(19) **Bundesrepublik Deutschland**
Deutsches Patent- und Markenamt

(10) **DE 697 36 283 T2** 2007.06.28

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 891 611 B1**
(21) Deutsches Aktenzeichen: **697 36 283.3**
(86) PCT-Aktenzeichen: **PCT/FR97/00505**
(96) Europäisches Aktenzeichen: **97 915 537.1**
(87) PCT-Veröffentlichungs-Nr.: **WO 1997/036264**
(86) PCT-Anmeldetag: **21.03.1997**
(87) Veröffentlichungstag der PCT-Anmeldung: **02.10.1997**
(97) Erstveröffentlichung durch das EPA: **20.01.1999**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **05.07.2006**
(47) Veröffentlichungstag im Patentblatt: **28.06.2007**

(51) Int Cl.[8]: ***G07F 7/10*** (2006.01)
E05B 49/00 (2006.01)

(30) Unionspriorität:

620240	**22.03.1996**	**US**
9604798	**17.04.1996**	**FR**

(84) Benannte Vertragsstaaten:
AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, NL, PT, SE

(73) Patentinhaber:
Actividentity Europe S.A., Suresnes, FR

(72) Erfinder:
AUDEBERT, Yves, Los Gatos 95032 CA, US

(74) Vertreter:
Hauck Patent- und Rechtsanwälte, 20354 Hamburg

(54) Bezeichnung: **ZUGANGSKONTROLLSYSTEM ZU EINER FUNKTION, IN DER DIE CHIFFRIERUNG MEHRERE DYNAMISCHE VERÄNDERLICHE ENTHÄLT**

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein elektronisches System zur Kontrolle des Zugangs zu einer Funktion oder zur Authentifizierung einer Person oder einer Nachricht, das insbesondere einem Anwender erlaubt, unter bestimmten Bedingungen einen Dienst oder eine andere Leistung zu erlangen, der bzw. die von einer spezialisierten Diensteinheit, die dem betreffenden System zugeordnet ist, erbracht werden muss.

[0002] Insbesondere betrifft die Erfindung ein System zur Kontrolle des Zugangs zu einem Rechner oder auch allgemein zu einem Datennetz, dessen Nutzung Personen vorbehalten ist, die sich ordnungsgemäß legitimiert haben. Derartige Netze können beispielsweise dazu dienen, jede Art von Diensten sicherzustellen, die, meist als wirtschaftliche Gegenleistung, eine Transaktion umfassen, wie das Teleshopping, das Abonnementsfernsehen, das Homebanking, die interaktiven Fernsehspiele oder auch die vertrauliche Faksimileübertragung usw.

[0003] Ein Beispiel für ein solches System des Standes der Technik ist in dem US-Patent Nr. 3 806 874 beschrieben. Dieses Patent beschreibt ein System zur Identifizierung oder Authentifizierung von Personen, in welchem durch Chiffrieren von dezimalen zeitabhängigen Daten, die binärcodiert sind, und zweier fester Zahlen ein Passwort erzeugt wird. In diesem System erzeugt eine Identifizierungseinheit (oder Karte) erste und zweite Datenfolgen (Passwörter) in Abhängigkeit von einer persönlichen Identifikationsnummer, geheimen Daten und binären zeitabhängigen Daten, die von einem ersten Zeitgeber abgeleitet sind. Die persönliche Nummer wird an eine Verifizierungseinheit (oder einen Server) übermittelt. Die Verifizierungseinheit erzeugt erste und zweite Datenfolgen, indem sie die persönliche Identifikationsnummer, die geheimen Daten und binärcodierte, dezimale zeitabhängige Daten, die von einem zweiten Zeitgeber abgeleitet sind, chiffriert. Die zeitabhängigen Daten werden unabhängig voneinander von den Zeitgebern geliefert, die sich in der Identifizierungseinheit bzw. in der Verifizierungseinheit befinden.

[0004] Insbesondere umfasst die Identifizierungseinheit **10** einen ROM-Primärspeicher **12**, in dem eine persönliche Identifikationsnummer gespeichert ist, und eine geheime Schaltung **20**, die geheime Daten in einem geheimen Speicher **26** speichert, der ermöglicht, die ersten und zweiten Datenfolgen zu erzeugen. Die geheimen Daten sind für jeden Anwender verschieden und ihm unbekannt. Die geheime Schaltung **20** umfasst eine Chiffrierschaltung, welche die ersten und zweiten Folgen liefert, indem sie Eingangsdaten, zusammengesetzt aus der persönlichen Identifikationsnummer, geheimen Daten und binärcodierten, dezimalen zeitabhängigen Daten, die von dem Zeitgeber **42** erzeugt sind, chiffriert.

[0005] In dem Server umfasst eine geheime Schaltung **31**, die der geheimen Schaltung **20** der Karte entspricht, einen geheimen Speicher **33** und empfängt eine zeitabhängige Eingabe von einem Zeitgeber **53**. Genauso empfängt die geheime Schaltung **31** eine Eingabe (die persönliche Identifikationsnummer) aus dem Primärspeicher **12** der Identifizierungseinheit **10**. Die geheime Schaltung **31** umfasst eine Chiffrierschaltung, welche die erste und die zweite Datenfolge (Passwörter) erzeugt, indem sie die Eingangsdaten, zusammengesetzt aus der persönlichen Identifikationsnummer, geheimen Daten und binärcodierten, dezimalen zeitabhängigen Daten, die von dem Zeitgeber **53** abgeleitet sind, chiffriert.

[0006] Die ersten Datenfolgen werden in einem Komparator **30** der Karte verglichen. Wenn sie übereinstimmen, wird ein Annahmesignal erzeugt. Der Komparator vergleicht (1) die erste Datenfolge, die von dem Server während des gleichen Zeitraums erhalten wurde, in dem die erste Datenfolge in der Verifizierungseinheit erzeugt wurde, mit (2) der ersten Datenfolge, die während des gleichen Zeitraums in der Karte erzeugt wurde. Anders ausgedrückt: Der Komparator **30** muss von dem Server die erste Datenfolge während desselben Zeitraums empfangen, in dem sie erzeugt worden ist, damit diese empfangene Datenfolge mit der ersten Datenfolge, die während desselben Zeitraums in der Verifizierungseinheit erzeugt worden ist, übereinstimmt. Die gleiche Überlegung gilt für die zweiten Datenfolgen, die im Komparator **41** verglichen werden.

[0007] Die geheimen Schaltungen **20** und **31** des US-Patents Nr. 3 806 874 erzeugen Passwörter (Prüfnummern) durch Chiffrieren der persönlichen Identifikationsnummer, geheimer Daten und binärcodierter, dezimaler zeitabhängiger Daten, um die ersten und zweiten Datenfolgen zu erzeugen. Damit die Datenfolgen übereinstimmen, müssen die zeitabhängigen Daten, die in der Identifizierungseinheit und in der Verifizierungseinheit verwendet werden, identisch sein. Folglich müssen die Zeitgeber **42** und **53** synchron sein, damit sie in etwa gleichzeitig die gleichen zeitabhängigen Daten erzeugen.

[0008] Das Patent US 4 601 011 beschreibt ein Authentifizierungssystem, das ein Passwort erzeugt, indem es eine feste Zahl mit einem Schlüssel chiffriert, der aus zwei Teilen gebildet ist, wovon der erste sich nicht ändert und der zweite sich jedes Mal ändert, wenn der Schlüssel zum Chiffrieren verwendet wird.

[0009] Dieses System umfasst mindestens eine tragbare elektronische Einheit (Karte) und mindestens eine elektronische Verifizierungseinheit (Server), die unter bestimmten Bedingungen Berechti-

gungen für einen Zugang zu einem Rechner erteilen soll. Das System erzeugt Passwörter, die in einer ersten Variante zeitabhängig sind und in einer zweiten Variante von der Anzahl der in der tragbaren Einheit erzeugten Passwörter abhängen. Diese Letztere umfasst ein Chiffriermodul, das ein Passwort chiffriert, das für jeden Übertragungsvorgang verschieden ist, wobei ein zweiteiliger Schlüssel verwendet wird. Der Server empfängt das Passwort von der Karte und erzeugt durch Chiffrieren einer festen Zahl (entsprechend der in der Karte chiffrierten festen Zahl) mit dem ersten Teil des Schlüssels (im Speicher gespeichert) und dem zweiten Teil des Schlüssels (von der Karte empfangen) ein internes Passwort. Ein Komparator **50** vergleicht das empfangene Passwort mit dem internen Passwort und liefert in Abhängigkeit vom Ergebnis des Vergleichs eine Ausgabe, die den Zugang zu dem Rechner **56** gewährt oder verweigert.

