MECHANISM OF MATCHING BETWEEN A RECEIVER AND A SECURITY MODULE

TECHNICAL FIELD

This invention relates to a system for controlling the transfer of information between a receiver and a security module, especially for a pay television system, as well as to a method of controlling the transfer of scrambled information.

BACKGROUND OF THE INVENTION

A pay television descrambling system is composed of a receiver and a security module. This module may be detachable or fixed. The purpose of the receiver is to descramble the signals received. The main purpose of the security module is to control the operation by verifying the descrambling authorization and by providing, as required, the information necessary for operating the descrambling module, for example by providing descrambling vectors, also called control words.

The existing systems use receivers which interrogate their security modules, and the latter reply by providing the information necessary for descrambling. At a given time, for the same transmitted broadcast, all the security modules reply with the same information. Because the information flows between the security module and the receiver at a low rate (of about 20 to 30 bytes/s), defrauders may use this information in order to broadcast it publicly, for example via the Internet.

Such a system is described in the document "DVD Conditional Access" written by David Cutts in the journal called "Electronics & Communication Engineering Journal" of February 1997. It is described a standardized system to unscramble audio and video streams coming from different service providers. The security module, called CA (Conditional Access) is in charge of delivering the control words CW. This module can additionally uses a smart card (SM) for the descrambling function. Once the information are descrambled in the CA module, the control words CW are returned in the decoder for obtaining the uncoded information

In a prior publication entitled "Conditional Access Broadcasting:Datacare 2, an Over-Air Enabled System for General Purpose Data Channels", published on August 1st 1988 in the journal BBC Research and Development Report No 10, it is described an independent module (Conditional Access Module) in charge of receiving and decrypting the information necessary for the descrambling. This module manages the key dedicated to the system and delivers the control words necessary for the descrambling of the video broadcasts. In this type of module, once the control words are decrypted, they are transmitted uncoded to the unit in charge of the descrambling.

The problem then arises of how to make a receiver and a security module interdependent so that:

- the given security module can be used only in the receiver for which the said security module was intended,

- the information stream exchanged between the security module and the receiver is unique. This uniqueness prevents the public broadcasting of this stream from allowing other receivers to work without the security module provided for this purpose.

SUMMARY OF THE INVENTION

The proposed solution to the above mentioned problem uses at least one encryption key specific to the receiver. This (or these) key(s) is(are) called a matching key. At least one of the keys is different for each receiver. This (or these) key(s) is(are) installed in the non-volatile memory of the receiver, either during the manufacture of the said receiver or at a subsequent step. The receiver provides no means of access to this (or these) key(s) to the external world.

One possible means of programming this key into the security module is to use the central information system which manages the group of receivers and which can embed, in the video transmission stream, information for programming this key into the secret non-volatile memory of the security modules. The formatting of this procedure is, of course, kept secret.

When transferring confidential information and/or information necessary for the operation of the system from the security module to the receiver (typically, control words, but other information may be thus transferred), the security module encrypts this information using one or more unique matching keys common to the single receiver/security module pair. Any method of encryption can be used provided the security module knows it, and the receiver knows the corresponding method of decryption. Once this information has been received by the receiver, it is then decrypted by the said receiver using the known method of decryption and the matching key stored in its non-volatile memory. The said information is then uncoded information and can be used by the said receiver.

The invention therefore proposes a system for controlling the transmission of information between a receiver and a security module, especially for a pay television system, in which the transmitted information is encrypted and decrypted by means of at least one unique encryption key stored, on the one hand, in the receiver and, on the other hand, in the security module.

The invention also relates to a system for descrambling scrambled information and to a pay television system comprising a transmission control system.

Moreover, the invention relates to a method of controlling the transmission of information between a receiver and a security module, especially for a pay television system, characterized in that at least one unique matching key is stored, on the one hand, in the receiver and, on the other hand, in the security module and in that the information transmitted between the receiver and the security module is encrypted and decrypted by means of at least one said unique encryption key.

This solution according to the invention solves the problem posed. This is because:

- a security module inserted into a receiver other than that for which the said security module has been matched will provide this other receiver with a stream of confidential information and/or of information necessary for the operation of the system which is encrypted with a key that does not correspond to that used for decrypting it. The result is therefore unusable;

- a stream of confidential information and/or of information necessary for the operation of the system coming from a security module cannot be distributed to several receivers. Only the receiver matched with the card providing this stream of confidential and/or necessary information is able to decrypt the said stream successfully.

