(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
19. Dezember 2002 (19.12.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/102103 A2

(51) Internationale Patentklassifikation[7]: H04Q 7/32

(21) Internationales Aktenzeichen: PCT/EP02/06397

(22) Internationales Anmeldedatum:
11. Juni 2002 (11.06.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 28 300.8 12. Juni 2001 (12.06.2001) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **VATER, Harald** [DE/DE]; An den Schulgärten 23, 35398 Giessen (DE). **BOCKES, Markus** [DE/DE]; An der Tuchbleiche 3, 81927 München (DE). **HECKMANNS, Ulrich** [DE/DE]; Spicherenstrasse 12, 81667 München (DE).

(74) Anwalt: **KLUNKER, SCHMITT-NILSON, HIRSCH**; Winzererstrasse 106, 81797 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) **Title:** AUTHENTICATION METHOD

(54) **Bezeichnung:** AUTHENTISIERUNGSVERFAHREN

(57) **Abstract:** The invention relates to a method for producing an authentication response parameter SRES for authenticating a subscriber identification unit in a network, especially GSM-network, in a service provider. The authentication response parameter SRES is calculated by using an individual authentication key Ki from a question parameter RAND, allocated to said subscriber identification unit .A modifying parameter AM associated with the service provider is used in at least one step of the inventive method during calculation.

(57) **Zusammenfassung:** Es wird ein Verfahren zur Erzeugung eines Authentisierungsantwortparameters SRES zur Authentisierung einer Teilnehmeridentifizierungseinheit in einem Netzwerk, insbesondere GSM-Netz, bei einem Dienstanbieter beschrieben, bei dem der Authentisierungsantwortparameter SRES unter Verwendung eines der Teilnehmeridentifizierungseinheit zugeordneten individuellen Authentisierungsschlüssels Ki aus einem Anfrageparameter RAND berechnet wird. Dabei wird in mindestens einem Verfahrensschritt bei der Berechnung ein dem Dienstanbieter zugeordneter Modifizierungsparameter AM verwendet.

WO 02/102103 A2

Authentisierungsverfahren

Die vorliegende Erfindung betrifft ein Verfahren zur Erzeugung eines Authentisierungsantwortparameters zur Authentisierung einer Teilnehmeridentifizierungseinheit in einem Netzwerk bei einem Dienstanbieter (Provider). Darüber hinaus betrifft die Erfindung ein Authentisierungsverfahren für ein Netzwerk unter Verwendung eines solchen Verfahrens zur Erzeugung des Authentisierungsantwortparameters, eine Teilnehmeridentifizierungseinheit und eine Authentisierungszentrale zur Durchführung des Verfahrens sowie ein Computerprogramm mit entsprechenden Programmcode-Mitteln, um das Verfahren mittels eines Computers auszuführen.

In Mobilfunknetzen wird bekanntermaßen die Mobilität der Teilnehmer dadurch erreicht, dass die einzelnen Netzbetreiber jeweils ein möglichst weit verbreitetes, engmaschiges Netz von Basisstationen zur Verfügung stellen, über welche der einzelne Teilnehmer mit Hilfe seines Endgeräts bzw. Mobilfunkgerätes mit dem Mobilfunknetz kommunizieren kann. Aufgrund dieser Funkschnittstellen ist das gesamte System relativ empfindlich gegenüber Missbrauch des Netzes durch unauthorisierte Benutzer und gegenüber Lauschangriffen auf die übertragenen Informationen, da in der Regel von jedem beliebigen Ort die Möglichkeit besteht, die Funksignale abzuhören oder zu übermitteln, ohne dass ein direkter mechanischer Eingriff in das Mobilfunknetz, beispielsweise ein Anklemmen von Kabeln etc., nötig ist. Die gleiche Problematik stellt sich auch in anderen Netzwerken, wie beispielsweise dem Internet, in denen auf relativ leicht für die Öffentlichkeit zugänglichem Wege Daten ausgetauscht werden, und in denen der Zugang zu vielen Diensten

oder Datenbereichen im Prinzip ohne mechanische Eingriffe leicht und oftmals unbemerkt möglich ist.
Aus diesem Grunde sind insbesondere in derartigen, leicht zugänglichen Netzwerken besondere Maßnahmen erforderlich, um sowohl die Nutzer des Netzes bzw. des Dienstes im Netz als auch den Dienstanbieter gegen solche unerwünschten Eingriffe zu schützen. Hierbei stehen zwei Hauptsicherheitsziele im Vordergrund:

Ein Ziel ist die Authentifizierung und somit die Zugangskontrolle des einzelnen Teilnehmers zum angebotenen Dienst, beispielsweise beim Mobilfunknetz der Aufbau einer Verbindung zu einem anderen Fernsprechteilnehmer. Ein weiteres Hauptziel ist der Schutz der übertragenen Informationen an sich.

Der Zweck einer Authentisierung ist die Überprüfung der Identität und Authentizität eines Kommunikationspartners. Dabei reicht es aus, wenn eine einseitige Authentisierung durchgeführt wird, das heißt, wenn das Netzwerk bzw. der Dienstanbieter die Authentizität des Teilnehmers bzw. des Endgeräts bzw. einer darin befindlichen Teilnehmeridentifizierungseinheit, welche sich beispielsweise auf einer Chipkarte befindet, feststellen kann. Die beiden Kommunikationsteilnehmer müssen zur Authentisierung ein gemeinsames Geheimnis besitzen, das mit Hilfe eines Authentisierungsverfahrens überprüft wird. Hierbei kann es sich beispielsweise um ein Passwort oder dergleichen handeln. Sinnvollerweise wird zur Authentisierung jedoch ein dynamisches Verfahren verwendet. Ein solches dynamisches Verfahren ist so aufgebaut, dass es vor einem Angriff durch Wiedereinspielen von aufgezeichneten Daten aus früheren Sitzungen geschützt ist, da für jede einzelne Authentisierung eine unterschiedliche Datengrundlage verwendet wird.

Dies ist z.B. möglich, indem in einem ersten Schritt das Netzwerk bzw. der Dienstanbieter an die Teilnehmeridentifizierungseinheit einen bestimmten Anfrageparameter (challenge) sendet, welcher in der Teilnehmeridentifizierungseinheit mit einem geheimen Authentisierungsschlüssel verschlüsselt wird, der nur der Teilnehmeridentifizierungseinheit und dem Netzwerk bzw. dem Dienstanbieter bekannt ist. Das Verschlüsselungsergebnis wird dann in einem zweiten Schritt zurückgesendet und vom Netzwerk bzw. vom Dienstanbieter mit einem aus dem gesendeten Anfrageparameter und dem gemeinsamen Schlüssel parallel erzeugten Antwortparameter (response) verglichen. Dieses Prinzip wird als sogenanntes „challenge and response-Prinzip" bezeichnet. Es ist das übliche Prinzip der Authentisierung im Chipkartenbereich. Als Anfrageparameter wird in der Regel eine Zufallszahl generiert. Im Folgenden wird daher auch von einer Zufallszahl als Anfrageparameter ausgegangen, wobei dies die Erfindung nicht auf die Verwendung einer Zufallszahl als Anfrageparameter einschränken soll.

