

METHOD AND SYSTEM FOR GENERATING CIPHERTEXT BY PIN ENTRY DEVICE

FIELD OF THE INVENTION

The present invention relates to a method and a system for generating ciphertext by a personal identification number (PIN) entry device or a PIN pad.

BACKGROUND

The following discussion of the background to the invention is intended to facilitate an understanding of the present invention. However, it should be appreciated that the discussion is not an acknowledgment or admission that any of the material referred to was published, known or part of the common general knowledge in any jurisdiction as at the priority date of the application.

A PIN entry device or a PIN pad is an electronic device that is used to receive and encrypt a cardholder's personal identification number in a card-based transaction. Generally, encryption through the use of PIN pads on bank automated teller machines (ATMs) or video teller machines (VTMs) is achieved by directly processing the encryption keys. A security concern arises when there is illegal access to a bank's encryption keys, which then allows the password of users to be easily stolen falling into the wrong hands.

To prevent the illegal access to a bank's encryption keys, some ATM manufacturers add an encryption chip on hardware of the PIN pad to encrypt the PIN pad input. However, it is expensive to add such an encryption chip on the hardware hence the cost of manufacturing an ATM will be increased, which is to the disadvantage of ATM manufacturers.

Therefore, there is an urgent need to address the technical issues of low security PIN pads and the high costs associated by the addition of an encryption chip on the hardware of PIN entry devices or PIN pads. The present invention seeks to provide a method and a system to overcome at least in part some of the aforementioned disadvantages.

SUMMARY OF THE INVENTION

Throughout this document, unless otherwise indicated to the contrary, the terms `comprising`, `consisting of`, and the like, are to be construed as non-exhaustive, or in other words, as meaning `including, but not limited to`.

In accordance with a first aspect of the present invention, there is provided a method for generating ciphertext by a personal identification number (PIN) entry device. The method comprises: acquiring a password input by a user, decrypting a predetermined working key using a predetermined master key, and producing a ciphertext and a key code using a predetermined encryption algorithm and the working key, the encryption algorithm set in the PIN entry device and each of the working key and the master key loaded in a storage area of the PIN entry device; splitting the ciphertext into a first ciphertext and a second ciphertext according to the number of digits of the key code, and storing each of the first ciphertext and the second ciphertext in respective storage areas of the PIN entry device.

Preferably, the password is encrypted using the working key based on the encryption algorithm to generate the ciphertext and the key code, and wherein the ciphertext is a character string of predetermined digits, and the key code is the number of digits of the password input by the user.

Preferably, according to the number of digits of the key code, the ciphertext is split into the first ciphertext comprising characters of the same number of digits as that of the key code, and the second ciphertext comprising the remaining number of characters.

Preferably, the method further comprises verifying the password by a system.

Preferably, the password is verified by acquiring the first ciphertext and the second ciphertext in the storage areas of the PIN entry device; calculating the first ciphertext and the second ciphertext using hash algorithm to obtain a first string checksum and a second string checksum respectively to determine if the ciphertexts have been tampered with; if they have not been tampered with, merging the first ciphertext and the second ciphertext into the original ciphertext to verify the password input by the user, thereby completing the verification process.

Preferably, if the ciphertexts have been tampered with, the system terminates the verification process.

Preferably, the system merges the first ciphertext, the first string checksum, the second ciphertext and the second string checksum into a data package.

Preferably, prior to the first usage of the PIN entry device, the PIN entry device is initialized for determining the validity of the PIN entry device.

Preferably, the PIN entry device is initialized through setting environment variables and configuration parameters based on the Payment Card Industry (PCI) standard.

Preferably, if the PIN entry device is valid, setting the predetermined encryption algorithm for the PIN entry device and loading the predetermined master key and the predetermined working key into a storage area of the PIN entry device.

Preferably, the encryption algorithm of the PIN entry device uses a PIN encryption scheme selected from ISO9564-0, IBM3624 or ASCII, and the encryption algorithm is selected from DES or 3DES.

Preferably, the master key is loaded, the working key is loaded using the master key, and the storage area in the PIN entry device is selected for loading the keys therein.

