CH 656 761 A5

(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
BUNDESAMT FÜR GEISTIGES EIGENTUM

(11) CH 656 761 A5

(51) Int. Cl.⁴: H 04 L 9/02

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT A5

(21) Gesuchsnummer: 5664/81

(22) Anmeldungsdatum: 24.12.1980

(30) Priorität(en): 28.12.1979 US 108039

(24) Patent erteilt: 15.07.1986

(45) Patentschrift veröffentlicht: 15.07.1986

(73) Inhaber:
Racal-Milgo, Inc., Miami/FL (US)

(72) Erfinder:
Miller, William J., Miami Beach/FL (US)

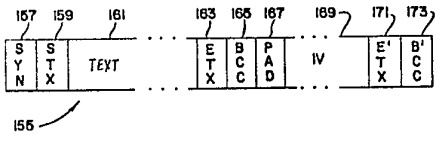
(74) Vertreter:
Hepatex-Ryffel AG, Zürich

(86) Internationale Anmeldung: PCT/US 80/01722 (En)

(87) Internationale Veröffentlichung: WO 81/01933 (En) 09.07.1981

(54) Datenübertragungsanlage, die eine Verschlüsselungs/Entschlüsselungs-Vorrichtung an jedem Ende wenigstens einer Datenverbindung aufweist.

(57) Die Übermittlung über Datenverbindungen unter Anwendung eines Binär-Synchron-Übermittlungsprotokolls, die gemäss der U.S.-Bundes-Datenverschlüsselungsnorm (DES) sicher gemacht werden soll, wird verbessert durch Verwendung einer Form (155) für die verschlüsselten Meldungen, in der sich die Start-Bitfolge (169) für den Algorithmus der Datenverschlüsselungsnorm am hinteren Ende der verschlüsselten Meldung (155) befindet. Zusätzliche Informations- oder Steuerworte (167, 171, 173) können ebenfalls am hinteren Ende der verschlüsselten Meldung (155) angereiht werden, ohne einen Durchsatz-Verlust zu bewirken, um die Sicherheit und Flexibilität der verschlüsselten Meldung sowohl in Punkt-zu-Punkt-Anlagen als auch in Mehrpunkt-Anlagen zu erhöhen.



PATENTANSPRÜCHE

1. Datenübertragungsanlage, die ein Synchron-Übermittlungsprotokoll verwendet und eine Verschlüsselungs/Entschlüsselungs-Vorrichtung (23, 27; 39, 45; 40, 45) an jedem Ende wenigstens einer Datenverbindung (25) aufweist, wobei eine der Verschlüsselungs/Entschlüsselungs-Vorrichtungen der bzw. jeder Datenverbindung eine Haupt-Vorrichtung (39; 40) und die andere die Neben-Vorrichtung (45) ist, jede Verschlüsselungs/Entschlüsselungs-Vorrichtung dazu eingerichtet ist, Meldungstext zu chiffrieren und zu dechiffrieren durch Addieren desselben mit dem nach einem Verschlüsselungs/Entschlüsselungsalgorithmus mit einem für die bzw jede Datenverbindung (25, 55, 57) vorgewählten geheimen Schlüssel (33) kombinierten Chiffretext, und die Vorbereitung der Haupt- und der Neben-Verschlüsselungs/Entschlüsselungs-Vorrichtung vor einer Chiffre-Übermittlung durch eine Start-Bitfolge (169) gesteuert wird, die bei der Haupt-Verschlüsselungs/Entschlüsselungs-Vorrichtung (39; 40) erzeugt wird und an die Neben-Verschlüsselungs/Entschlüsselungs-Vorrichtung (45) übermittelt wird, dadurch gekennzeichnet, dass die Anlage folgendes enthält:

Mittel (257, 191) zum Zuführen der Start-Bitfolge (169) zu der Haupt-Verschlüsselungs/Entschlüsselungs-Vorrichtung (39; 40) vor dem Beginn der Chiffrierung einer nächsten Meldung und

Mittel (257, 205) zum Zuführen der gleichen Start-Bitfolge (169) zu der Neben-Vorrichtung (45) als hinteres Ende der vorangehenden verschlüsselten Meldung (155), wobei die Start-Bitfolge (169) dem Dechiffrierteil (203, 207, 211) der Neben-Vorrichtung zugeführt wird, um sie für den Empfang der nächsten Chiffre (161) vorzubereiten.

2. Datenübertragungsanlage gemäss Anspruch 1, gekennzeichnet durch Mittel (257) zum Erzeugen der Start-Bitfolge (169) als Mehrbit-Zufallszahl.

3. Datenübertragungsanlage gemäss Anspruch 1 oder 2, dadurch gekennzeichnet, dass den Mitteln (257, 191) zum Zuführen der Start-Bitfolge (169) zu der Haupt-Verschlüsselungs/Entschlüsselungs-Vorrichtung (39; 40) Mittel (281) zugeordnet sind, um zusätzlich zur Start-Bitfolge (169) ein Informationswort (167, 171, 173) am hinteren Ende der verschlüsselten Meldung zu liefern.

4. Datenübertragungsanlage gemäss Anspruch 3, dadurch gekennzeichnet, dass das Informationswort (167, 171, 173) ein Abbruchzeichen enthält.

5. Datenübertragungsanlage gemäss Anspruch 3, dadurch gekennzeichnet, dass das Informationswort (167, 171, 173) Textende-Wortteile (171) und Blockprüf-Wortteile (173) enthält, die unverschlüsselt übermittelt werden.

6. Datenübertragungsanlage gemäss Anspruch 3, dadurch gekennzeichnet, dass das Informationswort (167, 171, 173) eine Folgenummer enthält.

7. Datenübertragungsanlage gemäss Anspruch 3, dadurch gekennzeichnet, dass das Informationswort (167, 171, 173) eine die Übermittlung betreffende Signalinformation enthält, z.B. eine diagnostische Information oder einen neuen Schlüssel.

Datenübertragungsanlagen mit Datenverbindungen sind im Stand der Technik bekannt. Eine Datenverbindung umfasst die Fernmeldeleitungen, Modems und anderen Fernmeldeeinrichtungen, die bei der Übermittlung von Dateninformation zwischen zwei oder mehr Stationen oder Terminals verwendet werden. Die eine Station ausmachenden Terminal-Ausrüstungen können zwischen einer Grundausrüstung mit Sende/Empfangs-Leser und einem Drucker bis zu einer Steuereinheit mit mehreren angeschlossenen Ein-/Ausgangs-Einrichtungen variieren. Die Fernmeldeleitungen und anderen Einrichtungen werden üblicherweise von öffentlichen Fernmeldeunternehmen zur Verfügung gestellt, oder es können entsprechende Einrichtungen von dem Einzelnen zur Verfügung gestellt werden, der die Datenverbindung errichtet. Die speziellen Modem- oder Datengerät-Ausrüstungen, die in jeder Station der Datenverbindung verwendet werden, hängen von der Art der verwendeten Fernmeldekanäle und der Arbeitsgeschwindigkeit der in jeder Station vorhandenen Terminal-Ausrüstungen ab.

Jede Übermittlung von Daten erfolgt über die Fernmeldeleitung in der Form einer Folge von binär codierten Signalen, in der Regel unter Verwendung eines Synchron-Übermittlungsprotokolls. Die Steuerung der Datenverbindung wird durch die Übermittlung und Erkennung von besonderen Leitungssteuer-Wortteilen bewirkt.

Das bekannte Synchron-Binärübermittlungsprotokoll (BSC) enthält eine Reihe von Regeln für die synchrone Übermittlung von binär codierten Daten. Alle Daten werden in der Synchron-Binärübermittlung als serieller Strom von Binärziffern (0- und 1-Bits) übermittelt. Synchron-Übermittlung heisst, dass die aktive Empfangsstation an einem Fernmeldekanal im Takt mit der Sendestation arbeitet, indem sie ein spezielles Bit-Muster (Synchron-Muster) am Anfang jedes Übermittlungsblockes erkennt.

Das Synchron-Binärübermittlungsprotokoll kann mit drei speziellen Übermittlungscodesätzen arbeiten. Jeder dieser Codesätze besteht aus grafischen Zeichen (numerisch, alphabetisch, spezial), Funktionszeichen (Horizontal, Tabelle, Streichung) und Datenverbindungs-Steuerzeichen (Vorspannanfang, Textanfang usw.). Jeder Code besitzt ein unterschiedliches Fassungsvermögen für die Gesamtzahl der grafischen und Funktions-Zuteilungen, und diese Fassungsvermögen spiegeln die Flexibilität jedes dieser Codes wider. Diese Codes sind im Stand der Technik bekannt als ausgedehnter binär codierter Dezimal-Austauschcode (extended binary coded decimal interchange code = EBCDIC), USA-Normcode für Informationsaustausch (United States of America Standard Code for Information Interchange = USASCII) und Sechs-Bit-Transcode.

Die Datenverbindung kann für den Betrieb von Punkt zu Punkt (zwei Stationen) oder zwischen mehreren Punkten (zwei oder mehr Stationen) ausgelegt sein. Beim Betrieb von Punkt zu Punkt kann eine Konfliktsituation entstehen, in der beide Stationen gleichzeitig versuchen, die Fernmeldeleitung zu benutzen. Um diese Möglichkeit klein zu halten, kündet eine Station durch Verwendung bestimmter Steuer-Wortteile, wie des Anfrage-Wortteils (ENQ), an, dass sie die Leitung belegen will. So bildet eine Reihe von Wortteilen, wie Synchron-Wortteilen (SYN) und Anfrage-Wortteilen (ENQ), das Signalisierungsmuster für das Anfordern der Steuerung über die Leitung und lässt ein Maximum an Zeit für die Leitungsüberwachung frei. Wenn gleichzeitig Ankündigungen auftreten, dann setzt eine Station den Belegungsversuch fort, um den Konfliktzustand zu beenden. Nachdem die Station die Steuerung der Leitung erworben hat, kann die Meldungs-Übermittlung beginnen.

In einer Anlage zwischen mehreren Punkten wird eine der Stationen in einem Netz als zentrale Station oder Hauptstation bestimmt. Die übrigen Stationen sind Nebenstationen. Die zentrale Station steuert alle Übermittlungen in der Datenverbindung zwischen mehreren Punkten, indem sie die Nebenstationen abfragt oder anwählt. Die Abfrage ist eine Einladung von der zentralen Station an eine bestimmte Nebenstation, Daten von der Nebenstation an die Zentrale zu senden. Das Anwählen ist eine Aufforderung von der zentralen Station an eine der Nebenstationen, mit der dieser befohlen wird, eine Datenmeldung von der Zentrale zu empfangen. Diese Abfrage- und Anwählmöglichkeiten gestatten der zentralen Station, die übermittelnde Station zu bestimmen und die Richtung der Übermittlung in der Anlage zu steuern. Jeder Station in einer Datenverbindung zwischen mehreren Punkten wird eine individuelle Stationsadresse

zugeteilt, die verwendet wird, um beim Abfragen oder Anwählen die Aufmerksamkeit einer Station zu gewinnen. Jede Stationsadresse besteht aus einem bis sieben Wortteilen, je nach den besonderen Anforderungen der Stationen.