[0010] Die Systeme der US-Patente 4 601 011 und 3 806 874 erzeugen beide identische Passwörter („Datenfolgen" oder „chiffrierte Prüfzahlen") in der Karte und in dem Server, wobei die zwei Einheiten die Passwörter unabhängig voneinander berechnen, indem sie ein Chiffrierprogramm an Daten ausführen, die mindestens einen festen persönlichen Code und mindestens eine Zahl in Abhängigkeit von der Zeit oder in Abhängigkeit davon variierend, wie oft ein Passwort in der Karte erzeugt worden ist, umfassen.

[0011] Das US-Patent 4 720 860 beschreibt ein weiteres Authentifizierungssystem, in dem eine statische Variable und eine dynamische Variable verwendet werden, um die Passwörter zu erzeugen. Nach diesem Patent muss der Anwender jedes Mal, wenn eine Transaktion ausgeführt werden soll, zu Beginn einer Zugangsanforderungsprozedur einen festen Code in die Karte eingeben. Der feste Code ist eine statische Variable. Eine zweite Variable wird derart erzeugt, dass sie sich dynamisch in Abhängigkeit von der Zeit, insbesondere in Abhängigkeit von dem Zeitpunkt, zu dem der feste Code von dem Anwender in die Karte eingegeben wird, ändert. Die zwei Variablen, wovon die eine folglich statisch und die andere dynamisch ist, werden dann als Eingangsparameter eines geheimen Chiffrieralgorithmus' verwendet, der dazu dient, in der Karte ein Passwort zu erzeugen.

[0012] Dieses Passwort wird auf der Karte angezeigt, und der Anwender wird aufgefordert, es an den Server zu übermitteln. Der feste Code wird ebenfalls an den Server übermittelt, der unter Verwendung des gleichen Chiffrieralgorithmus' und einer dynamischen Variablen, die im Prinzip den gleichen Wert wie jene aufweist, die in der Karte verwendet wird, ebenfalls das Passwort berechnet. Dieses Letztere wird mit dem vom Anwender an den Server übermittelten Passwort verglichen, und bei Übereinstimmung kann eine Erlaubnis für einen Zugang zu der Funktion erteilt werden. Dieses Zugangskontrollsystem verwendet folglich eine statische Variable, mit deren Hilfe der Chiffrieralgorithmus das Passwort berechnet, wozu er auch die dynamische Variable verwendet.

[0013] Bei diesem System wird die statische Variable in einem Speicher der Karte gespeichert und beispielsweise über eine Telefonleitung an den Server übermittelt. Folglich kann sie von Hackern, die betrügerische elektronische Verfahren anwenden, entdeckt werden.

[0014] Bei diesem System muss folglich der Algorithmus unbedingt geheim gehalten werden, um die Sicherheit des Systems zu schützen. Wenn die Sicherheit des Algorithmus' in Frage gestellt ist, dann ist die Sicherheit der Gesamtheit des Systems gefährdet, denn die statischen Variablen können eventuell durch betrügerische elektronische Verfahren entdeckt werden. Dies erklärt, weshalb nach diesem Patent Mittel vorgesehen sind, um den Algorithmus im Falle eines Betrugsversuchs auf der Karte zu zerstören (beispielsweise indem der Algorithmus in einen flüchtigen Speicher gespeichert wird).

[0015] Außerdem ist anzumerken, dass in den beiden US-Patenten Nr. 3 806 874 und 4 720 860 die zweite Variable ein zeitabhängiger dynamischer Wert ist. Da diese Variable notwendigerweise in der Karte und unabhängig davon zugleich im Server erzeugt werden muss, müssen die Zeitgeber der zwei Einheiten, die verwendet werden, um die dynamische Variable jeder Seite zu erzeugen, mit einer bestimmten Präzision synchronisiert sein. Um nicht zu präzise Zeitgeber bereitstellen zu müssen (was die Kosten des Systems beträchtlich erhöhen würde), muss ein Toleranzbereich zugelassen werden, in dem das aktuelle Passwort gültig bleibt. Je kürzer der Toleranzbereich ist, desto besser ist die Sicherheit gewährleistet, aber auch desto störender ist ein Synchronisationsfehler der Zeitgeber.

[0016] Unter Berücksichtigung dieses Toleranzbereichs ist das bei jeder Zugangsanforderung berechnete Passwort auch während der Dauer jedes Intervalls, das zwei Operationen zur Berechnung der dynamischen Variablen voneinander trennt, gültig. Ein solches Intervall kann eine verhältnismäßig lange Dauer haben (typisch 10 Minuten und beispielsweise sogar länger), so dass ein Betrüger, der sich zum Zeitpunkt einer Zugangsanforderung heimlich das Passwort einer Karte verschafft, Zeit haben wird, es während des gesamten vorerwähnten Intervalls auf dem Server zu benutzen, und auf diese Weise leicht eine Zugangserlaubnis erhalten können wird.

[0017] In dem US-Patent Nr. 4 800 590 wird ebenfalls ein Authentifizierungssystem beschrieben, das einen dynamischen zeitabhängigen Chiffrierschlüssel verwendet. Insbesondere verwendet dieses System als Eingangsparameter eines Chiffrieralgorith-

mus' einen Chiffrierschlüssel, der als dynamische Variable verwendet wird, die man in Abhängigkeit von der Zeit variieren lässt. Dieses Verfahren erfordert ein periodisches Aktualisieren des Chiffrierschlüssels, beispielsweise mit einer festgelegten Häufigkeit von einer Minute. Dieses Aktualisieren kann zwar für die Karte leicht durchgeführt werden, nicht jedoch für den Server. Das System kann nämlich eine sehr große Anzahl von Anwendern haben, die jeweils eine Karte besitzen, der eine dynamische Variable zugewiesen ist, die selbstverständlich einzig für diese Karte ist. Folglich muss in diesem System, das aus dem US-Patent 4 800 590 bekannt ist, der Server entweder periodisch durch iterative Berechnungen alle Chiffrierschlüssel auf einmal neu berechnen oder aber den Chiffrierschlüssel der betreffenden Karte aktualisieren, während diese einen Zugang anfordert. Es versteht sich, dass dann, wenn das System eine große Anzahl von Karten (typisch beispielsweise 100 000) umfasst, das Aktualisieren der Chiffrierschlüssel schnell zu einer für den Server zu großen Rechenbelastung wird. Dieses Patent beschreibt auch die Möglichkeit, den Schlüssel als Antwort auf ein Einwirken des Anwenders auf eine Taste zu aktualisieren; jedoch ist diese Ausführungsform unvorteilhaft, denn sie schränkt die Häufigkeit der Modifikation des Schlüssels ein.

[0018] Das US-Patent 5 060 263 beschreibt ebenfalls ein System, das ein dynamisches Passwort erzeugt. In diesem System erzeugt ein Passwort-Generator jedes Passwort durch Chiffrieren des zuvor erzeugten Passworts, das als Variable verwendet wird. Eine große Anzahl von festen Chiffrierschlüsseln ist in der Karte gespeichert. Um die Sicherheit zu erhöhen, erzeugt der Server eine Zufallszahl, die einen der Schlüssel bezeichnet, der zur Erzeugung des Passworts verwendet wird. Die Karte muss die Chiffriersequenzen (mit Hilfe eines öffentlichen Algorithmus' vom Typ DES) genau so oft wiederholen, wie es Schlüssel in der Karte gibt, wobei der Ausgang auf den Eingang zurückgeschleift wird.

[0019] In diesem bekannten System haben die Schlüssel folglich feste Werte, obgleich sie zufällig gewählt sind. Sie können jedoch in betrügerischer Absicht im Speicher der Karte entdeckt werden. Außerdem muss die in dem Server erzeugte Zufallszahl zur Karte übermittelt werden; sie kann folglich in betrügerischer Absicht während der Übermittlung abgefangen werden. Ein weiteres Problem dieses System stellt sich, wenn der Anwender der Karte eine Zugangsanforderung an den Server nicht abschließt. In diesem Fall kann es ernste Probleme eines Synchronisationsverlusts geben, denn jedes Passwort ist auf der Grundlage des vorhergehenden Passworts erzeugt, so dass die Abweichung mit der Zeit immer größer wird. Es muss dann ein Mechanismus vorgesehen werden, der ermöglicht, die Synchronisation wiederherzustellen.

