OPIC
Office de la propriété intellectuelle du Canada

CIPO
Canadian Intellectual Property Office

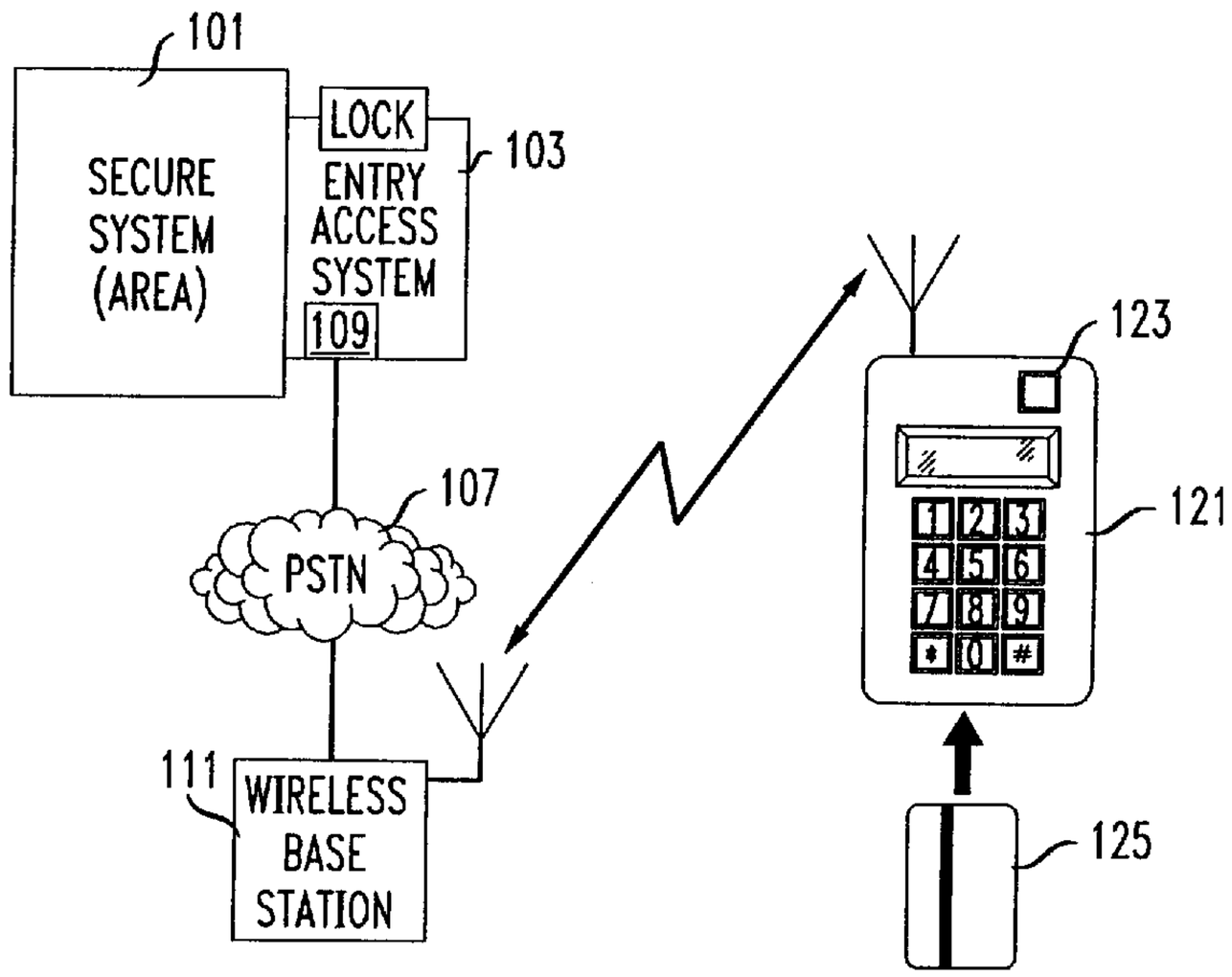
(12) (19) (CA) **Brevet-Patent**

(11) (21) (C) **2,197,367**
(22) 1997/02/12
(43) 1997/11/30
(45) 2000/02/01

(72) Miller, Robert Raymond II, US
(73) AT&T CORP., US

(51) Int.Cl.[6] H04L 9/32
(30) 1996/05/29 (657,448) US

(54) **SYSTEME D'ACCES A DISPOSITIF DE SECURITE**
(54) **SECURITY ACCESS SYSTEM**



(57) L'invention est un système d'accès comportant un mécanisme de verrouillage permettant d'autoriser l'accès à une aire fermée ou à un ordinateur. L'accès est approuvé en réponse à une interaction entre le demandeur d'accès et le système d'accès, cette interaction étant constituée par un échange de numéros à chiffres multiples et par l'utilisation de pièces d'identité et de numéros d'identification pour produire un numéro de vérification à plusieurs chiffres afin d'authentifier la demande d'accès.

(57) An entry access system includes a locking mechanism enabling authorized entry at a secured entry point to a closed access area or computing device. Entry is approved in response to an interaction between an intended entrant and the entry access system that involves an interchange of multidigit numbers and use of ID and PINs for generation of a multidigit check number to establish authenticity of a request for entry.

Security Access System

Abstract

An entry access system includes a locking mechanism enabling authorized entry at a secured entry point to a closed access area or computing device. Entry is approved in response to an interaction between an intended entrant and the entry access system that involves an interchange of multidigit numbers and use of ID and PINs for generation of a multidigit check number to establish authenticity of a request for entry.

Security Access System

Field of the Invention

This invention relates to secure access entry systems and in particular to such a system based on a use of telephones and telephone systems including; cellular, PCS wireless, public switched telephone systems, wired telephone systems all in combination with the use of a smart card for storage of access information.

Background of the Invention

A secured access entry is effective to prevent unauthorized entry only to the extent that an intruder is unable to reconstruct any authorized entry means of access such as a key, a combination, a password, etc. If the entry means is relatively simple to enhance the performance of an authorized entrant it is too often ascertained by an unauthorized entrant for unauthorized entry. On the other hand a sophisticated complicated entry means may inadvertently defeat even the authorized entrant. It is necessary to devise an entry authorization system for entry that is friendly to authorized entrants and yet able to defeat unauthorized entry attempts.