Nachdem die Aufmerksamkeit einer Station gewonnen worden ist und diese zusagend antwortet, kann die Meldungsübermittlung beginnen. Die Meldung besteht aus einem oder mehreren Blöcken von Textdaten. Die Meldung wird in Textblöcken übermittelt, um eine genauere und wirksamere Fehlerkontrolle zu ermöglichen. Die Daten in einem Textblock werden durch einen Textanfang-Wortteil (STX) identifiziert. Zusätzlich folgt unmittelbar auf die Daten in jedem Textblock, ausser dem letzten, ein Übermittlungsblockende-Wortteil (ETB) oder ein Zwischenblock-Wortteil (ITB). Auf die Daten im letzten Textblock einer Meldung folgt unmittelbar ein Textende-Wortteil (ETX).

Wegen der weiten Verbreitung von mit hoher Geschwindigkeit arbeitenden, sehr genauen, zu verringerten Kosten erhältlichen Datenübertragungsanlagen in der modernen Gesellschaft ergeben sich ernste Probleme hinsichtlich der Sicherheit der übermittelten Textdaten. Die üblichen Transaktionen, die früher persönlich, telefonisch oder durch schriftliche Korrespondenz erledigt wurden, werden zunehmend mittels der neuen Datenübertragungsanlagen durchgeführt. Diese Anlagen sind anfällig für Abhören und Verfälschung. Eine Möglichkeit, Verfälschungen von über Datenverbindungen übermitteltem Datentext zu verhindern, besteht darin, Verschlüsselungssysteme anzuwenden. Verschlüsselungssysteme stellen Verfahren zur Verfügung, um Information derart zu verschlüsseln oder umzuformen, dass sie für diejenigen, für die die Information nicht zugänglich sein soll, unverständlich und daher nutzlos ist.

Das nationale amerikanische Normenbüro hat, da es für die Entwicklung von nationalen Informationsverarbeitungsnormen verantwortlich ist, der Allgemeinheit eine Datenverschlüsselungsnorm (DES) vorgeschlagen, die einen speziellen Algorithmus verwendet, welcher zu einem bestimmten und unzweideutigen Satz von Instruktionen führt. Der vom nationalen Normenbüro festgelegte Algorithmus der Datenverschlüsselungsnorm verwendet einen individuellen Parameter, welcher Schlüssel genannt wird. Der Algorithmus wurde von der International Business Machines Corporation (IBM) entwickelt. Die IBM stellte den Algorithmus dem nationalen Normenbüro als nationale Informationsverarbeitungsnorm zur Verfügung. Die IBM hat auch Lizenzierungsverfahren geschaffen für den Bau von elektronischen Geräten, die diesen Algorithmus ausführen. Der Algorithmus selbst wurde im amtlichen Register (Federal Register) im März 1975 veröffentlicht (40 FR 12007).

Der Algorithmus der Datenverschlüsselungsnorm (DES) und seine Funktion sind auch beschrieben in dem Artikel «Security of Computer Communication» in der Zeitschrift IEEE Communications Society Magazine, Band 16, Nr. 6, November 1978, Seiten 33 - 40. Ähnliche Verschlüsselungsverfahren sind ferner in den US-Patentschriften 4 160 120 und 4 203 166 beschrieben.

Der Zweck der Datenverschlüsselungsnorm besteht darin, ein Verschlüsselungsverfahren zur Verfügung zu stellen, welches empfindliche oder wertvolle Textdaten schützen kann, die über Computeranlagen und Datenverbindungsnetze übermittelt werden. Die Verwendung einer Vielzahl von verschiedenen Verschlüsselungs-Algorithmen würde dazu führen, dass die Datenübermittlungsausrüstungen grundsätzlich nicht kompatibel wären. Durch die Schaffung einer einzigen Datenverschlüsselungsnorm (DES) wird die nötige grundsätzliche Kompatibilität des Übermittlungsnetzes gewährleistet.

Der Algorithmus der Datenverschlüsselungsnorm ist im Grunde eine umlaufende Blockproduktchiffre der Blockgrösse 64, die auf einer Schlüssellänge von 64 Bits, einschliesslich acht Paritäts-Bits, basiert. Der Algorithmus ist in der Veröffentlichung des amerikanischen nationalen Normenbüros über die Informationsverarbeitungsnorm vollständig beschrieben. Alle Einzelheiten des Algorithmus sind öffentlich bekannt. Die Sicherheit der Textdaten in einer Anlage, die den Verschlüsselungs/Entschlüsselungs-Algorithmus verwendet, ist durch die Verwendung des Schlüssels gegeben, der von jeder Gruppe von berechtigten Benutzern einer gegebenen Fernmelde-Datenverbindung erzeugt wird. Dieser Schlüssel wird zufallsmässig erzeugt und nur an die berechtigten Benutzer verteilt. Der Schlüssel muss geschützt und geheimgehalten werden. Jede Gefährdung des Schlüssels gefährdet alle Daten und Mittel, die unter Verwendung dieses Schlüssels verschlüsselt werden.

Der Algorithmus der Datenverschlüsselungsnorm des nationalen Normenbüros beschreibt im Prinzip die Verschlüsselung von 64 Daten-Bits zu einer 64-Bit-Chiffre basierend auf einem 64-Bit-Schlüssel und die Entschlüsselung einer 64-Bit-Chiffre zu einem 64-Bit-Datenblock basierend auf dem gleichen 64-Bit-Schlüssel. Die Schritte und Tabellen des Algorithmus sind vollständig vorgeschrieben, und in dem Algorithmus selbst bleiben keine Wahlmöglichkeiten. Variationen bei der Ausführung und Verwendung des Algorithmus ermöglichen Flexibilität hinsichtlich seiner Anwendung an verschiedenen Stellen in einer Computeranlage oder in einem Übermittlungsnetz. Zu diesen Variationen gehört unter anderem, wie das Eingangssignal zusammengestellt ist, ob die Daten selbst oder eine andere Eingangssignalquelle für den Algorithmus verwendet wird, wie der Schlüssel erzeugt und verteilt wird, wie oft der Schlüssel gewechselt wird usw.

Die grundlegende Ausführung des Algorithmus kann am einfachsten mit Hilfe von für den speziellen Zweck konstruierten elektronischen Einrichtungen erfolgen. Er kann jedoch auch ausgeführt werden, indem die Durchführung des Algorithmus in einen Mikroprozessor einprogrammiert wird. In beiden Fällen liegt die Ausführung des Algorithmus ohne weiteres in den Möglichkeiten eines Fachmanns. Die insgesamt durch den Algorithmus geschaffene Sicherheit beruht auf zwei Grunderfordernissen: Geheimhaltung des Chiffrierschlüssels und zuverlässiges Funktionieren des Algorithmus.

Das nationale amerikanische Normenbüro beschreibt in der Veröffentlichung der vorgeschlagenen nationalen Normen Nr. 1026 und 1027 minimale Sicherheitsanforderungen, die bei der Ausführung der Datenverschlüsselungsnorm auf dem Fernmeldegebiet erfüllt werden müssen. Die genannte Veröffentlichung bzw. die nationalen Normen Nr. 1026 und 1027 stellen für die Ausführung der Datenverschlüsselungsnorm drei anerkannte Betriebsarten zur Verfügung, die in der ebenfalls vom nationalen amerikanischen Normenbüro herausgegebenen Veröffentlichung «Federal Information Processing Standards Publication 81» im einzelnen beschrieben sind.

Die Betriebsart mit Chiffre-Rückführung ist diejenige, die für die Verschlüsselung und Entschlüsselung von Daten für die Übermittlung und Fernmeldekanäle bestimmt ist. Im Prinzip sieht die Betriebsart mit Chiffre-Rückführung des Algorithmus der Datenverschlüsselungsnorm vor, dass als Eingangssignal für den Algorithmus nicht die Daten selbst verwendet werden, sondern statt dessen eine Reihe von Ausgangs-Daten, die zuvor durch den Chiffrier-Algorithmus erzeugt wurde. Die Betriebsart mit Chiffre-Rückführung beinhaltet in ihrer Auslegung ein Speichersystem. In irgend einem Zeitpunkt (t) hängt das Ausgangssignal von vorhergehenden Ausgangssignalen des Algorithmus ab. Die Arbeitsweise des Algorithmus kann als verkettete Arbeitsweise betrachtet werden. Der übermittelte chiffrierte Text ist in der Weise verkettet, dass jede Chiffre in irgend einem Zeitpunkt (t) von allen vorhergehenden Chiffren abhängig ist, die seit dem Start der Arbeit übermittelt worden sind.

Start der Arbeit bedeutet, dass ein 64-Bit-Eingangssignal (Start-Bitfolge) im Zeitpunkt (t) erzeugt wird und in das (Chiffrier-Algorithmus-) Eingangsregister des Senders eingespeichert wird. Von diesem Zeitpunkt an ist dann der ganze chiffrierte

Text von dieser anfänglichen Eingangsregister-Füllung abhängig.

Zum Füllen des Eingangsregisters im Empfänger muss beim Start der Arbeit eines von zwei Ereignissen eintreten. Entweder muss der Empfänger unabhängig die gleiche anfängliche Füllung erzeugen, oder der Sender muss genügend chiffrierten Text übermitteln, um das Eingangsregister des Empfängers mit dem gleichen chiffrierten Text zu füllen, wie er beim Start der Arbeit im Eingangsregister des Senders vorhanden war.

In der nationalen Norm Nr. 1027 hat das nationale amerikanische Normenbüro die Durchführung des Starts der Arbeit als die Verwendung einer Start-Bitfolge beschrieben, die eine Länge von wenigstens 48 Bits hat. Diese Start-Bitfolge wird dem Sender zugeführt und als Klartext unmittelbar vor jedem chiffrierten Meldungstext zum Empfänger übermittelt. Unter Anwendung des Synchron-Übermittlungsprotokolls wäre ein typischer Aufbau einer Datenmeldung der folgende:

SYN, STX, (TEXT), ETX, BCC

Eine verschlüsselte Datenmeldung, wie sie in der nationalen Informationsverarbeitungsnorm Nr. 46 beschrieben ist, wäre wie folgt aufgebaut:

SYN, STX, (IV), (TEXT), ETX, BCC

Die Start-Bitfolge (IV) würde eine Länge von 8 Bytes haben (jedes Byte zu 8 Bits) und offen übermittelt werden. Der Text ist verschlüsselt. Der Textende-Wortteil (ETX) ist ebenfalls verschlüsselt. Der Blockprüf-Wortteil (BCC) kann fakultativ verschlüsselt sein.

Der Textende-Wortteil ist verschlüsselt, weil der Empfänger, nachdem er begonnen hat, den empfangenen chiffrierten Text zu dechiffrieren, nicht feststellen kann, wann er den Dechiffrierprozess abbrechen soll, wenn er nicht den Textende-Wortteil dechiffriert. Wenn der Textende-Wortteil offen übermittelt würde, wäre es möglich, dass das Dechiffriergerät durch chiffrierte Wortteile inaktiviert werden könnte, die den offen übermittelten Textende-Wortteil imitieren könnten.