Nach durchgeführter Authentisierung werden die Informationen übertragen, die gegen Angriffe geschützt werden müssen. Die Sicherung der übertragenen Daten zwischen dem Endgerät und dem Netzwerk bzw. dem Dienstanbieter geschieht vorzugsweise durch eine geeignete Nachrichtenverschlüsselung, wobei sinnvollerweise auch hier für jede Verbindung ein neuer Schlüssel verwendet wird. Dies ist z. B. dadurch möglich, dass der zunächst für die Authentisierung verwendete Anfrageparameter (bzw. die Zufallszahl), welchen das Netzwerk bzw. der Dienstanbieter an die Teilnehmeridentifizierungseinheit sendet, zusätzlich dazu verwendet wird, einen (temporären) Nachrichtencodierungsschlüssel zur Verschlüsselung der übersendeten Daten zu erzeugen.

Das zuvor beschriebene Prinzip der Teilnehmerauthentisierung und Nachrichtenverschlüsselung wird nachfolgend detailliert am Beispiel des unter dem Begriff GSM (Global System for Mobile Communications) bekannten Standards für Mobiltelefone erläutert. Es wird jedoch noch einmal darauf hingewiesen, dass die Erfindung nicht auf die Anwendung in Mobilfunknetzen, insbesondere nach diesem Standard, beschränkt ist.

Ein GSM-Mobilfunknetz ist aus mehreren Base Station Systemen (BSS) aufgebaut, die von einem Mobile Switching Center (MSC) verwaltet werden, welches als besondere Komponente ein sogenanntes Authentisierungszentrum (Authentication Center; AUC) besitzt. Das AUC ist eine besondere Sicherheitsinstanz, welche über die notwendigen Schlüssel und Algorithmen für die Authentisierung der Mobilfunkgeräte bzw. der darin befindlichen Teilnehmeridentifizierungseinheiten verfügt.

Das Gegenstück zu den Base Station Systemen (BSS) bilden die individuellen Mobilfunkgeräte. Ein Mobilfunkgerät besteht im Wesentlichen aus dem eigentlichen Gerät an sich, welches das Funkteil, eine Codier-/Decodiereinheit (Codec) zur Aufbereitung, insbesondere zur Ver- und Entschlüsselung der übermittelten Daten, eine Tastatur, ein Display und weitere übliche Komponenten aufweist. Ein weiterer wesentlicher Bestandteil des Mobilfunkgeräts ist eine Teilnehmeridentifizierungseinheit, welche im GSM-System SIM (Subscriber Identity Module) genannt wird. Üblicherweise befindet sich das SIM auf einer Chipkarte, welche in das eigentliche Gerät eingesetzt wird. Erst mit eingesetztem SIM ist das Mobilfunkgerät einsatzfähig.

Jedem SIM ist von Haus aus eine im gesamten GSM-System einzigartige Nummer, die sogenannte IMSI (International Mobile Subscriber Identity),

sowie eine geheime Nummer, der sogenannte Authentisierungsschlüssel (Subscriber authentication Key; Ki), zugeordnet. Diese Daten und insbesondere der Authentisierungsschlüssel (Ki) sind in dem SIM in einem besonders geschützten Bereich abgespeichert.

Auf der anderen Seite weist das Authentication Center (AUC) des jeweiligen Mobilfunknetzes eine Datenbank auf, in der die Identifizierungsnummern (IMSI) gemeinsam mit den zugeordneten Authentisierungsschlüsseln (Ki) hinterlegt sind.

Wird ein Mobilfunkgerät (im Folgenden auch Mobilstation genannt) in einem Mobilfunknetz eingebucht, so wird von der Mobilstation bzw. dem SIM zunächst die IMSI an das Mobilfunknetz übermittelt. Damit ist die Mobilstation im Mobilfunknetz eindeutig identifiziert. Zur Authentisierung wird vom Mobilfunknetz an die Mobilstation eine zufällig erzeugte Zahl (allgemein mit RAND oder RND bezeichnet) übermittelt.

Sowohl das SIM der Mobilstation als auch das Authentication Center erzeugen aus dieser Zufallszahl mittels eines festgelegten Algorithmus, der im GSM-System „A3" genannt wird, unter Verwendung des geheimen individuellen Authentisierungsschlüssels Ki des SIM einen Authentisierungsantwortparameter (allgemein Signed Response genannt; SRES). Nach dem derzeitigen Standard hat die Zufallszahl eine Länge von 128 Bit. Ebenso hat der Authentifizierungsschlüssel üblicherweise eine Länge von 128 Bit. Das Ergebnis der mit dem Algorithmus A3 erzeugten Authentisierungsantwortparameters SRES ist im derzeitigen Standard 32 Bit lang. Der SRES wird vom SIM an das Mobilfunknetz übermittelt, wo die Antwort mit dem vom Authentication Center AUC parallel erzeugten Authentisierungsantwort-

parameter verglichen wird. Bei Übereinstimmung kann davon ausgegangen werden, dass das SIM den richtigen Schlüssel Ki besitzt. Es ist somit authentisiert.

Weiterhin weisen sowohl das SIM als auch das Authentication Center AUC einen sogenannten A8-Algorithmus auf. In diesem A8-Algorithmus wird aus der Zufallszahl, wiederum unter Verwendung des Authentisierungsschlüssels Ki der jeweiligen SIM, ein Nachrichtencodierungsschlüssel (ciphering Key; Kc; Länge: 64 bit) erzeugt. Dieser Nachrichtencodierungsschlüssel Kc dient dazu, die während der Verbindung zu übermittelnden (Sprach-)Daten zwischen Mobilstation und Mobilfunknetz zu verschlüsseln und somit gegen ein Abhören zu sichern. Der Nachrichtencodierungsschlüssel Kc wird folglich bei jedem Authentisierungsvorgang abhängig von der Zufallszahl RAND neu erzeugt, was die Sicherheit der Übermittlung gegen Abhören erheblich erhöht. Die im Codec des Mobilfunkgeräts befindliche Verschlüsselungseinheit ist in der Lage, die Sprachdaten in Echtzeit mit dem Nachrichtencodierungsschlüssel Kc unter Nutzung eines sogenannten A8-Algorithmus ver- bzw. zu entschlüsseln. Auf der anderen Seite werden im Mobilfunknetz mit dem dort parallel erzeugten identischen Schlüssel die übermittelten Daten entsprechend ver- bzw. entschlüsselt.

