for PCT/DE95/00738

Procedure for the encryption and decryption of digital information by means of a decryption facility

The invention relates to a procedure for the encryption and decryption of digital information by means of a decryption facility, the decryption facility guaranteeing access to authorised persons and preventing access by unauthorised persons.

Digital information is increasingly being sent via unsecured distribution channels. This information, however, can be secured if the authorised person is the only one to receive the key and to be able to decrypt the information. The transfer of the key must be organised in such a way that only authorised persons may use the key and that it is not possible to pass it on.

An encryption/decryption unit (EDU) is described in publication US 84/01856. The aim of this invention is to enable the secure exchange of a key via unsecured data lines (e.g. telephone lines). Every EDU contains a central processing unit (CPU), memory with random access (ROM), in which key exchange keys (KEK) are stored and a "data-encryption standard" (DES) coprocessor; all imbedded in a ceramic module, to make it impossible to monitor the command processing. Furthermore, every EDU contains a special circuit which enables the CPU to process encrypted commands. When a connection is established between two EDUs, each EDU selects a part key. This part key is transferred to the partner in encrypted form and tested. The two keys are then combined to form the so-called session key. This session key is then used to encrypt and transfer the information.

One disadvantage of this invention lies in the fact that a two-way connection is required to exchange the key. This is required with this method because each EDU produces a part of the key which is then transferred to the other EDU and combined to form the complete key. Furthermore, it is possible in this way to send information to recipient groups with the same encryption since a different key is generated for each connection of two EDUs.

Publication EP 0266748 describes a coprocessor with decryption properties and non-readable key plates. These key plates are transferred to the coprocessor using a transfer module. Once the key plates (for a specific program) are transferred to the coprocessor, the transfer module becomes redundant. This prevents the key plates from being transferred more than once to several coprocessors. This makes it possible to decrypt programs to decrypt programs to which the key plates were transferred in the coprocessor.

The disadvantage of this invention, however, is that a transfer token must be transferred to a special memory unit (hardware transfer module) which then becomes redundant on use. This naturally entails handling problems. This module must be redirected to the end customer. This means that the information cannot be decrypted again as the transfer module has become redundant. Moreover, it is not possible to transfer the key via electronic media.

According to publication FR-A-2 681 165, a procedure is known for the encrypted transfer of information between two microprocessors which each have a memory file with several addresses and the same contents in each card. Using this procedure, the information is encrypted in the first card, transferred in encrypted form from the first to the second card and finally decrypted on the second card. This procedure is characterised by the fact that the encryption and decryption only use the contents of one part of the memory file as key. This part is identified by means of address data which is used by the first card and transferred to the second. This means that two black boxes exist in which the same reference file is stored. Since this reference file is unknown to third parties, an address can be exchanged between the two cards which indicates a position in the reference file. The contents of this position are then used as symmetric key in both cards in order to encrypt and decrypt data (keys). The disadvantage of this solution is that the data from one card is transferred to the second card. Furthermore, it is not possible in this solution to exchange the individual encryption algorithms centrally in the end devices in order to dynamise the conversion of the keys and the data.

The solution according to publication EP-A-0 033 014 is the standardisation of the encryption and decryption algorithms used, without any value being placed on these algorithms being transferred securely. It should be noted that these algorithms are to be used at a later stage to encrypt and decrypt the contents and actual quantities of data. The solution assumes that both parties share an interest in keeping the algorithms secret or must be sure that they will be. The disadvantage of the solution is that the receivers of the message, if they pursue this intention, can independently transfer the key programs to any number of key PCs making it possible for unauthorised third parties to access the messages.

The task of the invention is to develop a procedure for the encryption and decryption of digital information by means of a decryption facility, using which information can be distributed in a user-friendly way to several receivers and where the encryption of the information requires little technical administrative effort, whereby keys can be distributed securely and transferred in a manner which guarantees them secure against detection. Moreover, it should not even be possible for the owner of the decryption facility to pass on a key since the distributed algorithms for encryption and decryption of the transferred key cannot be exchanged between encryption and decryption facilities.

To fulfil this requirement, it is possible to use some method of encrypting the keys. The modern possibilities of breaking an encryption algorithm rely on the presence of so-called plain texts (unencrypted information) and the corresponding cipher texts (encrypted information). To break block systems such as the DEA, the text volume must be very large. This is necessary to implement methods such as Biham and Shamir's differential cryptoanalysis. At the present time this method is the best attack on block encryption systems such as the DEA in existence (described in Eli Biham and Ali Shamir "Differential Cryptoanalysis of DES-like Cryptosystems" in Journal of Cryptology vol. 4 pp 3-72, 1991).