Wenn bei der durch die Norm des nationalen Normenbüros vorgeschlagenen Meldungsform in der Übermittlung des chiffriertenTextes ein Fehler auftritt, dann kann der Empfänger nicht mehr richtig entschlüsseln, weil die Verschlüsselungs-Synchronisation zwischen Sender und Empfänger verloren ginge. Wenn das geschieht, kann der Empfänger den Textende-Wortteil nicht erkennen und wird weiter entschlüsseln, solange Wortteile übermittelt werden.

In gewissen Datenverbindungsnetzen werden alle Übermittlungen unter Verwendung des Blockprüf-Wortteils (BCC) auf Fehler geprüft. Diese Prüfungen werden in Zwischen-Knotenstellen der Datenverbindung vorgenommen, die keinen Zugang zum geheimen Schlüssel haben. Weil in der vom nationalen Normenbüro vorgeschlagenen Meldungsform der Textende-Wortteil und fakultativ auch der Blockprüf-Wortteil verschlüsselt sind, wird die Prüfung auf Fehler unter Verwendung des Blockprüf-Wortteils in den Zwischen-Knotenstellen sehr umständlich.

In dem vom nationalen Normenbüro vorgeschlagenen Normformat ist die Start-Bitfolge (IV) nach dem Textanfang-Wortteil in den Bit-Strom der Datenmeldung eingefügt. Die Einfügung der Start-Bitfolge in die Meldungsform bewirkt eine Verzögerung um die Länge der Bitfolge, 6 Bytes. Diese Verzögerung verursacht eine Verringerung des Durchsatzes in einer Zweiweg-Übermittlung auf der Datenverbindung.

Die vorliegende Erfindung betrifft eine Datenübertragungsanlage nach dem Oberbegriff des Patentanspruchs 1.

Die Aufgabe der Erfindung besteht darin, diese Anlage so auszubilden, dass ohne Verringerung des Datendurchsatzes der Empfänger verbesserte Möglichkeiten für die Feststellung erhält, dass bei der Übermittlung des verschlüsselten Textes ein Fehler aufgetreten ist, und dass ferner eine Überprüfung der verschlüsselten Meldung auf Fehler in Zwischen-Knotenstellen einer Datenverbindung ohne Dechiffrierung der Meldung durchführbar ist.

Die Aufgabe wird in der erfindungsgemässen Anlage gelöst durch die im kennzeichnenden Teil des Patentanspruchs 1 angegebenen Mittel.

Im Betrieb der Anlage werden also die Start-Bitfolge sowie gegebenenfalls zusätzliche Informationsworte am Ende der Meldung angeordnet. Neben der Start-Bitfolge, die in der Regel eine Länge von wenigstens 6 Bytes hat, können Informationsworte (INF), Textende-Wortteile (ETX) und Blockprüf-Wortteile (BCC) am hinteren Ende der Normalform für die Synchron-Binärübermittlung nach der Meldung Textende und Blockprüfung angefügt werden. Die Informationsworte können Signalinformation zur Verwendung zwischen den Verschlüsselungs/Entschlüsselungs-Vorrichtungen, Abbruchzeichen (ABORT) und Folgenummern (SEQ) enthalten.

Nachstehend folgt eine Beschreibung einer bevorzugten Ausführungsform der Erfindung, die in den beiliegenden Zeichnungen dargestellt ist, in welchen gleiche Hinweisziffern in allen Figuren gleiche Teile bezeichnen und in welchen

Fig. 1 ein verallgemeinertes Blockschema einer Datenverbindung zwischen zwei Punkten ist, die einen Verschlüsselungs/Entschlüsselungs-Algorithmus verwendet,

Fig. 2 ein Blockschema einer Datenverbindung zwischen mehreren Punkten ist, die einen Verschlüsselungs/Entschlüsselungs-Algorithmus verwendet,

Fig. 3 ein Blockschema einer Datenverbindung mit mehreren Anschlüssen ist, in der nur ein Zweig der Datenverbindung einen Verschlüsselungs/Entschlüsselungs-Algorithmus verwendet,

Fig. 4 eine gekürzte Darstellung der Meldungsform für die Übermittlung zwischen einer Zentrale und einem Nebenterminal an einer Datenverbindung ist, die eine Synchron-Binärübermittlungs-Form verwendet,

Fig. 5 eine gekürzte Darstellung der Meldungsform für die Übermittlung zwischen einer Zentrale und einem Nebenterminal ist, in der eine Synchron-Binärübermittlungs-Form verwendet wird,

Fig. 6 eine gekürzte Darstellung der Meldungsform für die Übermittlung zwischen einer Zentrale und zwei Nebenterminals ist, wobei eine Synchron-Binärübermittlung angewandt wird und das zentrale Terminal die beiden Nebenterminals abfragt, um festzustellen, ob diese an die Zentrale übermitteln wollen,

Fig. 7 eine gekürzte Darstellung der Meldungsform für die Übermittlung in einer Datenverbindung ist, die eine Synchron-Binärübermittlung verwendet, wobei das zentrale Terminal mit mehreren Nebenterminals in Verbindung tritt, in dem es jeweils eines der Nebenterminals anwählt, um Meldungen an dasselbe zu senden,

Fig. 8 eine gekürzte Darstellung der vom nationalen amerikanischen Normenbüro vorgeschlagenen Meldungsform für eine verschlüsselte Meldung ist, die nach dem Algorithmus der Datenverschlüsselungsnorm des nationalen Normenbüros in der Betriebsart mit Chiffre-Rückführung verschlüsselt ist,

Fig. 9 eine gekürzte Darstellung einer Meldungsform ist, die in einer Datenverbindung verwendet werden kann, welche nach dem Synchron-Binärübermittlungsprotokoll arbeitet, wobei die Meldung nach dem Algorithmus der Datenverschlüsselungsnorm des nationalen Normenbüros in der Betriebsart mit Chiffre-Rückführung verschlüsselt wird, gemäss der vorliegenden Erfindung,

Fig. 10 eine Blockschemadarstellung der Einrichtungen ist, die im Sender für die Durchführung des erfindungsgemässen Chiffrierprozesses nach dem Algorithmus der Datenverschlüsse-

lungsnorm des nationalen Normenbüros mit Chiffre-Rückführung vorgesehen sind,

Fig. 11 eine Blockschemadarstellung der Einrichtungen ist, die im Empfänger für die Durchführung des erfindungsgemässen Dechiffrierprozesses nach dem Algorithmus der Datenverschlüsselungsnorm des nationalen Normenbüros vorgesehen sind,

Fig. 12 eine Fliessdiagrammdarstellung des Prozesses nach dem Algorithmus der Datenverschlüsselungsnorm des nationalen Normenbüros ist,

Fig. 13 eine Fliessdiagrammdarstellung des Prozesses der Kombinationsfunktion (F) ist, die für die Ausführung des Algorithmus der Datenverschlüsselungsnorm in Fig. 12 verwendet wird,

Fig. 14 eine Blockschemadarstellung von Einrichtungen ist, die im Sender für die Durchführung des erfindungsgemässen Chiffrierprozesses nach dem Algorithmus der Datenverschlüsselungsnorm des nationalen Normenbüros in einer Betriebsart mit Chiffre-Rückführung vorgesehen sind, in einer Datenverbindung zwischen mehreren Punkten, in der jedem Nebenterminal ein eigener Schlüssel zugeteilt ist,

Fig. 15 ein Fliessdiagramm ist, welches das Programm illustriert, das in einem Mikroprozessor der Verschlüsselungsvorrichtung verwendet wird, um die Regeln eines Textblockes zu verarbeiten, und zwar im Empfänger oder im Sender einer Datenverbindung, und

Fig. 16 einen Teil eines Fliessdiagramms zeigt, der zu dem Fliessdiagramm der Fig. 15 hinzugefügt werden kann und die Verarbeitung von zusätzlicher Signalinformation, neben dem Startvektor, im Empfänger und im Sender der Datenverbindung illustriert.

Es wird zunächst auf die Fig. 1 Bezug genommen, in der das grundlegende Konzept der gesicherten Kommunikation durch Übermittlung von chiffriertem Text dargestellt ist. Eine Terminal- oder Datenverbindung, bestehend aus einem Computer oder Terminal 21 an einem Ende und einem Terminal 29, das ein zweiter Computer, eine Anzeige mit Kathodenstrahlröhre usw. sein kann, am anderen Ende ist durch ein Übermittlungsmedium 25 verbunden. Am Ausgang des Computers empfängt eine Chiffriervorrichtung 23 die digitalen Daten von dem Computer 21. Die Chiffriervorrichtung 23 verschlüsselt die Daten, die sie empfängt, unter der Steuerung durch einen geheimen Schlüssel 33, der ihr zugeführt wird, und gemäss dem Verschlüsselungs-Algorithmus, von dem sie gesteuert ist. Der entstehende chiffrierte Text wird dann über das Übermittlungsmedium 25 zum Empfangsende, dem Terminal 29, übermittelt, wo er zunächst von einer Entschlüsselungsvorrichtung 27 empfangen wird. Der Entschlüsselungsvorrichtung 27 wird ebenfalls der geheime Schlüssel 33 zugeführt. Die Entschlüsselungsvorrichtung 27 dechiffriert den chiffrierten Text gemäss dem Dechiffrierungs-Algorithmus und dem zugeführten Schlüssel 33. Der dechiffrierte Text (Normaltext) wird dann dem Terminal 29 zur Verwendung zugeführt.

Der am Sendeort in der Verschlüsselungsvorrichtung 23 verwendete Schlüssel ist der gleiche Schlüssel, der auch am Empfangsort in der Entschlüsselungsvorrichtung 27 verwendet werden muss. Die Übermittlung des Schlüssels vom Sendeort zum Empfangsort der Datenverbindung kann in vielen verschiedenen Weisen erfolgen. Der Schlüssel kann von Hand transportiert werden oder über das Übermittlungsmedium übermittelt werden. Wenn der Schlüssel übermittelt wird, kann er für jede Meldung, die vom Sender zum Empfänger übermittelt wird, dynamisch geändert werden; er muss aber seinerseits mit einem Haupt-Schlüssel verschlüsselt werden, welcher nicht ändert.

Nun wird auf die Fig. 2 Bezug genommen, in der eine Datenverbindung zwischen mehreren Punkten dargestellt ist, wobei eine zentrale Station, enthaltend den Computer 21, ein Haupt-Datenschlüsselgerät 39 und das Haupt-Modem 41, mit mehreren Empfänger/Sender-Nebenstationen in Verbindung steht. Die zentrale Station, bestehend aus dem Computer 21, dem Haupt-Datenschlüsselgerät 39 und dem Haupt-Modem 41, leitet die Verbindung zwischen den Nebenterminals 29, 37 und 35 nach Anwähl- oder Abfrage-Regeln. Das Haupt-Datenschlüsselgerät 39, das gemäss der vorliegenden Erfindung zum Chiffrieren und Dechiffrieren in der Lage ist, hat die Fähigkeit, mehrere geheime Schlüssel zu speichern und zu verwenden, welche einzeln den verschiedenen Nebenterminals zugeteilt sind.