The system may comprise a mechanism for verifying the matching procedure The central information system may write a number, personal to the receiver, in the security module matched with the said receiver, for example a number generated randomly by the latter, or may simply use its serial number. One means open to the receiver is to freely verify this personal number written in the security module and to compare it with that stored in its non-volatile memory.

This mechanism has the advantage of not using improper data. The result of encryption followed by decryption by a different key usually provides a pseudo-random result. If the result is not recognized as being false and if this result is used as it is, this could result in the receiver or the equipment connected to it being damaged.

Certain types of receivers have a detachable descrambling module. This module is responsible for a number of operations, among which is the operation of descrambling the signals received Confidential information is then transferred between the detachable security module and this detachable descrambling module. The mechanism of encryption of the communication, described above, between a receiver and a security module is then transferred, as it is, between the detachable security module and the detachable descrambling module.

Likewise, the method of matching, described above, between the security module and the receiver is then transferred, as it is, between the detachable security module and the detachable descrambling module.

Descrambled signals are then transferred between the detachable descrambling module and the receiver. The mechanism of encrypting the communication, along with the mechanism of matching, described above, between the security module and the receiver, is then transferred, as it is, between the receiver and the detachable descrambling module.

The functions provided by the detachable descrambling module and the detachable security module may be carried out by a single module, called a detachable descrambling-security module. The matching mechanism described above is then transferred, as it is, between the detachable descrambling-security module and the receiver.

In all the cases described above, the matching key or keys may be used to encrypt a stream of confidential data and/or of data necessary for operating the system in the opposite direction, by reversing, respectively:

- the receiver and the detachable security module;

- the detachable descrambling module and the detachable security module;

- the receiver and the detachable descrambling module;

- the receiver and the detachable descrambling-security module.

In all cases where a matching key is specific to one item of equipment (a receiver or a detachable module), the same principles apply to the use of a matching key (or several matching keys) specific to a group of items of equipment

BRIEF DESCRIPTION OF THE FIGURES

Figure 1 illustrates a configuration employing a receiver and a detachable security module.

Figure 2 illustrates a configuration employing a receiver, a detachable descrambling module and a detachable security module.

Figure 3 illustrates a configuration employing a receiver and a detachable descrambling-security module.

DETAILED DESCRIPTION

The receiver A in Figure 1 receives a stream of scrambled video information 1 from a source such as a satellite receiver or by cable. This stream, of the order of several megabits per second, is shaped in the receiver A and then transmitted to a control unit B which is responsible for

the descrambling and for managing the authorization for access to the scrambled video information. To do this, this control unit B periodically interrogates the detachable security module C (channel 3) which replies to the latter with a stream of confidential data and/or of data necessary for the operation of the control unit B (channel 4) These exchanges take place at low rates and can be easily processed by the microprocessors of smart cards available on the market. According to the invention, the detachable security module C comprises at least one encryption key K in a non-volatile memory which encrypts the confidential data and/or the data necessary for operation of the control unit B (channel 4) towards the receiver A. This key K is unique to the receiver A and written to the detachable security module C, making the information stream 4 unique to this system. The public broadcasting of this information 4 will no longer be of any use to other receivers as, in the case of the latter, since they are not in possession of the same key K, the information stream is completely incomprehensible. By means of the information 4, the control unit B can recover the descrambled video signal 2, this being processed and then transmitted in standard form (PAL, SECAM, NTSC) to the video monitor.

A variant of the invention employs encryption, of the same kind, of the information 3 sent to the detachable security module C either using the same key K or using a different key J, which is unique and specific to the system formed by the receiver A and the detachable security module C. Thus, any attempt to recover the key K from the information stream 4 is made much more difficult.

Figure 2 illustrates a variant using a detachable descrambling module D which incorporates the control unit B. In this case, the scrambled video stream 1 is shaped by the receiver A and sent to the detachable descrambling module D. The mode of operation described in the case of Figure 1 between the receiver A and the detachable security module C is this time applied to the conversation between the detachable descrambling module D and the detachable security module C. The key K is written in a secret part of the detachable descrambling module D instead of the receiver A. Thus, the information provided by the detachable security module C to the detachable descrambling module D is encrypted and therefore of no value to another detachable descrambling module D.