In another aspect the entry means may operate by a transmission of passwords over an insecure transmission facility. The protection afforded may be compromised by interception of this information by an unauthorized recipient.

Summary of the Invention

An entry access system includes a locking mechanism enabling authorized entry at a secured entry point to a closed access area or computing device. Entry is approved in response to an interaction between a intended entrant and the entry access system that involves an interchange of ID and PINs and generation of a multidigit number encrypted to establish a relation between valid ID and PIN combinations. Transmission of ID and related numbers is encrypted internally at both ends so that interception of the number is useless to an unauthorized intercepting recipient.

In a particular embodiment an intended entrant/user accesses a system ID in a personal communicator by entering or enabling entry of a PIN number into the device. A smart card, in one preferred embodiment, is inserted into the personal communicator and provides the ID number which the user accesses by entry of the PIN which is compared to a PIN stored in the card. The communicator is connected by telephone link to the entry access system by dialing of the communicator user or automatically in response to the smart card. The entry access system correlates the received ID with a PIN stored in its data base. An arbitrary multidigit number is

constructed and transmitted to the communicator.

At the communicator the multidigit number is received and a new number is generated, using encryption algorithm techniques with the PIN as a key. The new number is retransmitted back to the entry access system where a check number is generated, using the new number, and using the PIN as a key. The check number is compared with the original generated arbitrary number. If they match access is granted to the entry applicant.

The generated numbers may be transmitted openly between stations without compromising system security since the encryption processes are limited to internal processes at each end. Attainment of the transmitted numbers through interception by an unauthorized recipient is of no value in gaining access to the secure area.