In der in Fig. 2 gezeigten Anlage würden dem Haupt-Datenschlüsselgerät 39 drei Schlüssel zur Verfügung stehen, einer für das Terminal 29, einer für das Terminal 37 und einer für das Terminal 35. Die Verwendung von Modems in einer Datenverbindung lässt erkennen, dass das Übermittlungsmedium 25 gemietete Telefonleitungen oder Leitungen, die dem Benutzer der Anlage abgegeben werden, oder das allgemeine Telefonnetz enthalten könnte.

Der Computer 21 stellt zusammen mit dem Modem 41 in der zentralen Station eine Zweiwegverbindung zu irgend einer der Nebenstationen in der Datenverbindungsanlage entweder nach einer Abfragetechnik oder nach einer Anwähltechnik her. Die Neben-Datenschlüsselgeräte 45, 47 und 53 unterscheiden sich vom Haupt-Datenschlüsselgerät 39 darin, dass das Haupt-Datenschlüsselgerät in der Lage ist, mehr als einen Chiffrier/Dechiffrier-Schlüssel zu speichern und zu verwenden, während die Neben-Datenschlüsselgeräte das nicht sind. Zudem ist das Haupt-Datenschlüsselgerät 39 auch in der Lage, neue Chiffrier-Schlüssel zu erzeugen, die über einen geeigneten Übermittlungsweg an die Neben-Datenschlüsselgeräte 45, 47, 53 übermittelt werden können. Die Modems 41, 43, 49 und 51 können irgendwelche aus einer Anzahl von Modems sein, die dem Fachmann bekannt sind. Sie würden ausgewählt auf der Grundlage der Kanäle 25, 55 und 57, die in der Datenverbindung zwischen mehreren Punkten verwendet werden. Der verwendete Kanal bestimmt weitgehend die Übermittlungsgeschwindigkeit der Daten, wobei die Terminals in der zentralen Station und den Nebenstationen ebenfalls einen wichtigen Faktor bilden.

Nun wird auf die Fig. 3 Bezug genommen, in der eine Datenverbindungsanlage zwischen mehreren Punkten dargestellt ist, in welcher nur ein Anschluss für die gesicherte Datenübermittlung eingerichtet ist, während die übrigen Anschlüsse lediglich Klartext übermitteln und empfangen können. Die Anlage gemäss Fig. 3 unterscheidet sich nicht grundsätzlich von der Anlage gemäss Fig. 2, mit der Ausnahme, dass im zentralen Datenschlüsselgerät 40, das mit einem Computer 21 und dem Haupt-Modem 41 in der zentralen Station angeordnet ist, nur ein Chiffrierschlüssel gespeichert ist, der für die Chiffrierung und Dechiffrierung von Meldungen verwendet wird, welche zwischen dem Computer 21 und dem Terminal 29, die zusammen den zu sichernden Teil der Datenverbindung ausmachen, übermittelt werden. Die anderen Nebenstationen, das Terminal 61 und das Terminal 59, die mit der zentralen Station über Übermittlungsmedien 55 bzw. 57 und Modems 51 bzw. 49 in Verbindung stehen, übermitteln und empfangen Daten im Klartext. Wenn der Computer 21 und das Modem 41 der zentralen Station mit den Terminals 59 und 61 in Verbindung stehen, weil der Sender/Empfänger der zentralen Station diese Nebenstationen abgefragt oder angewählt hat, ist das Haupt-Datenschlüsselgerät 40 im wesentlichen ausgeschaltet, so dass es seine Chiffrier- oder Dechiffrierfunktion nicht ausübt. Nur wenn die zentrale Station mit dem Nebenterminal 29 in Verbindung steht, übt das zentrale Datenschlüsselgerät 40 seine Chiffrierfunktion beim Übermitteln von Daten und seine Dechiffrierfunktion beim Empfangen von Daten vom Nebenterminal 29 aus.

Das Synchron-Binärübermittlungsprotokoll (BSC) ermöglicht die geordnete Leitung der Zweiweg-Übermittlung zwischen einer zentralen Station und einer Nebenstation in einer Daten-

verbindung zwischen zwei Punkten oder zwischen mehreren Punkten.

Die Fig. 4 zeigt eine Folge von Meldungsformen zwischen einer zentralen Station 63, welche Information an eine Nebenstation 65 zu übermitteln wünscht, die die Information empfangen soll. Wenn der zentrale Sender im Betrieb von Punkt zu Punkt oder zwischen mehreren Punkten eine Leitung belegen will, dann sendet er einen Steuerblock 67, welcher aus Synchron-Wortteilen und einem Anfrage-Wortteil besteht. Die Synchron-Wortteile sind mit (SYN) bezeichnet, und die Anfrage ist mit (ENQ) bezeichnet. In der Regel wird der Wortteil (ENQ) verwendet, um in einer Leitungsverbindung von Punkt zu Punkt die Leitung zu belegen. In einer Leitungsverbindung zwischen mehreren Punkten wird er verwendet, um das Ende einer Abfrage- oder Anwählfolge anzuzeigen. Das Nebenterminal antwortet auf den Wortteil (ENQ), indem es an die Zentrale einen Steuerblock übermittelt, welcher aus Wortteilen (SYN) und Bestätigungs-Wortteilen (ACK0) besteht. Der Wortteil (ACK0) ist eine positive Antwort auf eine Anwahl durch die Zentrale in einer Anlage zwischen mehreren Punkten oder auf eine Leitungsbelegung durch die Zentrale in einer Anlage zwischen zwei Punkten. Die Bestätigungs-Antwort zeigt an, dass der Empfänger für den Empfang eines Blocks von Daten bereit ist.

Dementsprechend wird die zentrale Einheit einen Datentextblock 69 übermitteln, welcher aus Synchron-Wortteilen (SYN), Textanfang-Wortteilen (STX), dem Text, Textblockende-Wortteilen (ETB) und Blockprüf-Wortteilen (BCC) besteht. Das empfangene Nebenterminal 65 sucht nach dem Empfang der Wortteile (ETB) die Wortteile (BCC) und verwendet sie dazu, die übermittelten Daten dieses Textblockes auf Fehler zu überprüfen. Wenn keine Fehler vorkommen, antwortet der Nebenempfänger 65, indem er einen Steuerblock 73 an den zentralen Sender zurücksendet, welcher Steuerblock aus Wortteilen (SYN) und Bestätigungs-Wortteilen (ACK1) besteht. Die Wortteile (ACK1) zeigen dem zentralen Sender an, dass der vorangegangene Block von Textdaten ohne Fehler empfangen worden ist und dass der nächste Block von Textdaten übermittelt werden kann. Dementsprechend würde die Zentrale, wenn sie noch weitere Daten zu übermitteln hat, wieder mit einem Textblock ähnlich dem Textblock 69 beginnen, der mit Synchron-Wortteilen (SYN) 75 anfängt.

Nun wird auf die Fig. 5 Bezug genommen, in der die Meldungsformen für eine begrenzte Konversation in einer Übermittlung zwischen einer Zentrale und einem Nebenterminal dargestellt sind. Das zentrale übermittelnde Terminal würde in einer Anlage zwischen zwei Punkten die Leitung belegen durch Aussenden eines Steuerblockes 81, welcher aus Wortteilen (SYN) und Wortteilen (ENQ) besteht. Die Antwort vom Nebenterminal wäre ein Steuerblock 83, der aus Wortteilen (SYN) und Wortteilen (ACK0) besteht. Nach dem Empfang der Wortteile (ACK0) würde die Zentrale ihren Meldungsblock übermitteln, der aus Wortteilen (SYN), Wortteilen (STX), Text und, wenn das alles war, was die Zentrale übermitteln wollte, Textende-Wortteilen (ETX) und Wortteilen (BCC) besteht. Nach dem Empfang der Wortteile (ETX) und (BCC) kann die Nebenstation, wenn sie Daten an die Zentrale übermitteln will, mit einem Textblock 87 statt mit dem in Fig. 4 gezeigten (ACK1)-Steuerblock antworten.

Die Konversations-Antwort der Nebenstation 79 an die Zentrale 77 erfolgt durch Übermittlung eines Textblockes 87 an die Zentrale. Der Textblock besteht aus den Wortteilen (SYN), Wortteilen (STX), Text, Daten, Wortteilen (ETX) und Wortteilen (BCC). Die Zentrale würde auf den Empfang dieses Textblockes reagieren, indem sie die empfangenen Daten auf Fehler überprüft. Wenn keine Fehler vorkommen, würde die Zentrale einen Steuerblock 89 an die Nebenstation 79 übermitteln, bestehend aus Wortteilen (SYN) und Wortteilen (ACK1).

Nun wird auf die Fig. 6 Bezug genommen, in der die Formen des Meldungsverkehrs im Betrieb zwischen mehreren Punkten dargestellt ist, wenn eine zentrale Station zwei verschiedene Nebenstationen abfragt. Man wird sich erinnern, dass in der Abfrage-Betriebsart die zentrale Station eine Reihe von Nebenterminals fragt, ob sie Daten an das zentrale Terminal zu übermitteln wünschen. In Fig. 6 ist ein zentrales Terminal 91 dargestellt, das mit einer Nebenstation A, Terminal 93, und einer Nebenstation B, Terminal 95, in Verbindung steht.

Zum Beginn der Abfolge sendet das zentrale Terminal 91 einen Auslöse-Steuerblock 97 aus, bestehend aus Puffer-Wortteilen (PAD), Wortteilen (SYN), Übermittlungsende-Wortteilen (EOT), einem weiteren Wortteil (PAD), einem Wortteil (SYN), mehreren Stations-Identifizierungs-Wortteilen (A) für die Station (A) und einem Wortteil (6) zur Identifizierung einer speziellen Ausrüstung, beispielsweise eines Lesers, Wortteilen (ENQ) und einem weiteren Wortteil (PAD). Der Wortteil (EOT) dient zum Rückstellen aller Nebenstationen an der Leitung. Der Wortteil (ENQ) wird verwendet, um das Ende einer Abfrage-Folge anzuzeigen. Die Wortteile (PAD), die aus einer Reihe von lauter binären 1 bestehen können, gewährleisten vollständige Übermittlung und Empfang der ersten oder letzten bedeutungsvollen Bits des vorhergehenden Wortteils. Die Wortteile (SYN) sollen lediglich dafür sorgen, dass die Empfangsstationen im Takt mit den Sendestationen arbeiten.

Da der die Abfolge auslösende Block 97 die Adresse des Nebenterminals A enthält, antwortet das Terminal A mit einem Steuerblock 99, welcher Wortteile (PAD), Wortteile (SYN), Wortteile (EOT) und einen anderen Wortteil (PAD) enthält. Diese Antwort zeigt an, dass das Terminal A nichts zu übermitteln hat. Während der Zeit, in der das Nebenterminal A den Steuerblock 99 an die Zentrale übermittelt, muss das zentrale Terminal auf den Empfang der Antwort vom Nebenterminal warten. Während dieser Zeit werden daher gemäss der BiSynch-Form keine Daten übermittelt.

