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.