In accordance with a second aspect of the present invention, there is provided a system for generating ciphertext by a personal identification number (PIN) entry device; wherein the PIN entry device is operable to acquire a password input by a user, decrypt a predetermined working key using a predetermined master key, and produce a ciphertext and a key code using a predetermined encryption algorithm and the working key, the encryption algorithm set in the PIN entry device and each of the working key and the master key loaded in a storage area of the PIN entry device; the PIN entry device is further operable to split the ciphertext into a first ciphertext and a second ciphertext according to the number of digits of the key code and storing each of the first ciphertext and the second ciphertext in respective storage areas of the PIN entry device.

Preferably, the password is encrypted using the working key based on the encryption algorithm to generate the ciphertext and the key code, and wherein the ciphertext is a character string of predetermined digits, and the key code is the number of digits of the

password input by the user.

Preferably, according to the number of digits of the key code, the ciphertext is split into the first ciphertext comprising characters of the same number of digits as that of the key code, and the second ciphertext comprising the remaining number of characters.

Preferably, according to the number of digits of the key code, the ciphertext is split into the first ciphertext comprising characters of the same number of digits as that of the key code, and the second ciphertext comprising the remaining number of characters.

Preferably, the system further comprises a system for verifying the password.

Preferably, the system is operable to verify the password by acquiring the first ciphertext and the second ciphertext in the storage areas of the PIN entry device; calculating the first ciphertext and the second ciphertext using hash algorithm to obtain a first string checksum and a second string checksum respectively to determine if the ciphertexts have been tampered with; if they have not been tampered with, merging the first ciphertext and the second ciphertext into the original ciphertext to verify the password input by the user, thereby completing the verification process.

Preferably, if the ciphertexts have been tampered with, the system terminates the verification process.

Preferably, the system merges the first ciphertext, the first string checksum, the second ciphertext and the second string checksum into a data package.

Preferably, prior to the first usage of the PIN entry device, the PIN entry device is initialized for determining the validity of the PIN entry device.

Preferably, the PIN entry device is initialized through setting environment variables and configuration parameters based on the Payment Card Industry (PCI) standard.

Preferably, if the PIN entry device is valid, setting the predetermined encryption algorithm for the PIN entry device and loading the predetermined master key and the predetermined working key into a storage area of the PIN entry device.

Preferably, the encryption algorithm of the PIN entry device uses a PIN encryption

scheme selected from ISO9564-0, IBM3624 or ASCII, and the encryption algorithm is selected from DES or 3DES.

Preferably, the master key is loaded, the working key is loaded using the master key, and the storage area in the PIN entry device is selected for loading the keys therein.

In accordance with a third aspect of the present invention, there is provided a method for generating ciphertext by a PIN entry device substantially as herein described with reference to the accompanying drawing as appropriate.

In accordance with a fourth aspect of the present invention, there is provided a system for generating ciphertext by a PIN entry device substantially as herein described with reference to the accompanying drawing as appropriate.

Other aspects and advantages of the invention will become apparent to those skilled in the art from a review of the ensuing description, which proceeds with reference to the following illustrative drawings of various embodiments of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will now be described, by way of illustrative example only, with reference to the accompany drawing, of which:

Figure 1 is a flowchart of a method for generating ciphertext by a personal identification device (PIN) entry device in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

Particular embodiments of the present invention will now be described with reference to the accompanying drawing. The terminology used herein is for the purpose of describing particular embodiments only and is not intended to limit the scope of the present invention. Additionally, unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art to which this invention belongs.

In order to solve the technical issues of low security of personal identification number (PIN) entry devices or PIN pads and high cost associated by the addition of an encryption

chip on the hardware of PIN entry devices or PIN pads, the present invention provides a method and a system for effectively preventing PIN pad input from being cracked or hacked into and for generating ciphertext using a PIN pad at a low cost. In order to achieve the above-mentioned technical objectives, the technical solution of the present invention in accordance with an embodiment of the present invention is a method for generating ciphertext by a PIN entry device or a PIN pad, comprising the steps of:

