)

b0, b1 = "00" (REPRODUCTON OF COPY IS POSSIBLE)

"01" (ONLY THE UNIT USED IN MAKING A COPY IS ALLOWED TO REPRODUCE THE COPY)

"11" (REPRODUCTION OF COPY IS IMPOSSIBLE)

FIG. 7

Marks & Clerk

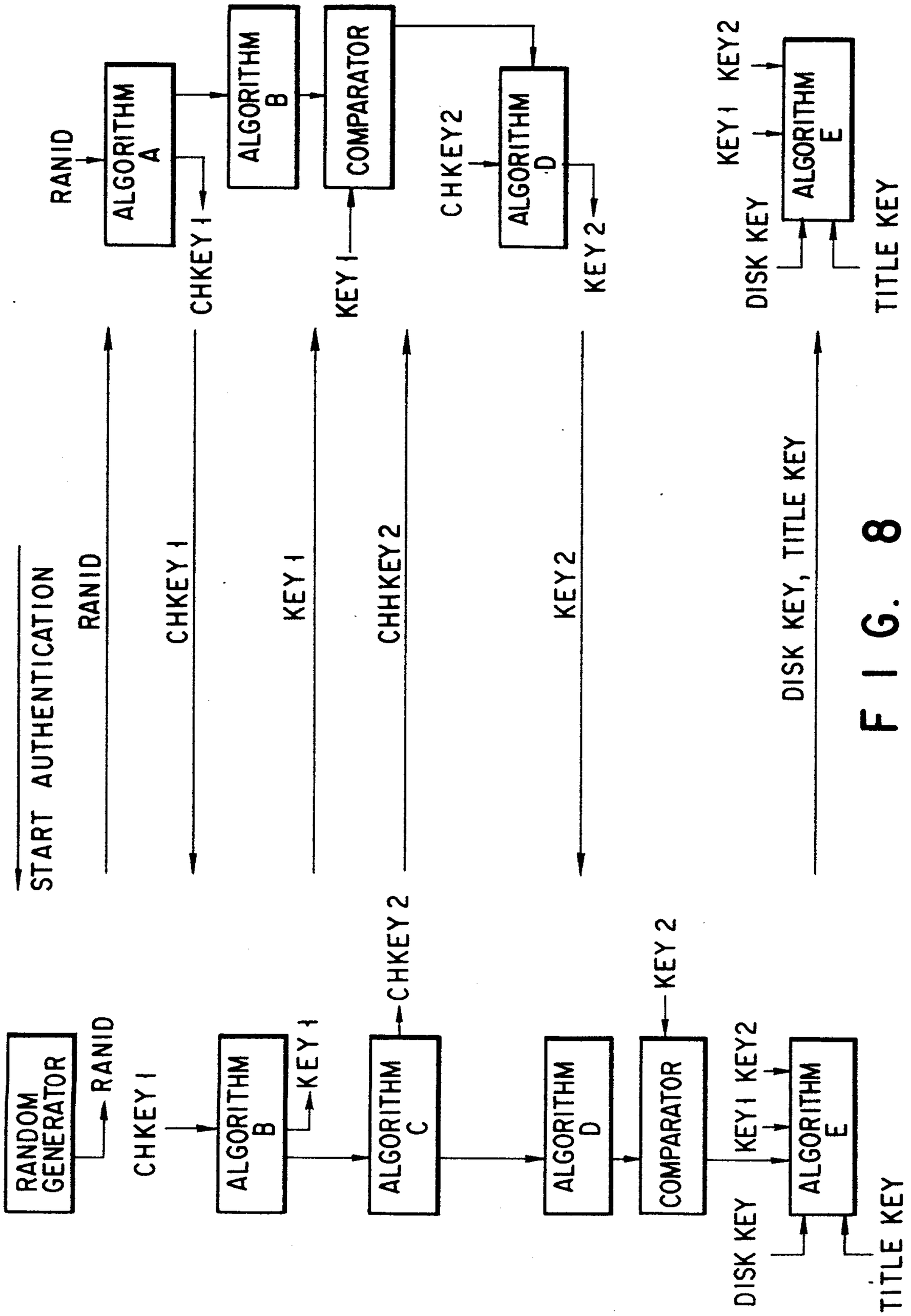

CPU
REPRODUCING UNIT
DRIVE UNIT
START AUTHENTICATION
RANID
CHKEY1
KEY1
CHHKEY2
KEY2
DISK KEY, TITLE KEY
RANDOM GENERATOR
ALGORITHM A
ALGORITHM B
ALGORITHM C
ALGORITHM D
ALGORITHM E
COMPARATOR
CHKEY2
DISK KEY
TITLE KEY
KEY1
KEY2