Zur Authentisierung und Sicherung wird also bei jeder Neueinbuchung einer Mobilstation in ein Mobilfunknetz ein sogenanntes „Triplet" von drei Parametern - der Zufallszahl (RAND), dem daraus abgeleiteten Authentisierungsantwortparameter (SRES) und dem Nachrichtencodierungsschlüssel (Kc) - benötigt, wobei lediglich die Zufallszahl vom Mobilfunknetz an die Mobilstation gesendet wird und diese den Authentisierungsantwortparame-

ter zurücksendet. Jedes Triplet (RAND, SRES, Kc) wird nur einmal benützt und dann verworfen.

Zur Einsparung von Rechen- und Übermittlungszeiten für die Triplets werden üblicherweise zu einem bestimmten Zeitpunkt vom Authentisierungszentrum AUC für jeden Teilnehmer des zugehörigen Mobilfunknetzes mehrere Triplets erzeugt und in einem speziellen Sicherheitsparameter-File gespeichert. Da diese drei Parameter (RAND, SRES, Kc) völlig ausreichen, um ein bestimmtes SIM zu authentisieren und eine verschlüsselte Verbindung aufzubauen, besteht somit die Möglichkeit, fremden GSM-Netzen vom Heimatnetz ein bestimmtes Triplet zur Verfügung zu stellen, ohne dass der geheime Authentisierungsschlüssel (Ki) oder der in der Regel geheime Algorithmus herausgegeben werden muß, welche üblicherweise in speziellen Sicherheitseinrichtungen innerhalb des Authentication Center aufbewahrt werden. Somit ist eine einfache Möglichkeit gegeben, dass sich ein Teilnehmer eines Mobilfunknetzes, beim sogenannten „Roaming", in einem fremden Netz als Gast einbuchen kann.

Aufgrund der Authentisierungsmöglichkeit mittels lediglich dreier temporärer Parameter ohne eine Herausgabe der streng geheimzuhaltenden Schlüssel bzw. Codier-Algorithmen, ist ein solches Verfahren auch gut zur Verwendung im Internet oder anderen öffentlich zugänglichen Netzwerken geeignet. Auch hier kann beispielsweise von einer Authentisierungszentrale verschiedenen Dienstanbietern oder auch verschiedenen unabhängigen Servern eine Anzahl von Triplets für eine bestimmte Teilnehmeridentifizierungseinheit zur Verfügung gestellt werden, mit denen diese dann in der Lage sind, eine bestimmte Teilnehmeridentifizierungseinheit zu authentisieren und verschlüsselt Daten auszutauschen. Darüber hinaus kann das Ver-

fahren aber auch zur zusätzlichen Sicherung in abgeschlossenen, gesicherten Netzwerken, z. B. Geldautomatennetzen, eingesetzt werden.

Ein spezieller A3-Algorithmus zur Erzeugung eines Authentisierungsantwortparameters zur Authentisierung einer Teilnehmeridentifizierungseinheit in einem GSM-Netz ist in der WO 97/15161 beschrieben. Nach dem dort genannten Verfahren ist vorgesehen, die 128 Bit lange Zufallszahl mit einem speziellen Algorithmus zunächst in einen 152 Bit langen Parameter umzuwandeln. Dieser Eingangsparameter wird einem sogenannten CAVE-Algorithmus zugeführt, welcher daraus einen 18 Bit langen Ausgangsparameter erzeugt. Dieser 18 Bit lange Ausgangsparameter wird dann in einen 32 Bit langen Authentisierungsantwortparameter umgewandelt. Das dort beschriebene Verfahren hat den Zweck, den in amerikanischen Mobilfunkstandards verwendeten CAVE-Algorithmus für den GSM-Standard nutzbar zu machen. Das Verfahren hat jedoch den Nachteil, dass der gesamte Algorithmus festgelegt ist und nur mit großem Aufwand variiert werden kann.

Wie bereits oben beschrieben, ist es wünschenswert, wenn nicht nur die individuellen Authentisierungsschlüssel Ki der einzelnen Teilnehmeridentifizierungseinheiten eines Mobilfunknetzes geheimgehalten werden, sondern auch der Algorithmus individualisiert wird, um so eine höhere Sicherheit zu erreichen

Der Erfindung liegt daher die Aufgabe zugrunde, ein entsprechendes Verfahren zur Erzeugung des Authentisierungsantwortparameters zur Verfügung zu stellen, welches einfach und kostengünstig individuell veränderbar ist. Des Weiteren stellt sich die Aufgabe, ein entsprechendes Authentisierungsverfahren sowie eine Teilnehmeridentifizierungseinheit und eine Au-

thentisierungszentrale zur Durchführung des Verfahrens zur Verfügung zu stellen.

Diese Aufgabe wird durch ein Verfahren zur Erzeugung eines Authentisierungsantwortparameters gemäß Anspruch 1, ein Authentisierungsverfahren gemäß Anspruch 5, eine Teilnehmeridentifizierungseinheit gemäß Anspruch 7 und eine Authentisierungszentrale gemäß Anspruch 9 gelöst. In den abhängigen Ansprüchen sind vorteilhafte Ausgestaltungen der Erfindung angegeben.

Erfindungsgemäß wird das Verfahren zur Erzeugung des Authentisierungsantwortparameters aus dem Anfrageparameter, vorzugsweise einer Zufallszahl, dadurch individualisiert, dass in mindestens einem Verfahrensschritt bei der Berechnung ein dem jeweiligen Dienstanbieter zugeordneter individueller Modifizierungsparameter verwendet wird. Das heißt, es wird wie bei einem Schlüssel ein zusätzlicher Parameter eingeführt, welcher an einer bestimmten Stelle innerhalb des Algorithmus genutzt wird. Die Veränderung dieses Modifizierungsparameters bedeutet folglich gleichzeitig eine Veränderung des Algorithmus. Auf diese Weise ist es möglich, auch für eine Großzahl von verschiedenen Dienstanbietern jeweils individuelle Authentisierungsverfahren zur Verfügung zu stellen, die genauso sicher und schnell sind wie die mit dem unveränderten Algorithmus durchgeführten Verfahren.

Der Modifizierungsparameter kann beispielsweise mit einem Zufallszahlgenerator erzeugt werden. Dies kann zum Beispiel von einem Hersteller der Teilnehmeridentifizierungseinheiten, insbesondere Chipkartenhersteller, durchgeführt werden, welcher in der Regel auch die Identifizierungsnum-

mern und die Authentisierungsschlüssel für die einzelnen Teilnehmeridentifizierungseinheiten in gesicherter Umgebung erzeugt und in die Teilnehmeridentifizierungseinheiten implementiert. Ebenso kann der Modifizierungsparameter vom Hersteller der Teilnehmeridentifizierungseinheiten, genau wie der Algorithmus, die Identifizierungsnummern und die Authentisierungsschlüssel für die Teilnehmeridentifizierungseinheiten, zum einen auf sicherem Wege an das Authentisierungszentrum übermittelt werden und zum anderen in gesicherter Umgebung hinterlegt werden.