[0020] Das Dokument EP 0 605 996 A1 offenbart ein System, in welchem von einem Codierer **28** ein Sicherungscode übermittelt wird, der einen Teil, der durch einen Wert des Übermittlungszählers **22** repräsentiert ist, einen Teil, der durch einen Identifikationscode **24** repräsentiert ist, und einen Teil, der durch einen so genannten „rolling code" **26** repräsentiert ist, umfasst. Dieser Sicherungscode ist folglich die Aneinanderreihung von drei Elementen, die vom Codierer **28** zum Decodierer **42** übermittelt werden. Dieser Letztere trennt sie im Hinblick auf ihre individuelle Verarbeitung durch den Empfänger **40**.

[0021] Zwei dieser Elemente, der Wert des Übermittlungszählers **22** und der „rolling code" **26**, sind dynamische Variablen. Sie dienen jedoch nicht zur Erzeugung von Eingangsparametern eines Chiffrieralgorithmus', der ein Passwort hervorbringt.

[0022] Die Erfindung hat zum Ziel, ein System zur Zugangskontrolle oder zur Authentifizierung von Personen und/oder von Nachrichten zu schaffen, das eine bessere Sicherheit gegen Betrügerei bietet.

[0023] Sie hat demzufolge ein System zur Zugangskontrolle oder zur Authentifizierung von Personen und/oder von Nachrichten gemäß dem Anspruch 1 zum Gegenstand.

[0024] Die dynamischen Variablen müssen in der ersten und zweiten Einheit kohärent sein; sie müssen folglich eine im Voraus festgelegte Beziehung aufweisen, beispielsweise identisch sein.

[0025] Aus diesen Merkmalen folgt zunächst, dass die ersten Einheiten des Systems in ihrem Speicher für die Berechnung des Passworts keine statische Variable enthalten, die in betrügerischer Absicht, beispielsweise durch Spionieren, entdeckt werden könnte. Ein weiterer Vorteil besteht darin, dass der Chiffrieralgorithmus nicht unbedingt geheim sein muss; und wenn dies so ist, kann man sich Mittel zum Zerstören dieses Algorithmus' im Betrugsfall ersparen.

[0026] Es trifft zu, dass dann, wenn ein öffentlicher Algorithmus verwendet wird, mindestens eine der dynamischen Variablen geheim sein muss, aber im Falle einer in betrügerischer Absicht erfolgten Entdeckung einer solchen Variablen (die der Karte eigen ist) verliert nur die betreffende Karte ihre Sicherheit, während das System an sich sie in vollem Umfang beibehält.

[0027] So umfassen nach einem weiteren Merkmal der Erfindung die ersten und zweiten Generatormittel jeweils dritte und vierte Rechenmittel, um mindestens eine erste der dynamischen Variablen gemäß einer Funktion zu erzeugen, welche die Anzahl der Zugangsanforderungen, die von der ersten Einheit vor

der laufenden Zugangsanforderung vorgebracht wurden, einbezieht.

[0028] Aus diesem besonders vorteilhaften Merkmal folgt, dass aufgrund der Erfindung die Aktualisierung einer ersten der dynamischen Variablen, die beispielsweise als Chiffrierschlüssel verwendet wird, nicht periodisch durchgeführt zu werden braucht und in dem Server keine Neuberechnung oder „Neueinstellung" des Werts der berechneten dynamischen Variablen für eine frühere Zugangsanforderung in Bezug auf den Momentanwert dieser berechneten dynamischen Variablen, der sich zu dem Zeitpunkt, zu dem eine Zugangsanforderung vorgebracht wird, in der Karte befindet, erfordert. Die Rechenarbeit des Servers ist folglich auf das Minimum herabgesetzt.

[0029] Sicherlich ist es möglich, dass die Anzahl der von der Karte verbuchten Zugangsanforderungen größer als jene der von dem Server registrierten ist, weil es sein kann, dass nicht immer der Anwender der Karte eine Zugangsanforderung abschließt. Jedoch wird in diesem Fall der Server schlimmstenfalls nur eine sehr kleine Anzahl von Iterationen wieder aufnehmen müssen, um die dynamische Variable neu zu berechnen. Außerdem wird man durch den Aufbau den Unterschied zwischen den Anzahlen der Zugangsanforderungen, die jeweils in den zwei Einheiten verbucht werden, zwangsweise begrenzen können.

[0030] Auch ist festzustellen, dass dann, wenn sich eine Person in betrügerischer Absicht ein Passwort verschafft, das gerade von einem Anwender einer bestimmten Karte erhalten worden ist, und auf rechtmäßige Weise von dieser Letzteren an den Server übermittelt wird, aufgrund der Erfindung dieses Passwort nicht zu einer Zugangsberechtigung führen wird. Eine neue Zugangsanforderung wird nämlich, selbst wenn sie sehr rasch danach vorgebracht wird, ein Passwort erzeugen, das von jenem, das in dem Server berechnet wird, verschieden ist, denn die dynamische Variable der Karte wird sich dann durch die Erhöhung der Anzahl der Zugangsanforderungen verändert haben.

[0031] In einer besonderen Ausführungsform kann das Zugangskontrollsystem zweite Mittel zum Berechnen des Passworts aufweisen, die das empfangene Passwort gemäß mindestens einem Dechiffrieralgorithmus dechiffrieren, wobei als Dechiffrierschlüssel ein Eingangsparameter verwendet wird, der von einer ersten dynamischen Variablen abhängig ist, die in der zweiten Einheit erzeugt ist, um eine dynamische Variable abzuleiten, die einer der in der ersten Einheit erzeugten dynamischen Variablen entsprechen muss. In diesem Fall umfasst diese zweite Einheit ebenfalls Vergleichsmittel, welche die mittels der zweiten Rechenmittel abgeleitete dynamische Variable mit einer zweiten der dynamischen Variablen, die in der zweiten Einheit erzeugt sind, vergleichen, und Mittel, die, wenn die Vergleichsmittel zwischen der mittels der zweiten Rechenmittel abgeleiteten dynamischen Variablen und der zweiten der Variablen, die in der zweiten Einheit erzeugt ist, eine im Voraus festgelegte Beziehung feststellen, eine Erlaubnis für den Zugang zu der Funktion erteilen.

[0032] Weitere Merkmale und Vorteile der Erfindung werden im Laufe der folgenden Beschreibung deutlich, die nur beispielhaft gegeben ist und sich auf die beigefügte Zeichnung bezieht, worin

[0033] Fig. 1 ein Grundschema eines erfindungsgemäßen Zugangskontrollsystems ist;

[0034] Fig. 2 ein vereinfachter Ablaufplan ist, der das Prinzip des Ablaufs der Operationen in dem erfindungsgemäßen System veranschaulicht, wenn eine Zugangsanforderung verarbeitet wird;

[0035] Fig. 3 einen Ablaufplan für die Art und Weise der Berechnung eines Chiffrierschlüssels zeigt, der für die Berechnung des Passworts verwendet wird.

[0036] In Fig. 1 ist ein stark vereinfachtes Schema eines erfindungsgemäßen Zugangskontrollsystems dargestellt.

[0037] Es wird vorausgesetzt, dass das System einen bedingten Zugang zu einer Funktion gewährt, die in Fig. 1 durch das Rechteck **1** symbolisch dargestellt ist. Der Ausdruck „Funktion" ist in einer sehr weiten Bedeutung aufzufassen. Er bezeichnet jede Funktion, zu welcher der Zugang an die Bedingung einer Berechtigung bzw. Erlaubnis geknüpft ist, die eine Authentifizierung einschaltet, die eine Verifizierung des Werkzeugs (Karte), mit dessen Hilfe die Anforderung vorgebracht wird, und vorzugsweise auch eine Identifizierung der Person, die den Zugang zu der Funktion anfordert, voraussetzt, um zu wissen, ob die Anforderung rechtmäßig ist.

[0038] Die Funktion kann von jeder Art sein, beispielsweise eine Zugangsfunktion zu einem Raum, zu einem Datennetz oder zu einem Rechner, zu einer Finanztransaktion (Teleshopping, Homebanking, interaktives Fernsehspiel, Abonnementsfernsehen) usw. Außerdem fallen Authentifizierungsfunktionen, sei es für Personen, sei es für Nachrichten, ausdrücklich in den Schutzbereich der vorliegenden Erfindung, obwohl sich in der gesamten Beschreibung eher auf eine Prozedur bezogen wird, die Anforderungen des Zugangs zu einer Funktion voraussetzt.

[0039] So ist in Fig. 1 zu sehen, dass gemäß einer besonderen Ausführungsform das folgende System der Erfindung mindestens eine erste Einheit **2**, „Karte" genannt, und mindestens eine zweite Einheit **3** umfasst. Es wird hervorgehoben, dass das Zugangs-

kontrollsystem erfindungsgemäß eine große Anzahl von ersten Einheiten und eine oder mehrere zweite Einheiten, jedoch in jedem Fall in einer im Allgemeinen deutlich geringeren Anzahl, umfassen kann. Die Anzahlen der Einheiten **2** und **3** sind folglich keineswegs die Erfindung einschränkend.