It may thus be seen that the information sent to the receiver A consists of a stream of descrambled video information 6 which can be readily exploited, for example for illicit copies. In one variant of the invention, the stream 6 is encrypted in the detachable descrambling module D before being sent to the receiver A for descrambling by the decrypting unit E'. This operation is carried out using a key K' specific only to the receiver A/detachable descrambling module D system. Consequently, the information stream 6 no longer has any meaning and can be understood only by the receiver A having the same key K'.

The receiver A may add, to the scrambled video stream 1, control information intended for the detachable descrambling module D. In order to prevent this information from being public and from opening a door to understanding the encryption mechanism, this information is encrypted by the encryption unit E in order to obtain a scrambled video stream 6 containing encrypted control information.

Figure 3 illustrates a variant of the invention in which the detachable security module is incorporated into a detachable descrambling-security module F. The function of this module is to descramble and to manage the authorization of the video signals received by the receiver A. According to the invention, this module includes a unique encryption key specific to the receiver A and written in this detachable descrambling-security module F. Likewise, the descrambled video stream 6 is encrypted by this key and sent in this form to the receiver A. The latter, by means of the decryption unit E' and by using the same unique key, will be able to recover the uncoded video signal.

By analogy with the operation described in relation to Figure 2, the control information contained in the scrambled video stream 1 may be encrypted by means of a unique encryption key by the unit E before it is sent to the detachable descrambling-security module F.

In all the examples described in relation to Figures 1 to 3, the matching may be checked. In the case of Figure 1, the receiver A writes a personal number, for example its serial number, in the detachable security module C. Thus, the receiver can at any instant verify that the detachable security module C is indeed that which is intended for it. In the context of the example illustrated in Figure 2, the check may be made at two levels,

namely a first level between the detachable descrambling module D and the detachable security module C and a second level between the detachable descrambling module D and the receiver A. This second level is particularly important if the unscrambled information 6 sent to the receiver A is encrypted.

In the solution shown in Figure 3, the matching is checked between the receiver A and the detachable descrambling-security module F.

In one embodiment of the invention, the receiver A is an MPEG decoder using control words (information necessary for descrambling the signal) in order to descramble the video signal These control words are provided by the detachable security module C. This module, for example a smart card, includes a non-volatile memory for storing them.

In one embodiment of the invention, the detachable descrambling module D is a PCMCIA-type card which includes an MPEG decoder (control unit B).

In one embodiment of the invention, the detachable descrambling-security module F is produced in the form of a smart card which incorporates an MPEG decoder and a security module C'.

In one embodiment of the invention, the unique encryption key K is common to a group of receivers. This possibility is advantageous, for example in a school having several receivers to which the same detachable security module is applied depending on the requirements. Likewise, several detachable security modules include the same encryption key in order to be able to be placed in any one of the receivers in the group. In this case, the matching check is carried out on a number which is no longer specific to one receiver but to a group of receivers. A combination may be produced with a number composed of two parts, one part defining the group and the other the receiver. The uniqueness of the personal number is respected, the matching conformity test then being carried out on more than just the group part of this number.

CLAIMS

1. Pay-TV reception system comprising a receiver (A) connected to security means (C, D, F), this receiver (A) receiving descrambling information from the security means (C, D, F), characterized in that at least some of the information (4, 6) sent from the security means (C, D, F) to the receiver (A) are encrypted by a unique encryption key.

2. Pay-TV reception system according to Claim 1, characterized in that the unique encryption key is common to a group of receivers.

3. Pay-TV reception system according to Claim 1 or 2, characterized in that at least some of the information (3, 5) sent from the receiver (A) to the security means (C, D, F) is encrypted by a unique encryption key.

4. Pay-TV reception system according to Claims 1 to 3, characterized in that the receiver (A) includes a personal number which may be written in the security means (C, D, F), it being possible for the said receiver (A) to verify at any time the conformity of this personal number written in the said security means (C, D, F).

5. Pay-TV reception system according to Claim 4, characterized in that the personal number comprises a part specific to a group of receivers and a part specific to one receiver and in that the conformity of the matching is verified on the part specific to the group of receivers.