In accordance with one aspect of the present invention there is provided a method of providing access to a secure system through an entry access system in which access is granted in response to a protocol process, comprising the steps of: providing a user with a system ID and a PIN; storing the system ID in a communication device and allowing a user to access use of the ID by entry of the PIN; establishing a telephone communication link between the communication device and the entry access system; entering the PIN into the communication device to allow transmission of the ID to the entry access system; at the entry access system correlating the received ID with a stored PIN assigned to the user; transmitting from the entry access system a multidigit number to the communication device derived from the stored PIN; receiving the multidigit number at the communication device and transforming by encryption techniques to attain a new number by using the PIN as a key; returning the transformed new number to the entry access system; transforming the received number at the entry access system utilizing the PIN as key and utilizing the same encryption techniques to attain a check number; deactivating the lock if the check number is identical to the new number.

In accordance with another aspect of the present invention there is provided an entry access system for controlling access to a secure system, comprising: means for communicating over a telephone network; a data base of ID and PIN numbers; means for generating an arbitrary multidigit number in response to an ID communicated by an intended entrant to the secure system; means for converting the multidigit number into

DTMF multitones; telephone communication means connected for transmitting the multitones into a telephone network for transmission to the intended entrant; means for receiving a number generated by encryption methods of a communicator of the intended entrant from an ID and PIN of the entrant, via the telephone network; means for generating a check number using the stored PIN as a key and comparing it to the multidigit number; a locking mechanism for enabling/disabling entry to the secure system operative to identity of the multidigit number and the generated check number.

Brief Description of the Drawing

FIG. 1 is a schematic of a secured access system according to the principles of the invention;

FIG. 2 is a schematic of a protocol arrangement included in the entry access system for allowing access according to the principles of the invention; and

FIG. 3 is a flow chart illustrating a process in which the entry access system operates.

Detailed Description

A secured system shown in FIG. 1 has an area, computer or data storage 101 which is secured from entry by the entry access system 103 which controls a locking mechanism 105 which needs to be released before a user can gain access to the interior of the secure system (i.e., area). The entry access system includes a telephone station set 109 connected to the public switched telephone network (PSTN) 107.

The PSTN 107 is connected to a wireless base station 111. The user desiring entry to the secure system 101 in the illustrative embodiment has a mobile communicator 121 in wireless communication with the wireless base station 111. Communicator 121 preferably has a touch tone decoder 123 for receiving and transmitting numbers as DTMF dual frequencies. The invention is not limited to wireless communication but may communicate, in the alternative, through a wired station set external to the secure area. The communicator is arranged to accept a smart card 125 which includes data storage relevant to the card holder. The smart card may include information such as an ID number, a PIN (i.e., also stored at the entry access system) or other information relevant to the user. In the alternative, to a

A

smart card, certain of this information may be entered by the user through the communicator keyboard.

A more detailed disclosure of the entry access system is shown in the FIG. 2. The entry access system includes a stored data base 201 of ID numbers of the authorized entrants to the secure system. This is connected to the bus 202. Also connected to the bus are a data base 203 of PIN numbers of authorized entrants and in/out unit 205 for connecting to a subscriber telephone set of the entry access system. An encryption engine 207 is operative for examining input PIN and ID numbers and generating a arbitrary multidigit number. This number is converted to DTMF multitones by the generator 209 in the illustrative embodiment for transmission, via the in/out unit 205 and telephone network to the user's communication unit.

The multidigit number returned to the entry access system from the communicator is applied the encryption engine 207 which compares it with the original transmitted number. If the two compare a signal is transmitted through the in /out unit to admit access to the user.

An illustrative process by which entry is approved into the system is shown schematically in the flow process chart of FIG. 3. Beginning at the start, terminal 301, the flow proceeds to execute the instructions of block 303 reflecting the action of the user of inserting user's smart card, which contains user relevant information such as the user's PIN, into the personal communicator or communication device, which may be a cellular telephone or PCS communicator.