Nach dem Empfang der Antwort 99 von der Nebenstation A wird sich dann das erste zentrale Terminal in der gleichen Weise an die Nebenstation B wenden, wobei es jedoch die Reihe der Wortteile (PAD) und (SYN) und (EOT) nicht wie vorher auszusenden braucht, da die ganze Anlage schon vorbereitet ist. Für das Aufrufen der Nebenstation B wird das zentrale Terminal daher den Block 101 aussenden, der aus Wortteilen (PAD), Wortteilen (SYN), einigen Wortteilen (B) mit der Adresse der Nebenstation B, einem Wortteil (6) mit der Adresse des Lesers, Wortteilen (ENQ) und einem weiteren Wortteil (PAD) besteht. Die Nebenstation B, 95, antwortet mit einem Textblock 103, welcher Wortteile (PAD), Wortteile (SYN), einen Vorspannanfang-Wortteil (SOH), der anzeigt, dass ein Vorspann-Wortteil folgt, und einen Vorspann-Wortteil (HEAD) enthält. Ein Vorspann-Wortteil enthält Hilfsinformationen, z.B. Leitinformationen, oder Vorranginformationen, die in der Zentrale für die Verarbeitung des übermittelten Textes benutzt werden. Nach dem Vorspann-Wortteil bzw. -Wortteilen folgen ein Textanfang-Wortteil, der Text, Übermittlungsblockende-Wortteile (ETB), ein Wortteil (BCC) und ein Wortteil (PAD).

Als Reaktion auf den Empfang eines Textblockes 103 erzeugt die Zentrale 91 einen Steuerblock 105, welcher Wortteile (PAD), Wortteile (SYN), Wortteile (ACK1) und einen weiteren Wortteil (PAD) enthält. Der Wortteil (ACK1) zeigt lediglich an, dass die Textinformation ohne Fehler empfangen worden ist. Das Terminal 95 der Nebenstation B wünscht möglicherweise, noch fortzufahren und einen weiteren Datenblock zu übermitteln; es würde das tun durch Erzeugen eines Textblockes 107, welcher Wortteile (PAD), Wortteile (SYN), Wortteile (STX), den Text, Wortteile (ETX), einen Wortteil (BCC) und einen Wortteil (PAD) enthalten kann. Wie ersichtlich ist, werden der Vorspannanfang-Wortteil und der Vorspann-Wortteil im zwei-

ten Block 107 nicht verwendet, da die Zentrale schon weiss, was sie mit dem empfangenen Text zu tun hat.

Da ein Textende-Wortteil (ETX) übermittelt worden ist, weiss die Zentrale, dass das das Ende der Textübermittlung ist. Das zentrale Terminal 91 würde dann mit einem Steuerblock 109 antworten, der den fehlerfreien Empfang des Textes von der Nebenstation B anzeigt. Der Steuerblock 109 würde Wortteile (PAD), Wortteile (SYN), einen Wortteil (ACK0) und einen weiteren Wortteil (PAD) enthalten. Als Antwort auf diesen Block würde die Nebenstation B 95 einen Steuerblock 111 erzeugen, welcher Wortteile (PAD), Wortteile (SYN), einen Übermittlungsende-Wortteil (EOT) und einen weiteren Wortteil (PAD) enthält. Der Übermittlungsende-Wortteil (EOT) im Block 111, der von der Nebenstation B 95 an das zentrale Terminal 91 gesandt wird, zeigt an, dass die Nebenstation B nichts weiter zu senden hat.

Dementsprechend beginnt das zentrale Terminal 91 seine Abfrage-Folge von neuem und sendet einen Block 113 aus, welcher ein Auslöse-Block ist und mit dem Block 97 identisch ist. Wenn die Nebenstation A 93 noch immer nichts an das zentrale Terminal zu senden hat, sendet sie als Antwort wieder einen Steuerblock 115, welcher Wortteile (PAD), Wortteile (SYN), einen Wortteil (EOT) und einen weiteren Wortteil (PAD) enthält. Das zentrale Terminal 91 sendet dann wieder einen Abfrage-Block 117 an die Nebenstation B 95, welcher mit dem Abfrage-Block 101 identisch ist.

Die Fig. 7 zeigt die Formen des Meldungsverkehrs zwischen einer Zentrale und zwei Nebenstationen 123 und 125 in einer Anwähl-Folge. Die Anwähl-Folge ist, wie man sich erinnern wird, eine Folge, mit der sich das zentrale Terminal 121 bei den Nebenterminals 123 und 125 in der Datenverbindung erkundigt, ob sie in der Lage sind, Daten von der Zentrale zu empfangen. Zum Beginnen der Folge sendet das zentrale Terminal 121 einen Auslöse-Block 127, welcher Wortteile (SYN), Wortteile (EOT), einen Wortteil (PAD), einen weiteren Wortteil (SYN), zwei Wortteile (a) zur Identifizierung der Nebenstation, einen Wortteil (1) zur Identifizierung einer Ausrüstung im Terminal, beispielsweise eines Druckers, einen Wortteil (ENQ) und einen weiteren Wortteil (PAD) enthalten kann.

Da das Terminal 123 der Nebenstation A angesprochen wurde, würde die Nebenstation A mit einem Steuerblock 129 antworten, welcher Wortteile (PAD), Wortteile (SYN), einen negativen Bestätigungs-Wortteil (NAK) und einen weiteren Wortteil (PAD) enthalten kann. Der Wortteil (NAK) zeigt dem zentralen Terminal an, dass die Nebenstation A nicht für den Empfang von Text vom zentralen Terminal 121 bereit ist.

Das zentrale Terminal kann sich dann bei der Nebenstation B erkundigen, indem es einen Steuerblock 131 sendet, welcher Wortteile (SYN), Wortteile (EO), einen Wortteil (PAD), einen weiteren Wortteil (SYN), mehrere Wortteile (b) mit der Adresse der Nebenstation, einen Wortteil (1) zur Identifizierung einer Ausrüstung im Terminal, einen Wortteil (ENQ) und einen weiteren Wortteil (PAD) enthalten würde. Da die Nebenstation B 125 angesprochen wurde, antwortet diese mit einem Steuerblock 133, welcher Wortteile (PAD), Wortteile (SYN), einen Wortteil (ACK0) und einen weiteren Wortteil (PAD) enthält. Der Wortteil (ACK0) ist eine positive Bestätigung, die dem zentralen Terminal 121 anzeigt, dass die Nebenstation B für den Empfang von Text vom zentralen Terminal bereit ist. Als Antwort auf den Steuerblock 133 würde das zentrale Terminal 121 seine Daten in einem Textblock 135 übermitteln, welcher Wortteile (PAD), Wortteile (SYN), einen Wortteil (STX), Text, einen Wortteil (ETX), einen Wortteil (BCC) und einen Wortteil (PAD) enthalten würde.

Nach dem Empfang des Blockes 135, und wenn in der Übermittlung keine Fehler aufgetreten sind, was von der empfangenen Nebenstation B unter Verwendung der Blockprüf-Wortteile geprüft wird, würde die Nebenstation durch Aussenden eines Steuerblockes 137 an die Zentrale antworten. Der Steuerblock 137 würde Wortteile (PAD), Wortteile (SYN), einen Wortteil (ACK1) und einen weiteren Wortteil (PAD) enthalten. Der Wortteil (ACK1) zeigt an, dass der zuvor übermittelte Textblock ohne Fehler empfangen worden ist. Als Antwort auf den Block 137 würde das zentrale Terminal 121 einen Steuerblock 139 übermitteln, welcher aus Wortteilen (PAD), Wortteilen (SYN), einem Wortteil (ETX) und einem weiteren Wortteil (PAD) bestehen würde und dem Terminal 125 der Nebenstation B anzeigen würde, dass die Zentrale keine weiteren Daten übermitteln will.

Die vorstehende Erläuterung von Meldungsformen in der Zweiweg-Synchron-Binärübermittlung gilt für Datenverbindungen zwischen zwei Punkten und zwischen mehreren Punkten. Wenn der in solchen Datenverbindungen zu übermittelnde Text geheim bleiben soll, muss er verschlüsselt werden. Wenn die Verschlüsselung gemäss dem Algorithmus nach der Datenverschlüsselungsnorm des nationalen Normenbüros der USA in der Betriebsart mit Chiffre-Rückführung erfolgen soll, dann muss, gemäss Fig. 8, die vom nationalen Normenbüro vorgeschlagene Datenblockform für einen Textblock 141 verwendet werden. Der Datenblock 141 besteht aus Wortteilen (SYN) 143, Wortteilen (STX) 145, einer Start-Bitfolge (IV) 147, die einen Umfang von 6 bis 8 Bytes hat, wobei in der Synchron-Binärübermittlung jedes Byte 8 Bits umfasst, einem Textblock 149, der verschlüsselt ist, einem Wortteil (ETX) 155, der ebenfalls verschlüsselt ist, und einem Blockprüf-Wortteil (BCC) 153, der verschlüsselt sein kann oder offen übermittelt werden kann.

Die Start-Bitfolge 147 wird im Empfänger der Nebenstation dazu verwendet, den Dechiffrierprozess zu starten, so dass die im Text 141 übermittelten Text-Wortteile 149 richtig dechiffriert werden können, wie im Nachstehenden eingehender erläutert wird. Der Algorithmus der Datenverschlüsselungsnorm, in der Betriebsart mit Chiffre-Rückführung, erfordert, dass der Chiffrier-Algorithmus und der Dechiffrier-Algorithmus vom genau gleichen Ausgangszustand ausgehen. Die Start-Bitfolge 147 wird daher dazu verwendet, den Chiffrierprozess zu starten, der in dem sendenden zentralen Terminal zu dem chiffrierten Text 149 führt.

Die gleiche Start-Bitfolge wird dann zwischen dem Wortteil (STX) 145 und dem chiffrierten Text 149 in den chiffrierten Textblock 141 gegeben, so dass er vom empfangenen Nebenterminal empfangen werden kann, bevor der chiffrierte Text 149 empfangen wird, um den Dechiffrier-Algorithmus der Datenverschlüsselungsnorm in der Nebenstation in Vorbereitung für die Dechiffrierung des chiffrierten Textes 149 zu starten. Aus der in Fig. 8 dargestellten Form des chiffrierten Textes 141 ist zu ersehen, dass durch die Einschliessung der Start-Bitfolge 147 zwischen dem Wortteil (STX) 145 und dem chiffrierten Text 149 des Textblockes der Durchsatz der Datenverbindung um die Länge der Start-Bitfolge 147 verringert wird.

Beim Betrachten der Meldungsformen für den Verkehr in Anlagen zwischen zwei Punkten und zwischen mehreren Punkten, wie sie in den Fig. 4, 5, 6 und 7 dargestellt sind, kann festgestellt werden, dass nach der Synchron-Binärübermittlungs-Regel eine beträchtliche Zeitspanne zwischen Meldungen beim Richtungswechsel vorhanden ist. Richtungswechsel treten ständig auf, weil bei der Synchron-Binärübermittlung eine Rückantwort von einem Terminal sowohl beim Abfragen als auch beim Anwählen oder im Dialog erforderlich ist, bevor wieder in der gleichen Richtung übermittelt werden kann.