It is important to make the process for encrypting the key as difficult as possible to discover.

It is necessary, therefore, to keep the volume of plain/cipher texts available to third parties as low as possible, particularly with regard to the key transfer.

This can be achieved by encrypting the keys with frequently changing encryption algorithms. This means that third parties wishing to decrypt the keys must develop a new "cracking algorithm" every time the encryption process is changed.

This also means that specific keys can be made available to specific persons or groups only, these persons or groups having exclusive knowledge of the key decryption process.

It is also necessary to create a special processor as part of this process. This provides a cheap and secure method of distributing the keys and protecting the key decryption process against being passed on.

It is also necessary to ensure that it is not possible for the authorised receivers of a key decryption process from passing this on.

According to the invention, this is solved by the characteristics listed in Patent Claim 1 and Patent Claim 2. Preferred developments of the result from the subclaims.

The invention is depicted using Figure 1, which shows the decryption facility for key decryption algorithms, and the process for implementing encryption and decryption of digital information.

To explain in detail the decryption facility for key decryption algorithms shown in Figure 1, it is depicted as used in several PCs, whereby digital information is sent to selected owners of decryption facilities.

The depicted decryption facility consists of an integrated circuit 1, which is assigned a central processing unit CPU 2, an internal, non-readable, volatile

memory with random access RAM 3 as working memory and an internal, non-readable, non-volatile memory with random access ROM 4 [in which two internal, non-readable decryption algorithms (EI and EA) are stored] and an interface 5, which is set up between the central processing unit CPU 2 and the PC 6 and is linked to the PC 6 via the data path a , and is partially integrated into an integrated circuit 1.

The transfer of a key decryption algorithm to a decryption facility takes place as follows:

The distributor selects an encryption algorithm EEU. This is to be used to encrypt the key when it is later transferred. Of course this encryption algorithm must be kept secret and must be secure enough to provide security when encrypting keys. Several variations of the DES, for example (e.g. with different S boxes), or other encryption processes would be suitable here.

The decryption algorithm EE which corresponds with the encryption algorithm EEU is now encrypted to obtain the illegible algorithm EEV.

Now every user of the decryption facility who wishes to obtain a key can report to the distribution point. Contact can be made e.g. verbally (including by telephone), in written form or electronically. The user must identify him or herself using the public serial number of the decryption facility. Since this serial number is assigned only once, it is possible for the decryption facility and its users to be uniquely identified by the decryption facility. The distribution point can now decide whether the receiver is authorised to receive the decryption algorithm. This may depend on payment.

If the receiver is authorised, the encrypted decryption algorithm EEV is transferred to the user of the decryption facility and is decrypted in the decryption facility to obtain the algorithm EE.

Keys which were encrypted using the encryption algorithm EEU can now be decrypted.

for PCT/DE95/00738

The example below describes the process.

A volume of digital information is to be sent to selected customers. All of them are to be sent the entire information but not all are to have access to all of the information. One economical realisation here is, e.g. the distribution of this information via CD-ROM. These data media can be produced economically in large numbers and are capable of storing very large volumes of data. It appears to make sense, therefore, to place all of the information in encrypted form on a CD-ROM, send it to all customers and assign authorisation to the customers so that they can use the information. With this invention, authorisation is transferred as follows.

The CDs are distributed to all customers. Customer A is in possession of the decryption facility with the serial number SN=1.

Customer A is to receive information B. This information is encrypted on the CD-ROM using encryption algorithm EAU which corresponds with the usual internal decryption algorithm EA using the key K according to the formula

$$NV := EAU(NE, K)$$

Now Customer A must receive the key.

The information distributor prepares the transfer of the key to the decryption facility. The information distributor selects an encryption algorithm EEU, which is to be used to encrypt the key which will be transferred later. This encryption key is only ever transferred in encrypted form, never openly.

The internal decryption algorithms EI and the corresponding encryption algorithms EIU for all decryption facilities which have been issued to customers are available to the manufacturer of the decryption facility / the information distribution point in a database.

Let us say that EI1 is the internal decryption algorithm EI of the decryption facility (with internal serial number SN=1) belonging to Customer A. Let us also assume

that EI1U is the encryption algorithm corresponding to EI1 and is known only to the manufacturer of the decryption facility.

The key K, which is to be transferred to the decryption facility, is now encrypted. This entails the latter being encrypted using the encryption algorithm EEU corresponding to the decryption algorithm EE which is to be transferred to form the illegible key S, according to the following formula.