Bei dem Verfahren können übliche Verschlüsselungsverfahren wie beispielsweise das weiter unten noch näher erläuterte Triple-DES-Verfahren verwendet werden. Diese Verfahren bieten derzeit eine größtmögliche Sicherheit. Der Modifizierungsparameter kann beispielsweise dadurch einbezogen werden, dass er vor der Verschlüsselung logisch mit dem Anfrageparameter verknüpft wird. Selbstverständlich ist es auch möglich, den Modifizierungsparameter mit einem Zwischenergebnis im Ablauf des Verfahrens zu verknüpfen oder den Modifizierungsparameter mehrfach innerhalb des Verfahrensablaufs zu verwenden.

Zur weiteren Erhöhung der Sicherheit wird der Anfrageparameter in mindestens zwei Anteile zerlegt und die Anteile in unterschiedlichen Verfahrensschritten bei der Berechnung verwendet. Hierdurch wird eine zusätzliche Durchmischung des Anfrageparameters erreicht.

In einer bevorzugten Ausführungsvariante des Verfahrens wird bei der Berechnung des Authentisierungsantwortparameters ein Ausgangs- oder Zwischenergebnis zur Berechnung des Nachrichtencodierungsschlüssels verwendet. Auf diese Weise wird der Gesamtalgorithmus zur Erzeugung des

Verschlüsselungsergebnisses ohne zusätzlichen Aufwand ~~komplizierter und somit~~ sicherer.

Ein erfindungsgemäßes Authentisierungsverfahren für ein Netzwerk weist folgende Verfahrensschritte auf. Es wird zunächst ein Anfrageparameter, vorzugsweise eine Zufallszahl (im Folgenden wird ohne Einschränkung der Erfindung wieder von einer Zufallszahl als Anfrageparameter ausgegangen), generiert. Dies kann entweder in einer Authentisierungszentrale oder auch in einem separaten Zufallsgenerator geschehen. Diese Zufallszahl wird dann über das Netzwerk an eine Teilnehmeridentifizierungseinheit eines Endgeräts des Benutzers übermittelt. In der Teilnehmeridentifizierungseinheit wird dann mit dem zuvor erläuterten erfindungsgemäßen Verfahren der Authentisierungsantwortparameter und ggf. der Nachrichtencodierungsschlüssel erzeugt. Dieser Authentisierungsantwortparameter wird an das Netzwerk zurückübermittelt und dort mit dem von der Authentisierungszentrale unter Verwendung desselben Authentisierungsschlüssels parallel ermittelten Authentisierungsantwortparameter verglichen. Bei Übereinstimmung der beiden Parameter gilt der Teilnehmer bzw. die entsprechende Teilnehmeridentifizierungseinheit als identifiziert.

Eine erfindungsgemäße Teilnehmeridentifizierungseinheit muss zunächst Speichermittel aufweisen, in denen ein der jeweiligen Teilnehmeridentifizierungseinheit zugeordneter individueller Authentisierungsschlüssel und ein dem Dienstanbieter zugeordneter Modifizierungsparameter gespeichert sind. Bei den Speichermitteln kann es sich um völlig separate Speicher, aber auch um Speicherbereiche innerhalb eines Gesamtspeichers handeln. Es handelt sich sinnvollerweise hierbei um einen nichtflüchtigen Speicher.

Des Weiteren muss die Teilnehmeridentifizierungseinheit Mittel zur Erzeugung eines Authentisierungsantwortparameters aus einer Zufallszahl nach dem erfindungsgemäßen Verfahren aufweisen. Hierbei kann es sich um eine spezielle Hardware-Schaltung handeln, welche beispielsweise direkt binär den Algorithmus ausführt. Ein solch spezieller hardwaremäßiger Aufbau der Schaltung ist zwar aufwendig aber dafür sehr leistungsfähig, was die Rechengeschwindigkeit betrifft. Im einfacheren Fall kann es sich um eine CPU handeln, beispielsweise in einem Microcontroller, in welchem das Verfahren softwaremäßig in Form eines Computerprogramms mit geeigneten Programmcode-Mitteln implementiert ist. Insbesondere kann es sich bei einer solchen Teilnehmeridentifizierungseinheit um eine Chipkarte, zum Beispiel im Fall des GSM-Systems um eine SIM-Card handeln.

Es versteht sich von selbst, dass, wenn die jeweilige Teilnehmeridentifizierungseinheit zur Nutzung von Diensten verschiedener Dienstanbieter berechtigt, entsprechend mehrere Modifizierungsparameter gespeichert sind. Hierdurch zeigt sich ein weiterer Vorteil der Erfindung, da zur Nutzung einer Teilnehmeridentifizierungseinheit für verschiedene Dienstanbieter nicht zwangsläufig mehrere komplette Algorithmen in der Teilnehmeridentifizierungseinheit implementiert werden müssen, sondern lediglich ein Grundalgorithmus, der durch die gespeicherten Modifizierungsparameter dienstanbieterspezifisch individualisiert wird. Insbesondere bei der Verwendung von Chipkarten als Teilnehmeridentifizierungseinheiten ist dies wegen der beschränkten Kapazität der Chips von großem Vorteil.

Eine erfindungsgemäße Authentisierungszentrale in einem Netzwerk muss dementsprechend Speichermittel mit einer Datenbasis aus verschiedenen, den einzelnen Teilnehmeridentifizierungseinheiten zugeordneten Authenti-

sierungsschlüsseln und mit einem dem jeweiligen Dienstanbieter zugeordneten Modifizierungsparameter aufweisen. Darüber hinaus benötigt auch diese Authentisierungszentrale Mittel zur Erzeugung eines Authentisierungsantwortparameters aus einer Zufallszahl nach dem erfindungsgemäßen Verfahren. Auch hier ist eine Realisierung des Verfahrens wahlweise durch Aufbau einer speziellen Schaltung oder durch einen Computer mit einem geeigneten Software-Programm möglich.

Bei einem Mobilfunknetz handelt es sich bei der Authentisierungszentrale um die übliche AUC.

Bei anderen Netzwerken, beispielsweise im Internet, kann es sich um eine unabhängige Authentisierungszentrale handeln, welche als Dienstleister für verschiedene Dienstanbieter die Authentisierung übernimmt und entsprechende, besonders gesicherte Zonen zur Speicherung der verschiedenen Schlüssel aufweist. Im Prinzip ist es aber auch möglich, dass einzelne Dienstanbieter ihre eigene Authentisierungszentrale besitzen, die jeweils über das Internet mit einer am Endgerät des Teilnehmers befindlichen Teilnehmeridentifizierungseinheit kommuniziert. Auch in einem solchen Fall bietet es sich an, die Teilnehmeridentifizierungseinheit beispielsweise innerhalb einer Chipkarte anzuordnen und dementsprechend am Endgerät, beispielsweise einem PC, ein Chipkarten-Lesegerät zu integrieren, mit dem auf die Teilnehmeridentifizierungseinheit zugegriffen wird.

