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

(10) **DE 697 27 641 T2** 2004.12.23

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 0 841 770 B1**
(21) Deutsches Aktenzeichen: **697 27 641.4**
(96) Europäisches Aktenzeichen: **97 308 890.9**
(96) Europäischer Anmeldetag: **04.11.1997**
(97) Erstveröffentlichung durch das EPA: **13.05.1998**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **18.02.2004**
(47) Veröffentlichungstag im Patentblatt: **23.12.2004**

(51) Int Cl.[7]: **H04L 9/30**
H04L 9/32

(30) Unionspriorität:
744682 **06.11.1996** **US**

(84) Benannte Vertragsstaaten:
DE, FR, GB, SE

(73) Patentinhaber:
Nokia Corp., Espoo, FI

(72) Erfinder:
Luo, Tie, Arlington, US

(74) Vertreter:
Becker, Kurig, Straus, 80336 München

(54) Bezeichnung: **Verfahren zum Senden einer sicheren Botschaft in einem Telekommunikationssystem**

Beschreibung

[0001] Diese Erfindung betrifft Verschlüsselungstechniken für Telekommunikationssysteme, und insbesondere eine Vorrichtung und ein Verfahren zum Senden einer sicheren Nachricht in einem Telekommunikationssystem unter Verwendung von öffentlichen Verschlüsselungsschlüsseln (public keys).

[0002] Die Fortschritte in der Technologie von Telekommunikationssystemen haben zu einer Vielfalt von Telekommunikationssystemen und Diensten geführt, die für die Benutzung verfügbar sind. Diese Systeme schließen Mobilfunktelefonnetzwerke, persönliche Kommunikationssysteme, verschiedene Funkrufempfänger-Systeme und verschiedene drahtgebundene und drahtlose Datennetzwerke ein. Mobilfunktelefonnetzwerke, die in den Vereinigten Staaten derzeit in Verwendung sind, beinhalten das AMPS Analogsystem, das digitale IS-136 Zeitvielfachzugriffs(TDMA)-System und das digitale IS-95 Digital-Codevielfachzugriffs(CDMA)-System ein. In Europa wird das digitale Globale System für mobile Kommunikation (GSM) am häufigsten verwendet. Diese Mobilfunksysteme arbeiten im Bereich von 800–900 MHz. Persönliche Kommunikationssysteme (PCS) werden in den Vereinigten Staaten derzeit ebenfalls entwickelt. Viele PCS-Systeme werden für den Bereich von 1800–1900 MHz entwickelt, wobei jedes auf einem der Haupt-Mobilfunkstandards basiert.

[0003] In jedem der vorstehend genannten Telekommunikationssysteme kann es häufig für die Betreiber des Systems wünschenswert sein, den Benutzern des Systems sichere Kommunikationen bereitzustellen. Dies kann das Senden einer sicheren Nachricht zwischen zwei Mobilstationen einschließen, die in dem System betrieben werden. In vielen Fällen kann die Nachricht eine Textnachricht von endlicher Länge sein, so wie eine Textnachricht.

[0004] In analogen Systemen, so wie AMPS, ist es sehr schwierig, Sicherheit für Kommunikationen bereitzustellen. Die analoge Natur des Signals, das die Kommunikation zwischen zwei Benutzern trägt, erlaubt keine einfache oder wirksame Verschlüsselung. Tatsächlich wird in Standard-AMPS keine Verschlüsselung verwendet und Kommunikationen, die zwischen einer Mobilstation und einer Basisstation gesendet werden, können überwacht und abgefangen werden. Jeder, der einen Empfänger besitzt, der auf die Frequenzen eingestellt werden kann, die für die Kommunikationskanäle verwendet werden, kann eine Nachricht zu jeder Zeit abfangen, ohne erfasst zu werden. Die Möglichkeit des Abfangens ist ein negativer Faktor gewesen, der mit analogen Systemen so wie AMPS verbunden ist. Aufgrund dieses Potenzials zum Abfangen sind Systeme vom AMPS-Typ für bestimmte Geschäfts- oder Regierungsverwendungen nicht beliebt gewesen, in denen das Senden einer sicheren Nachricht eine Notwendigkeit ist.

[0005] Die neueren digitalen Systeme so wie GSM, IS-136 und IS-95 sind so entwickelt worden, um Verschlüsselungsdienste für die Kommunikations-Privatsphäre zu beinhalten. Die digitale Natur der Sprach- oder Datensignale, die die Kommunikationen zwischen zwei Benutzern in diesen digitalen Systemen tragen, gestattet es, die Signale durch eine Verschlüsselungsvorrichtung zu bearbeiten, um ein Kommunikationssignal zu erzeugen, das zufällig oder pseudo-zufällig in seiner Art erscheint, bis es bei einem autorisierten Empfänger entschlüsselt wird. Wenn es gewünscht wird, eine sichere Nachricht in einem solchen System zu senden, kann das Verschlüsselungsmerkmal des Systems verwendet werden, um die Nachricht zu verschlüsseln. Als ein Beispiel könnte das Kurznachrichten-Merkmal (SMS), das in diesen Standards spezifiziert ist, verwendet werden, um eine Textnachricht zu senden, die gemäß dem Verschlüsselungs-Algorithmus des Systems verschlüsselt ist.

[0006] In dem GSM-, IS-136- und IS-95-System wird die Verschlüsselung bei Nachrichtenübermittlungen zwischen jedem Benutzer und dem System ausgeführt, indem ein geheimer Schlüsselwert, "privater bzw. geheimer Schlüssel", verwendet wird, wobei der Schlüssel nur dem System und dem Benutzer bekannt ist, der mit dem System kommuniziert. Die Systemstandards, die für PCS-Netzwerke in Betracht gezogen werden, können ebenfalls Verschlüsselungsdienste einschließen, die auf den Verschlüsselungstechniken basieren, die in dem digitalen Standard spezifiziert sind, von dem ein jeweiliger PCS-Standard abgeleitet ist, d. h. GSM, IS-136 und IS-95.

[0007] Bei GSM steuert der Systembetreiber den Sicherheitsvorgang durch Ausgeben eines Subscriber-Identitätsmoduls (SIM) an jeden Systembenutzer. Das SIM ist ein Einsteck-Chip oder eine Karte, der bzw. die in eine Mobilstation eingesetzt werden muss, mit der ein Benutzer beabsichtigt, Anrufe zu tätigen oder zu empfangen. Das SIM enthält eine 128-Bit Zahl, genannt die Ki, die für jeden Benutzer eindeutig ist. Die Ki wird sowohl für eine Authentifizierung als auch zum Ableiten eines Verschlüsselungsschlüssels verwendet. Bei GSM wird ein Authentifizierungsanfrage- und -Antwort-Vorgang verwendet, um jeden Benutzer zu authentifizieren und aus Ki Verschlüsselungsbits für den Benutzer zu erzeugen. Der Frage- und Antwort-Vorgang kann unter der Diskretion bzw. nach Belieben des Heimatsystems ausgeführt werden.

[0008] Wenn ein GSM-Mobilteil in seinem Heimatsystem betrieben wird, wird, nachdem der Benutzer sich identifiziert hat, indem er seine internationale Mobilsystemidentität/temporäre Mobilsystemidentitäten (IMSI/TMSI) eingesandt hat, eine 128-Bit Zufalls-

zahl (RAND) in dem System erzeugt, und mit der Ki des Mobilteils des Benutzers kombiniert, um eine 32-Bit Antwort (SRES) zu erzeugen. Das System überträgt dann die RAND an das Mobilteil, welches wiederum seinen eigenen SRES-Wert aus der Ki des Mobilteils des Benutzers berechnet, und diese RAND zurück an das System überträgt. Wenn die zwei SRES-Werte übereinstimmen, wird bestimmt, dass das Mobilteil authentisch ist. Verschlüsselungsbits für Kommunikationen zwischen dem Mobilteil und den Systemen werden sowohl in dem Mobilteil als auch dem Netzwerk durch Algorithmen erzeugt, die die RAND und die Ki verwenden, um einen Verschlüsselungsschlüssel "Kc" zu erzeugen. Kc wird dann an beiden Enden verwendet, um sichere Kommunikationen bereitzustellen. Wenn ein GSM-Mobilteil Roaming ausführt, werden die RAND-, SRES- und Kc-Werte zu einem besuchten System übertragen, auf die Registrierung des Benutzers in dem besuchten System hin, oder auf eine spezifische Anfrage von einem besuchten System hin. Der Ki-Wert ist niemals anderweitig verfügbar als in dem Heimatsystem und dem SIM des Benutzers.