FIG. 8

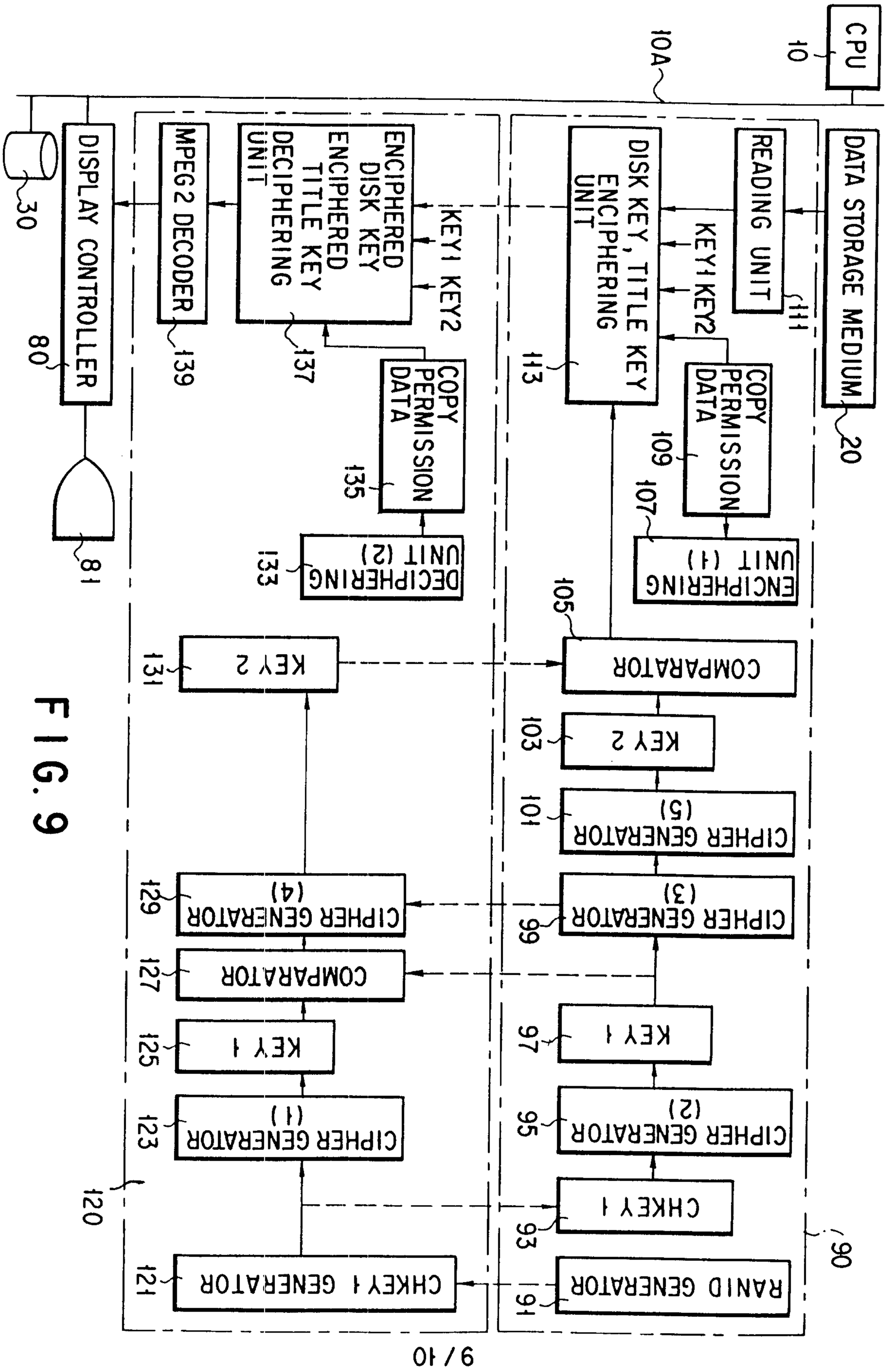