A subsequent instruction illustrated in block 305 has the user place a call to an entry point telephone receiver contained in the entry point access system. This receiver responds, as per the instructions of block 307 to indicate readiness to receive a transmitted ID number of the user as indicated. If the system is not ready at this time the flow returns to the input of block 307 until the ID number can be received. Indications of readiness may be by audio return or by display on the display of the communicator.

Upon the readiness to receive state being indicated the user ID is transmitted to the entry point receiver as indicated by the instructions of block 309. Upon receipt of the user ID the entry point system retrieves the related PIN from its own data base as indicated by the instructions indicated in block 311. The entry point encryption engine utilizes the ID number to formulate a multidigit number and transmits this number to the user's communicator as indicated by the instructions of block 313. The user's communicator includes encryption circuitry which generates

another number from the received number and the user's PIN as indicated by the instructions of block 315. The user's PIN may be entered directly by user or recovered from an inserted smart card.

The another number is returned to the entry point, as indicated in block 317; and at the entry point system the originally generated number is acted upon by the encryption engine in combination with the stored PIN at the entry point to regenerate a check number as per block 319. If the regenerated check number is identical to the transmitted number from the communicator the entry is unlocked as per decision block 321. If the numbers do not match the process is terminated leaving the entry locked.

While a particular process and apparatus have been illustratively disclosed other variations may be implemented without departing from the spirit and scope of the invention. In one alternative embodiment the number of the entry point would be released only by application of the PIN releasing the number as stored on the smart card. While the communicator is shown as wireless the process may be implemented using a wired communication connection.

Another variation would include a timeout period in which to enter valid information, after which the system is disabled or the process terminated.

Claims:

1. A method of providing access to a secure system through an entry access system in which access is granted in response to a protocol process, comprising the steps of:

providing a user with a system ID and a PIN;

storing the system ID in a communication device and allowing a user to access use of the ID by entry of the PIN;

establishing a telephone communication link between the communication device and the entry access system;

entering the PIN into the communication device to allow transmission of the ID to the entry access system;

at the entry access system correlating the received ID with a stored PIN assigned to the user;

transmitting from the entry access system a multidigit number to the communication device derived from the stored PIN;

receiving the multidigit number at the communication device and transforming by encryption techniques to attain a new number by using the PIN as a key;

returning the transformed new number to the entry access system;

transforming the received number at the entry access system utilizing the PIN as key and utilizing the same encryption techniques to attain a check number;

deactivating the lock if the check number is identical to the new number.

2. An entry access system for controlling access to a secure system, comprising:

means for communicating over a telephone network;

a data base of ID and PIN numbers;

means for generating an arbitrary multidigit number in response to an ID communicated by an intended entrant to the secure system;

means for converting the multidigit number into DTMF multitones;

telephone communication means connected for transmitting the multitones into a telephone network for transmission to the intended entrant;

means for receiving a number generated by encryption methods of a communicator of the intended entrant from an ID and PIN of the entrant, via the telephone network; means for generating a check number using the stored PIN as a

key and comparing it to the multidigit number;

a locking mechanism for enabling/disabling entry to the secure system operative to identity of the multidigit number and the generated check number.

3. A method of providing access to a secure system through an entry access system, as claimed in claim 1, wherein:

the step of storing the system ID and PIN includes inserting a smart card in the communication device.

4. A method of providing access to a secure system through an entry access system, as claimed in claim 1, wherein:

the step of entering of the PIN includes the step of releasing the PIN from a smart card inserted into the communication device.

5. A method of providing access to a secure system through an entry access system, as claimed in claim 1, further including:

the step of limiting response in deactivating the lock to operations performed within a specified time limit.

6. An entry access system for controlling access to a secure system, as claimed in claim 2, further comprising:

the telephone communication means including a connection through the network to a wireless station for communicating with a wireless communicator of the intended entrant.

7. An entry access system for controlling access to a secure system, as claimed in claim 6, further comprising

the wireless communicator receiving ID and PIN from a smart card inserted into the wireless communicator.