Wie bereits anfangs erwähnt, ist die Authentisierung in Mobilfunknetzen ein Haupteinsatzgebiet des erfindungsgemäßen Verfahrens. Ein weiteres Einsatzgebiet ist die Authentisierung gegenüber bestimmten Dienstanbietern im Internet. Ebenso kommt selbstverständlich eine Authentisierung mit die-

sem Verfahren in anderen Netzwerken, beispielsweise in Netzwerken von Geldautomaten oder anderen Systemen, wie Zugangskontrollsystemen oder dergleichen, in Frage.

Die Erfindung wird im Folgenden unter Hinweis auf die beigefügten Zeichnungen anhand von verschiedenen Ausführungsbeispielen näher erläutert. Die dort dargestellten Merkmale und auch die bereits oben beschriebenen Merkmale können nicht nur in den genannten Kombinationen, sondern auch einzeln oder in anderen Kombinationen erfindungswesentlich sein. Es zeigen:

Fig. 1 eine schematische Darstellung des Ablaufs des erfindungsgemässen Verfahrens gemäß einem ersten Ausführungsbeispiel;

Fig. 2 eine schematische Darstellung des Ablaufs des erfindungsgemäßen Verfahrens gemäß einem zweiten Ausführungsbeispiel;

Fig. 3 eine schematische Darstellung des Ablaufs des erfindungsgemäßen Verfahrens gemäß einem dritten Ausführungsbeispiel.

In den in den Figuren dargestellten Ausführungsbeispielen wird der Einfachheit halber wieder von einer Verwendung des erfindungsgemäßen Verfahrens zur Authentisierung in einem Mobilfunknetz ausgegangen.

In Figur 1 ist eine relativ einfache Version des erfindungsgemäßen Verfahrens dargestellt. Hierbei wird die Zufallszahl RAND zunächst mit dem Modifizierungsparameter AM (Algorithm Modifier) verknüpft. Bei dieser Verknüpfung handelt es sich im vorliegenden Fall um eine XOR (exclusive OR)

-Verknüpfung. Es kann aber auch eine andere beliebige logische Verknüpfung gewählt werden.

Eine solche XOR-Verknüpfung entspricht einer bitweisen Addition der beiden Binärzahlen, wobei die Kombinationen 1 + 1 sowie 0 + 0 jeweils 0 ergeben und ausschließlich die Kombination 1 + 0 sowie 0 + 1 jeweils 1 ergeben. Dies hat zur Folge, dass eine XOR-Verknüpfung einer beliebigen Bitfolge mit einer Bitfolge aus lauter Nullen die Bitfolge nicht verändert. Ein Modifizierungsparameter 000...0 ändert daher den Grundalgorithmus nicht. Indem der Modifizierungsparameter AM auf Wunsch der Dienstanbieter von 000...0 auf für jeden Dienstanbieter definierte unterschiedliche Bitfolgen gesetzt wird, können die Daten für jedes Dienstanbieternetz unter Beibehaltung des selben Grundalgorithmus individuell verschlüsselt werden.

Der Modifizierungsparameter AM hat die gleiche Bitlänge wie die Zufallszahl RAND. Im GSM-System hat folglich der Modifizierungsparameter AM in dem Ausführungsbeispiel gemäß Figur 1, genau wie die Zufallszahl RAND, die Länge von 128 Bit.

Das Verknüpfungsergebnis wird dann mittels des Triple-DES-Verschlüsselungsverfahrens unter Verwendung des individuellen Authentisierungsschlüssels Ki der Teilnehmeridentifizierungseinheit verschlüsselt. Bei dem einfachen DES-Verfahren handelt es sich um ein im Chipkartenbereich relativ häufig benutztes, sogenanntes symmetrisches Verschlüsselungsverfahren (Das heißt, es wird der gleiche Schlüssel für die Ver- und Entschlüsselung verwendet). Die Schlüssellänge beträgt in der Regel 64 Bit, wobei im DES-Verfahren allerdings üblicherweise jedes achte Bit ein Paritätsbit ist, welches lediglich zur Kontrolle der übrigen Bits im Schlüssel dient

und daher nicht signifikant für das Ergebnis ist. Bei der Verwendung eines 128-Bit-Schlüssels Ki, welcher keine Paritätsbits enthält (zum Beispiel Schlüssel im GSM-System) wird bei der vorgesehenen Verschlüsselung jedes achte Bit einfach ignoriert. Das DES-Verschlüsselungsverfahren gilt als äußerst sicher. Der einzige bisher erfolgversprechende Angriff gegen ein solches System ist eine sehr aufwendige Suche nach dem Schlüssel durch Ausprobieren, wobei eine enorme Rechenkapazität erforderlich ist.

Zur Verhinderung eines solchen direkten Angriffs wird daher das Triple-DES-Verfahren verwendet, bei dem drei DES-Operationen mit abwechselnder Ver- und Entschlüsselung hintereinander geschaltet werden. Das heißt, es wird zunächst ein Klartext, im vorliegenden Fall das Verknüpfungsergebnis der Zufallszahl RAND und des Modifizierungsparameters AM in einem DES-Verfahren mit einem ersten Schlüssel verschlüsselt, dann mit einem zweiten Schlüssel wieder in einem DES-Verfahren entschlüsselt und schließlich wieder erneut verschlüsselt, wobei im vorliegenden Fall für die zweite Verschlüsselung wiederum der gleiche Schlüssel verwendet wird, wie bei der ersten Verschlüsselung. Selbstverständlich können auch drei unterschiedliche Schlüssel verwendet werden. Im vorliegenden Fall besteht der Authentisierungsschlüssel Ki aus 128 Bit, wobei die 64 höherwertigen Bits (most significant bits; msb) einen ersten Schlüssel K1 bilden, welcher für die Verschlüsselung innerhalb des Triple-DES-Verfahrens verwendet wird, und die niederwertigeren 64 Bit (least significant bits; lsb) von Ki den zweiten Schlüssel K2 bilden, welcher für die Entschlüsselung innerhalb des Triple-DES-Verfahrens verwendet wird.

Mathematisch lässt sich dies durch die Schreibweise

$$3\text{-}DES_{Ki}(C) = DES_{KI}(DES^{-1}{}_{K2}(DES_{KI}(C)))$$

darstellen, wobei $DES_{KI}(C)$ die einfache DES-Verschlüsselung eines 64 bit-Klartextes C mit dem Schlüssel K1 und $DES^{-1}{}_{K2}(C)$ eine entsprechende Entschlüsselung mit dem Schlüssel K2 bedeutet.

Auf die weiteren genauen Einzelheiten des DES-Verfahrens bzw. des Triple-DES-Verfahrens soll hier nicht eingegangen werden. Es handelt sich hierbei zwar um die bevorzugte Form des Verschlüsselungsverfahrens innerhalb des erfindungsgemäßen Verfahrens. Es kann aber auch ein beliebiges anderes geeignetes Verschlüsselungsverfahren anstelle des Triple-DES-Verfahrens verwendet werden.