[0009] Die IS-136- und IS-95-Authentifizierungs- und Verschlüsselungs-Vorgänge sind mit einander identisch und den GSM-Authentifizierungs- und Verschlüsselungs-Vorgängen ähnlich. In IS-136- und IS-95-Systemen wird ebenso ein Frage-/Antwort-Verfahren verwendet. Das IS-136- und das IS-95-Verfahren verwenden einen Sicherheitsschlüssel, genannt der "A-Schlüssel". Der 64-Bit-A-Schlüssel für jedes Mobilteil wird durch die Systembetreiber bestimmt. Der A-Schlüssel für jedes Mobilteil wird in dem Heimatsystem des Mobilteil-Besitzers und in dem Mobilteil selbst gespeichert. Der A-Schlüssel kann dem Mobilteil-Besitzer anfänglich in einer sicheren Art und Weise übermittelt werden, so wie der Post der Vereinigten Staaten. Der Besitzer kann dann den A-Schlüssel über das Tastenfeld in das Mobilteil eingeben. Alternativ kann der A-Schlüssel in der Fabrik oder am Wartungsort in die Mobilstation programmiert werden. Der A-Schlüssel wird verwendet, um mit einem vorbestimmten Algorithmus geteilte geheime Daten (SSD) sowohl in dem Mobilteil als auch dem Heimatsystem zu erzeugen. Die SSD können für jedes Mobilteil periodisch von dem A-Schlüssel des jeweiligen Mobilteils abgeleitet und auf den neuesten Stand gebracht werden, durch die Verwendung eines Funkprotokolls, das nur durch den Heimatsystembetreiber initiiert werden kann.

[0010] Bei IS-136- und IS-95-Authentifizierung und -Verschlüsselung wird eine globale 32-Bit Authentifizierungsanfrage erzeugt und in vorbestimmten Intervallen innerhalb von Systemen in dem Dienstbereich des Mobilteils gesendet. Wenn ein Mobilteil einen Systemregistrierungs/Anrufeinstell-Zugriff in dem Heimatsystem versucht, wird die derzeitige globale Authentifizierungsantwort verwendet, um in dem Mobilteil eine 18-Bit Authentifizierungsantwort aus dem SSD des Mobilteils zu berechnen. Eine Zugriffsanforderungsnachricht, enthaltend die Authentifizierungsantwort und einen Anrufzählwert für das Mobilteil, wird dann von dem Mobilteil an das Heimatsystem gesendet. Wenn die Zugriffsanforderung empfangen worden ist, wird das Heimatsystem seinen eigenen Antworwert unter Verwendung der globalen Authentifizierungsanfrage und der SSD des Mobilteils berechnen. Wenn das Mobilteil als authentisch verifiziert worden ist, durch Vergleich der Authentifizierungsantworten, der SSD des Mobilteils und anderer relevanter Daten, einschließlich des Anrufzählwerts, wird das Mobilteil registriert.

[0011] Wenn ein Mobilteil einen Systemregistrierungs-/Anrufeinstell-Zugriff in einem besuchten System versucht, wird die globale Authentifizierungsanfrageantwort verwendet, um in dem Mobilteil die 18-Bit Authentifizierungsantwort aus dem SSD des Mobilteils zu berechnen. Eine Zugriffsanforderungsnachricht wird dann von dem Mobilteil zu dem besuchten System gesendet. Für anfängliche Registrierungszugriffe in einem besuchten System schließt die Zugriffsanforderungsnachricht die Authentifizierungsantwort ein, die in dem Mobilteil berechnet wird. Die Authentifizierungsantwort und globale Authentifizierungsanfrage werden dann zu dem Heimatsystem des Mobilteils gesendet, wo das Heimatsystem seinen eigenen Antwortwert berechnen wird, unter Verwendung der globalen Authentifizierungsanfrage und des SSD des Mobilteils. Wenn das Mobilteil als authentisch verifiziert worden ist, durch Vergleich der Authentifizierungsantworten, werden dann der SSD des Mobilteils und andere relevante Daten, einschließlich des Anrufzählwerts, zu dem besuchten System gesendet, und das Mobilteil wird registriert. Wenn ein das Mobilteil betreffender Anruf eingestellt wird, wird ein derzeitiger Authentifizierungsantwortwert und ein Anrufzählwert von dem Mobilteil zu dem System gesendet, zusammen mit der Anrufeinstellinformation. Wenn die Anrufeinstellinformation empfangen worden ist, beschafft das besuchte System den gespeicherten SSD und die Anrufzählwerte für das anfragende Mobilteil wieder. Das besuchte System berechnet dann einen Authentifizierungsantwortwert, um zu verifizieren, dass der empfangene SSD-Wert und die derzeitige globale Authentifizierungsanfrage die gleiche Antwort erzeugen wie die in dem Mobilteil erzeugte. Wenn die Authentifizierungsantworten und Anrufzählwerte übereinstimmen, wird dem Mobilteil ein Anrufzugriff gestattet. Wenn Kommunikationssicherheit gewünscht wird, wird ein Verschlüsselungsschlüssel sowohl in dem Mobilteil als auch dem System erzeugt, indem die globale Authentifizierungsanfrage und der SSD des Mobilteils als Eingabe verwendet werden, um Verschlüsselungsschlüssel-Bits zu erzeugen.

[0012] Weiterer Hintergrund für solche Techniken,

wie den beim GSM- und dem IS-136- und dem IS-95-System verwendeten, kann gefunden werden in dem Artikel "Techniques for Privacy and Authentication in Personal Communications Systems" von Dan Brown in IEEE Personal Communications, vom August 1995, auf den Seiten 6–10.

[0013] Obwohl die vorstehend beschriebenen Geheimschlüsselverfahren, die in den GSM-, IS-136- und IS-95-Systemen verwendet werden, Kommunikationssicherheit bereitstellen, ist keines dieser Verfahren vollständig immun gegenüber Abfangen und Abhören. Alle diese Verfahren erfordern, dass ein A-Schlüssel oder Ki-Wert eines Benutzers sowohl in der Mobilstation als auch dem Heimatsystem bekannt sind. Sie erfordern ebenso, dass der SSD- oder Kc-Wert des Benutzers an beiden Enden der Kommunikationsverbindung bekannt ist, d. h. in dem System und in dem Mobilteil. Jeder dieser Werte kann potenziell korrumpiert werden und einem potenziellen Abfänger bekannt werden. Ein Individuum, das den Ki- oder A-Schlüssel eines Benutzers kennt, oder ein Individuum, das den Kc oder SSD des Benutzers in Intersystem-Kommunikationen abfängt, könnte potenziell Kommunikationen abfangen und abhören, die beabsichtigt waren, sicher und geheim zu sein. Zusätzlich, da alle Schlüssel von Benutzern bei einer Basisstation, mit der sie kommunizieren, verfügbar sind, könnte in verschlüsselte Kommunikationen, die zwei Mobilstationen betreffen, die durch eine Basisstation eines Systems verbunden sind, an der Basisstation eingebrochen werden.

[0014] Öffentliche-Schlüssel-Verschlüsselungsverfahren sind Verfahren, in denen einem Benutzer ein Verschlüsselungsschlüssel zugewiesen wird, der öffentlich ist, d. h. bekannt sein und öffentlich offengelegt werden kann, aber ebenso ein geheimer Entschlüsselungsschlüssel zugewiesen wird, der nur dem Benutzer bekannt ist. Nur ein Entschlüsselungsschlüssel eines beabsichtigten empfangenden Benutzers kann eine verschlüsselte Nachricht entschlüsseln, die für den beabsichtigten empfangenden Benutzer vorgesehen ist, d. h. eine Nachricht, die unter Verwendung des Entschlüsselungsschlüssel des beabsichtigten empfangenden Benutzers verschlüsselt ist. In einem Öffentliche-Schlüssel-Verschlüsselungs-Telekommunikationssystem wäre es dem Benutzer gestattet, den Entschlüsselungsschlüssel für sich zu behalten, außerhalb der Basisstationen oder des Systems. Da der Schlüssel, der zum Entschlüsseln einer Nachricht notwendig ist, nur dem empfangenden Benutzer bekannt ist, können Öffentliche-Schlüssel-Verschlüsselungsverfahren sicherere Kommunikationen bereitstellen als sie mit den derzeitigen Verschlüsselungstechniken erhalten werden können, die zum Beispiel in GSM, IS-136 und IS-95 verwendet werden.

[0015] In einem Mobilfunksystem, das herkömmliche Öffentliche-Schlüssel-Verschlüsselung verwendet, ist es erforderlich, wenn eine Mobilstation X eine verschlüsselte Nachricht zur Mobilstation Y senden würde, dass die Mobilstation X sowohl den öffentlichen Verschlüsselungsschlüssel für die Mobilstation Y als auch den Algorithmus kennt, der mit dem Verschlüsselungsschlüssel der Mobilstation Y verwendet werden muss. Es wäre ebenso erforderlich, dass das Mobilteil X in der Lage ist, die Verschlüsselung der Nachricht unter Verwendung des Verschlüsselungsschlüssels und Algorithmus der Mobilstation Y auszuführen. Diese Erfordernisse herkömmlicher Öffentliche-Schlüssel-Verschlüsselung können einige Schwierigkeiten darstellen oder in bestimmten Situationen nicht gerade optimal für die Verwendung in Mobilfunksystemen sein.