i) Examining whether the PIN pad is valid. If the PIN pad is not valid, terminating the whole generating process of ciphertext; if it is valid, continuing the process by setting the algorithm for generating ciphertext by PIN pad; and loading a master key and a working key such as a bank's master key and working key to a storage area in the PIN pad;

ii) Processing the password input by the customer. This comprises acquiring the password input by a customer, decrypting the working key using the master key, and producing ciphertext and key code using the algorithm set in step i and the working key; splitting the ciphertext into a first ciphertext (ciphertext A) and a second ciphertext (ciphertext B) according to the number of digits of key code and storing the two parts in the storage areas in the PIN pad respectively;

iii) Verifying the password input by the customer by a system such as a bank system. This comprises producing string checksum by calculating the split ciphertext using hash algorithm; sending the ciphertext and string checksum to the bank system for decryption and certification; verifying the ciphertext and string checksum by the bank system to determine whether they are tampered with or not; if they are not tampered with, merging ciphertext A and ciphertext B into the original ciphertext to verify the password input by the customer, thereby completing the whole verification process.

Said step i of said method for generating ciphertext by PIN pad, wherein the validity of PIN pad is examined by initializing PIN pad through setting environment variables and configuration parameters based on the Payment Card Industry (PCI) standard. As the current PCI standard is PCI 3.0, it is preferable that the environment variables and configuration parameters set are based on PCI 3.0. However, it would be appreciated that the environment variables and configuration parameters can be set to a higher PCI standard as and when a newer or more up to date PCI version or standard becomes available. If the initialization is successfully carried out, then the PIN pad is determined

as valid; if not, the PIN pad is invalid. The initialization of the PIN pad is performed only once prior to the first usage of the PIN pad. Once the PIN pad is determined as valid, initialization of the PIN pad is not required for subsequent usage of the PIN pad.

Said step i of said method for generating ciphertext by PIN pad, wherein the encryption algorithm of the PIN pad uses one PIN encryption schemes from ISO9564-0, IBM3624 or ASCII, and its encryption algorithm is DES or 3DES.

Said step i of said method for generating ciphertext by PIN pad, wherein the master key is loaded first, then working key is loaded using master key and storage areas in PIN pad are chosen for loading keys in it.

Said step ii of said method for generating ciphertext by PIN pad, wherein the password input by the customer is acquired, the master key is decrypted to get the working key, then according to encryption algorithm set previously, the password is encrypted using working key to generate ciphertext and key code, wherein the ciphertext is a character string of preset digit, the key code is the number of digits of the password input by the customer.

Said step ii of said method for generating ciphertext by PIN pad, wherein according to the digit of key code, the ciphertext is split into ciphertext A with the characters of the same number of digits as that of the key code, and ciphertext B that includes the rest numbers of characters.

Said step iii of said method for generating ciphertext by PIN pad, wherein the system acquires ciphertext A in the storage area of PIN pad, calculates it using hash algorithm to get a first string checksum (string checksum A'); acquires ciphertext B, calculates it using hash algorithm to get a second string checksum (string checksum B'); and then merges ciphertext A, string checksum A', ciphertext B and string checksum B' into a data package, which is sent to bank system for decryption and certification.

Said step iii of said method for generating ciphertext by PIN pad, wherein the bank system calculates ciphertext A and ciphertext B by hash algorithm to get the checksum A' and the checksum B' for verification to determine whether they are tampered with or not; if they are no tampered with, the bank system merges ciphertext A and ciphertext B into the original complete ciphertext, and then verifies the password input by the customer;

otherwise the system terminates the verification process directly.

The technical effect of present invention is as follows: through splitting on a basis of the number of digits of key code, storing and sending ciphertext, ciphertext security level is further improved; disruption of encryption logic is avoided and stability is enhanced since the ciphertext is split based on original key code with original encryption scheme of the bank's keys unchanged.