Das auf diese Weise verschlüsselte Verknüpfungsergebnis der Zufallszahl RAND und des Modifizierungsparameters AM wird in Figur 1 als OUT_{SRES} bezeichnet. Dieses Ergebnis OUT_{SRES} hat die gleiche Bitlänge wie die Eingangsparameter, d.h. im vorliegenden Ausführungsbeispiel 128 Bit. Im GSM-Standard weist der Authentisierungsantwortparameter SRES jedoch lediglich eine Bitlänge von 32 Bit auf. Daher werden von dem Verschlüsselungsergebnis OUT_{SRES} lediglich die niederwertigen 32 Bit als Authentisierungsantwortparameter SRES verwendet. Im Falle von 128 Bit-Eingangsparametern wird der DES im sogenannten CBC-Mode (cipher block chaining) betrieben. Wenn die Eingangsparameter lediglich eine Länge von 64 Bit aufweisen, im nicht verketteten DES-Modus gearbeitet.

In dem in Figur 2 dargestellten Ausführungsbeispiel wird ein etwas komplizierteres Verfahren verwendet. Hierbei wird die Zufallszahl RAND zunächst in einen höherwertigen Anteil R_1 und einen niederwertigeren Anteil

R_2 gleicher Bitlänge zerlegt. Das heißt, die Anteile R_1 und R_2 sind bei einer Verwendung des Verfahrens nach der GSM-Norm jeweils 64 Bit lang. Dementsprechend hat auch der Modifizierungsparameter AM eine Länge von 64 Bit. Auch bei diesem Verfahren erfolgt, wie bei dem Verfahren gemäß Figur 1, zunächst eine logische XOR-Verknüpfung der Zufallszahl RAND und des Modifizierungsparameters AM.

Auch in diesem zweiten Ausführungsbeispiel erfolgt dann eine Verschlüsselung des Verknüpfungsergebnisses mit einem Triple-DES-Verfahren unter Verwendung des Authentisierungsschlüssels Ki der Teilnehmeridentifizierungseinheit. Das hieraus gewonnene Verschlüsselungsergebnis T_1, welches wiederum eine Länge von 64 Bit aufweist, wird zunächst in einem weiteren Verfahrensschritt mit dem höherwertigen Anteil R1 der Zufallszahl RAND verknüpft und dieses Verknüpfungsergebnis wird erneut unter Verwendung des Authentisierungsschlüssels Ki mit einem Triple-DES-Verfahren verschlüsselt. Erst aus diesem doppelt verschlüsselten Verfahren, bei welchem die Zufallszahl RAND durcheinandergemischt worden ist, wird schließlich der Authentisierungsantwortparameter SRES gewonnen. Wie im ersten Ausführungsbeispiel werden auch hier vom letzten Verschlüsselungsergebnis OUT_{SRES}, in Figur 2 auch T_2 genannt, lediglich die niederwertigsten 32 Bit als Authentisierungsantwortparameter SRES verwendet.

Figur 3 zeigt eine weitere Ausgestaltung des Verfahrens gemäß Figur 2, bei dem gleichzeitig ein Nachrichtencodierungsschlüssel Kc aus der Zufallszahl RAND erzeugt wird. Hierzu wird das gemäß dem Verfahren in Figur 2 gewonnene Verschlüsselungsergebnis T_2 erneut mittels einer XOR-Operation mit dem niederwertigen Anteil R_2 der Zufallszahl RAND verknüpft. Dieses Verknüpfungsergebnis wird dann erneut mittels des Authentisierungs-

schlüssels Ki mit einem Triple-DES-Verfahren verschlüsselt. Aus dem Verschlüsselungsergebnis Out_{KC} wird dann der Nachrichtencodierungsschlüssel Kc gewonnen.

In dem dargestellten Ausführungsbeispiel sind zwei verschiedene Möglichkeiten angedeutet. Entweder besteht der Nachrichtencodierungsschlüssel Kc aus den 54 höherwertigen Bits des Verschlüsselungsergebnisses Out_{KC} und die zehn niederwertigsten Bits des Nachrichtencodierungsschlüssel Kc werden auf 0 gesetzt, oder es wird das gesamte Verschlüsselungsergebnis Out_{KC} unverändert als Nachrichtencodierungsschlüssel Kc verwendet.

In einer Ausführungsform des Verfahrens ist konkret vorgesehen, dass lediglich ein sogenanntes „Flag-Bit" als Indikator gesetzt wird (nicht dargestellt) und vor Ausgabe des Nachrichtencodierungsschlüssels Kc automatisch dieses Flag-Bit abgefragt wird. Ist das Flag-Bit gleich 0, werden automatisch die letzten Bits von Out_{KC} gleich 0 gesetzt, ist das Flag-Bit dagegen 1, bleibt Out_{KC} unverändert.

Selbstverständlich ist es ebenso möglich, die letzten zehn Bits definiert auf 1 zu setzen oder auch eine längere oder kürzere Anzahl von Endbits auf einen bestimmten vorgegebenen Wert zu setzen. Die genauen Spezifikationen hängen von den Erfordernissen des Dienstanbieters ab bzw. hängen davon ab, ob innerhalb des Informationsverschlüsselungsverfahrens zwischen Endgerät und Netzwerk bzw. Dienstanbieter ein Schlüssel mit einer bekannten Anzahl an sogenannten Tail-Bits benötigt wird. Einige Verschlüsselungsverfahren benötigen bekannte Tail-Bits, um am Ende eines Blocks bzw. vor Beginn eines neuen Blocks den Codierer in einen bekannten Zustand zu setzen.

Das in Figur 3 dargestellte Verfahren verknüpft daher, in der Notation der GSM-Norm, auf günstige Weise den A3-Algorithmus für die Erzeugung des Authentisierungsanwortparameters SRES mit dem A8-Algorithmus für die Erzeugung des Nachrichtencodierungsschlüssels Kc, sodass der A8-Algorithmus sicher aufgebaut ist, andererseits aber ein Großteil des Rechenaufwands ohnehin bereits für den A3-Algorithmus genutzt wurde, und somit anders als bei vollständig getrennten parallelen Algorithmen, der Berechnungsaufwand gering ist.