Die vorliegende Erfindung nutzt diese Verzögerung zwischen Meldungen in derselben Richtung aus, indem sie die Start-Bitfolge sowie zusätzliche Steuerinformation am hinteren Ende eines Textblockes anordnet, wie es in Fig. 9 mit einem Textblock 155 dargestellt ist. Eine solche Meldungsform, gemäss der vorliegenden Erfindung und unter Verwendung der Synchron-Binärübermittlungs-Kriterien, würde Wortteile (SYN)

157 enthalten, gefolgt von Wortteilen (STX) 159, dem Text 161, Wortteilen (ETX) 163, Wortteilen (BCC) 165, Wortteilen (INF) 167, dem Startvektor 169, einem zweiten Textende-Wortteil (ETX') 171 und einem zweiten Blockprüf-Wortteil (BCC') 173.

Die Text-Wortteile 161, der Textende-Wortteil 163 und die Blockprüf-Wortteile 165 des Textblockes 155 wären nach dem Algorithmus der Datenverschlüsselungsnorm mit Chiffre-Rückführung verschlüsselt. Die nachfolgenden Steuer-Wortteile, wie der Wortteil (INF) 167, die Start-Bitfolge 169, der zweite Wortteil (ETX') 171 und der zweite Wortteil (BCC') 173, würden offen übermittelt, ebenso wie die Wortteile (SYN) 157 und die Wortteile (STX) 159, mit denen der Meldungsblock 155 beginnt.

Wie in Verbindung mit der in Fig. 8 dargestellten verschlüsselten Meldungsform erläutert worden ist, erfordert die Anwendung des Algorithmus der Datenverschlüsselungsnorm in der Betriebsart mit Chiffre-Rückführung, dass das übermittelnde Terminal eine Start-Bitfolge an das empfangene Terminal sendet. Vor dem Empfang des chiffrierten Textes im empfangenden Terminal wird die Start-Bitfolge dazu verwendet, den Zustand des Chiffrier-Algorithmus im Empfänger in den gleichen Zustand zu bringen, in dem der Chiffrier-Algorithmus im Sender in dem Zeitpunkt war, als mit der Verschlüsselung des zu übermittelnden chiffrierten Textes begonnen wurde. Dies ist der Grund dafür, dass im chiffrierten Textblock gemäss Fig. 8 die Start-Bitfolge in dem Block unmittelbar vor den Text-Wortteilen erscheinend dargestellt ist.

Im chiffrierten Textblock 155 gemäss der vorliegenden Erfindung sind die Start-Bitfolge 169 sowie zusätzliche Informationen, Textende- und Blockprüf-Wortteile am hinteren Ende des chiffrierten Textblockes angeordnet. Die vorliegende Erfindung setzt voraus, dass der dechiffrierende Empfänger die zu Beginn einer Meldungsübermittlung vorhandene Start-Bitfolge schon mit einem vorangehenden chiffrierten Textblock erhält und dann diese Start-Bitfolge zum Starten seines Chiffrier-Algorithmus in Vorbereitung für den Empfang des nächsten Textblockes verwendet.

Es wird somit, bezugnehmend auf Fig. 9, angenommen, dass der chiffrierte Textblock 155 der zweite Textblock einer Reihe ist. Wenn das der Fall ist, dann wird die Start-Bitfolge 169 am hinteren Ende des Textblockes 155 vom Chiffrier-Algorithmus im Empfänger dazu verwendet, den Algorithmus für den chiffrierten Textblock (nicht dargestellt) zu starten, der auf den chiffrierten Textblock 155 folgen wird. Es erübrigt sich, zu sagen, dass ganz zu Beginn der Datenübermittlung, sowohl in einer Abfrage-Betriebsart als auch in einer Anwähl-Betriebsart in einer Anlage mit mehreren Betriebsarten, das zentrale Terminal mit der Übermittlung des Auslöse-Steuerblockes auch die erste Start-Bitfolge übermitteln könnte. Alle nachfolgenden Start-Bitfolgen werden dann während der Zeit übermittelt, in der ein Nebenterminal der Zentrale antwortet, wodurch die Durchsatz-Leistungsfähigkeit der Anlage, im Vergleich zu der in Fig. 8 gezeigten bekannten Meldungsform von chiffrierten Texten, beträchtlich erhöht wird.

In gewissen Datenverbindungen zwischen mehreren Punkten werden Zwischen-Knotenstellen verwendet. Eine solche Anlage ist zwar in den Zeichnungen nicht dargestellt, kann jedoch einfach als eine Reihe von Empfangs- und Sendestellen entlang dem Übermittlungsmedium zwischen dem Sender des chiffrierten Textblockes und dem Empfänger des chiffriertenTextblockes beschrieben werden. In vielen solchen Anlagen sind diese Zwischen-Knotenstellen dazu eingerichtet, den übermittelten Text unter Verwendung der Blockprüf-Wortteile (BCC), die den Textende- oder Übermittlungsblockende-Wortteilen folgen, auf Übermittlungsfehler zu überprüfen. Der chiffrierte Textblock gemäss Fig. 8 würde es den Zwischen-Knotenstellen nicht ermöglichen, eine solche Funktion auszuüben, weil die Wortteile (ETX) verschlüsselt sind und die Wortteile (BCC) aus Sicherheitsgründen vorzugsweise ebenfalls verschlüsselt sind. Die Zwischen-Knotenstellen haben keinen Zugang zum Schlüssel und sind auch nicht in der Lage, einen Dechiffrierprozess durchzuführen, selbst wenn ihnen der Schlüssel zur Verfügung stehen würde. Die Überprüfung auf Übermittlungsfehler in diesen Zwischen-Knotenstellen ist daher recht schwierig und umständlich.

Die vorliegende Erfindung zieht die Übermittlung eines zusätzlichen Textende-Blockprüf-Wortteils nach der Start-Bitfolge 169 des chiffrierten Textblockes 155 in Betracht. Der zweite Textende-Wortteil (ETX') 171 und der zweite Blockprüf-Wortteil (BCC') 173 werden offen übermittelt. Der Blockprüf-Wortteil (BCC') 173 ist an die verschlüsselte Version des Textblockes 155 gebunden, welche den chiffrierten Text 161, den chiffrierten Wortteil (ETX) 163, den chiffrierten Wortteil (BCC) 165 sowie den offenen Wortteil (PAD) 167, wenn vorhanden, und die offene Start-Bitfolge 169 enthält. Daher kann die ganze Reihe von verschlüsselten und offenen Wortteilen in den Zwischen-Knotenstellen eines Netzes mit mehreren Knotenstellen auf Übermittlungsfehler überprüft werden. Die Zwischen-Knotenstellen können einen empfangenen Meldungsblock auf Übermittlungsfehler prüfen, ohne den chiffrierten Text dechiffrieren zu müssen. Das kann auch im Endempfänger geschehen, der die Fähigkeit hat, den chiffrierten Text sowie den Blockprüf-Wortteil 165, der ebenfalls chiffriert ist, zu dechiffrieren.

Die Wortteile (INF) 167 des chiffrierten Textblockes 155 gemäss vorliegender Erfindung können irgend einen aus einer Reihe von Wortteilen enthalten, die wie folgt dargestellt wird:

(INF) ⇆ (SEQ) (ABORT) (SIG)

Die Wortteile (INF) könnten also Folgenummern (SEQ) sein, die lediglich eine zusätzliche Zahl, einen oder zwei Wortteile lang, darstellen, welche verschlüsselt ist. Der Empfänger dechiffriert die Folgenummer (SEQ) und stellt sicher, dass die Folge der aus mehreren Blöcken bestehenden Meldung in Ordnung ist. So würde für den ersten chiffrierten Textblock einer Reihe die Folgenummer angeben, dass das der erste chiffrierte Textblock ist. Die Verwendung der Folgenummer, wie sie von der vorliegenden Erfindung in Betracht gezogen wird, erleichtert die Feststellung von Störungen durch Aufzeichnung und erneute Wiedergabe. Störungen durch Aufzeichnung und erneute Wiedergabe entstehen durch Verwendung eines Bandaufzeichnungsgerätes zum unberechtigten Wiederholen der empfangenen verschlüsselten Meldungen und Zuführen derselben zu der mit Chiffre-Rückführung arbeitenden Entschlüsselungsvorrichtung. Wenn der Schlüssel nicht geändert worden ist, wird der Empfänger die Meldungen richtig entschlüsseln und für gewisse Operationen, z.B. betreffend Kapitalien, Depositengelder, Warenbestellungen usw., verwenden. Dies würde katastrophale Folgen haben, indem beispielsweise zwei Bestellungen oder zwei Depositenanordnungen statt einer im entschlüsselnden Empfänger empfangen werden.

Die Verwendung des Abbruchzeichens (ABORT) im chiffriertenTextblock 155 gemäss vorliegender Erfindung ist sehr vorteilhaft. Das Abbruchzeichen (ABORT) in der Stellung der Wortteile (INF) 157 des chiffrierten Textblockes 155 kann offen übermittelt werden. Wenn ein Übermittlungsfehler im chiffrierten Text aufgetreten ist, kann die empfangene Entschlüsselungsvorrichtung den Textende-Wortteil 163 nicht erkennen und würde normalerweise weiter alle nachfolgenden Wortteile entschlüsseln oder zu entschlüsseln versuchen. Bei Verwendung eines Abbruchzeichens (ABORT) in der Stellung des Wortteils (INF) 167 des chiffrierten Textblockes 155 würde der Empfänger das Abbruchzeichen (ABORT) erkennen, das dem Empfänger das Auftreten eines Übermittlungsfehlers anzeigt, so dass der Empfänger den Dechiffrierprozess stoppen kann.

In einer Datenverbindungsanlage zwischen mehreren Punkten kann das Abbruchzeichen (ABORT) auch dazu dienen, das Ende einer Meldung für diejenigen Terminal-Einheiten in der Verbindung anzuzeigen, die nicht den richtigen Schlüssel besitzen. Wenn mit anderen Worten das zentrale Sender/Empfänger-Terminal eine Nebenstation A anspricht und dabei den Schlüssel von A verwendet, dann könnten beispielsweise die Nebenstationen B und C, welche versuchen, einen chiffrierten Text zu dechiffrieren, der gemäss dem Schlüssel A verschlüsselt wurde, diesen chiffrierten Text unter Verwendung ihrer Schlüssel B und C nicht korrekt dechiffrieren, so dass sie den Textende-Wortteil 163 nicht erkennen würden. Dementsprechend würde das Fehlen der Feststellung des Textende-Wortteils 163 vor dem Auftreten des Abbruchzeichens (ABORT) in der Stellung 167 des chiffrierten Textblockes 155 anzeigen, dass die Meldung nicht für diese besonderen Empfänger-Terminals bestimmt war.

Die Signalinformation (SIG) in (INF) könnte irgendeine Information darstellen, die der Sender dem Empfänger mitteilen will, z.B. eine diagnostische Information oder neue Schlüssel.