[0016] Eine Schwierigkeit bei der Verwendung von Öffentliche-Schlüssel-Verschlüsselungstechniken ist, dass die Berechnungen, die bei der Verschlüsselung und Entschlüsselung beteiligt sind, im Sinne von Berechnungskapazitäten einiges mehr erfordern können, als es bei Geheime-Schlüssel(private keys)-Systemen erforderlich ist. In einer Mobilstation können solche Berechnungskapazitäten begrenzt sein. Die Erfordernisse an Kapazitäten können sogar noch größer sein, wenn zwei Mobilstations-Benutzer wünschen, eine Nachricht sicher auszutauschen, wobei jeder Benutzer einen anderen Verschlüsselungs-/Entschlüsselungsalgorithmus verwendet. Dies könnte zum Beispiel der Fall sein, wenn eine Roaming ausführende Mobilstation in ein System eintritt, in dem der Systembetreiber seinen eigenen einzigartigen Algorithmus implementiert hat, der von dem Algorithmus des Heimatsystems der Roaming ausführenden Mobilstation verschieden ist. In diesem Fall wäre es erforderlich, dass jede betreffende Mobilstation in der Lage wäre, eine Verschlüsselung mit dem Algorithmus des anderen Benutzers, und Entschlüsselung mit dem betreffenden Algorithmus der Mobilstation des Benutzers auszuführen. Eine solche Anforderung könnte zum Beispiel schwierig zu erfüllen sein, wenn der für die Verschlüsselung verwendete Algorithmus mehr Berechnungskapazitäten erfordern würde, als in der Mobilstation verfügbar sind, die die Verschlüsselung ausführt. Ebenso müssten der Kode und die Daten zum Ausführen betreffender Algorithmen in jeder Mobilstation gespeichert sein oder vor dem Beginn der Verschlüsselung zu der Mobilstation übertragen werden, was weitere Anforderungen an die Berechnungskapazitäten einer Mobilstation erzeugt.

[0017] Eine andere potenzielle Schwierigkeit bei der Verwendung von Öffentliche-Schlüssel-Verschlüsselungstechniken in einem Mobilfunksystem betrifft das Erfordernis, dass die sendende Mobilstation den Verschlüsselungsschlüssel der empfangenden Mobilstation kennen sollte, um sicherzustellen, dass die Nachricht nur für die sendende oder empfangende

Mobilstation verfügbar ist. In bestimmten Öffentliche-Schlüssel-Verschlüsselungstechniken können die Verschlüsselungsschlüssel jeder sehr groß bzw. lang sein, möglicherweise eine Abfolge von Zahlen, und es kann schwierig sein, die Verschlüsselungsschlüssel für alle potenziellen empfangenden Mobilstationen in einer einzigen Mobilstation zu speichern. Es kann ebenfalls schwierig sein, den Schlüssel einer empfangenden Mobilstation zu einer sendenden Mobilstation zu übertragen, auf einer "bei Bedarf" Basis, zum Beispiel während der Anrufeinstellung, wenn der Schlüssel sehr lang ist.

[0018] Eine Besprechung des Konzepts der Kommutivität in der Kryptographie wird gegeben in "On the Power of Commutivity in Cryptography" A. Shamir, Automata, Languages and programming, Siebzigstes Kolloquium Noordwijkerhout, Niederlande, 14–18 Juli 1980, 582–585. Dies offenbart, wie Zufallsschlüssel verwendet werden können, um eine Nachricht zu verschlüsseln, und sie dann zurückzugeben unter Verwendung von Funktionen, die Kommutivität und Inversibilität zeigen.

[0019] Die vorliegende Erfindung stellt ein Verfahren zum Senden einer sicheren Nachricht in einem Telekommunikationssystem bereit, unter Verwendung von Öffentliche-Schlüssel-Verschlüsselung. Das Verfahren ist in einer solchen Weise implementiert, dass ein bestimmter Verschlüsselungsschlüssel eines Benutzers nur der Transceivervorrichtung des bestimmten Benutzers bekannt ist. Das Verfahren ist ebenso implementiert, so dass die Transceivervorrichtung des bestimmten Benutzers nur in der Lage sein muss, den Verschlüsselungs-/Entschlüsselungsalgorithmus und Verschlüsselungsschlüssel zu verwenden. Dies wird erreicht, indem eine bestimmte Abfolge zum Austauschen von Nachrichten zwischen zwei Sende-/Empfangsvorrichtungen verwendet wird. Das Verfahren vermeidet Sicherheitsprobleme, die mit der Verwendung von Geheime-Schlüssel-Verfahren verbunden sind, und gestattet ebenso jeder Mobilstation, nur ihren eigenen Öffentliche-Schlüssel-Verschlüsselungs/-Entschlüsselungs-Algorithmus auszuführen. Das Verfahren erfordert nicht, dass eine Sende-/Empfangsvorrichtung in der Lage sein muss, Verschlüsselung unter Verwendung des Verschlüsselungsschlüssels und -Algorithmus einer beabsichtigten Empfänger-Sende-/Empfangsvorrichtung auszuführen, wie in herkömmlicher Öffentliche-Schlüssel-Verschlüsselung. Berechnungskapazitäten in einer Sende-/Empfangsvorrichtung können daher für einen bestimmten Algorithmus optimiert werden.

[0020] Das Verfahren der Erfindung ist in Anspruch 1 genauer ausgedrückt.

[0021] Das Verfahren kann nützlich sein, um hochsichere Kurznachrichten(SMS)-Teledienste bereitzustellen, wenn eine sichere Nachricht zwischen zwei Mobilstationen, oder einer Mobilstation und einem Mobilfunknetzwerk ausgetauscht wird, wobei jede Mobilstation oder das Netzwerk einen unterschiedlichen Verschlüsselungs-/Entschlüsselungsalgorithmus verwendet. Das Verfahren kann ebenso beim Austauschen geheimer Schlüssel zwischen zwei kommunizierenden Mobilstationen oder einer Mobilstation und einem Netzwerk nützlich sein, so dass weniger berechnungsintensive Geheim-Schlüssel-Algorithmen für längere Kommunikationen so wie Sprachübertragungen verwendet werden können. Zusätzlich kann das Verfahren verwendet werden, um eine sichere Authentifizierungssignatur von einer Mobilstation zu einer anderen Mobilstation oder einem Netzwerk zu übertragen.

[0022] In einer Ausführungsform der Erfindung ist ein Verfahren für Punkt-zu-Punkt-Verschlüsselung einer Nachricht, die zwischen zwei Benutzern ausgetauscht wird, in einem Telekommunikationssystem implementiert, das mindestens eine Basisstation und eine Vielzahl von Mobilstationen aufweist. In der Punkt-zu-Punkt-Ausführungsform wird keine Entschlüsselung in den Basisstationen des Systems ausgeführt. Einem Benutzer der Mobilstation M1 wird ein öffentlich bekannter (dem System bekannter) Verschlüsselungsschlüssel Em1 und ein Entschlüsselungsschlüssel Dm1 zugewiesen, der nur der Mobilstation M1 bekannt ist (die Ausdrücke "Verschlüsselungsschlüssel Emx" und "Entschlüsselungsschlüssel Dmx" werden hierin verwendet werden, um sich sowohl auf den Algorithmus als auch die Schlüsselwerte zu beziehen, die in dem Algorithmus verwendet werden, d. h. Emx ist der Verschlüsselungs-/Entschlüsselungsschlüsselalgorithmus, der die Verschlüsselungsschlüsselwerte verwendet, und Dmx ist der Verschlüsselungs-/Entschlüsselungsschlüsselalgorithmus, der die Entschlüsselungsschlüsselwerte verwendet). Einem anderen Systembenutzer der Mobilstation M2 wird ein öffentlich bekannter Verschlüsselungsschlüssel Em2 und ein Entschlüsselungsschlüssel Dm2 zugewiesen, der nur der Mobilstation M2 bekannt ist, wobei Dm1Em2 = Em2Dm1. Dm1Em2 = Em2Dm1 setzt die Einschränkung, dass Dm1 zuerst auf eine Nachricht anzuwenden, und dann Em2 anzuwenden, das gleiche ist wie Em2 zuerst und dann Dm1 auf die Nachricht anzuwenden. Nur M1 kennt Dm1 und nur M2 kennt Dm2. Ebenso muss M1 nur Em1 und den bestimmten Verschlüsselungs-/Entschlüsselungs-Algorithmus (A1) von M1 kennen, und M2 muss nur Em2 und den bestimmten Verschlüsselungs-/Entschlüsselungs-Algorithmus (A2) von M2 kennen.

[0023] Wenn ein Benutzer, der eine Mobilstation M1 besitzt, eine sichere Kommunikation c an einen Benutzer einer Mobilstation M2 zu senden wünscht, wird die Kommunikation c bei M1 unter Verwendung von Em1 und A1 verschlüsselt, um eine Nachricht

Em1(c) zu erzeugen. M1 sendet dann Em1(c) zu einer Basisstation B1 des Systems. Die Basisstation B1 verschlüsselt dann Em1(c) unter Verwendung von Em2 und A2, um die Nachricht Em2(Em1(c)) zu erzeugen, und sendet sie zurück an M1. Em2(Em1(c)) wird als nächstes bei M1 unter Verwendung von Dm1 und A1 entschlüsselt. Da Dm1Em2 = Em2Dm1 ist, führt Entschlüsseln von Em2(Em1(c)) unter Verwendung von Dm1 zu Em2(c). M1 sendet dann Em2(c) an B1. B1 sendet nun Em2(c) zur Basisstation B2, die den Bereich steuert bzw. kontrolliert, in dem sich die Mobilstation M2 befindet. Em2(c) wird als nächstes zu der Mobilstation M2 gesendet und durch die Mobilstation M2 unter Verwendung von Dm2 und A2 entschlüsselt, um die Kommunikation c zu erzeugen, die von der Mobilstation M1 zu der Mobilstation M2 gesendet worden ist.