With reference to Figure 1, there is described a method for generating ciphertext by a PIN entry device or a PIN pad in accordance with an embodiment of the present invention. To ensure encryption security of a password input by a customer, a method of the present invention includes the following steps:

First, reliability of the PIN entry device or PIN pad is confirmed; before a password input by a customer is encrypted and stored, the system initializes the PIN pad:

1. Initializing PIN pad through setting environment variables and configuration parameters based on PCI standard to determine whether the PIN pad is valid, if the initialization is successfully carried out, then the PIN pad is determined as valid; if not, the PIN pad is invalid.
2. Setting the algorithm for generating ciphertext by the PIN pad, wherein PIN encryption schemes may be used, the PIN encryption schemes include the following but are not limited to ISO9564-0, IBM3624 or ASCII, and encryption algorithms include but are not limited to DES or 3DES.
3. Loading the bank's keys after acquiring a key pair from the bank, in which the key pair includes a master key and a working key, the latter is loaded following the former because the working key can only be encrypted using the master key; there is a total of 16 storage areas numbered 0-15 in the PIN pad, which can be randomly selected for the storage of the keys. It would be appreciated that the total number of storage areas can be more than 16 or less than 16.

After the PIN pad is initialized, the method includes the steps of:

4. Acquiring the password input by the customer, first reading the master key so as to decrypt the working key, then encrypting the password using the encryption algorithm set

previously and the working key to produce character ciphertext. In present embodiment, the character ciphertext is assumed to contain 16 characters, and a key code of "*" is generated at the same time, in present embodiment, the number of digits of the password input by customer is assumed to be 6, thereby the key code is displayed as "*****". It would be appreciated that the number of characters can be more than 16 or less than 16. It would also be appreciated that the number of digits of the password can be more than 6 or less than 6, depending on requirements imposed by the respective financial institutions such as a bank.

5. Dividing the ciphertext according to the number of digits of the key code, if the number of digits of the key code is 6, the ciphertext shall be split into a first ciphertext (ciphertext A) that contains the former 6 characters and a second ciphertext (ciphertext B) that contains the latter 10 characters.

6. Storing the ciphertext A and the ciphertext B in the optional 16 storage areas respectively.

When the bank needs to verify the password input by the customer, the method includes the following steps:

7. The system or bank system acquires the ciphertext A from the storage areas and calculates the ciphertext A using hash algorithm to produce 16-digit first string checksum (string checksum A'); acquires the ciphertext B from the storage areas and calculates the ciphertext B using hash algorithm to produce 16-digit second string checksum (string checksum B').

8. Merging the ciphertext A, string checksum A', ciphertext B, string checksum B' into a 48-digit data package and sending the data package to bank system for decryption and verification.

9. The bank system calculates the ciphertext A and ciphertext B using hash algorithm to produce the checksum A' and checksum B' to verify whether they are tampered with or not.

10. If they are not tampered with, the ciphertext A and ciphertext B shall be merged into the original complete ciphertext so as to verify the password input by the customer, thereby

completing the whole verification process.

In accordance with another aspect of the present invention, there is described a system for generating ciphertext by a personal identification number (PIN) entry device in accordance with an embodiment of the present invention. The PIN entry device is operable to acquire a password input by a user, decrypt a predetermined working key using a predetermined master key, and produce a ciphertext and a key code using a predetermined encryption algorithm and the working key, the encryption algorithm set in the PIN entry device and each of the working key and the master key loaded in a storage area of the PIN entry device. The PIN entry device is further operable to split the ciphertext into a first ciphertext and a second ciphertext according to the number of digits of the key code and storing each of the first ciphertext and the second ciphertext in respective storage areas of the PIN entry device.

The password is encrypted using the working key based on the encryption algorithm to generate the ciphertext and the key code, and wherein the ciphertext is a character string of predetermined digits, and the key code is the number of digits of the password input by the user.

According to the number of digits of the key code, the ciphertext is split into the first ciphertext comprising characters of the same number of digits as that of the key code, and the second ciphertext comprising the remaining number of characters.

According to the number of digits of the key code, the ciphertext is split into the first ciphertext comprising characters of the same number of digits as that of the key code, and the second ciphertext comprising the remaining number of characters.

The system further comprises a system, such as a bank system, for verifying the password. This system is operable to verify the password by acquiring the first ciphertext and the second ciphertext in the storage areas of the PIN entry device; calculating the first ciphertext and the second ciphertext using hash algorithm to obtain a first string checksum and a second string checksum respectively to determine if the ciphertexts have been tampered with; if they have not been tampered with, merging the first ciphertext and the second ciphertext into the original ciphertext to verify the password input by the user, thereby completing the verification process. If the ciphertexts have been tampered with,

the system terminates the verification process.