FIG. 1

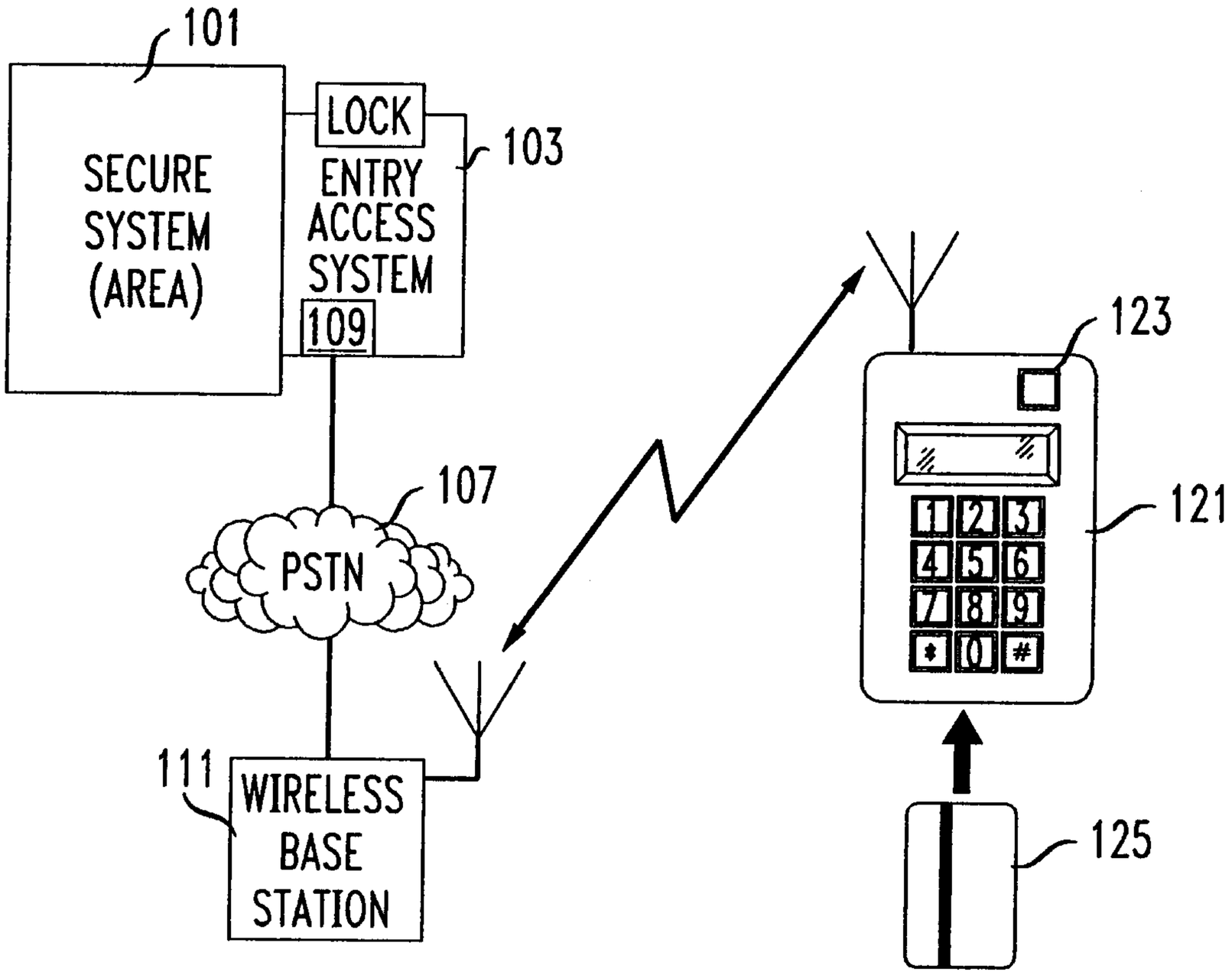