[0024] In einer anderen Ausführungsform der Erfindung kann ein Verfahren von nicht-Punkt-zu-Punkt-Verschlüsselung von Kommunikationen zwischen zwei Mobilstationen in einem Telekommunikationssystem implementiert werden. Einem Systembenutzer der Mobilstation M1 wird ein öffentlich bekannter (dem System bekannter) Verschlüsselungsschlüssel Em1 und ein Entschlüsselungsschlüssel Dm1 zugewiesen, der nur der Mobilstation M1 bekannt ist. M1 verwendet einen Verschlüsselungs-/Entschlüsselungs-Algorithmus A1. Einem anderen Systembenutzer der Mobilstation M2 wird ein öffentlich bekannter Verschlüsselungsschlüssel Em2 und ein Entschlüsselungsschlüssel Dm2 zugewiesen, der nur der Mobilstation M2 bekannt ist. M2 verwendet einen Verschlüsselungs-/Entschlüsselungs-Algorithmus A2. Ebenso wird jeder Basisstation Bx des Systems ein öffentlich bekannter Verschlüsselungsschlüssel Ebx und ein Entschlüsselungsschlüssel Dbx zugewiesen, der nur der Basisstation Bx bekannt ist. Jede Basisstation führt ebenso Verschlüsselung/Entschlüsselung gemäß eines Algorithmus Abx aus. Die Schlüssel sind so ausgewählt, dass für jedes Paar einer Basisstation Bx und Mobilstation Mx, die miteinander kommunizieren können, DmxEbx = EbxDmx ist.

[0025] In dieser Ausführungsform, wenn der Benutzer, der die Mobilstation M1 besitzt, eine sichere Kommunikation c an einen Benutzer einer Mobilstation M2 zu senden wünscht, wird die Kommunikation c bei M1 unter Verwendung von Em1 und A verschlüsselt 1, um eine Nachricht Em1(c) zu erzeugen. M1 sendet dann Em1(c) zu einer Basisstation B1 des Systems. Die Basisstation B1 verschlüsselt dann Em1(c) unter Verwendung von Eb1 und Ab1, um die Nachricht Eb1(Em 1(c)) zu erzeugen, und sendet sie zurück an M1. Eb1(Em 1(c)) wird als nächstes bei M1 unter Verwendung von Dm1 und Am1 entschlüsselt. Da Dm1Eb2 = Eb2Dm1 ist, führt Entschlüsseln von Eb1(Em 1(c)) unter Verwendung von Dm1 zu Eb1(c). M1 sendet dann Eb1(c) an B1. B1 entschlüsselt dann Eb1(c) unter Verwendung von Db1 und Ab1, um c zu erzeugen, und sendet c zu einer Basisstation B2, die den Bereich steuert, in dem sich die Mobilstation M2 befindet. Die Kommunikation c zwischen B2 und M2 kann dann in einer identischen Weise verschlüsselt werden, wie der, die für die Übertragung zwischen M1 und B1 beschrieben worden ist, mit B2, Eb2, Db2 und Ab2 anstelle von M1, Em1, Dm1 und Am1, und M2, Em2, Dm2 und Am2 anstelle von B1, Eb1, Db1 und Ab1.

[0026] Ein vollständigeres Verständnis des Verfahrens der vorliegenden Erfindung kann mit Bezug auf die folgende detaillierte Beschreibung erhalten werden, wenn sie in Verbindung mit der begleitenden Zeichnung gelesen wird, worin:

[0027] **Fig.** 1 ein Blockdiagramm eines Telekommunikationssystems darstellt, das gemäß einer Ausführungsform der Erfindung konstruiert ist;

[0028] **Fig.** 2 ein Flußdiagramm ist, das Vorgangsschritte zeigt, die ausgeführt werden, um Punkt-zu-Punkt-verschlüsselte Kommunikationen innerhalb eines Telekommunikationssystems gemäß einer Ausführungsform der Erfindung bereitzustellen; und

[0029] **Fig.** 3 ein Flußdiagramm ist, das Vorgangsschritte zeigt, die ausgeführt werden, um nicht-Punkt-zu-Punkt-verschlüsselte Kommunikationen innerhalb eines Telekommunikationssystems gemäß einer Ausführungsform der Erfindung bereitzustellen.

[0030] **Fig.** 1 stellt ein Blockdiagramm eines Telekommunikationssystems **100** dar, das gemäß einer Ausführungsform der Erfindung konstruiert ist. Das System **100** umfasst Basisstationen B1 und B2, ein drahtgebundenes Netzwerk **142**, und Mobilstationen M1 und M2. Obwohl es gezeigt ist, zwei Basisstationen und zwei Mobilstationen einzuschließen, kann das System **100** mehr oder weniger Basisstationen oder Mobilstationen als in **Fig.** 1 gezeigt umfassen. Die Mobilstationen M1 und M2 können Mobiltelefone sein, die Sprachkommunikationen zwischen einem Benutzer von M1 oder M2 bereitstellen, und eines anderen Mobiltelefons, oder zwischen dem Benutzer und einem drahtgebundenen Telefon, das mit dem drahtgebundenen Netzwerk **142** verbunden ist. Die Mobilstationen M1 und M2 können ebenso jede andere An von mobiler Kommunikationsvorrichtung sein, die in der Lage ist, gemäß dem Systemstandard für das System **100** betrieben zu werden, so wie eine persönliche Kommunikationsvorrichtung oder ein Laptop-Computer, die mittels eines drahtlosen Modems arbeiten. Das drahtgebundene Netzwerk **142** kann ein öffentliches Fernsprechwählnetz (PSTN) oder ein privates drahtgebundenes Netzwerk für das System **100** sein, das Mobilvermittlungszenter zur

Steuerung von Anrufweiterleitung, -Registrierung und -Übergabe von einem Mobilteil von einer Basisstation zu einer anderen im System **100** einschließt. In dem System **100** können Mobilstation M1 und M2 sich innerhalb des Abdeckungsbereichs des Systems **100** bewegen, während sie mit den Basisstationen des Systems **100** durch Funkfrequenzverbindungen kommunizieren. In **Fig.** 1 sind die Mobilstation M1 und M2 gezeigt, wie sie jeweils mit Basisstationen B1 und B2 über Funkfrequenzverbindungen **144** bzw. **146** kommunizieren. Das System **100** kann gemäß irgendeinem Telekommunikationssystemstandard betrieben werden, der eine digitale Schnittstelle über die Funkfrequenzverbindungen zwischen Mobilstationen M1 und M2, und Basisstationen B1 und B2 bereitstellt. Die Auslegung und der Betrieb von digitalen Telekommunikationssystemen ist bekannt und wird hier nicht im Detail beschrieben werden. Das System **100** kann auf jede Zahl von Arten implementiert werden. Zum Beispiel kann die digitale Funkfrequenz-Schnittstelle im System **100** gemäß einem Standard arbeiten ähnlich den Telecommunications Industry Association/Electronic Industry Association (TIE/EIA) IS-136, IS-95 und PCS 1900 Standards oder dem europäischen GSM Standard.

[0031] Die Mobilstation M1 schließt eine Transceiver-Einheit **104** ein, die mit einer Antenne **102** gekoppelt ist, um Funksignale von einer Basisstation des Systems **100** zu empfangen, oder dahin zu übertragen. Die Mobilstation M1 schließt eine Benutzerschnittstelle **108** ein, die eine Computertastatur oder ein Mobiltelefon-Handgerät mit einem Tastenfeld, Mikrofon und Ohrhörerteil sein kann. Eine Steuereinheit **106** in der Mobilstation M1 steuert die Funkfrequenzkanalauswahl und andere Systemfunktionen auf die herkömmliche Weise, und eine Logikeinheit **112** steuert den allgemeinen Betrieb der Mobilstation. Die Logikeinheit **112** kann ebenso verwendet werden, um Verschlüsselungs- und Enschlüsselungsfunktionen zu implementieren, die für Kommunikationssicherheit verwendet werden. Eine Anzeigevorrichtung **110** stellt eine allgemeine visuelle Schnittstelle zu dem Benutzer der Mobilstation M1 bereit, und steht unter der Steuerung der Logikeinheit **112**. Die Mobilstation M2 schließt eine Transceivereinheit **116** ein, eine Benutzerschnittstelle **120**, eine Steuereinheit **118**, eine Logikeinheit **124**, und eine Anzeigevorrichtung **122**, wobei alle die Funktion aufweisen, wie für den entsprechenden Abschnitt der Mobilstation M1 beschrieben.