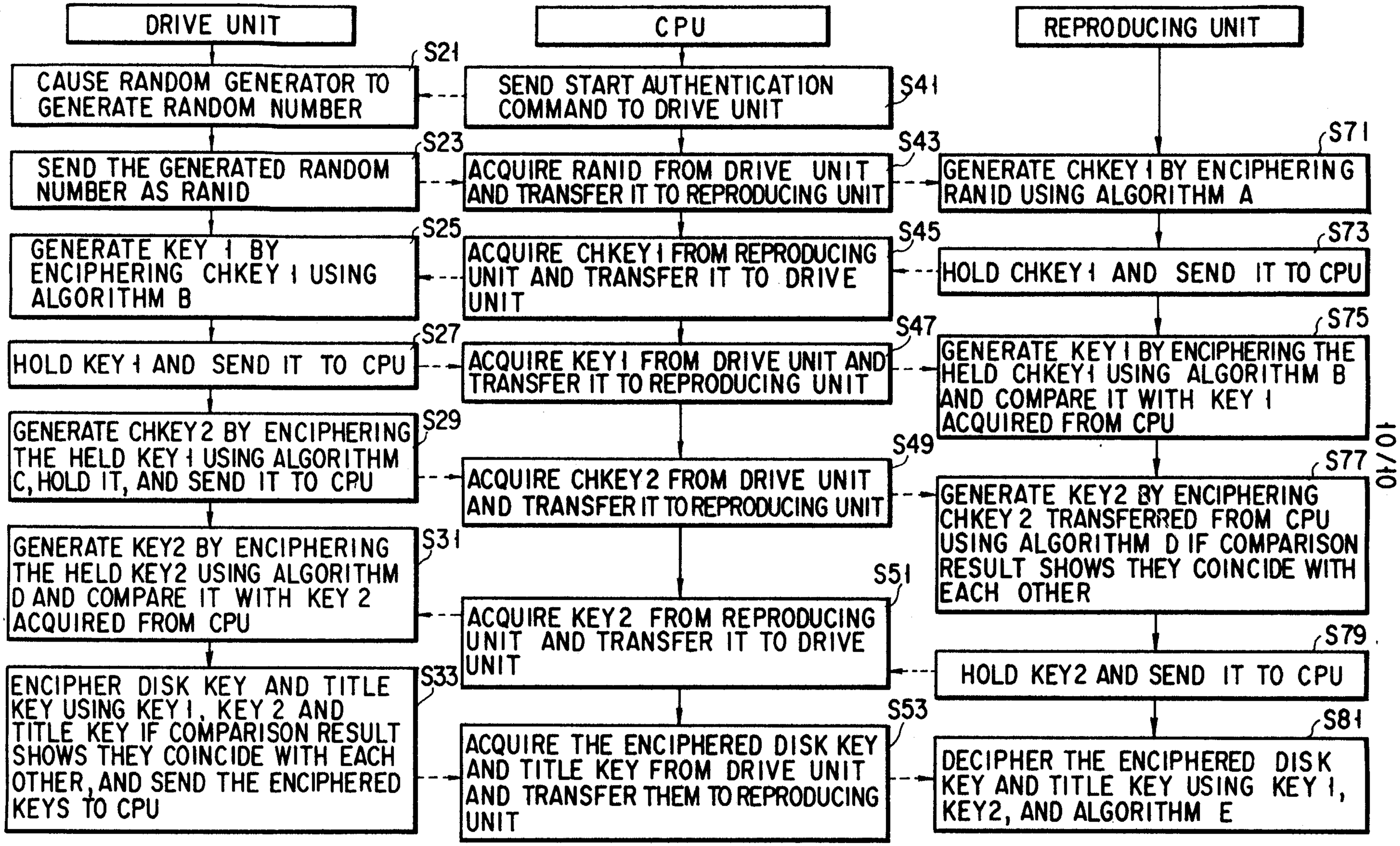
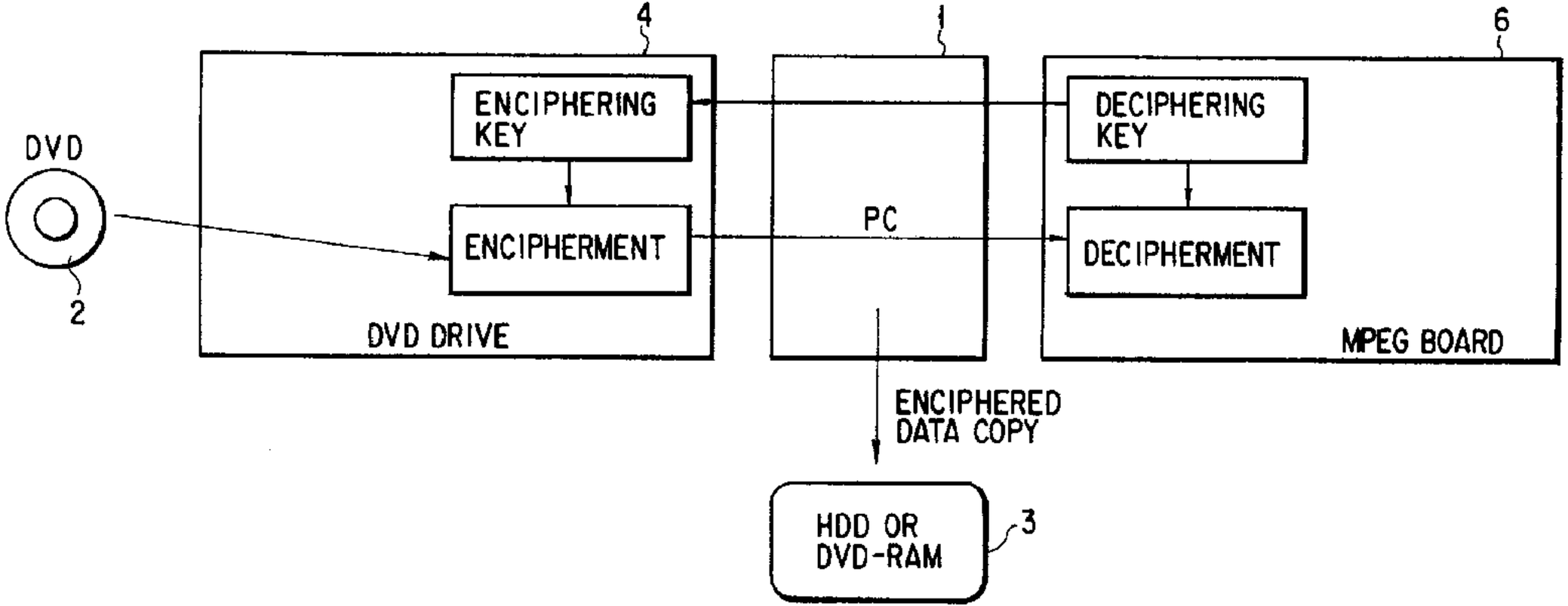