[0040] Die erste Einheit oder Karte **2** ist vorzugsweise tragbar und personalisiert, um einem bestimmten Anwender persönlich zugeordnet zu werden. Sie hat beispielsweise die Form eines Taschenrechners oder einer Kreditkarte und trägt eine öffentliche Identifikationsnummer **5**, die in Fig. 1 schematisch dargestellt ist. Diese Nummer kann nicht chiffriert in diese eingetragen sein und dieser bei ihrer Initialisierung zugewiesen werden. Die Identifikation kann auch aus dem Namen des Anwenders oder jeder anderen Information, die ihm eigen ist, gebildet sein. Eine weitere Nummer, die persönliche Identifikationsnummer oder PIN, ist geheim und normalerweise nur dem berechtigten Anwender der Karte bekannt. Um die Karte zu benutzen, muss der Anwender die PIN in diese eingeben, wobei die Karte dann die eingegebene PIN mit einem in der Karte gespeicherten Wert vergleicht. Falls die eingegebene PIN und der gespeicherte Wert übereinstimmen, erhält der Anwender die Erlaubnis zur Benutzung der Karte, andernfalls wird die Karte kein Passwort erzeugen können. Die öffentliche Identifikationsnummer identifiziert die Karte an sich unter allen Karten, mit denen das System arbeiten kann, gegenüber der Einheit **3**.

[0041] Die Karte **2** umfasst ein Tastenfeld **6**, das die Eingabe von Informationen wie beispielsweise der schon erwähnten Identifikationsnummern ermöglichen soll, sowie verschiedene Funktionstasten **7**. Sie umfasst auch ein Anzeigefeld **8** und ist mit einer integrierten Schaltung **9** ausgestattet, die insbesondere einen ordnungsgemäß programmierten Mikrocontroller sowie die üblichen ROM- und RAM-Speicher umfasst.

[0042] Die Karte **2** umfasst auch eine Kommunikationseinrichtung **10**, die ermöglicht, mit der Einheit **3** entweder direkt oder aber über eine Übertragungsverbindung über eine mehr oder weniger große Entfernung zu kommunizieren. Diese Einrichtung kann in verschiedenen Erscheinungsformen auftreten, beispielsweise als eine Telefonverbindung vom Typ DTMF, eine Vorrichtung zur Datenübertragung mittels Infrarotstrahlen, eine so genannte Online-Vorrichtung, bei der die Karte in einen geeigneten Leser oder irgendeine andere im Fach wohlbekannte Übermittlungseinrichtung eingeführt wird.

[0043] Die zweite Einheit **3** umfasst zunächst Schnittstellenmittel, die ermöglichen, die Kommunikation mit der Karte **2** mit Hilfe der Kommunikationseinrichtung **10** sicherzustellen. In der Ausführungsform, die in Fig. 1 und Fig. 2 gezeigt ist, sind diese Schnittstellenmittel durch ein Rechteck **12** symbolisch dargestellt; sie können in zahlreichen Formen auftreten. Es kann sich beispielsweise um einen speziell zugeeigneten Leser handeln, jedoch können die Schnittstellenmittel auch in Form einer Rechner-Datenstation auftreten, die beispielsweise in ein Netz eingebunden ist, oder auch eines Personalcomputers, der mit einer Infrarotschnittstelle ausgestattet ist usw. Ihre Besonderheit ist, dass sie in einer geeigneten Form mit der Karte oder den Karten, die ihnen zugeordnet ist bzw. sind, kommunizieren können.

[0044] Die Schnittstellenmittel **12** können ein Tastenfeld **13** und ein Anzeigefeld **14** aufweisen, um einem Anwender zu ermöglichen, die an einen Teil **15** der zweiten Einheit **3** zu übermittelnden Informationen, wie beispielsweise Passwörter oder zu authentifizierende Daten, die Funktion **1** betreffend, einzugeben. Die Eingabe dieser Daten kann jedoch auch auf andere Art verwirklicht werden, insbesondere automatisch, ohne Eingreifen des Anwenders, beispielsweise durch das einfache Einführen der Karte in die Schnittstelle **12** oder mittels einer der Funktionstasten **7**, die beispielsweise das Aussenden modulierter Infrarotstrahlen auslöst.

[0045] Die Schnittstelle **12** kommuniziert mit dem anderen Teil **15** der Einheit **3**, in der vorliegenden Beschreibung „Server" genannt. Diese Kommunikation, die symbolisch durch die Verbindung **16** dargestellt ist, kann durch jedes geeignete Mittel über eine kurze oder lange Wegstrecke erfolgen. Die Informationen, die über diese Verbindung befördert werden, sind insbesondere das in dem Server **15** zu überprüfende Passwort und eventuell in dem Server zu authentifizierende und zu verarbeitende Daten.

[0046] Der Server **15** umfasst insbesondere einen Prozessor **17** und einen Speicher **18**. Der Prozessor ist imstande, unter bestimmten Bedingungen die Funktionen **1** freizugeben, die von den Zugangsanforderungen, die von den verschiedenen Karten vorgebracht werden, angestrebt sind, wobei diese Funktionen intern oder extern sichergestellt werden können. Es ist anzumerken, dass der Server im Allgemeinen mit einer großen Anzahl von Karten über Schnittstellen, wie die Schnittstelle **12**, zusammenwirkt.

[0047] Fig. 2 zeigt einen vereinfachten Ablaufplan der verschiedenen Operationen, die ablaufen, wenn von einem Anwender einer Karte eine Anforderung des Zugangs zu einer Funktion vorgebracht wird. Fig. 2 ist in zwei Teile geteilt, wobei der Teil links der punktierten Linie **19** die Operationen darstellt, die in der Karte **2** ausgeführt werden, und der Teil rechts von dieser Linie jene zeigt, die im Teil **15** oder Server der Einheit **3** ablaufen.

[0048] Zum Starten der Prozedur muss die öffentliche Identifikationsnummer **5** an den Server **15** übermittelt werden. Diese Operation kann auf verschiedene Art verwirklicht werden. Beispielsweise kann sie direkt an den Server übermittelt werden, sobald die Karte in die Schnittstelle **12** eingeführt ist. Sie kann durch den Anwender selbst direkt mittels des Tastenfeldes **13** des Servers oder aber mittels des Tastenfeldes **6** der Karte **2** eingetippt und durch die Kommunikationseinrichtung **10** übertragen werden. Die Kommunikation kann auch über eine Fernverbindung wie eine Telefonleitung oder über den Funkweg erfolgen.

[0049] Der Anwender muss genauso seine Legitimierung angeben, indem er unter **20** seinen persönlichen Identifikationscode oder PIN-Code eintippt, der im Speicher der Karte gespeichert ist. Im Falle der Nichtübereinstimmung wird die Zugangsanforderung unter **22** sofort zurückgewiesen, wobei dem Anwender eventuell mehrere aufeinander folgende Versuche zugestanden werden können, bevor er mit einer definitiven Ablehnung konfrontiert wird, falls alle Versuche erfolglos sind.

[0050] Wenn hingegen der eingegebene PIN-Code und der gespeicherte PIN-Code übereinstimmen, löst das Programm unter **23** die Operation zur Berechnung des Passworts aus.

[0051] Diese Berechnung umfasst ein Chiffrieren mit Hilfe eines Chiffrieralgorithmus', der geheim oder öffentlich sein kann (Block **24**). In diesem letzteren Fall kann es sich um einen Algorithmus handeln, der von den Fachleuten auf diesem Gebiet als DES (Data Encryption Standard) bezeichnet wird.

[0052] Erfindungsgemäß verwendet der betreffende Algorithmus Eingangsparameter in Abhängigkeit von dynamischen Variablen, wovon es in dem dargestellten Fall drei gibt. Zwei davon sind: eine Variable Nn, die in einem Register **25** gespeichert ist und die Anzahl der mittels der Karte gestellten Zugangsanforderungen repräsentiert, und eine Variable T, die aus dem momentanen Zustand eines Zählers **26** gebildet ist. Wenn jede Karte initialisiert wird, können diese Variablen jeweils auf Anfangswerte N0 und/oder T0 festgesetzt werden, die nicht notwendig gleich null sind und die geheim oder öffentlich sein können. Ebenso können Nn und T je nach den Funktionen variieren, wodurch Parameter wie u. a. die Anzahl der Zugangsanforderungen, eine Funktion der Anzahl der Zugangsanforderungen und die momentane Zeit zur Anwendung gebracht werden.