6. Pay-TV reception system according to Claims 1 to 5, characterized in that the receiver (A) includes a control unit (B) and in that the security means consist of a detachable security module (C) in which the confidential information (4) and/or the information (4) necessary for the operation of the control unit (B) is stored.

7. Pay-TV reception system according to Claims 1 to 5, characterized in that the security means comprise a detachable descrambling-security module (F) comprising a control unit (B) and a security unit (C'), these units being responsible for descrambling and for authorizing the video information.

8. Pay-TV reception system comprising a receiver (A) connected to security means (C, D, F), this receiver (A) receiving descrambling information from the security means (C, D, F), characterized in that these security means comprise a detachable security module (C) and a detachable descrambling module (D) which includes a control unit (B) and in that at least some of the confidential information (4) and/or of the information (4) necessary for the operation of the control unit (B) is encrypted before being sent to the detachable descrambling module (D) by the detachable security module (C) by means of a unique encryption key.

9. Pay-TV reception system according to Claim 8, characterized in that at least some of the information (3) sent from the detachable descrambling module (D) to the security module (C) is encrypted by a unique encryption key.

10. Pay-TV reception system according to Claim 8 or 9, characterized in that the detachable descrambling module (D) includes a personal number which may be written in the detachable security module (C), it being possible for the said detachable descrambling module (D) to verify at any time the conformity of this personal number written in the said detachable security module (C).

11. Pay-TV reception system according to Claim 10, characterized in that the personal number comprises a part specific to a group of detachable descrambling modules (D) and a part specific to one detachable descrambling module (D) and in that the conformity of the matching is verified on the part specific to the group of detachable descrambling modules (D).

12. Pay-TV reception system according to Claims 9 to 11, characterized in that at least some of the information (5) sent from the receiver (A) to the detachable descrambling module (D) is encrypted by a unique encryption key.

13. Pay-TV reception system according to Claims 9 to 12, characterized in that at least some of the information (6) sent from the detachable descrambling module (D) to the receiver (A) is encrypted by a unique encryption key.

14. Pay-TV reception system according to either of Claims 12 and 13, characterized in that the receiver (A) includes a personal number which may be written in the detachable descrambling module (D), it being possible for the said receiver (A) to verify at any time the conformity of this personal number written in the said detachable descrambling module (D).

15. Method of controlling the transmission of information in a Pay-TV reception system between a receiver (A) and security means (C, D, F), these security means sending to the receiver (A) descrambling information allowing the decryption of the video and audio signals, characterized in that at least one unique encryption key is stored, on the one hand, in the receiver (A) and, on the other hand, in the security means and in that the information transmitted between the receiver (A) and the security means is encrypted and decrypted by means of at least one of the said unique encryption keys.

16. Method according to Claim 15, characterized in that a number personal to the receiver (A) is written in the security means during an initialization operation and in that the receiver (A) may check at any time the conformity of this personal number written in the said security means.

17. Detachable security module (C) intended to be connected to a receiver (A) as part of a Pay-TV reception system, which includes at least one non-volatile memory intended for storing the confidential data and/or the data necessary for operating the descrambling system and the means of transmission with the receiver (A), characterized in that this detachable security module (C) includes means for encrypting the transmission and in that this memory also includes at least one encryption key which acts on the means for encrypting the transmission.

18. Detachable descrambling module (D) beeing part of a pay-TV reception system, comprising a control unit (B), first means of transmission (3, 4) with a detachable security module (C), second means of transmission (5, 6) with a receiver (A), and a non-volatile memory, characterized in that it includes first encryption means and in that this memory includes at least one encryption key which acts on the first encryption means intended for encrypting the transmission of the first transmission means (3, 4).

19. Detachable descrambling module (D) according to Claim 18, characterized in that it includes second encryption means and in that this memory includes at least one encryption key which acts on the second encryption means intended for encrypting the transmission of the second transmission means (5, 6).

20. Pay television descrambling receiver (A) comprising means of transmission to security means (C, D, F), as well as a non-volatile memory, characterized in that it includes means for encrypting/decrypting the transmission from and to the security means (C, D, F) and in that this memory includes at least one encryption key which acts on the means for encrypting/decrypting the transmission.