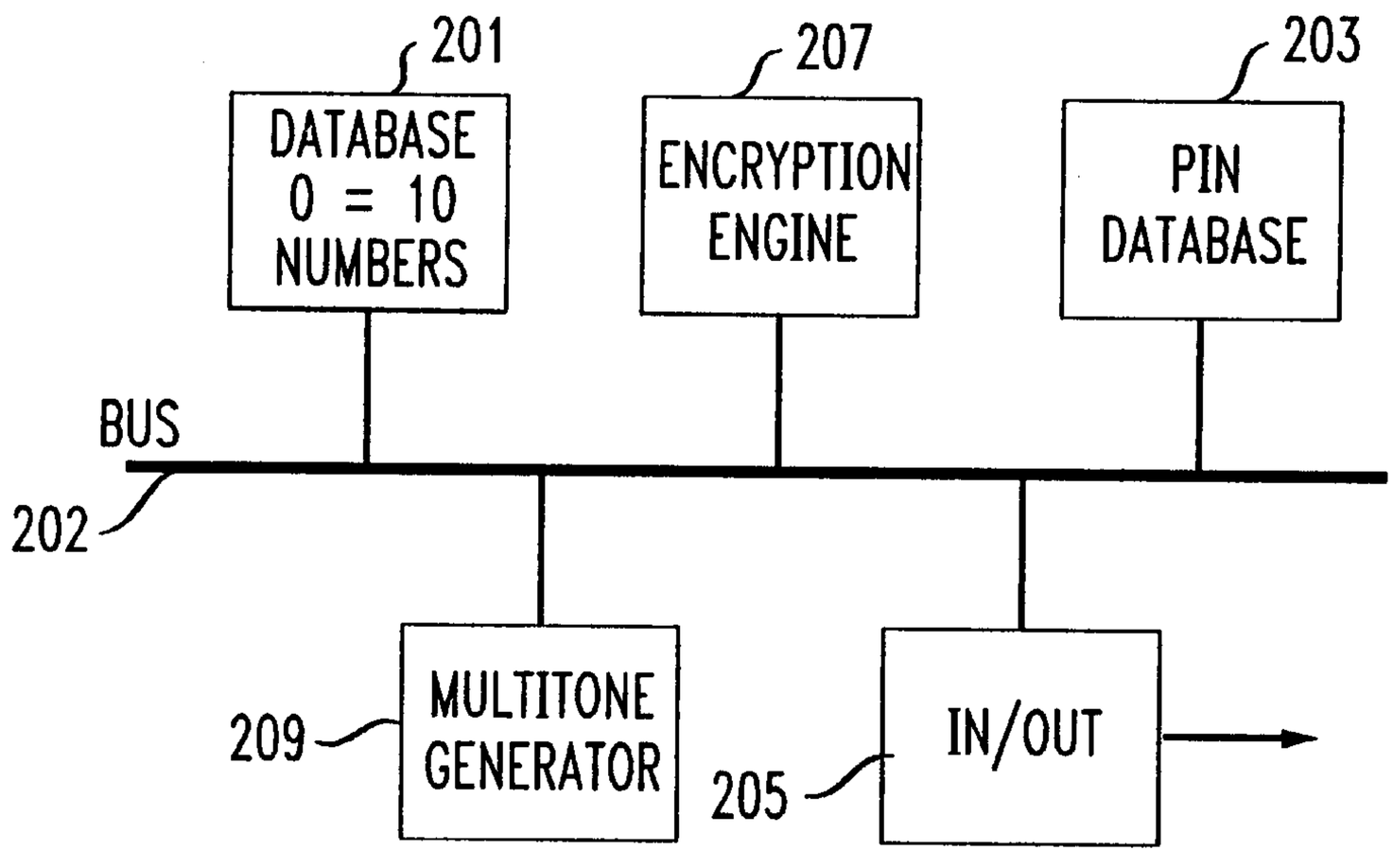