[0032] Die Basisstation B1 enthält eine Transceivereinheit **136**, die mit einer Antenne **134** gekoppelt ist, um Funksignale von den Mobilstationen zu empfangen und dahin zu übertragen. B1 enthält ebenso eine Steuereinheit **138** und einen Prozessor **140**. Die Steuereinheit **138** steuert die Funkkanal-Auswahl und -Zuweisung, indem die angemessenen Steuernachrichten an Mobilstationen erzeugt werden, und steuert ebenso andere notwendige Systemfunktionen so wie die Verbindung mit dem drahtgebundenen Netzwerk **142**. Der Prozessor **140** kann verwendet werden, um Verschlüsselungs- und Entschlüsselungsfunktionen zu implementieren und auszuführen, die für Kommunikationssicherheit verwendet werden. Die Basisstation B2 enthält eine Transceivereinheit **128**, eine Antenne **126**, eine Steuereinheit **130** und einen Prozessor **132**, wobei alle die Funktion aufweisen, wie für den entsprechenden Abschnitt der Basisstation B1 beschrieben.

[0033] In einer Ausführungsform der Erfindung kann eine verschlüsselte Nachricht von einem Benutzer zu einem anderen Benutzer in dem System **100** übermittelt werden, ohne dass die Nachricht entlang des Pfads von Benutzer zu Benutzer entschlüsselt wird. Die Nachricht kann nur von dem beabsichtigten Empfänger entschlüsselt werden. Die Ausführungsform kann verwendet werden, um Punkt-zu-Punkt-Kommunikationen zwischen irgendwelchen zwei Punkten in dem System bereitzustellen, einschließlich zwischen zwei Mobilstationen, zwischen einer Basisstation und einer Mobilstation, und zwischen einer Mobilstation und einer passend ausgerüsteten drahtgebundenen Teilnehmerstation.

[0034] Für sichere Punkt-zu-Punkt-Nachrichtenübertragung wird allgemein jeder Mobilstation Mx des Systems **100** ein öffentlich bekannter Verschlüsselungsschlüssel Emx und ein Entschlüsselungsschlüssel Dmx zugewiesen, der nur an der Mobilstation Mx bekannt ist. Für irgendwelche bzw. jede zwei Mobilstationen M1 und M2, die zu kommunizieren wünschen, muss Dm1Em2 gleich Em2Dm1 sein. Jedoch können die Verschlüsselungsalgorithmen Am1, Am2, die bei jeder von M1 und M2 verwendet werden, verschieden sein. Wenn der Benutzer von MS1 wünscht, eine sichere Kommunikation c an einen Benutzer von MS2 zu senden, wird die Kommunikation c bei MS1 unter Verwendung von Em1 und Am1 verschlüsselt, um eine verschlüsselte Nachricht Em1(c) zu erzeugen. MS1 sendet dann Em1(c) an die Basisstation B1 des Systems. Die Basisstation B1 verschlüsselt Em1(c) unter Verwendung von Em2 und Am2, um die Nachricht Em2(Em1(c)) zu erzeugen und sendet sie zurück an MS1. MS1 verschlüsselt als nächstes Em2(Em1(c)) unter Verwendung von Dm1 und Am1. Da Dm1Em2 = Em2Dm1 ist, führt Verschlüsseln von Em2(Em1(c)) unter Verwendung von Dm1 zu Em2(c). MS1 sendet dann Em2(c) an B1. B1 sendet nun Em2(c) zur Basisstation B2, die den Bereich steuert, wo sich MS2 befindet. Em2(c) wird als nächstes an MS2 gesendet und von MS2 unter Verwendung von Dm2 und Am2 entschlüsselt, um die entschlüsselte Kommunikation c zu erzeugen, die von MS1 an MS2 gesendet worden ist.

[0035] Es wird nun Bezug genommen auf **Fig.** 2, darin ist ein Flußdiagramm dargestellt, das Vor-

gangsschritte zeigt, die ausgeführt werden, um Punkt-zu-Punkt-verschlüsselte Kommunikationen innerhalb eines Telekommunikationssystems gemäß einer Ausführungsform der Erfindung bereitzustellen. Als ein erläuterndes Beispiel wird der Fall einer verschlüsselten Nachrichtenübertragung zwischen der Mobilstation M1 und der Mobilstation M2 von **Fig.** 1 verwendet, um den Vorgang zu beschreiben, wobei M1 den Rabin-Algorithmus verwendet, und M2 den Rivest, Shamir und Adleman (RSA)-Algorithmus verwendet. Eine Hintergrundbeschreibung des Rabin-Algorithmus wird in dem Buch "Cryptography, Theorie and Practice" von Stinson gegeben, veröffentlicht durch CRC, 1995, auf den Seiten 143–148. Eine detaillierte Beschreibung des RSA-Algorithmus wird gegeben in dem Buch "Digital Money" von Lynch et al., veröffentlicht durch John Wiley and Sons, 1996, auf den Seiten 76–86.

[0036] Die Schlüsselfunktionen Em1 und Dm1 für die Mobilstation M1 können gemäß den Rabin-Kriterien ausgewählt werden. In dem Rabin-Algorithmus für dieses Beispiel werden zwei Primzahlen p und q ausgewählt unter Verwendung einer ausgewählten, vordefinierten Zahl N, wobei $p \times q = N$, und $p = 4k_1 + 3$, und $q = 4k_2 + 3$, und wobei k_1 und k_2 Konstanten sind. N kann öffentlich bekannt sein, während p und q geheimgehalten werden müssen. Em1 ist definiert als $Em1(c) = (c)^2 \bmod N$, und DM1 ist definiert als $DM1(c)=c^{1/2} \bmod N$, wobei c die zu übertragende Nachricht ist. Um DM1(c) für $c^{1/2}$ zu lösen werden die Gleichungen $x^2 = c \bmod p$, und $x^2 = c \bmod q$ unter Verwendung der Lösungen $x_1 = \pm c^{(p+1)/4}$, und $x_2 = \pm c^{(q+1)/4}$ gelöst. Wenn die zwei Werte a und b gefunden werden, so dass $ap + bq = 1$ ist, dann kann $c^{1/2}$ mit der Gleichung $c^{1/2} = bq\, x_1 + apx_2 \bmod N$ gefunden werden.

[0037] Die Schlüsselfunktionen Em2 und Dm2 für die Mobilstation M2 können gemäß den Rivest, Shamir und Adleman (RSA)-Kriterien ausgewählt werden. In RSA werden zuerst zwei (große) Primzahlen p und q ausgewählt, wobei $p \times q = N$. In dieser Ausführungsform ist N für M2 gleich dem N, das für M1 verwendet wird. Dies vereinfacht das Einhalten bzw. Erreichen der Bedingung, dass Dm1Em2 = Dm2Em1. Jedoch können andere Werte von N verwendet werden, so lange wie Dm1Em2 = Em2Dm1 ist. Zwei andere Werte a2 und b2 werden dann ausgewählt, wobei $(a2)(b2) = 1 \bmod (p - 1)(q - 1)$. N und a2 können öffentlich sein, und b2 muss geheimgehalten werden. Em2 und Dm2 sind dann definiert als $Em2(c) = (c)^{a2} \bmod N$, und $Dm2 = (c)^{b2} \bmod N$.

[0038] Der Vorgang beginnt bei Schritt **200**, wo der Verschlüsselungsvorgang in M1 initiiert wird. In Schritt **202** wird die Kommunikation c durch die Logikeinheit **112** unter Verwendung von Em1 und Am1 verschlüsselt, um die verschlüsselte Nachricht $Em1(c) = (c)^2 \bmod N$ zu erzeugen. Der Vorgang geht dann weiter zu Schritt **204**, wo Em1(c) durch die Transceivereinheit **104** von M1 zu B1 übertragen wird. Nachdem Em1(c) durch die Transceivereinheit **136** empfangen wurde, verschlüsselt der Prozessor **140** von B1 Em1(c) in Schritt **206**, unter Verwendung von Em2 und Am2, um die verschlüsselte Nachricht $Em2(Em1(c)) = ((c)^2)^{a2} \bmod N$ zu erzeugen. Der Vorgang geht dann weiter zu Schritt **208**, wo Em2(Em1(c)) von B1 zurück nach M1 gesendet wird. Als nächstes in Schritt **210**, nachdem Em2(Em1(c)) von B1 empfangen wurde, entschlüsselt die Logikeinheit **112** von M1 Em2(Em1(c)) unter Verwendung von Am2 (dem Rabin-Algorithmus) wie vorstehend beschrieben. $(Em2(Em1(c)))^{1/2} = (((c)^2)^{a2})^{1/2}$. Die erzeugte Nachricht Dm1(Em2(Em1(c))) ist dann gleich $(c)^{a2} \bmod N$, oder der verschlüsselten Nachricht Em2(c).

[0039] Als nächstes sendet die Transceivereinheit **104** von M1 in Schritt **212** die verschlüsselte Nachricht Em2(c) an B1. Als nächstes, in Schritt **214**, sendet die Steuereinheit **138** von B1 dann Em2(c) durch das drahtgebundenes Netzwerk **142** an die Steuereinheit **130** von B2. Da die Nachricht verschlüsselt ist, ist dies eine sichere Kommunikation. Als nächstes, in Schritt **216**, nachdem Em2(c) durch die Steuereinheit **130** von B2 empfangen wurde, sendet die Transceivereinheit **128** Em2(c) an M2. In Schritt **218** wird Em2(c) in dem Prozessor **132** von M2 unter Verwendung von Dm2 und Am2 entschlüsselt, um $Dm2(Em2(c) = ((c)^{a2})^{b2} \bmod N$, oder $Dm2(Em2(c)) = c$ zu erzeugen. M2 hat nun die entschlüsselte Kommunikation c empfangen.