Aus Gründen der Übersichtlichkeit werden im Folgenden noch einmal alle verwendeten Abkürzungen sowie die in den Figuren genutzten Bezugszeichen aufgelistet:

RAND	Zufallszahl (random number)
R_1	höherwertiger Anteil von RAND
R_2	niederwertiger Anteil von RAND
AM	Modifizierungsparameter (Algorithm Modifier)
Ki	Authentisierungsschlüssel (authentication Key)
T_1	erstes Verschlüsselungsergebnis
T_2	zweites Verschlüsselungsergebnis
SRES	Authentisierungsantwortparameter (Signed Response)
Kc	Nachrichtencodierungsschlüssel (ciphering Key)
Out_{SRES}	Verschlüsselungsendergebnis
Out_{KC}	Verschlüsselungsendergebnis
DES	Data Encryption Standard (Verschlüsselungsverfahren)
KI	höherwertiger Anteil von Ki
K2	niederwertiger Anteil von Ki
XOR	„exclusive OR"-Verknüpfung
msb	höherwertigstes Bit (most significant bit)
lsb	niederwertigstes Bit (least significant bit)
GSM	Global System for Mobile Communications
SIM	Subscriber Identity Module (Teilnehmeridentifizierungseinheit im GSM-System)
BSS	Base Station System
MSC	Mobile Switching Center
AUC	Authentication Center (Authentisierungszentrale im GSM-System)

Patentansprüche:

1. Verfahren zur Erzeugung eines Authentisierungsantwortparameters (SRES) zur Authentisierung einer Teilnehmeridentifizierungseinheit in einem Netzwerk bei einem Dienstanbieter, bei dem der Authentisierungsantwortparameter (SRES) unter Verwendung eines der Teilnehmeridentifizierungseinheit zugeordneten individuellen Authentisierungsschlüssels (Ki) aus einem Anfrageparameter (RAND) berechnet wird, dadurch **gekennzeichnet**, dass in mindestens einem Verfahrensschritt bei der Berechnung ein dem Dienstanbieter zugeordneter Modifizierungsparameter (AM) verwendet wird.

2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, dass der Anfrageparameter (RAND) in mindestens zwei Anteile (R_1, R_2) zerlegt wird, und die Anteile (R_1, R_2) in unterschiedlichen Verfahrensschritten bei der Berechnung verwendet werden.

3. Verfahren nach Anspruch 2, **gekennzeichnet** durch folgende Schritte:

- Zerlegung des Anfrageparameters (RAND) in einen höherwertigen Anteil (R_1) und einen niederwertigen Anteil (R_2) gleicher Bitlänge,

- in einem ersten Verknüpfungsschritt, Verknüpfung des niederwertigen Anteils (R_2) des Anfrageparameters (RAND) mit dem Modifizierungsparameter (AM),

- Verschlüsselung eines Verknüpfungsergebnisses des ersten Verknüpfungsschritts unter Verwendung des Authentisierungsschlüssels (Kl) zu einem ersten Verschlüsselungsergebnis (T_1),

- in einem zweiten Verknüpfungsschritt, Verknüpfung des ersten Verschlüsselungsergebnis (T_1) mit dem höherwertigen Anteil (R_1) des Anfrageparameters (RAND),

- Verschlüsselung eines Verknüpfungsergebnisses des zweiten Verknüpfungsschritts vorhergehenden Schritts unter Verwendung des Authentisierungsschlüssels (Ki) zu einem zweiten Verschlüsselungsergebnis (T_2), und

- Ermittlung des Authentisierungsantwortparameters (SRES) aus dem zweiten Verschlüsselungsergebnis (T_2).

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch **gekennzeichnet**, daß die Verschlüsselung mindestens eines Verknüpfungsergebnisses in einem Triple-DES-Verfahren erfolgt.

5. Verfahren nach Anspruch 3 oder 4, dadurch **gekennzeichnet**, dass das zweite Verschlüsselungsergebnis (T_2) mit dem niederwertigen Anteil (R_2) des Anfrageparameters (RAND) verknüpft wird und ein dabei erhaltenes Verknüpfungsergebnis unter Verwendung des Authentisierungsschlüssels (Ki) verschlüsselt wird und aus einem daraus erhaltenen dritten Verschlüsselungsergebnis (Out_{KC}) ein Nachrichtencodierungsschlüssel (Kc) gewonnen wird.

6. Authentisierungsverfahren für ein Netzwerk mit folgenden Verfahrensschritten:

- Generierung eines Anfrageparameters (RAND),

- Übermittlung dieses Anfrageparameters (RAND) vom Netzwerk an eine Teilnehmeridentifizierungseinheit eines Endgeräts,

- Erzeugung eines Authentisierungsantwortparameters (SRES) aus dem Anfrageparameter (RAND) unter Verwendung eines Authentisierungsschlüssels (Ki) der Teilnehmeridentifizierungseinheit,

- Übermittlung des Authentisierungsantwortparameters (SRES) von der Teilnehmeridentifizierungseinheit an das Netzwerk, und

- Vergleich des von der Teilnehmeridentifizierungseinheit erhaltenen Authentisierungsantwortparameters (SRES) mit einem von einer Authentisierungszentrale unter Verwendung des Authentisierungsschlüssels (Ki) aus dem Anfrageparameter (RAND) ermittelten Authentisierungsantwortparameters (SRES), dadurch **gekennzeichnet**, dass der Authentisierungsantwortparameter (SRES) mittels eines Verfahrens gemäß einem der Ansprüche 1 bis 4 aus dem Anfrageparameter (RAND) erzeugt wird.

7. Authentisierungsverfahren nach Anspruch 6, dadurch **gekennzeichnet**, dass von der Teilnehmeridentifizierungseinheit und von der Authentisierungszentrale nach einem Verfahren gemäß Anspruch 5 ein Nachrich-

tencodierungsschlüssel (Kc) erzeugt wird, welcher zur Verschlüsselung von zu übermittelnden Daten zwischen Endgerät und Netzwerk dient.

8. Teilnehmeridentifizierungseinheit mit Speichermitteln, in denen ein der Teilnehmeridentifizierungseinheit zugeordneter individueller Authentisierungsschlüssel (Ki) und ein einem Dienstanbieter zugeordneter Modifizierungsparameter (AM) gespeichert sind, und mit Mitteln zur Erzeugung eines Authentisierungsantwortparameter (SRES) aus einem Anfrageparameter (RAND) nach einem Verfahren gemäß einem der Ansprüche 1 bis 4.

9. Teilnehmeridentifizierungseinheit nach Anspruch 8, **gekennzeichnet** durch Mittel zur Erzeugung eines Nachrichtencodierungsschlüssels (Kc) nach einem Verfahren gemäß Anspruch 5.

10. Authentisierungszentrale für ein Netzwerk mit Speichermitteln, in denen einzelnen Teilnehmeridentifizierungseinheiten zugeordnete, individuelle Authentisierungsschlüssel (Ki) und ein einem Dienstanbieter zugeordneter Modifizierungsparameter (AM) gespeichert sind, und mit Mitteln zur Erzeugung eines Authentisierungsantwortparameters (SRES) aus einem Anfrageparameter (RAND) nach einem Verfahren gemäß einem der Ansprüche 1 bis 4.

11. Authentisierungszentrale nach Anspruch 9, **gekennzeichnet** durch Mittel zur Erzeugung eines Nachrichtencodierungsschlüssels (Kc) nach einem Verfahren gemäß Anspruch 5.

12. Computerprogramm mit Programmcode-Mitteln, um alle Schritte gemäß einem der Ansprüche 1 bis 5 durchzuführen, wenn das Programm auf einem Computer ausgeführt wird.