S:= EEU (K).

This encrypted key S is transferred to the decryption facility.

Of course, to decrypt this key, the decryption facility belonging to Customer A also needs the decryption algorithm EE. Since this must be kept secret, however, it is transferred in encrypted form.

This entails the decryption algorithm EE being encrypted using the encryption algorithm EIU corresponding to the internal decryption algorithm EI of the decryption facility to form the illegible algorithm EEV, according to the following formula:

EEV:= EI1U (EE).

This encrypted algorithm EEV is transferred to the decryption facility belonging to Customer A. This can be done e.g. verbally (including by telephone), in written form or electronically.

The encrypted algorithm which is transferred and the encrypted key are relatively short. This makes it virtually impossible to crack the internal decryption algorithm of the decryption facility EI. As shown above, for cracking algorithms to be used with any chance of success to break the encryption, a large number of plain and cipher texts must be present. This is virtually impossible here because of the small volume of information forwarded.

The receiver's decryption facility is now made operational.

The process when the power supply is switched on or following a break in processing is as follows:

The central processing unit CPU 2 runs a self test with the internal, non-readable, non-volatile memory with random access ROM 4 and the internal, non-readable volatile memory with random access RAM 3. This could take place e.g. via checksum formation.

The user of the decryption facility now enters the encrypted decryption algorithm EEV in the PC 6 or reads it in in another form.

The encrypted decryption algorithm EEV is now read into the decryption facility via the interface 5.

Next the decryption algorithm which is present in encrypted form EEV is decrypted with the help of the decryption algorithm EI stored in the internal, non-readable, non-volatile memory with random access ROM 4 using the internal decryption process EI. This entails the central processing unit CPU 2 carrying out the instructions of the decryption algorithm EI stored in the internal, non-readable, non-volatile memory with random access ROM 4 and decrypting the encrypted decryption algorithm EEV as follows:

EE:= EI1 (EEV).

Since the internal decryption algorithm EI1 matches the encryption algorithm EIU1 with which the decryption algorithm EE was encrypted, this process reproduces the original decryption algorithm EE.

This is stored in the internal, non-readable, volatile memory with random access RAM 3 which means that it cannot be discovered by external sources. This means that it is not possible to pass on the decryption algorithm since it is worthless in encrypted form and is not available in unencrypted form.

The decryption facility is now ready for use and it is now possible to compute the key K.

The decryption of a key which has been transferred to the customers in encrypted form takes place as follows:

The CPU loads the key S via the interface 5.

The non-readable key computation function EE in the decryption facility is now used to compute the key according to the formula:

$$K := EE(S).$$

This key K can never be found outside the decryption facility and cannot be detected. This means that it is not possible for anyone to pass it on.

The information from the CD-ROM is now loaded via the interface 6.

Next it is decrypted by the central processing unit CPU 2 with the usual decryption algorithm of the decryption facility EA using the key K:

$$NE := EA(NV, K)$$

The decrypted information NE is then output by the central processing unit CPU 2 via the interface 5 and is thus available to the customer.

Access to the encrypted information can thus be made flexible. It is possible to make parts of the information on a CD-ROM available to specific groups of receivers or individual receivers without it being possible for them to pass on the keys. This means that keys can be encrypted with different encryption algorithms and decrypted with different decryption algorithms without the decryption algorithm having to be known or having to be available beforehand in the decryption facility.

The transferred key decryption algorithm cannot be passed on or detected since it is transferred individually for each decryption facility in encrypted form, is stored there in non-readable form and is made available for internal use of the decryption

facility with the corresponding serial number only. This makes it possible to exclude decryption facilities too from receiving information.

Reference numbers used

1 integrated circuit

2 central processing unit CPU

3 internal, non-readable, volatile memory with random access RAM

4 internal, non-readable, non-volatile memory with random access ROM

5 interface

6 PC

a data path

Abbreviations used

CPU	=	central processing unit
DEA	=	data encryption standard
EA	=	internal decryption algorithm for decrypting information
EAU	=	encryption algorithm for information distributor for encryption of information, corresponding to EA
EI	=	internal decryption algorithm for decryption of transferred decryption algorithms
EI1	=	internal decryption algorithm for the decryption facility with serial number SN=1
EIU	=	encryption algorithm corresponding to internal decryption algorithm EI
EI1U	=	encryption algorithm corresponding with the internal decryption algorithm EI1 for the decryption facility with the serial number SN=1
EE	=	decryption algorithm for the decryption of encrypted keys
EEV	=	encrypted decryption algorithm
EEU	=	encryption algorithm corresponding to EE
NE	=	non-encrypted or decrypted information
NV	=	encrypted information
Key K =		key for the decryption of messages
Key S =		key which has been encrypted using the encryption algorithm EEU for the decryption of messages