Gemäss der Darstellung in den Fig. 2 und 3 sind für die Übermittlung von chiffriertem Text von einem Ende einer Datenverbindung zu einem anderen zwei Verschlüsselungs/Entschlüsselungs-Vorrichtungen erforderlich. Diese Verschlüsselungs/Entschlüsselungs-Vorrichtungen können entweder von zugeordneten spezialisierten Schaltungen gebildet werden oder von Einrichtungen mit Mikroprozessoren, welche nach eingebauten Instruktionen für die Durchführung des Verschlüsselungs/Entschlüsselungs-Algorithmus und nach Programminstruktionen für das Bilden von Textblöcken oder Antworten auf Textblöcke arbeiten, entsprechend dem verwendeten Protokoll, z.B. dem in diesem Text beschriebenen Synchron-Binärübermittlungsprotokoll.

Die bevorzugte Ausführungsform der vorliegenden Erfindung ist ein Mikroprozessor, der festprogrammiert ist, um den Chiffrier/Dechiffrier-Algorithmus nach der Datenverschlüsselungsnorm durchzuführen, und programmierbar ist, um die chiffrierten Textblöcke in der erfindungsgemässen Form gemäss Fig. 9 zu formen. In einer solchen Einrichtung wird der Chiffrier/Dechiffrier-Algorithmus tatsächlich als Unter-Routine zum Steuerprogramm durchgeführt, das die Übermittlung und den Empfang der chiffrierten Textblöcke 155 leitet.

Fig. 10 zeigt die im Sender angewandte Chiffrier-Routine für den Algorithmus der Datenverschlüsselungsnorm in der Betriebsart mit Chiffre-Rückführung. Fig. 11 zeigt die Dechiffrier-Routine, die im Empfänger durchgeführt würde.

Zuerst wird auf die Verschlüsselung von Daten Bezug genommen, die von einem übermittelnden Terminal erhalten werden (Fig. 10). Der Klartext würde von dem Terminal (nicht dargestellt) über eine 8-Bit-Parallelleitung 175 einem Exklusiv-ODER-Tor 177 mit 16-Bit-Eingang zugeführt, das auch an den Ausgang eines Ausgangspuffers 189 angeschlossen ist. Die resultierenden 8 Bits auf einer Leitung 179 bilden den chiffrierten Text, welcher für die Übermittlung einem Modem (nicht dargestellt) zugeführt wird. Dieses resultierende Ausgangssignal wird zusätzlich auch zu einem Eingangspuffer 181 rückgeführt. Dieser Rückführungsprozess wird fortgesetzt, bis der Eingangspuffer, der ein 64-Bit-Puffer ist, vollständig gefüllt ist. In diesem Zeitpunkt wird das Ausgangssignal des Puffers 181 dem Verschlüsselungs-Eingangsregister 183 zugeführt. Der Inhalt des Verschlüsselungs-Eingangsregisters wird als 64-Bit-Parallelwort dem Verschlüsselungs-Algorithmus 185 zugeführt, der im Nachstehenden erläutert ist. Nachdem der resultierende Chiffrierprozess durchgeführt ist, wird das resultierende 64-Bit-Wort dem Verschlüsselungs-Ausgangsregister 187 zugeführt. Ein Ausgangspuffer 189 entnimmt den Inhalt des Verschlüsselungs-Ausgangsregisters 187 und führt diesen sequentiell in 8-Bit-Bytes dem Exklusiv-ODER-Tor 177 zu.

Der in der Verschlüsselungsfunktion 185 durchgeführte Verschlüsselungsprozess wird von einem 64-Bit-Schlüssel gesteuert, der dem Verschlüsselungs-Algorithmus 185 von dem Schlüsselregister 193 zugeführt wird.

Der Dechiffrierprozess ist eine exakte Wiederholung des Chiffrierprozesses, wie aus Fig. 11 ersichtlich ist. Der einzige Unterschied besteht darin, dass der Prozess vom chiffrierten Text ausgeht statt vom Klartext. Der chiffrierte Text wird von einem Modem (nicht dargestellt) in einer 8-Bit-Form über eine Leitung 195 einem Exklusiv-ODER-Tor 197 sowie einem Eingangspuffer 201 als Eingangssignal zugeführt. Der Eingangspuffer 201 ist ein 64-Bit-Puffer, der mit 8-Bit-Bytes gefüllt wird. Wenn er ganz gefüllt ist, wird der Inhalt des Eingangspuffers 201 dem Verschlüsselungs-Register 203 zugeführt. Wenn der Chiffrierprozess beginnen soll, wird der Inhalt des Verschlüsselungs-Eingangsregisters 203 dem Chiffrier-Algorithmus 207 zugeführt, der den erhaltenen chiffrierten Text unter der Steuerung durch den Schlüssel, welcher von einem Schlüsselregister 209 geliefert wird, bearbeitet, um ein 64-Bit-Wort an ein Verschlüsselungs-Ausgangsregister 211 abzugeben. Der Inhalt des Ausgangsregisters 211 wird durch einen Ausgangspuffer 213 entnommen und in 8-Bit-Bytes dem Exklusiv-ODER-Tor 197 zugeführt, wo er mit dem empfangenen chiffrierten Text kombiniert wird, um den Klartext in 8-Bit-Bytes auf einer Leitung 199 zu bilden. Das Exklusiv-ODER-Tor 197 übt effektiv die Dechiffrierfunktion aus.

Die vorliegende Erfindung verwendet den Verschlüsselungs-Algorithmus der Datenverschlüsselungsnorm in der Betriebsart mit Chiffre-Rückführung sowohl im Sender als auch im Empfänger. Die genau gleichen Schlüssel-Bits, die für den Chiffriervorgang verwendet wurden, werden auch für den Dechiffriervorgang verwendet. Der einzige Unterschied zwischen dem Chiffrierprozess und dem Dechiffrierprozess besteht somit darin, dass der Chiffrierprozess vom Klartext ausgeht, während der Dechiffrierprozess vom chiffrierten Text ausgeht.

Damit der Dechiffrierprozess funktioniert, muss der Dechiffrierprozess im Empfänger (Fig. 11) mit dem gleichen 64-Bit-Wort beginnen, mit dem auch der Chiffrierprozess im Sender (Fig. 10) beginnt. Aus diesem Grund wird vor dem Beginn des Chiffrierprozesses eine Start-Bitfolge aus einem Start-Bitfolge-Register 191 in das Verschlüsselungs-Eingangsregister 183 eingespeichert. Die Start-Bitfolge ist eine Zufallszahl kleiner oder gleich 64 Bits, die in bekannter Weise erzeugt wird. Nachdem die Start-Bitfolge in das Verschlüsselungs-Eingangsregister 183 eingespeichert worden ist, wird sie sonst nicht mehr verwendet. Vor dem Einspeichern in das Verschlüsselungs-Eingangsregister 183 war sie in den vorangegangenen chiffrierten Textblock eingefügt worden, der zum Empfänger übermittelt wurde. Im Empfänger war sie dem Start-Bitfolge-Register 205 zugeführt worden, um vor dem Empfang des nächsten chiffrierten Textes in das Entschlüsselungs-Eingangsregister 203 eingespeichert zu werden.

Wie in der vorstehenden Beschreibung bezüglich der vorliegenden Erfindung angegeben, wird in das Start-Bitfolge-Register 205 des Empfängers die Start-Bitfolge vom hinteren Ende eines vorgängig empfangenen chiffrierten Textblockes eingespeichert. Damit ist der Entschlüsselungsteil des Empfänger/Senders schon im voraus für die Dechiffrierung des nächsten zu empfangenden chiffrierten Textblockes vorbereitet.

Der Verschlüsselungsvorgang 185 und der Entschlüsselungsvorgang 207 sind jeweils eine festprogrammiert gesteuerte Unter-Routine des Hauptsteuerprogramms der Verschlüsselungs/Entschlüsselungs-Vorrichtungen der Datenverbindung. Die beiden Vorgänge sind identisch. Die Ausführung des Algorithmus ist in allgemeiner Form in den Fig. 12 und 13 dargestellt.

Der Algorithmus wirkt auf ein 64-Bit-Eingangssignal im Verschlüsselungs-Eingangsregister 183. Die 64 Bits werden einer anfänglichen Permutationsfunktion 213 unterworfen, die einfach aus einer vorgeschriebenen Folgeänderung oder Neuord-

nung der 64 Bits besteht. Die neugeordneten 64 Bits werden dann in zwei Gruppen zu 32 Bits aufgeteilt und einem linken bzw. rechten Register 215 bzw. 217 zugeführt. Das Ausgangssignal des rechten Registers wird dann einem zweiten linken Register 223 zugeführt und ferner auch in einer bestimmten Kombinationsfunktion (F) 219 (in Fig. 13 dargestellt) mit dem im Schlüsselregister 193 gespeicherten Schlüssel kombiniert. Das Resultat dieser Kombination des 32-Bit-Wortes wird dann zusammen mit dem Inhalt des linken Registers 215 einem Exklusiv-ODER-Tor 221 zugeführt, und dann in das zweite rechte Register 225 geleitet.

Diese Abfolge wird sechzehnmal durchgeführt, was von einer Logikfunktion 227 für das zweite linke Register und von einer Logikfunktion 229 für das zweite rechte Register 225 gesteuert wird. Nachdem sie sechzehnmal durchgeführt worden ist, werden die Inhalte des zweiten linken Registers 223 und des zweiten rechtenRegisters 225 einer Permutationsfunktion 231 zugeführt, welche die Umkehrung der anfänglichen Permutation 213 ist. Das Resultat aus der Ausgangs-Permutationsfunktion 231 wird dann einem Verschlüsselungs-Ausgangsregister 187 als der chiffrierte Text zugeführt.

Die Kombinationsfunktion (F) 219 ist in Fig. 13 dargestellt. Die Funktion (F) kombiniert die 32 Bits im rechten Register 217 in einer bestimmten Weise mit bis zu 64 Bits des Schlüssels im Schlüsselregister 193. Die 32 Bits vom rechten Register 217 werden durch eine Dehnungsfunktion 233 zu einem 48-Bit-Wort gedehnt, welches in einem Register 237 gespeichert wird. Bis zu 64 Bits des Schlüssels 193 werden durch eine Komprimierungsfunktion 235 zu einem 48-Bit-Wort komprimiert, welches in einem Register 239 gespeichert wird. Die beiden 48-Bit-Worte aus den Registern 237 und 239 werden zusammen einem Exklusiv-Oder-Tor 241 zugeführt. Die resultierenden 48 Bits werden an eine Auswahlschaltung 243 geliefert, welche 8 individuelle Auswahlfunktionen enthält, die jeweils einen 6-Bit-Block als Eingangssignal annehmen und gemäss einer bestimmten Tabelle einen 4-Bit-Block als Ausgangssignal abgeben. Das 32-Bit-Ausgangssignal von den acht Auswahlfunktionen wird in einer Permutationsfunktion 245 nach einer bestimmten Tabelle permutiert, um die 32 Bits für ein Register 247 zu erzeugen. Die Bits im Register 247 werden zusammen mit den 32 Bits vom linken Register 215 (Fig. 12) durch das Exklusiv-ODER-Tor 221 geleitet.

Die genaue Definition dieses Algorithmus ist, wie in der Einleitung dieses Textes angegeben, bekannt und in den verschiedenen im Vorstehenen erwähnten Veröffentlichungen publiziert. Daher wird eine weitere Beschreibung des eigentlichen Algorithmus nicht als nötig erachtet. Der Algorithmus an sich bildet nicht die vorliegende Erfindung.