[0040] In einer anderen Ausführungsform der Erfindung wird ein nicht-Punkt-zu-Punkt-Verfahren verwendet, um eine Nachricht von einem Benutzer zu einem anderen Benutzer im System **100** zu übermitteln. In dieser Ausführungsform wird die Nachricht an der Basisstation in Kommunikation mit dem sendenden Benutzer entschlüsselt. Die Nachricht wird dann an die Basisstation in Kommunikation mit dem Empfänger der Nachricht gesendet und für die Übertragung an den Empfänger der Nachricht verschlüsselt. In dieser Ausführungsform muss jede der kommunizierenden Mobilstationen oder Basisstationen nur ihren eigenen Verschlüsselungsschlüssel und Verschlüsselungs-/Entschlüsselungs-Algorithmus kennen. Die kommunizierenden Entitäten müssen den Verschlüsselungs-Algorithmus von irgendeinem der anderen kommunizierenden Entitäten nicht kennen oder in der Lage sein, ihn auszuführen.

[0041] Allgemein wird in dieser Ausführungsform jeder Mobilstation Mx ein Verschlüsselungsschlüssel Emx und ein Entschlüsselungsschlüssel Dmx zugewiesen. Dmx ist nur an der Mobilstation x bekannt. Jeder Basisstation Bx des Systems **100** wird ein Verschlüsselungsschlüssel Ebx und ein Entschlüsselungsschlüssel Dbx zugewiesen. Dbx ist nur an der

Basisstation Bx bekannt. Für irgendein Paar von Mobilteil und Basisstation Mx und By, die miteinander zu kommunizieren wünschen, muss DmxEby gleich EbyDmx sein.

[0042] Wenn der Benutzer von M1 wünscht, eine sichere Kommunikation c an einen Benutzer von M2 zu senden, wird die Kommunikation c durch M1 unter Verwendung von Em1 und Am1 verschlüsselt, um eine Nachricht Em1(c) zu erzeugen. M1 sendet dann Em1(c) an die Basisstation B1 des Systems. Die Basisstation B1 verschlüsselt dann Em1(c) unter Verwendung von Eb1 und Ab1, um die Nachricht Eb1(Em1(c)) zu erzeugen, und sendet sie zurück an M1. M1 verschlüsselt als nächstes Eb1(Em1(c)) unter Verwendung von Dm1 und A1. Da Dm1Eb1 = Db1Em1 ist, führt Entschlüsseln von Eb1(Em1(c)) unter Verwendung von Dm1 und A2 zu Eb1(c). M1 sendet dann Eb1(c) an B1. M1 kann der einzige Benutzer sein, der die korrekte Eb1(c) an diesem Punkt an B1 sendet. B1 entschlüsselt nun Eb1(c) unter Verwendung von Db1 und Ab1, um c zu erzeugen. B1 sendet als nächstes c durch das System zu der Basisstation B2, die den Bereich steuert, wo sich der Benutzer M2 befindet. Die Kommunikation c zwischen B2 und M2 kann dann in einer identischen Weise zu der für die Übertragung zwischen M1 und B1 beschriebenen verschlüsselt werden, mit B2, Eb2, Db2 und Ab2 anstelle von M1, Em1, Dm1 und Am1, und M2, Em2, Dm2 und Am2 anstelle von B1, Eb1, Db1 und Ab1.

[0043] Es wird nun Bezug genommen auf **Fig.** 3, darin ist ein Flußdiagramm dargestellt, das Vorgangsschritte zeigt, die ausgeführt werden, um nicht-Punkt-zu-Punkt verschlüsselte Kommunikationen innerhalb eines Telekommunikationssystems gemäß einer Ausführungsform der Erfindung bereitzustellen. Das Flußdiagramm von **Fig.** 3 kann verwendet werden, um ein erläuterndes Beispiel zu beschreiben, das den Fall einer verschlüsselten Nachrichtenübertragung zwischen der Mobilstation M1 und der Mobilstation M2 von **Fig.** 2 beschreibt. In diesem Beispiel verwenden M1 und M2 den Rabin Algorithmus, und B1 und B2 verwenden den RSA Algorithmus. Der in **Fig.** 3 verwendete Vorgang verhindert, dass die Mobilteile M1 und M2 den an den Basisstationen verwendeten RSA Algorithmus verwenden müssen.

[0044] Die Schlüsselfunktionen Emy, Dmy für die Mobilstation My können entsprechend den Rabin Kriterien ausgewählt werden. In dem Rabin-Algorithmus, für dieses Beispiel, werden zwei Primzahlen p und q ausgewählt unter Verwendung einer ausgewählten Zahl N, wobei $p \times q = N$, und $p = 4k_1 + 3$, und $q = 4k_2 + 3$, und wobei k_1 und k_2 Konstanten sind. N kann öffentlich bekannt sein, während p und q geheimgehalten werden müssen. Emy ist definiert als $Emx(c) = (c)^2 \bmod N$, und DMy ist definiert als $DMy(c) = c^{1/2} \bmod N$. Um Dmy(c) für c zu lösen, werden die Gleichungen $x^2 = c \bmod p$, und $x^2 = c \bmod q$ unter Verwendung der Lösungen $x_1 = \pm c^{(p+1)/4}$ und $x_2 = \pm c^{(q+1)/4}$ gelöst. Wenn zwei Werte a und b gefunden werden, so dass $ap + bq = 1$ ist, dann kann c mit der Gleichung $c^{1/2} = bq\, x_1 + apx_2 \bmod N$ gefunden werden.

[0045] Die Schlüsselfunktionen Ebx und Dbx für die Basisstation x können gemäß den Rivest, Shamir und Adleman (RSA)-Kriterien ausgewählt werden. In RSA werden zuerst zwei (große) Primzahlen p und q ausgewählt, wobei $p \times q = N$. Zwei andere Werte ax und bx werden dann ausgewählt, wobei $(ax)(bx) = 1 \bmod (p - 1)(q - 1)$. Ebx und Dbx sind dann definiert als $Ebx(c) = (c)^{ax} \bmod N$, und $Dbx = (c)^{bx} \bmod N$. In dieser Ausführungsform ist N für B1 gleich dem N, das für M1 verwendet wird, und N für B2 gleich dem N, das für M2 verwendet wird. Dies vereinfacht das Einhalten der Bedingung, dass Dm 1Eb1 = Eb1Dm1 ist. Jedoch können andere Werte von N verwendet werden, so lange wie Dm1Eb1 = Eb1Dm1, und Dm2Eb2 = Eb2Dm2 ist.

[0046] Der Vorgang beginnt bei Schritt **300**, wo der Verschlüsselungsvorgang eingeleitet wird. Als nächstes wird in Schritt **302** die Kommunikation c bei der Logikeinheit **112** von M1 unter Verwendung von Em1 und Am1 verschlüsselt, um die verschlüsselte Nachricht $Em1(c) = (c)^2 \bmod N$ zu erzeugen. Der Vorgang geht dann weiter zu Schritt **304**, wo Em1(c) durch die Transceivereinheit **104** von M1 zu B1 übertragen wird. In Schritt **306**, nachdem Em1(c) durch die Transceivereinheit **136** empfangen wurde, verschlüsselt B1 Em1(c) unter Verwendung von Eb1 und Ab1, um die verschlüsselte Nachricht $Eb1(Em1(c)) = ((c)^2)^{a1} \bmod N$ zu erzeugen. Der Vorgang geht dann weiter zu Schritt **308**, wo Em2(Em1(c)) durch die Transceivereinheit **136** von B1 zurück nach M1 gesendet wird. Als nächstes in Schritt **310**, nachdem Em2(Em1(c)) von B1 durch die Transceivereinheit **104** empfangen wurde, entschlüsselt die Logikeinheit **112** von M1 Eb2(Em1(c)) unter Verwendung von Dm1 und dem Rabin-Algorithmus wie zuvor beschrieben. $(Eb2(Em1(c)))^{1/2} = (((c)^2)^{a2})^{1/2}$. Die erzeugte Nachricht Dm1(Eb2(Em1(c))) ist dann gleich $(c)^{a2} \bmod N$, oder der verschlüsselten Nachricht Eb2(c).

[0047] Als nächstes, in Schritt **312**, sendet M1 die verschlüsselte Nachricht Eb1(c) durch die Transceivereinheit **104** an B1, und in Schritt **314** entschlüsselt die Prozessoreinheit **140** von B1 dann Eb1(c) unter Verwendung von Db1, um $Db1(Eb1(c)) = ((c)^{a1})^{b1} \bmod N = c$ zu erzeugen. Nachdem die Kommunikation c bei dem Prozessor **140** B1 entschlüsselt worden ist, geht der Vorgang zu Schritt **316**, wo die Kommunikation c von der Steuereinheit **138** der Basisstation B1 durch drahtgebundene Netzwerk **142** an die Steuereinheit **130** Basisstation **B2** gesendet wird. Die Übertragung der Kommunikation c zwischen B2 und M2 kann dann in einer identischen Weise ausgeführt

werden wie die für die Übertragung zwischen M1 und B1 beschriebene. Dies wird durch die Schritte **318**–**330** dargestellt, die identisch zu den Schritten **302**–**314** sind, mit B2, Eb2, Db2 und Ab2 anstelle von M1, Em1, Dm1 und Am1, und M2, Em2, Dm2 und Am2 anstelle von B1, Eb1, Db1 und Ab1.