(:=) = is the result of

for PCT/DE95/00738

Patent claims

1. Procedure for the encryption and decryption of digital information by means of a decryption facility consisting of an integrated circuit (1) which is assigned a central processing unit CPU (2), an internal, non-readable, volatile memory with optional access RAM (3) as working memory and an internal, non-readable, non-volatile memory with optional access ROM (4) and an interface (5), whereby each encryption facility differs from all others as a result of the contents of the internal, non-volatile memory with optional access ROM (4) and is partially integrated into an integrated circuit (1), the interface (5) being between the central processing unit CPU (2) and the personal computer (6), whereby the interface (5) is connected to the personal computer (6) via a data path (a),
characterised by the fact that
the distributor of the decryption algorithm encrypts this using an encryption algorithm (EIU) which corresponds to the decryption algorithm (EI),
and which can be decrypted using the decryption algorithm, and the encryption algorithm (EIU) and decryption algorithm (EI) are stored unit-specifically in the internal, non-readable, non-volatile memory with optional access ROM (4) which is present internally in the receiving decryption unit, so that the decryption algorithm (EI) cannot be publicly accessed or detected, meaning that the user of the decryption facility enters the encrypted decryption algorithm in the decryption facility and this is decrypted within the decryption facility.

2. Procedure for the encryption and decryption of digital information by means of a decryption facility, characterised by the fact that
in Step 1
the decryption algorithm is encrypted by the distributor of the decryption algorithm using an encryption algorithm (EIU) which is known only to the manufacturer of

for PCT/DE95/00738

the decryption facility and corresponds to the decryption algorithm (EI) in the decryption unit as follows:

EEV:=EIU (EE)

and this encrypted algorithm (EEV) is transferred to the decryption facility, following which

in Step 2

the decryption facility, using the central processing unit CPU (2) with the internal, non-readable, non-volatile memory with optional access ROM (4) runs a self test and the encrypted decryption algorithm (EEV) is read in to the decryption facility via the interface (5) and then decrypted with the aid of the decryption algorithm (EI) stored in the internal, non-readable, non-volatile memory with optional access ROM (4), using the following decryption method (EI)

EE:=EI (EEV)

whereby the result of this step is to reproduce the original decryption algorithm (EE), which

in Step 3

is saved in the internal, non-readable, volatile memory with optional access RAM (3), where it is undetectable from outside, making the decryption facility ready for operation with the decryption algorithm (EE), the decryption of the key (S) taking place

in Step 4

as follows, the CPU loading the key (S) via the interface (5) and the key (S) being decrypted by the central processing unit CPU (2) using the decryption algorithm (EE) according to

K:=EE (S)

resulting in the key (K) being available for the decryption, and

in Step 5

the digital information is decrypted by the central processing unit CPU (2) with the internal decryption algorithm (EA) using the key (K), which does not appear outside the integrated circuit (1), according to

for PCT/DE95/00738

NE:=EA (NV,K)

and is output by the central processing unit CPU (2) via the interface (5) and so made available to the receiver.

SEE SEPARATE SHEET WITH DIAGRAM!

Summary

The invention is a procedure for the encryption and decryption of digital information by means of a decryption facility, the decryption facility granting access to authorised persons and denying access to unauthorised persons.

The task of the invention is to develop a procedure for the encryption and decryption of digital information by means of a decryption facility, using which information can be distributed in a user-friendly way to several receivers and where the encryption of the information requires little technical administrative effort, whereby keys can be distributed securely and transferred in a manner which guarantees them secure against detection. Furthermore, it should not be possible for the owner of a decryption device to pass on a key since the distributed algorithms for encryption and decryption of the transferred key cannot be exchanged between encryption and decryption facilities.

According to the invention, the task is solved by the distributor of the decryption algorithm encrypting the latter with an encryption algorithm (EIU) which corresponds to the decryption algorithm (EI) which is present internally in the relevant receiving decryption unit, and by the fact that the decryption algorithm (EI) cannot be openly accessed or discovered, and that the user of the decryption facility enters the encrypted decryption algorithm in the decryption facility and this algorithm is then decrypted inside the decryption facility.

(See Figure 1)