CPU
10
10A
DATA STORAGE MEDIUM
20
READING UNIT
111
KEY1 KEY2
DISK KEY, TITLE KEY ENCIPHERING UNIT
113
COPY PERMISSION DATA
109
107
ENCIPHERING UNIT (1)
105
COMPARATOR
KEY 2
103
CIPHER GENERATOR (5)
101
CIPHER GENERATOR (3)
99
KEY 1
97
CIPHER GENERATOR (2)
95
CHKEY 1
93
RAND GENERATOR
91
90
ENCIPHERED DISK KEY
ENCIPHERED TITLE KEY DECIPHERING UNIT
137
KEY1 KEY2
COPY PERMISSION DATA
135
DECIPHERING UNIT (2)
133
MPEG2 DECODER
139
DISPLAY CONTROLLER
80
30
81
KEY 2
131
CIPHER GENERATOR (4)
129
COMPARATOR
127
KEY 1
125
CIPHER GENERATOR (1)
123
CHKEY 1 GENERATOR
121
120

FIG.9



F I G. 10

Marks & Clerk


4
1
6
DVD
2
ENCIPHERING KEY
ENCIPHERMENT
DVD DRIVE
PC
DECIPHERING KEY
DECIPHERMENT
MPEG BOARD
ENCIPHERED DATA COPY
HDD OR DVD-RAM
3