[0048] Die Lehren dieser Erfindung sollten nicht ausgelegt werden, um nur auf die Verwendung mit den beschriebenen Telekommunikationsstandards beschränkt zu werden, und sollten ausgelegt werden, jedes ähnliche System einzuschließen. Weiterhin können andere Verschlüsselungsalgorithmen verwendet werden als die ausdrücklich vorstehend beschriebenen, um diese Erfindung auszuführen.

Patentansprüche

1. Verfahren zum Senden einer sicheren Nachricht in einem mobilen Telekommunikationssystem, einschließend eine Basisstation (B1) und eine Vielzahl von Mobilstationen (M1, M2), denen verschiedene Verschlüsselungsalgorithmen (Am1, Am2) zugewiesen worden sind, zum Aufbau von sicherer Funkkommunikation mit der Basisstation, wobei jede Mobilstation einen zugewiesenen individuellen Entschlüsselungsschlüssel und einen öffentlichen Verschlüsselungsschlüssel aufweist, wobei das Verfahren umfasst:
Verschlüsseln (**202**, **302**) einer ersten Nachricht (C) an einer ersten von jeder der Mobilstationen (M1) unter Verwendung des Verschlüsselungsschlüssels (Em1) und des Verschlüsselungsalgorithmus (Am1) der ersten Mobilstation, um eine zweite Nachricht (Em1(C)) zu erzeugen;
Übertragen (**204**; **304**) der zweiten Nachricht von der ersten Mobilstation (M1) zu der Basisstation (B1);
Verschlüsseln (**206**; **306**) der zweiten Nachricht an der Basisstation unter Verwendung eines Verschlüsselungsschlüssels (Em2; Eb1), verschieden von dem der ersten Mobilstation, um eine dritte Nachricht (Em2(Em1(C); Eb1(Em1(C)) zu bilden, wobei der verschiedene Verschlüsselungsschlüssel einen zugeordneten und verschiedenen Entschlüsselungsschlüssel (Dm2; Db1) aufweist;
Übertragen (**208**; **308**) der dritten Nachricht von der Basisstation (B1) zu der ersten Mobilstation (M1);
Entschlüsseln (**210**; **310**) der dritten Nachricht an der ersten Mobilstation (M1) mit dem Entschlüsselungsschlüssel und dem Algorithmus der ersten Mobilstation (Am1, Dm1), um eine vierte Nachricht (Em2(C); Eb1(C)) zu bilden;
Übertragen (**212**; **312**) der vierten Nachricht von der ersten Mobilstation (M1) zu der Basisstation (B1); und
Entschlüsseln (**218**; **314**) der vierten Nachricht unter Verwendung des verschiedenen Enschlüsselungsschlüssels (Dm2, Db1), um dadurch sichere Kommunikation zwischen der Basisstation (B1) und der ersten Mobilstation (M1) bereitzustellen, welcher der Algorithmen auch immer dazu zugewiesen ist.

2. Verfahren gemäß Anspruch 1, einschließend die Übertragung der vierten Nachricht (Em2(C)) zu einer zweiten der Mobilstationen (M2), wobei die verschiedenen Verschlüsselungs- und Entschlüsselungsschlüssel (Em2, Dm2) der zweiten Mobilstation zusammen mit einem zugeordneten verschiedenen Verschlüsselungsalgorithmus (Am2) zugewiesen werden, und wobei die Entschlüsselung (**218**) der vierten Nachricht an der zweiten Mobilstation (M2) ausgeführt wird.

3. Verfahren gemäß Anspruch 2; einschließend Senden der vierten Nachricht (Em2(C)) von der Basisstation (B1) zu einer weiteren Basisstation (B2) und Übertragen der vierten Nachricht von der weiteren Basisstation zu dem zweiten mobilen Endgerät (M2) zur Entschlüsselung.

4. Verfahren gemäß Anspruch 1, einschließend Entschlüsseln (**314**) der vierten Nachricht (Eb1(C)) an der Basisstation (B1), Weiterleiten (**316**) der entschlüsselten vierten Nachricht zu einer zweiten Basisstation (B2), Verschlüsseln (**318**) und Übertragen (**320**) der entschlüsselten vierten Nachricht zu einer zweiten Mobilstation (M2) und Entschlüsseln (**330**) der sich ergebenden Nachricht an der zweiten Mobilstation unter Verwendung des Enschlüsselungsschlüssels (Dm2), der der zweiten Mobilstation zugeordnet ist.

5. Telekommunikationssystem, das ausgelegt ist, ein Verfahren auszuführen, wie es in irgendeinem der vorhergehenden Ansprüche beansprucht wird.

6. System gemäß Anspruch 5, wobei individuelle Algorithmen (Am1, Am2), die jeweils individuellen Mobilstationen (M1, M2) zugewiesen sind, einen Algorithmus vom RSA-Typ und einen Algorithmus vom Rabin-Typ aufweisen.