If the ciphertexts have not been tampered with, the system merges the first ciphertext, the first string checksum, the second ciphertext and the second string checksum into a data package.

Prior to the first usage of the PIN entry device or PIN pad, the PIN entry device is initialized for determining the validity of the PIN entry device. The PIN entry device is initialized through setting environment variables and configuration parameters based on the Payment Card Industry (PCI) standard. As the current PCI standard is PCI 3.0, it is preferable that the environment variables and configuration parameters set are based on PCI 3.0. However, it would be appreciated that the environment variables and configuration parameters can be set to a higher PCI standard as and when a newer or more up to date PCI version or standard becomes available

If the PIN entry device is valid, the predetermined encryption algorithm for the PIN entry device is set and the predetermined master key and the predetermined working key are loaded into a storage area of the PIN entry device. The master key is first loaded, and the working key is loaded using the master key, and the storage area in the PIN entry device is selected for loading the keys therein. The encryption algorithm of the PIN entry device uses a PIN encryption scheme selected from ISO9564-0, IBM3624 or ASCII, and the encryption algorithm is selected from DES or 3DES. It would be appreciated that the present invention is not limited to the above-mentioned PIN encryption schemes and encryption algorithm, and other suitable PIN encryption schemes and encryption algorithm can also be used.

Advantageously, the present invention further improves the security of ciphertext by separately storing and sending the ciphertext according to the number of digits of a key code. As the generated ciphertext is split according to the original key code, which will not change the original way of encryption of key, the method and the system of the present invention of generating ciphertext by a PIN entry device or a PIN pad provides higher stability without causing logic disruption in decryption.

It is to be understood that the above embodiments have been provided only by way of exemplification of this invention, and that further modifications and improvements thereto,

as would be apparent to persons skilled in the relevant art, are deemed to fall within the broad scope and ambit of the present invention described herein. It is further to be understood that features from one or more of the described embodiments may be combined to form further embodiments of the invention.

CLAIMS

1. A method for generating ciphertext by a personal identification number (PIN) entry device, comprising:

acquiring a password input by a user, decrypting a predetermined working key using a predetermined master key, and producing a ciphertext and a key code using a predetermined encryption algorithm and the working key, the encryption algorithm set in the PIN entry device and each of the working key and the master key loaded in a storage area of the PIN entry device; splitting the ciphertext into a first ciphertext and a second ciphertext according to the number of digits of the key code, and storing each of the first ciphertext and the second ciphertext in respective storage areas of the PIN entry device.

2. The method for generating ciphertext by a PIN entry device according to claim 1, wherein the password is encrypted using the working key based on the encryption algorithm to generate the ciphertext and the key code, and wherein the ciphertext is a character string of predetermined digits, and the key code is the number of digits of the password input by the user.

3. The method for generating ciphertext by a PIN entry device according to claim 2, wherein according to the number of digits of the key code, the ciphertext is split into the first ciphertext comprising characters of the same number of digits as that of the key code, and the second ciphertext comprising the remaining number of characters.

4. The method for generating ciphertext by a PIN entry device according to any one of the preceding claims, further comprising verifying the password by a system.

5. The method for generating ciphertext by a PIN entry device according to claim 4, wherein the password is verified by acquiring the first ciphertext and the second ciphertext in the storage areas of the PIN entry device; calculating the first ciphertext and the second ciphertext using hash algorithm to obtain a first string checksum and a second string checksum respectively to determine if the ciphertexts have been tampered with; if they have not been tampered with, merging the first ciphertext and the second ciphertext into the original ciphertext to verify the password input by the user, thereby

completing the verification process.

6. The method for generating ciphertext by a PIN entry device according to claim 5, wherein if the ciphertexts have been tampered with, the system terminates the verification process.

7. The method for generating ciphertext by a PIN entry device according to claim 5, wherein the system merges the first ciphertext, the first string checksum, the second ciphertext and the second string checksum into a data package.