[0053] Jede der beiden Variablen Nn und Tn kann 32 Bit umfassen und zuvor, unter **27**, einer Verkettungsoperation unterzogen worden sein, wodurch ein Eingangsparameter von insgesamt 64 Bit dargeboten wird. Die unter **27** an den Variablen Nn und Tn ausgeführte Operation kann auch irgendeine andere Verarbeitung oder Verknüpfung wie die Verschachtelung, die Häckselung, eine EXKLUSIV-ODER- oder LIND-Verknüpfung usw. umfassen. Anders ausgedrückt: Die Operation unter **27** ist nicht auf diese verschiedenen Varianten beschränkt, sondern sie kann jede Operation sein, die mit dem Ziel ausgeführt wird, eine (64-Bit-)Ausgabe durch Verknüpfen oder Verarbeiten von Nn und Tn zu erzeugen.

[0054] Die dritte dynamische Variable ist ein Chiffrierschlüssel Kn, der von dem Algorithmus unter **24** verwendet wird, um den aus der Verkettungsoperation unter **27** resultierenden Eingangsparameter zu chiffrieren. Der Chiffrierschlüssel Kn ist in einem Register **28** gespeichert und wird bei jeder Zugangsanforderung aktualisiert, wie später erläutert wird. Gemäß Varianten kann der unter **24** angewendete Algorithmus ein Passwort in Abhängigkeit von den Momentanwerten von Nn, Tn und Kn berechnen oder Kn kann gemäß einem Schlüssel chiffriert werden, der einen Wert umfasst, der durch die Verkettung von Nn und Tn unter **27** erzeugt worden ist.

[0055] Das unter **24** durchgeführte Chiffrieren führt unter **29** zum Erzeugen eines Passworts A und unter **30** zum Inkrementieren des Zustandes des Zugangsanforderungsregisters **25**, das Nn speichert, um eine Einheit. Die inkrementierte Zahl Nn+1 wird in das Register **25** gespeichert und unter **31** einer Rechenoperation unterzogen, die dafür bestimmt ist, den neuen Wert Kn+1 der dritten dynamischen Variablen oder des geheimen Chiffrierschlüssels festzulegen. In einer Variante kann die Ausgabe vom Block **30** das Inkrementieren des Registers **25** um einen von einer Einheit verschiedenen Wert hervorrufen, beispielsweise kann auf einmal um zwei Einheiten (oder um jeden anderen Wert) inkrementiert werden. Genauso kann die Anzahl der Einheiten, um die inkrementiert wird, von einer Zugangsanforderung zur nächsten verschieden sein. Selbstverständlich muss das Inkrementieren dann mit jenem, das im Server **15** durchgeführt wird, abgestimmt sein.

[0056] Ein Beispiel für Operationen, die zur Berechnung des neuen Werts von Kn ausgeführt werden können, ist in Fig. 3 gezeigt. Diese Operationen werden im Einklang sowohl in der Karte **2** als auch im Server **15** ausgeführt. Die Werte Nn+1 und Kn werden unter **32** einer logischen Verknüpfungsoperation, beispielsweise einer EXKLUSIV-ODER-Verknüpfung, unterzogen. Die resultierende Zwischenvariable Z wird unter **33** einer Chiffrierung mittels eines bekannten oder öffentlichen Algorithmus' unterzogen, der gegebenenfalls der gleiche sein kann, der unter **24** verwendet wird. Das Chiffrieren kann mit Hilfe eines Chiffrierschlüssels durchgeführt werden, der vorzugsweise der Wert der momentanen dynamischen Variablen Kn ist, obwohl auch irgendein anderer geheimer Schlüssel Q (Block **34**) verwendet werden

könnte.

[0057] Das Ergebnis der Chiffrieroperation unter **33** ist der neue Wert Kn+1 des Chiffrierschlüssels, der bei der nächsten Zugangsanforderung verwendet wird. Dieser Wert wird in das Register **26** gespeichert.

[0058] Nach Erhalt des Passworts A, das auf dem Anzeigefeld **8** der Karte angezeigt wird, wird der Anwender aufgefordert, es der Einheit **3** zu übermitteln. Es ist anzumerken, dass dieses Passwort das vollständige Ergebnis der Chiffrieroperation unter **24** (mit einer Breite von 64 Bit) oder aber nur ein Teil dieses Ergebnisses, beispielsweise ein Wort von 32 Bit, sein kann. Dieses Übermitteln (symbolisch durch die punktierte Linie **35** dargestellt) kann beispielsweise durch Eintippen des Worts mittels des Tastenfeldes **13** der Schnittstelle **12** geschehen. Dieses Übermitteln kann auch automatisch auf dem Umweg über die Kommunikationseinrichtung **10** oder mittels jedes anderen geeigneten Kommunikationsmittels verwirklicht werden, wie oben beschrieben ist.

[0059] Bei Eingabe der öffentlichen Identifikationsnummer **5** in die Einheit **3** führt das Programm des Servers **15** im Einklang mit der Karte und mit Hilfe der dynamischen Variablen, die unabhängig von der Karte **2** erzeugt sind, Berechnungsoperationen aus, die jenen, die in der Karte **2** ausgeführt werden, völlig gleich sind. Diese Operationen sind folglich in Fig. 2 mit den gleichen Bezugszeichen, gefolgt von dem Buchstaben „a", bezeichnet worden; das Gleiche gilt für die Register und den Zähler, die dazu dienen, die dynamischen Variablen Nna, Ta und Kann zu erzeugen. Die Variable Kna wird als Antwort auf die Zugangsanforderung, beispielsweise durch Übertragen der Identifikationsnummer **5** zur Schnittstelle **12**, aus dem Speicher **18** des Servers **15** ausgelesen. Der Speicher **18** speichert die Variablen Kna aller Karten, mit denen der Server zusammenwirken soll.

[0060] Folglich erzeugt der Server **15**, ohne dass ihm die in der Karte **2** erzeugten dynamischen Variablen übermittelt worden sind, ein Passwort Aa, das mit dem vom Anwender an den Server **15** übermittelten Passwort A verglichen wird. Wenn die Karte authentisch ist, müssen die Passwörter A und Aa identisch sein oder zumindest gemäß im Voraus festgelegten Regeln übereinstimmen. Wenn der Test unter **36** zu einer bejahenden Antwort führt, wird die Funktion unter **1** freigegeben. Andernfalls wird unter **37** der Zugang verweigert.

[0061] Es muss festgehalten werden, dass in einem erfindungsgemäßen System bestimmte Probleme auftreten können, wenn eine der Variablen die Zeit ist oder eine Funktion der Zeit ist, wie oben beschrieben, denn die Drift der verwendeten Zeitgeber, sowohl in der Karte als auch in dem Server, kann nicht verhindert werden. Eine vorteilhafte Lösung dieser Probleme ist in der gleichzeitig im Namen des Anmelders der vorliegenden Erfindung hinterlegten Patentanmeldung mit dem Titel „Système de contrôle d'accès à une fonction comportant un dispositif de synchronisation d'horloges" beschrieben.

[0062] Es ist folglich festzustellen, dass erfindungsgemäß das Verfahren zur Authentifizierung der Karte, das zur Freigabe der Funktion unter **1** führt, mit Hilfe von mindestens zwei dynamischen Variablen ausgeführt wird, wobei die eine der Chiffrierschlüssel Kn (Kna) ist und die andere entweder die Anzahl Nn (Nna) der schon gestellten Zugangsanforderungen oder die Zeit T (Ta) ist oder aber die gemäß einer im Voraus festgelegten Funktion dieser Variablen berechnete Zahlen sind. Wie oben beschrieben können drei Variablen verwendet werden, etwa Kn (Kna), Nn (Nna) und T (Ta), wobei die Variablen Nn (Nna) und T (Ta) beispielsweise mittels einer Verkettungsoperation verknüpft sind.

[0063] Der Chiffrierschlüssel Kn (Kna) selbst driftet von einer Zugangsanforderung zur nächsten und ist dynamisch variabel in Abhängigkeit von dem Wert Nn (Nna), mit dem er logisch verknüpft und dann chiffriert werden kann, um den Chiffrierschlüssel Kn+1 (Kna+1) hervorzubringen, der dann bei der nächsten Zugangsanforderung verwendet wird.

[0064] Gemäß einer Variante der Erfindung kann eine Datenübertragung von der Karte **2** zur Einheit **3** und zum Server **15** vorgesehen werden, damit die Daten bei der Ausführung der Funktion **1**, selbstverständlich insoweit im Anschluss an den Test unter **36** die Erlaubnis dafür erteilt worden ist, verarbeitet werden können.