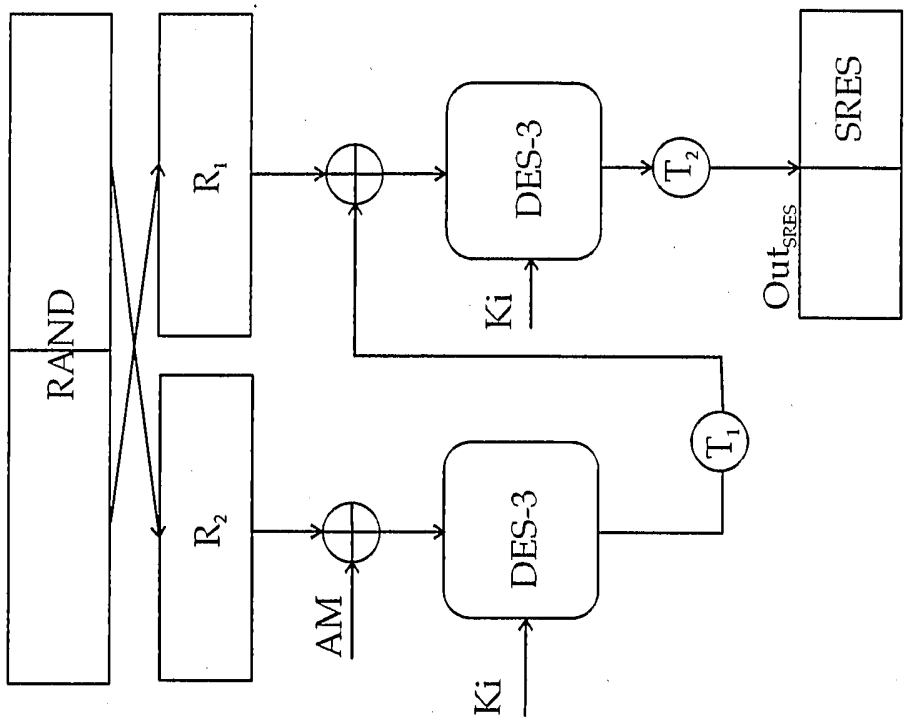
RAND
R1
R2
AM
Ki
DES-3
DES-3
T1
T2
Ki
Out SRES
SRES

Fig. 2

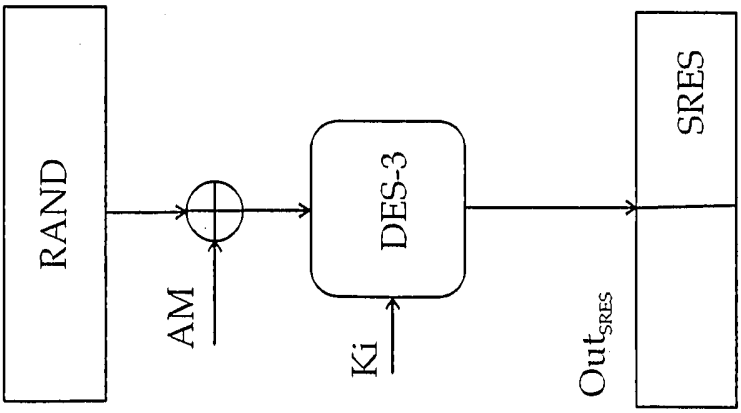
RAND
AM
Ki
DES-3
Out SRES
SRES

Fig. 1

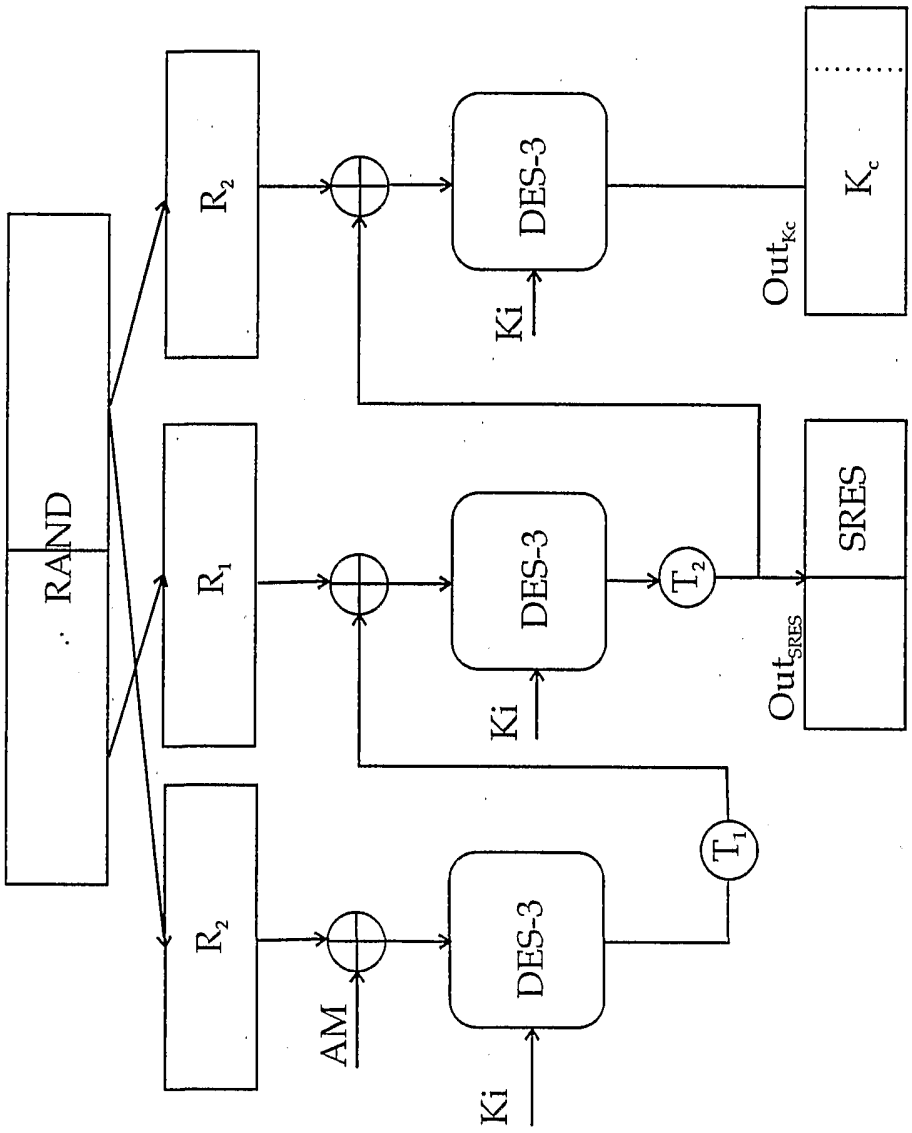
RAND
R2
R1
R2
AM
Ki
DES-3
Ki
DES-3
T2
T1
Ki
DES-3
Out_SRES
SRES
Out_Kc
Kc

Fig. 3