101
SECURE SYSTEM (AREA)
LOCK
ENTRY ACCESS SYSTEM
109
103
107
PSTN
111
WIRELESS BASE STATION
123
121
1 2 3
4 5 6
7 8 9
* 0 #
125

FIG. 2


201
DATABASE 0 = 10 NUMBERS
207
ENCRYPTION ENGINE
203
PIN DATABASE
BUS
202
209
MULTITONE GENERATOR
205
IN/OUT

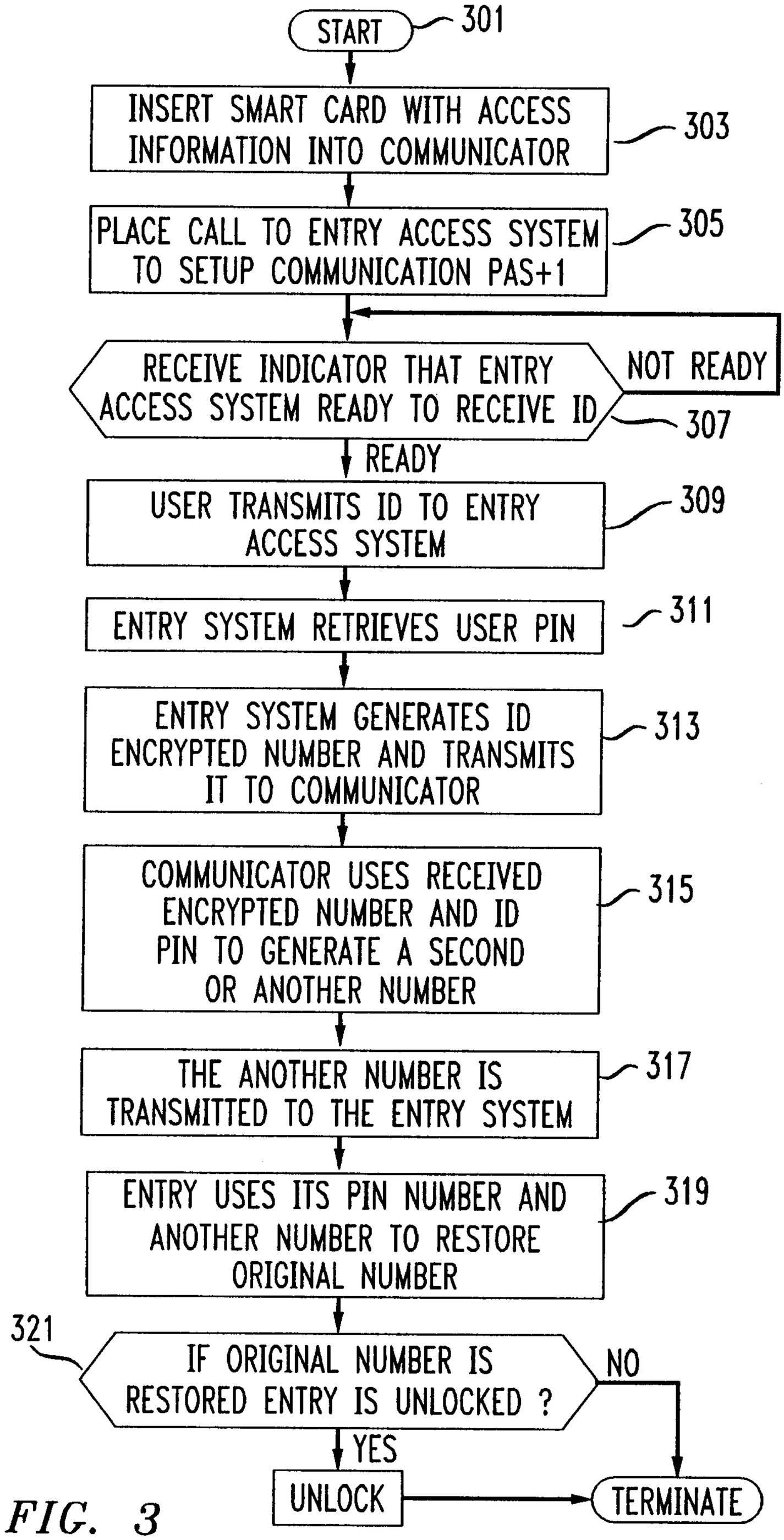


FIG. 3

Kirby, Eades, Gale, Baker