[0065] Beim Vorbringen seiner Zugangsanforderung gibt der Anwender unter **38** die Daten mit Hilfe des Tastenfeldes **6** in die Karte ein. Diese Daten werden unter **39** mit dem Wert aus der Verkettung der zwei Variablen Nn und T logisch verknüpft, wobei das Ergebnis als Eingangsparameter der Chiffrierprozedur verwendet wird, die unter **24** ausgeführt wird. In einer Variante können die Daten auch direkt mit dem Ergebnis der Chiffrieroperation unter **24** verknüpft werden. Es ist wesentlich, dass die Eingangsgröße der Operation **24** eine Funktion der zu übermittelnden Daten ist.

[0066] Ebenso werden die Daten dem Server **15** übermittelt, beispielsweise mit Hilfe des Tastenfeldes **13** der Schnittstelle **12** oder automatisch über Verbindungen **10** und **16**.

[0067] Die so unter **38a** in dem Server empfangen Daten werden dort auf die gleiche Weise wie in der Karte **2** verarbeitet. Die Daten können nämlich mittels einer logischen Verknüpfung unter **39a** mit dem Wert

aus der Verkettung von Nn und T kombiniert werden, wobei das Ergebnis als Eingangsparameter für das Chiffrierverfahren unter **24a** verwendet wird. In einer Variante können die Daten direkt mit dem Ergebnis der Chiffrieroperation unter **24a** verknüpft werden, oder aber die Daten können einen weiteren Schlüssel für die Rechenoperation unter **24a** bilden. Die Daten werden unchiffriert auch an die Einrichtung übergeben, welche die Ausführung der Funktion **1** zur Aufgabe hat.

[0068] Folglich kann die Authentizität von Daten durch Vergleichen der Passwörter A und Aa, die beide Funktion des Werts sind, der die Daten repräsentiert, verifiziert werden. Der Gebrauch der Funktion **1** wird folglich auch dann verweigert, wenn es keine Übereinstimmung zwischen den von beiden Seiten präsentierten Daten gibt.

[0069] Es werden nun weitere Ausführungsformen beschrieben, einige davon im Hinblick auf Änderungen, die in der Karte **2** erfolgen, wobei jedoch selbstverständlich ist, dass die gleichen Änderungen auch auf den Server **15** Anwendung finden, denn die Karte **2** und der Server **15** müssen identische oder übereinstimmende Passwörter erzeugen können.

[0070] Die in Fig. 1 und Fig. 3 veranschaulichte Operation **31** kann in Abhängigkeit von T variieren. Genauso kann der Algorithmus **33** bei jeder neuen Ableitung von Kn geändert werden; so auch der Algorithmus, der für die Berechnung unter **24** verwendet wird. Beispielsweise können die Module **24**, **24a** und **33**, **33a** mehrere Algorithmen speichern, die während der verschiedenen Operationen zur Berechnung der Passwörter unterschiedlich verwendet werden. In dem Server müssen dann synchronisierte Änderungen bezüglich der Funktion unter **31a** und der Algorithmen unter **24a** und **33a** vorgenommen werden.

[0071] Außerdem kann die Funktion **32** (Fig. 3) von einer EXKLUSIV-ODER-Funktion verschieden sein, etwa eine UND-Operation oder irgendeine andere logische Operation sein. Die Funktion **32** ist nicht unverzichtbar, da Nn+1 von dem Algorithmus unter **33** direkt verwendet werden kann, so dass mittels Kn oder Q chiffriert wird. Außerdem kann Q mit Nn+1 unter **32** einer EXKLUSIV-ODER-Operation unterworfen werden, wobei Kn oder K als Chiffrierschlüssel für das Chiffrieren der Ausgangsgröße verwendet werden, die durch die logische Operation unter **32** erzeugt wird.

[0072] Eine weitere Ausführungsform umfasst, ein UND-Gatter zwischen den Modulen **29** und **30** in Fig. 1 vorzusehen, wobei die Ausgangsgröße des Moduls **29** eine der Eingangsgrößen dieses UND-Gatters darstellt, wobei die andere Eingangsgröße von einem Signal gebildet ist, das vom Server **15** kommt und nur dann erzeugt wird, wenn das Modul **29a** eine Ausgangsgröße erzeugt. Dieses Signal des Servers **15** kann irgendein Typ von Kommunikationssignal sein, das über eine Telefonleitung befördert wird, oder irgendein moduliertes Signal, das über Infrarotstrahlen befördert wird. Auf diese Weise werden das Modul **25** in der Karte **2** und das Modul **25a** im Server **15** synchron inkrementiert. Es wird dann keinen Synchronisationsverlust der Werte Nn und Nna geben. Jedoch kann bei bestimmten Anwendungen der vorliegenden. Erfindung eine solche Kommunikation vom Server zurück zur Karte nicht erwünscht sein.

[0073] Eine weitere Variante besteht darin, die Daten unter **38** in den Speicher der Karte zu speichern. Wenn die Karte **2** beispielsweise eine Bankkarte ist, könnten die Daten unter **38** der Stand eines Bankkontos, eine Kontonummer usw. sein.

[0074] Das Ableiten von Kn gemäß den Funktionen **31** und **31a** kann auch wie folgt ausgeführt werden: Kn kann für jede Berechnung des Passworts zweimal abgeleitet werden. Dies kann beispielsweise vor und nach dem Berechnen des Passworts geschehen. Kn kann auch parallel zur Berechnung des Passworts noch einmal abgeleitet werden. Anders ausgedrückt: Kn kann während der Berechnung des Passworts noch einmal abgeleitet werden, wobei die Ausgangsgrößen des Moduls **24** und des Moduls **24a** dann direkt als Eingangsgrößen für das Modul **33** bzw. **33a** verwendet werden.

[0075] In einer Variante können die Werte Nn und T direkt in das Modul **24** eingegeben werden. Es ist möglich, die Daten direkt mit Nn oder T logisch zu verknüpfen oder aber in zwei Teile zu zerlegen, die mit Nn bzw. T verknüpft werden.

Patentansprüche

1. System zur Zugangskontrolle oder zur Authentifizierung von Personen und/oder von Nachrichten, durch welches wenigstens einem Anwender erlaubt werden kann, Zugriff auf eine Zugangsfunktion oder Funktion zur Authentifizierung von Personen und/oder Nachrichten zu haben, mit wenigstens einer ersten, für den Anwender personalisierten Einheit (**2**) und wenigstens einer zweiten Einheit zur Verifizierung (**3**), die den Zugang zu der Funktion steuern,
• wobei die erste Einheit (**2**) umfasst:
erste Generatormittel (**25**, **26**, **31**), um wenigstens zwei dynamische Variablen (Nn, T) zu erzeugen;
erste Rechenmittel (**24**), um ein erstes Passwort (A) mit Hilfe wenigstens eines ersten Chiffrieralgorithmus unter Verwendung von Eingangsparametern in Abhängigkeit von den in der ersten Einheit generierten dynamischen Variablen zu erzeugen; und Mittel (**10**, **12**, **35**), um der zweiten Einheit (**3**) das erste Passwort zu übermitteln;
• wobei die zweite Einheit (**3**) umfasst:

zweite Generatormittel (**25a**, **26a**, **31a**), um als Antwort auf eine Zugangsanforderung, die mit Hilfe einer bestimmten der ersten Einheiten gestellt worden ist, wenigstens zwei dynamische Variablen (Nna, Ta) zu erzeugen, die eben dieser bestimmten ersten Einheit zugeordnet sind;
zweite Rechenmittel (**24a**), um ein zweites Passwort (Aa) mit Hilfe wenigstens eines zweiten Chiffrieralgorithmus unter Verwendung von Eingangsparametern in Abhängigkeit von den in der zweiten Einheit generierten dynamischen Variablen (Nna, Ta) zu erzeugen;
Mittel (**36**), um das erste und zweite Passwort zu vergleichen;
Mittel, um eine Erlaubnis für den Zugang zu der Funktion (**1**) zu erteilen, wenn zwischen den Passwörtern ein im Voraus festgelegter Zusammenhang besteht,
dadurch gekennzeichnet, dass in jeder der Einheiten:
• der erste und zweite Chiffrieralgorithmus öffentliche Algorithmen sind und wenigstens eine der dynamischen Variablen geheim ist,
• wenigstens eine der dynamischen Variablen zeitunabhängig ist, und
• die ersten und zweiten Generatormittel (**25**, **26**, **31**, **25a**, **26a**, **31a**) dafür eingerichtet sind, dass sie ihre dynamischen Variablen im Einklang, jedoch auf unabhängige Weise erzeugen.