Es folgen 3 Blatt Zeichnungen

Anhängende Zeichnungen

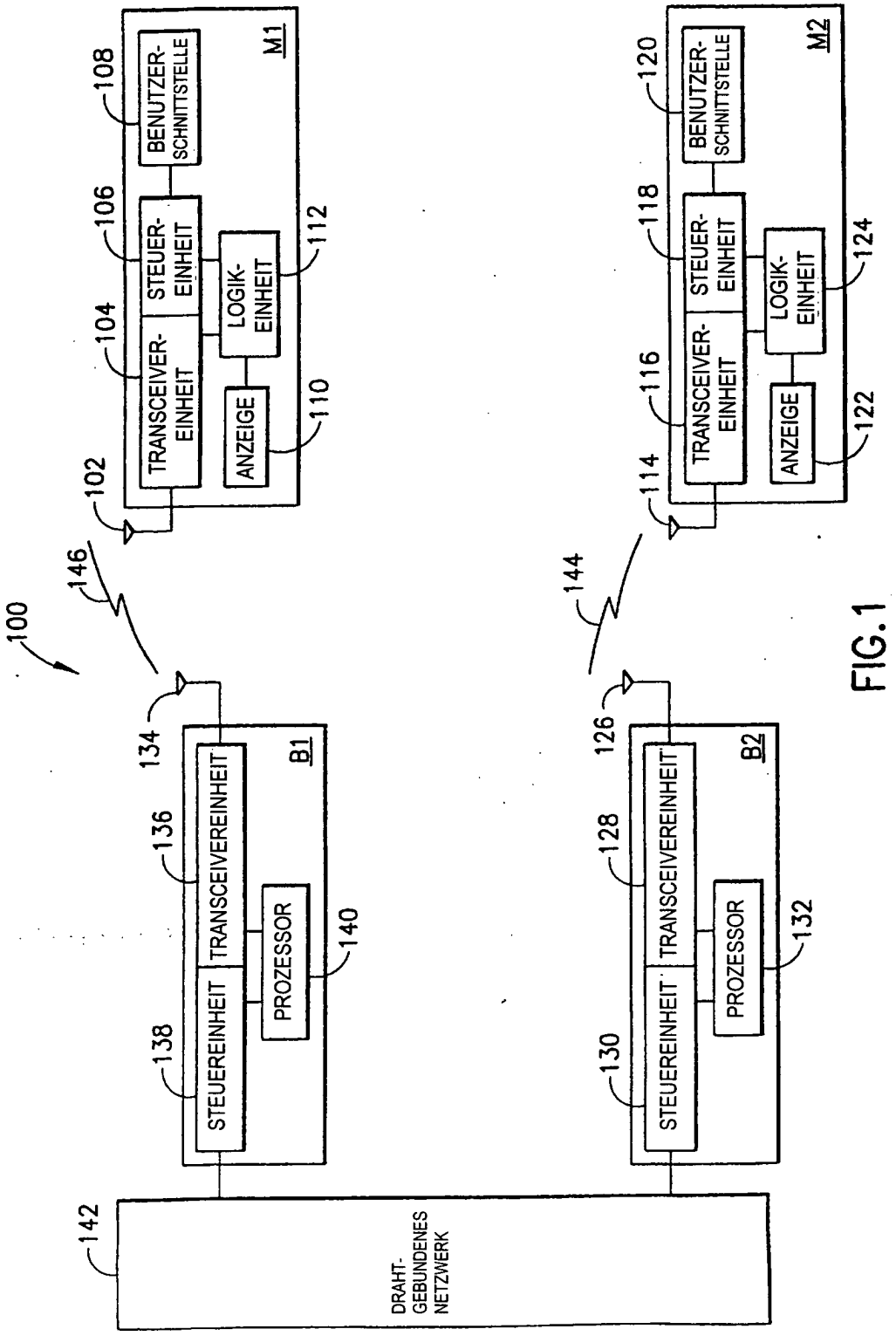

FIG.1

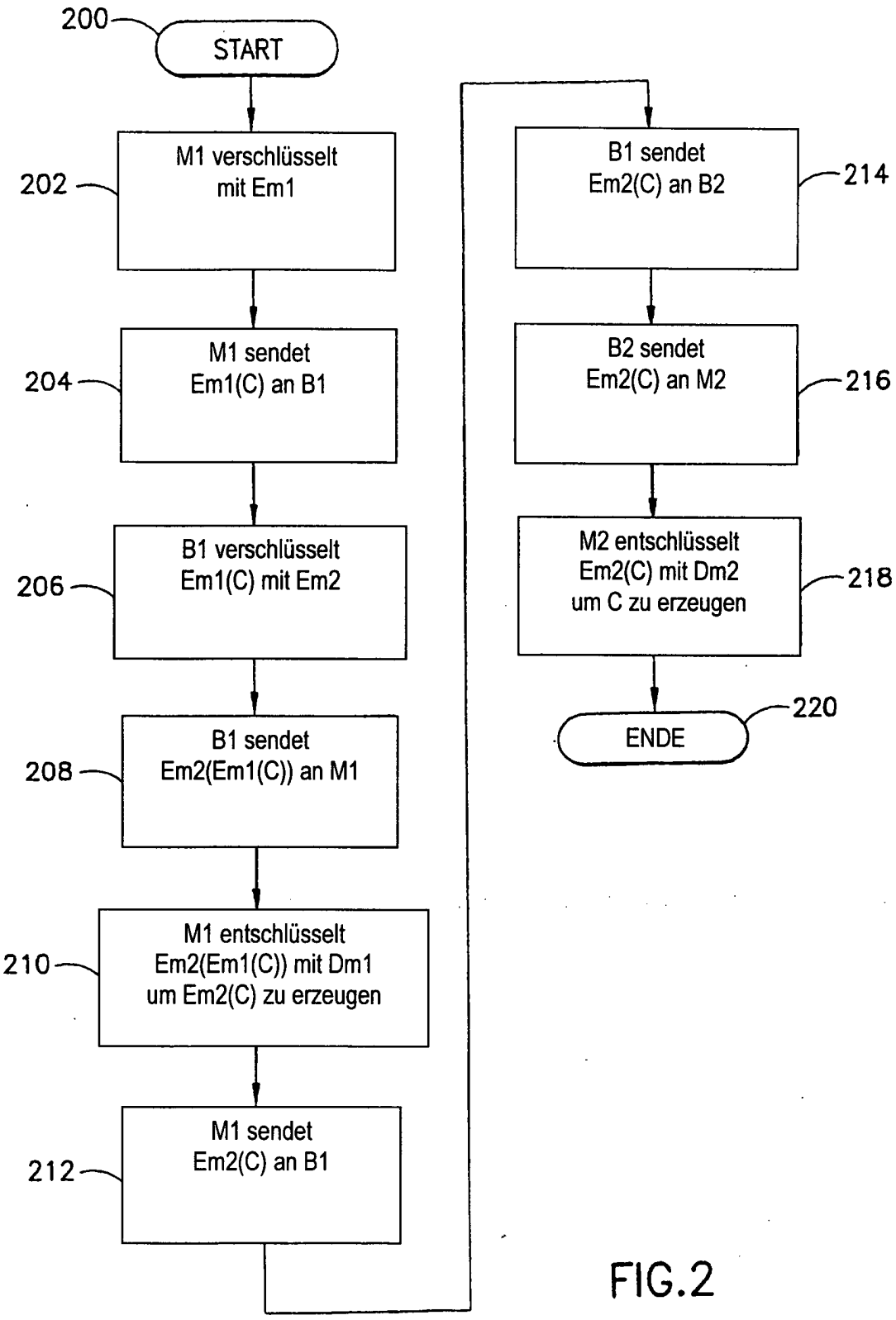
200
START
202
M1 verschlüsselt mit Em1
204
M1 sendet Em1(C) an B1
206
B1 verschlüsselt Em1(C) mit Em2
208
B1 sendet Em2(Em1(C)) an M1
210
M1 entschlüsselt Em2(Em1(C)) mit Dm1 um Em2(C) zu erzeugen
212
M1 sendet Em2(C) an B1
214
B1 sendet Em2(C) an B2
216
B2 sendet Em2(C) an M2
218
M2 entschlüsselt Em2(C) mit Dm2 um C zu erzeugen
220
ENDE

FIG.2

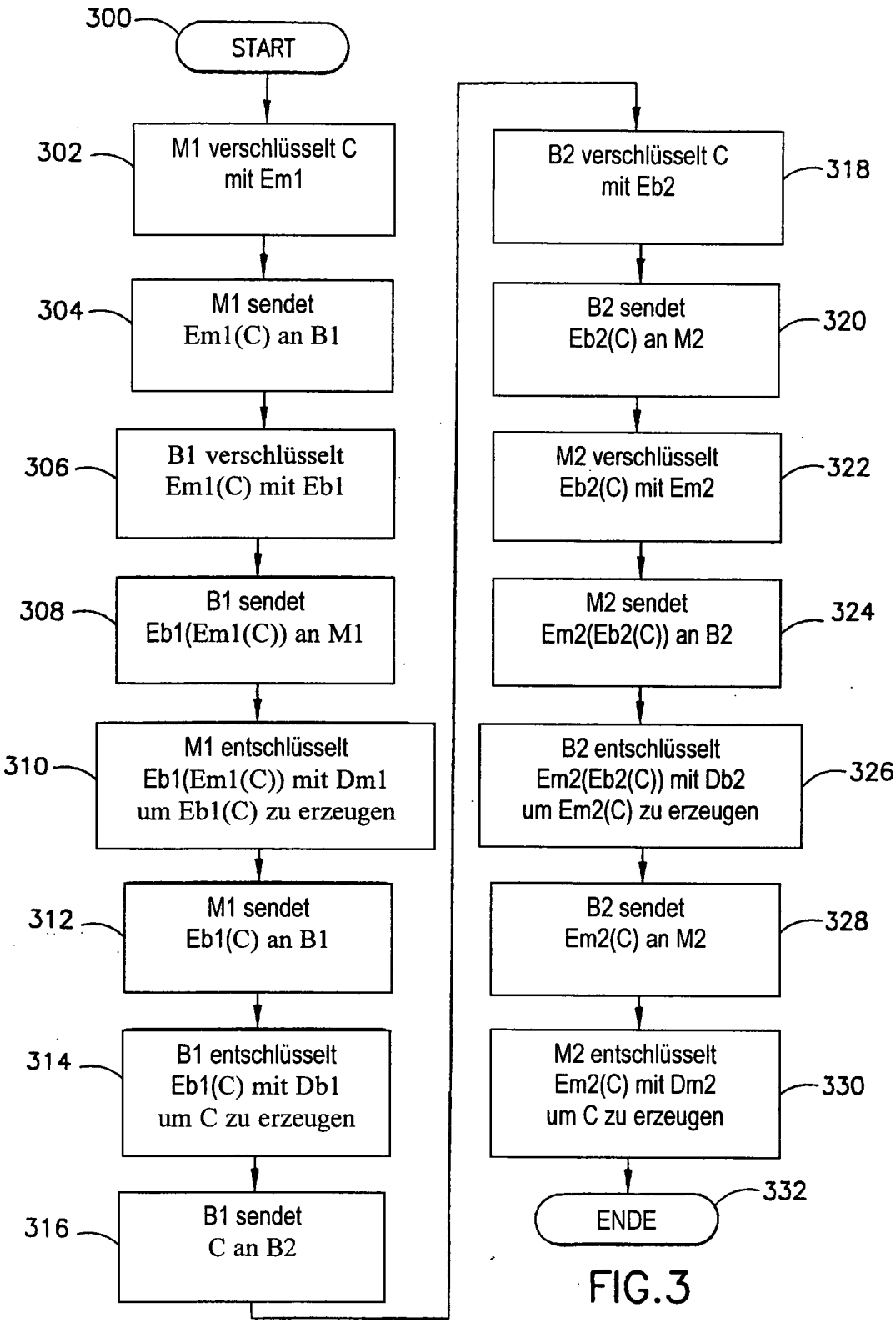
300
START
302
M1 verschlüsselt C mit Em1
304
M1 sendet Em1(C) an B1
306
B1 verschlüsselt Em1(C) mit Eb1
308
B1 sendet Eb1(Em1(C)) an M1
310
M1 entschlüsselt Eb1(Em1(C)) mit Dm1 um Eb1(C) zu erzeugen
312
M1 sendet Eb1(C) an B1
314
B1 entschlüsselt Eb1(C) mit Db1 um C zu erzeugen
316
B1 sendet C an B2
318
B2 verschlüsselt C mit Eb2
320
B2 sendet Eb2(C) an M2
322
M2 verschlüsselt Eb2(C) mit Em2
324
M2 sendet Em2(Eb2(C)) an B2
326
B2 entschlüsselt Em2(Eb2(C)) mit Db2 um Em2(C) zu erzeugen
328
B2 sendet Em2(C) an M2
330
M2 entschlüsselt Em2(C) mit Dm2 um C zu erzeugen
332
ENDE

FIG.3