8. The method for generating ciphertext by a PIN entry device according to claim 1, wherein prior to the first usage of the PIN entry device, the PIN entry device is initialized for determining the validity of the PIN entry device.

9. The method for generating ciphertext by a PIN entry device according to claim 8, wherein the PIN entry device is initialized through setting environment variables and configuration parameters based on the Payment Card Industry (PCI) standard.

10. The method for generating ciphertext by a PIN entry device according to claim 8 or 9, wherein if the PIN entry device is valid, setting the predetermined encryption algorithm for the PIN entry device and loading the predetermined master key and the predetermined working key into a storage area of the PIN entry device.

11. The method for generating ciphertext by a PIN entry device according to claim 10, wherein the encryption algorithm of the PIN entry device uses a PIN encryption scheme selected from ISO9564-0, IBM3624 or ASCII, and the encryption algorithm is selected from DES or 3DES.

12. The method for generating ciphertext by a PIN entry device according to claim 10, wherein the master key is loaded, the working key is loaded using the master key, and the storage area in the PIN entry device is selected for loading the keys therein.

13. A system for generating ciphertext by a personal identification number (PIN) entry device; wherein the PIN entry device is operable to acquire a password input by a user, decrypt a predetermined working key using a predetermined master key, and produce a ciphertext and a key code using a predetermined encryption algorithm and the working key, the encryption algorithm set in the PIN entry device and each of the working key

and the master key loaded in a storage area of the PIN entry device; the PIN entry device is further operable to split the ciphertext into a first ciphertext and a second ciphertext according to the number of digits of the key code and storing each of the first ciphertext and the second ciphertext in respective storage areas of the PIN entry device.

14. The system for generating ciphertext by a PIN entry device according to claim 13, wherein the password is encrypted using the working key based on the encryption algorithm to generate the ciphertext and the key code, and wherein the ciphertext is a character string of predetermined digits, and the key code is the number of digits of the password input by the user.

15. The system for generating ciphertext by a PIN entry device according to claim 14, wherein according to the number of digits of the key code, the ciphertext is split into the first ciphertext comprising characters of the same number of digits as that of the key code, and the second ciphertext comprising the remaining number of characters.

16. The system for generating ciphertext by a PIN entry device according to any one of claims 13 to 15, further comprising a system for verifying the password.

17. The system for generating ciphertext by a PIN entry device according to claim 16, wherein the system is operable to verify the password by acquiring the first ciphertext and the second ciphertext in the storage areas of the PIN entry device; calculating the first ciphertext and the second ciphertext using hash algorithm to obtain a first string checksum and a second string checksum respectively to determine if the ciphertexts have been tampered with; if they have not been tampered with, merging the first ciphertext and the second ciphertext into the original ciphertext to verify the password input by the user, thereby completing the verification process.

18. The system for generating ciphertext by a PIN entry device according to claim 17, wherein if the ciphertexts have been tampered with, the system terminates the verification process.

19. The system for generating ciphertext by a PIN entry device according to claim 17, wherein the system merges the first ciphertext, the first string checksum, the second ciphertext and the second string checksum into a data package.

20. The system for generating ciphertext by a PIN entry device according to claim 13, wherein prior to the first usage of the PIN entry device, the PIN entry device is initialized for determining the validity of the PIN entry device.

21. The system for generating ciphertext by a PIN entry device according to claim 20, wherein the PIN entry device is initialized through setting environment variables and configuration parameters based on the Payment Card Industry (PCI) standard.

22. The system for generating ciphertext by a PIN entry device according to claim 20 or 21, wherein if the PIN entry device is valid, setting the predetermined encryption algorithm for the PIN entry device and loading the predetermined master key and the predetermined working key into a storage area of the PIN entry device.

23. The system for generating ciphertext by a PIN entry device according to claim 22, wherein the encryption algorithm of the PIN entry device uses a PIN encryption scheme selected from ISO9564-0, IBM3624 or ASCII, and the encryption algorithm is selected from DES or 3DES.

24. The system for generating ciphertext by a PIN entry device according to claim 22, wherein the master key is loaded, the working key is loaded using the master key, and the storage area in the PIN entry device is selected for loading the keys therein.