2. Kontrollsystem nach Anspruch 1, dadurch gekennzeichnet, dass die ersten und zweiten Generatormittel (**25**, **26**, **31**, **25a**, **26a**, **31a**) dritte bzw. vierte Rechenmittel (**33**) umfassen, um wenigstens eine erste der dynamischen Variablen (Kn, Kna) gemäß einer Funktion zu erzeugen, die eine Anzahl von Zugangsanforderungen, die von der ersten Einheit (**2**) vor der laufenden Zugangsanforderung vorgebracht wurden, einbezieht.

3. Kontrollsystem nach Anspruch 2, dadurch gekennzeichnet, dass die dritten und vierten Rechenmittel (**33**) jeweils eine dynamische Zwischenvariable (Z) durch logisches Verknüpfen der Anzahl der zuvor vorgebrachten Zugangsanforderungen und des Momentanwerts der ersten dynamischen Variablen (Kn, Kna) erzeugen.

4. Kontrollsystem nach Anspruch 3, dadurch gekennzeichnet, dass die dritten und vierten Rechenmittel (**33**) mittels des dritten bzw. vierten Algorithmus' eine Chiffrierung der dynamischen Zwischenvariablen (Z) verwirklichen, wobei das Ergebnis dieser Chiffrierung einen neuen Wert (Kn+1, Kna+1) der ersten dynamischen Variablen darstellt.

5. Kontrollsystem nach Anspruch 4, dadurch gekennzeichnet, dass die dritten und vierten Rechenmittel (**33**) jeweils Mittel umfassen, um die dynamische Zwischenvariable (Z) unter Verwendung der ersten Variablen (Kn, Kna) als geheimen Chiffrierschlüssel für den dritten und vierten Algorithmus zu chiffrieren.

6. Kontrollsystem nach Anspruch 4, dadurch gekennzeichnet, dass die dritten und vierten Rechenmittel (**33**) jeweils Mittel umfassen, um die dynamische Zwischenvariable mit einem Chiffrierschlüssel (Q) zu chiffrieren, der sich von der ersten dynamischen Variablen unterscheidet und für den dritten bzw. vierten Algorithmus verwendet wird.

7. Kontrollsystem nach Anspruch 4, dadurch gekennzeichnet, dass die dritten und vierten Rechenmittel (**33**) das Ergebnis der Chiffrierung durch den dritten und vierten Chiffrieralgorithmus an die ersten bzw. zweiten Rechenmittel (**24**, **24a**) als Chiffrierschlüssel für den ersten und zweiten Algorithmus übermitteln.

8. Kontrollsystem nach einem der Ansprüche 2 bis 7, dadurch gekennzeichnet, dass die ersten und zweiten Generatormittel (**25**, **25a**) jeweils eine zweite der dynamischen Variablen in Abhängigkeit von der Anzahl der vorgebrachten Zugangsanforderungen (Nn, Nna) erzeugen und die zweite dynamische Variable den ersten bzw. zweiten Rechenmitteln (**24**, **24a**) übermitteln, und dadurch, dass die ersten und zweiten Rechenmittel (**24**, **24a**) einen Eingangsdatenwert, der die zweite dynamische Variable umfasst, mit Hilfe des ersten bzw. zweiten Chiffrieralgorithmus berechnen.

9. Kontrollsystem nach Anspruch 8, dadurch gekennzeichnet, dass die ersten und zweiten Generatormittel (**26**, **26a**) jeweils eine dritte der dynamischen Variablen in Abhängigkeit von der momentanen Zeit (T, Ta) erzeugen und die dritte dynamische Variable den ersten bzw. zweiten Rechenmitteln (**24**, **24a**) übermitteln, und dadurch, dass die ersten bzw. zweiten Rechenmittel (**24**, **24a**) die dritte dynamische Variable (T, Ta) in den Eingangsdatenwert einarbeiten.

10. Kontrollsystem nach Anspruch 9, dadurch gekennzeichnet, dass die ersten und zweiten Rechenmittel (**24**, **24a**) jeweils eine Verkettung der dritten Variablen und des Eingangsdatenwertes ausführen.

11. Kontrollsystem nach einem der Ansprüche 4 bis 10, dadurch gekennzeichnet, dass der dritte und vierte Chiffrieralgorithmus dem ersten und zweiten Chiffrieralgorithmus völlig gleich sind.

12. Kontrollsystem nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass die ersten und zweiten Generatormittel (**25**, **25a**, **26**, **26a**, **31**, **31a**) den ersten und zweiten Rechenmitteln (**24**, **24a**) jeweils eine erste der dynamischen Variablen (Kn, Kna) als Chiffrierschlüssel für den ersten und zweiten Algorithmus übermitteln und einen Eingangsdatenwert

(Nn, Nna) erzeugen, der eine zweite der Variablen umfasst, welche die Anzahl der von der ersten Einheit vor der laufenden Zugangsanforderung vorgebrachten Zugangsanforderungen repräsentiert, wobei der Eingangsdatenwert den ersten bzw. zweiten Rechenmitteln (**24**, **24a**) übermittelt wird, um dort mittels der ersten dynamischen Variablen chiffriert zu werden.

13. Kontrollsystem nach Anspruch 12, dadurch gekennzeichnet, dass die ersten und zweiten Generatormittel (**25**, **26**, **31**, **25a**, **26a**, **31a**) jeweils dritte und vierte Rechenmittel umfassen, um einen Chiffrierschlüssel (Kn, Kna) in Abhängigkeit von der Anzahl der vorgebrachten Zugangsanforderungen zu erzeugen.

14. Kontrollsystem nach Anspruch 13, dadurch gekennzeichnet, dass die dritten und vierten Rechenmittel (**33**) jeweils Speichermittel (**28**) umfassen und ausgehend von dem Momentanwert (Kn, Kna) des Chiffrierschlüssels einen neuen Wert (Kn+1, Kna+1) dieses erzeugen und den neuen Wert in den Speichermitteln (**28**) anstelle des Momentanwertes speichern.

15. Kontrollsystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die erste Einheit (**2**) Mittel (**6**, **38**) umfasst, um Daten zu speichern, die dafür bestimmt sind, der zweiten Einheit (**3**) übermittelt zu werden, damit sie verwendet werden können, um von der Funktion Gebrauch zu machen, dadurch, dass die zweite Einheit (**3**) Mittel (**12**, **38**) umfasst, um die Daten zu empfangen, und dadurch, dass die ersten und zweiten Generatormittel Mittel (**39**) umfassen, um die Daten an die ersten bzw. zweiten Rechenmittel (**24**, **24a**) zu übermitteln, damit sie als eine Komponente wenigstens einer der zu chiffrierenden dynamischen Variablen verwendet werden können.

16. System nach einem der Ansprüche 1 bis 15, dadurch gekennzeichnet, dass die erste Einheit (**2**) in Form einer tragbaren elektronischen Vorrichtung auftritt.

17. Kontrollsystem nach Anspruch 16, dadurch gekennzeichnet, dass es Kommunikationsmittel (**10**) in der ersten und zweiten Einheit umfasst, wobei die Kommunikationsmittel eine Telefonverbindung vom Typ DTMF und/oder eine Verbindung, die mittels Infrarotstrahlen funktioniert, umfassen.

18. Kontrollsystem nach einem der Ansprüche 1 bis 15, dadurch gekennzeichnet, dass es einen Kartenleser umfasst, der in der zweiten Einheit (**3**) vorgesehen ist, und dadurch, dass die erste Einheit (**2**) in Form einer Karte auftritt, die von dem Leser gelesen werden kann, so dass der Informationsaustausch zwischen der ersten Einheit (**2**) und der zweiten Einheit (**3**) möglich ist.

19. Kontrollsystem nach einem der Ansprüche 1 bis 18, dadurch gekennzeichnet, dass die im Voraus festgelegte Beziehung zwischen den Passwörtern die Gleichheit ist.

20. Kontrollsystem nach Anspruch 9, dadurch gekennzeichnet, dass die ersten und zweiten Rechenmittel (**24**, **24a**) jeweils die Verarbeitung der zweiten und dritten Variablen (Nn, T, Nna, Ta) sicherstellen, um den Eingangsdatenwert zu erzeugen.

21. Kontrollsystem nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass der erste und zweite Chiffrieralgorithmus verschieden sind, jedoch eine im Voraus festgelegte Beziehung aufweisen, die sich in der Beziehung zwischen dem ersten und dem zweiten Passwort (A, Aa) widerspiegelt.

22. System zur Zugangskontrolle oder zur Authentifizierung von Personen und/oder von Nachrichten, durch welches insbesondere wenigstens einem Anwender erlaubt werden kann, Zugriff auf eine Zugangsfunktion oder Funktion zur Authentifizierung von Personen und/oder Nachrichten zu haben, mit wenigstens einer ersten, für den Anwender personalisierten Einheit und wenigstens einer zweiten Einheit zur Verifizierung, die den Zugang zu der Funktion steuern,
wobei die erste Einheit umfasst:
erste Generatormittel, um wenigstens zwei dynamische Variablen zu erzeugen;
erste Rechenmittel, um mit Hilfe wenigstens eines Chiffrieralgorithmus, der Eingangsparameter in Abhängigkeit von Variablen verwendet, ein Passwort zu erzeugen; und
Mittel, um der zweiten Einheit das Passwort zu übermitteln;
wobei die zweite Einheit umfasst:
zweite Generatormittel, um als Antwort auf eine Zugangsanforderung, die mit Hilfe einer bestimmten der ersten Einheiten gestellt ist, wenigstens zwei dynamische Variablen zu erzeugen, die eben dieser ersten bestimmten Einheit zugeordnet sind;
zweite Rechenmittel, um das Passwort mit Hilfe wenigstens eines Dechiffrieralgorithmus unter Verwendung eines Eingangsparameters in Abhängigkeit von einer ersten der dynamischen Variablen, die in der zweiten Einheit erzeugt sind, um eine dynamische Variable abzuleiten, die einer der in der ersten Einheit erzeugten dynamischen Variablen entsprechen muss, als Dechiffrierschlüssel zu dechiffrieren;
Vergleichsmittel, um die mittels der zweiten Rechenmittel abgeleitete dynamische Variable mit einer zweiten der in der zweiten Einheit erzeugen dynamischen Variablen zu vergleichen;
Mittel, die dann, wenn die Vergleichsmittel feststellen, dass zwischen der mittels der zweiten Rechenmittel abgeleiteten dynamischen Variablen und der

zweiten dynamischen Variablen von den in der zweiten Einheit erzeugten dynamischen Variablen ein im Voraus festgelegter Zusammenhang besteht, eine Erlaubnis für den Zugang zu der Funktion erteilen;
dadurch gekennzeichnet, dass
die ersten und zweiten Generatormittel, die in der ersten bzw. zweiten Einheit vorgesehen sind, so konfiguriert sind, dass sie die dynamischen Variablen im Einklang, jedoch unabhängig voneinander liefern.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

FIG.: 1

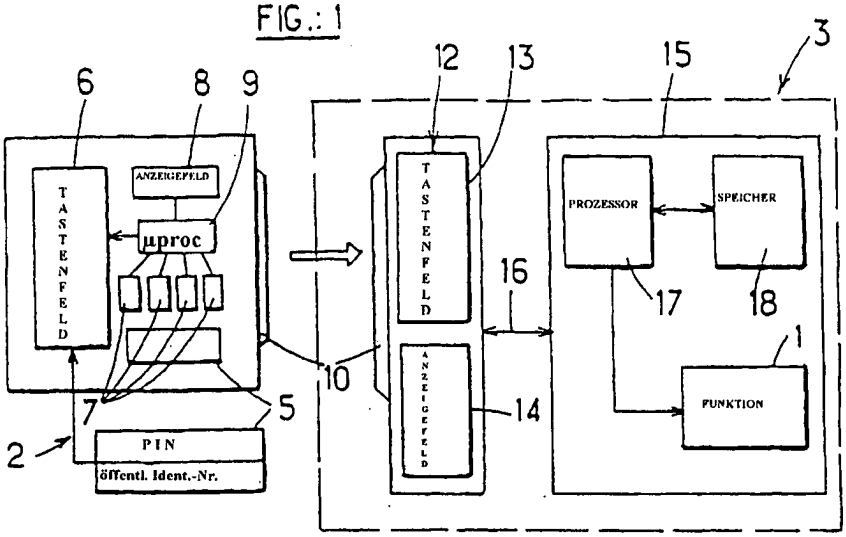


FIG.: 3

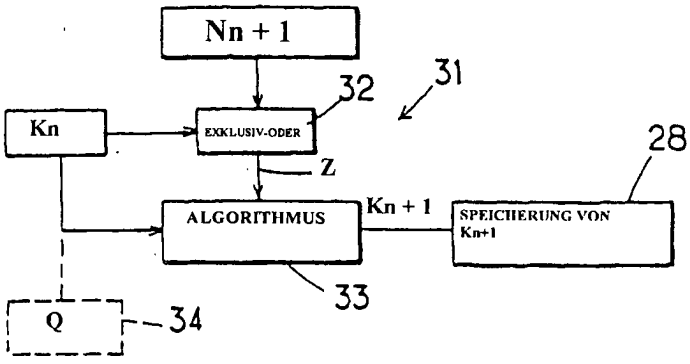
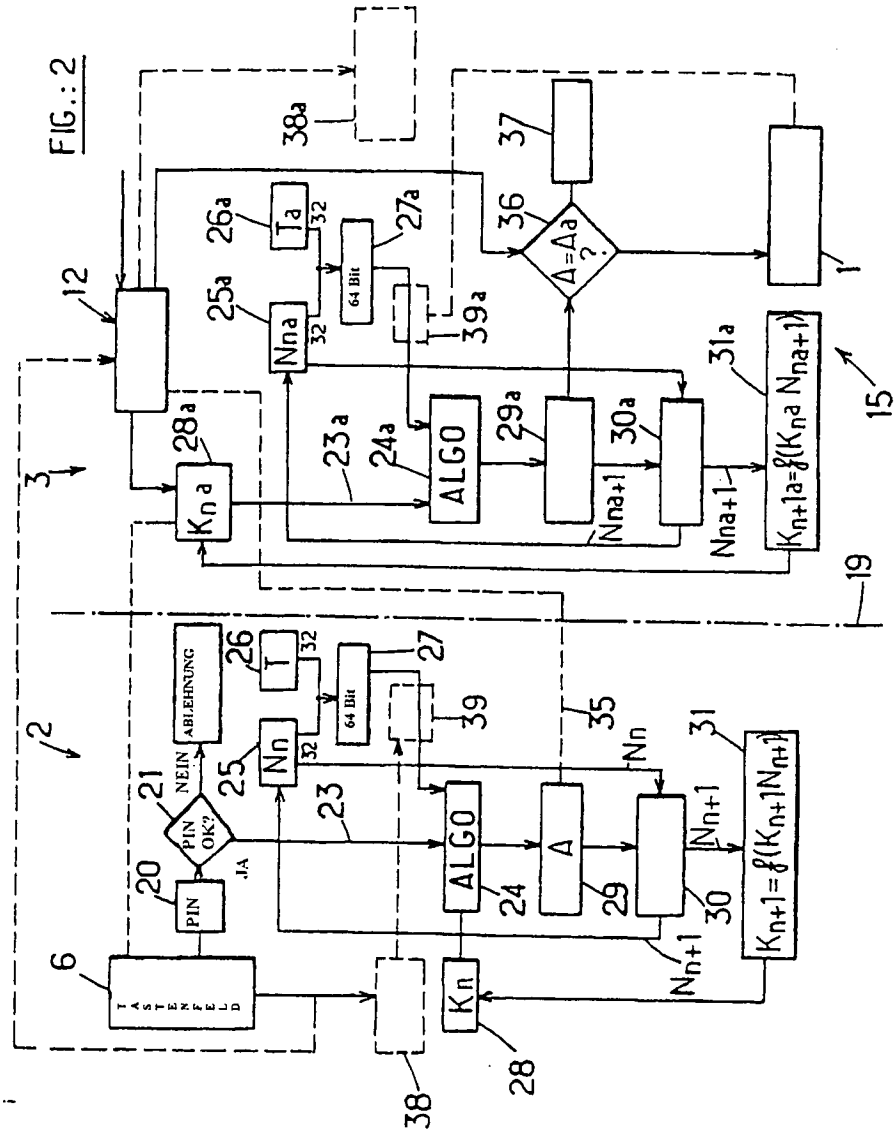


FIG.: 2


TASTENFELD
PIN
PIN OK?
NEIN
JA
ABLEHNUNG
ALGO
A
64 Bit
Kn
Nn
Nn+1
Kn+1=f(Kn+1 Nn+1)
Ta
Na
Δ=Δa ?
Kn a
Kn+1a=f(Kn a Nna+1)
Nna+1
Nna+1
1
2
3
6
12
15
19
20
21
23
24
25
26
27
28
29
30
31
35
36
37
38
39
23a
24a
25a
26a
27a
28a
29a
30a
31a
38a
39a