Nun wird auf die Fig. 14 Bezug genommen, in welcher der Verschlüsselungsvorgang und die zugeordneten Einrichtungen in einer zentralen Verschlüsselungs/Entschlüsselungs-Vorrichtung dargestellt sind, welche die Fähigkeit hat, je einen gesonderten geheimen Schlüssel für mehrere Empfänger in einer Datenverbindung zwischen mehreren Punkten zur Verfügung zu stellen. Der Verschlüsselungsvorgang ist der gleiche, wie er für eine Verschlüsselungs/Entschlüsselungs-Vorrichtung mit nur einem Schlüssel, gemäss Fig. 10, beschrieben worden ist, mit der Ausnahme, dass eine Verschlüsselungs/Entschlüsselungs-Vorrichtung mit mehreren Schlüsseln je ein gesondertes Schlüsselregister für jeden Schlüssel und ein gesondertes Ausgangsregister für jeden Schlüssel enthält. Die Ausführungsform der Fig. 14 illustriert somit eine Drei-Schlüssel-Anlage, in der ein Schlüssel A in einem Register 231, ein Schlüssel B in einem Register 233 und ein Schlüssel C in einem Register 235 gespeichert sind. Das Ausgangssignal des Verschlüsselungs-Algorithmus 229 wird entsprechend einem Verschlüsselungs-Ausgangsregisters A 237, einem Verschlüsselungs-Ausgangsregisters B 239 oder einem Verschlüsselungs-Ausgangsregisters C 241 zugeführt.

Die übrigen Einrichtungen und Funktionen sind ähnlich oder gleich wie die in Fig. 10 dargestellten. Die Arbeitsweise der Ausführungsform gemäss Fig. 14 ist ebenfalls gleich, mit der Ausnahme, dass für jede der verschiedenen Verschlüsselungs-Operationen, wie im Vorstehenden beschrieben, wie jeweils verlangt unterschiedliche Schlüssel verwendet werden können.

Die Programmierung für jede Verschlüsselungs/Entschlüsselungs-Vorrichtung mit Mikroprozessor, die die Übermittlung und den Empfang des chiffrierten Textes ermöglicht, wird durch das Fliessdiagramm von Fig. 15 und 16 erläutert. Das Fliessdiagramm von Fig. 15 illustriert den Vorgang, der sowohl bei der Verschlüsselung und Übermittlung als auch bei Empfang und Entschlüsselung abläuft.

Nach dem Start 247 geht die Verschlüsselungs/Entschlüsselungs-Vorrichtung, wenn sie in einer Empfangs-Betriebsart ist, in einen Such-Zustand 249, in welchem sie auf den Empfang von Wortteilen (SYN) 263 wartet. In der Empfangs-Betriebsart würde der Synchronisierungs-Zustand 251 die eingehende Synchron-Information zum Einstellen der internen Taktgeber verwenden. Wenn die eingehende Information durch den Synchronisierungs-Zustand 251 nicht als Wortteile (SYN) bestimmt wird, wird ein Befehl 265 zur Rückkehr zum Such-Zustand 249 gegeben.

Wenn die Verschlüsselungs/Entschlüsselungs-Vorrichtung in der Sende-Betriebsart ist, dann würde der Synchronisierungs-Zustand 251 den Befehl erhalten, die Wortteile (SYN) für die Übermittlung zu erzeugen. Wenn der Meldungsblock zu übermitteln wäre, würde der Synchronisierungs-Zustand 251 nach der Erzeugung der Synchron-Wortteile den Beginn des Vorspann-Zustandes veranlassen.

In der Empfangs-Betriebsart gibt der Synchronisierungs-Zustand 251 alle auf die Wortteile (SYN) folgenden Steuer-Wortteile an den Vorspann-Zustand 253 weiter. Wenn der Vorspann-Zustand 253 einen Textanfang-Wortteil (STX) empfängt, dann würden die auf diesen Textanfang-Wortteil folgenden Wortteile für die Verarbeitung an den Text-Zustand 255 weitergegeben. Der Vorspann-Zustand sucht auch nach anderen Steuer-Wortteilen und reagiert auf diese Wortteile entsprechend. Wenn anstelle eines Textblockes ein Steuerblock empfangen würde, dann würde ein Wortteil (PAD) das Ende des Steuerblockes anzeigen. was den Vorspann-Zustand veranlassen würde ein Signal 271 zum Starten des Abstellvorganges 259 des Empfängers abzugeben. Wenn der Vorspann-Zustand aktiv ist und keine Textanfang-Wortteile oder Wortteile (PAD) empfangen werden, 269, dann sucht er weiter nach als Steuer-Wortteile empfangenen Wortteilen und verarbeitet diese.

In der Sende-Betriebsart würde der Vorspann-Zustand 253 die geeigneten Textanfang-Wortteile oder anderen Steuer-Wortteile erzeugen, die im chiffrierten Textblock benötigt werden, der der Textinformation vorangeht.

Alle auf den Wortteil (STX) folgenden Wortteile werden vom Text-Zustand 255 bearbeitet. In der Empfangs-Betriebsart setzt der Text-Zustand die Chiffrier-Unter-Routine in Betrieb. In der Sende-Betriebsart wird ebenfalls die Chiffrier-Unter-Routine in Betrieb gesetzt. Der Chiffrierprozess geht weiter, bis der Blockprüf-Wortteil (BCC) dechiffriert oder empfangen wird. Die Verarbeitung des Blockprüf-Wortteils hat zur Folge, dass der Start-Bitfolge-Zustand 257 aktiviert wird, in welchem die 4 bis 8 Bytes der Start-Bitfolge entweder erzeugt werden (Sende-Betriebsart) oder in den Datenverschlüsselungsnorm-Algorithmus-Puffer eingespeichert werden (Empfangs-Betriebsart). Nach der Verarbeitung des letzten Bytes der Bitfolge geht der Prozess in den Abstell-Zustand 259. Das heisst, dass der Sender bzw. der Empfänger die Übermittlung bzw. den Empfang einstellt. Mit der Beendigung des Abstell-Zustandes 259 wird ein Signal erzeugt, 279, das die Routine erneut mit dem Suchvorgang 249 beginnen lässt.

Nun wird auf die Fig. 16 Bezug genommen, in welcher die

zusätzlichen Funktionen von (INF), (ETX') und (BCC') zwischen den Start-Bitfolge-Zustand (IV) 257 eingeschaltet dargestellt sind. Durch die Hinzufügung dieser beiden Zustände werden die Wortteile (INF) 167 (Fig. 9) und die Wortteile (ETX') 171 und (BCC') (Fig. 9) erzeugt, welche auch Teil des Anhanges am hinteren Ende sein können.

Wenn während des Empfanges oder während der Übermittlung der Wortteil (STX) festgestellt wird, wird zum Text-Zustand 255 übergegangen, welcher veranlasst, dass die übermittelten Daten chiffriert werden oder, wenn sie empfangen werden, dechiffriert werden. Bei der Verarbeitung des Blockprüf-Wortteils ändert sich der Text-Zustand in den Zustand (INF) 281, in welchem beim Empfang die Signale (INF) entsprechend ihrer Art verarbeitet werden, d.h. je nachdem, ob sie (SEQ), (ABORT) oder allgemeine Steuersignale (SIG) sind, wie im Vorstehenden erläutert. In der Sende-Betriebsart veranlasst der Zustand (INF) 281 die Erzeugung der geeigneten Signale, die unmittelbar vor der Start-Bitfolge des zu übermittelnden chiffrierten Textblockes angeordnet werden sollen. Nach der Verarbeitung der Signale (INF) wird zum Start-Bitfolge-Zustand übergegangen, worauf die Bytes der Start-Bitfolge verarbeitet werden, entweder indem sie erzeugt werden oder indem sie empfangen und in das Datenverschlüsselungsnorm-Algorithmus-Register eingespeichert werden. Am Ende des letzten Bytes, das verarbeitet wird, wird zum Zustand (ETX') und (BCC') 285 übergegangen, in welchem bei der Übermittlung diese beiden Wortteile erzeugt werden, so dass sie unmittelbar auf die Start-Bitfolge folgen. Beim Empfang werden diese beiden Wortteile festgestellt und in der geeigneten Weise verwendet. Wenn sie am Ende einer Datenverbindung mit mehreren Zwischen-Knotenstellen empfangen werden, können sie unberücksichtigt bleiben, denn ihre Hauptfunktion besteht darin, eine Überprüfung des chiffrierten Textes auf Übermittlungsfehler in Zwischen-Knotenstellen der Datenverbindung ohne Dechiffrierung der Meldungsblöcke zu ermöglichen.

Was beschrieben worden ist, ist eine Meldungs-Form für chiffrierte Textblöcke in einem Synchron-Binärübermittlungsprotokoll. Diese Form ist flexibel und kann in Datenverbindungen von Punkt zu Punkt oder zwischen mehreren Punkten verwendet werden sowie auch in Datenverbindungen, welche Zwischen-Knotenstellen enthalten, die in der Lage sind, auf Übermittlungsfehler zu prüfen. Die Meldungs-Form der vorliegenden Erfindung ermöglicht die Durchführung dieser Prüfung, ohne dass die Zwischen-Knotenstellen die Text-Meldung dechiffrieren müssten. Zudem werden die Fehlerprüfmöglichkeiten der Anlage als Folge der Struktur der Meldungs-Form verbessert. Die Meldungs-Formm ist in einer Weise strukturiert, die eine beträchtliche Menge an für den chiffrierten Textblock nötiger Information, wie die Start-Bitfolge, hinzufügt, ohne den Durchsatz der nach dem Synchron-Binärübermittlungsprotokoll arbeitenden Anlage zu verringern. Es versteht sich, dass sich die vorstehende Beschreibung auf eine bevorzugte Ausführungsform der Erfindung bezieht und dass daran Änderungen vorgenommen werden können, ohne die Grundidee und den Rahmen der Erfindung, wie sie in den beiliegenden Ansprüchen definiert ist, zu verlassen.

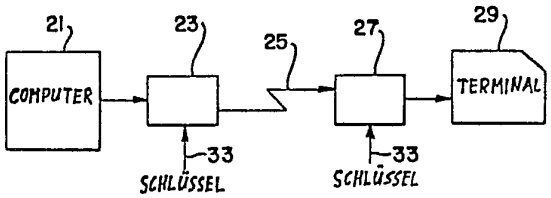


FIG. 1

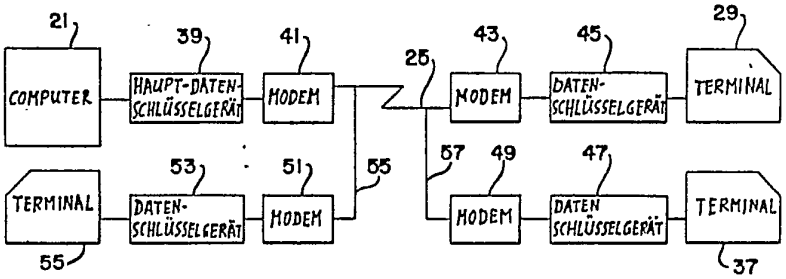


FIG. 2

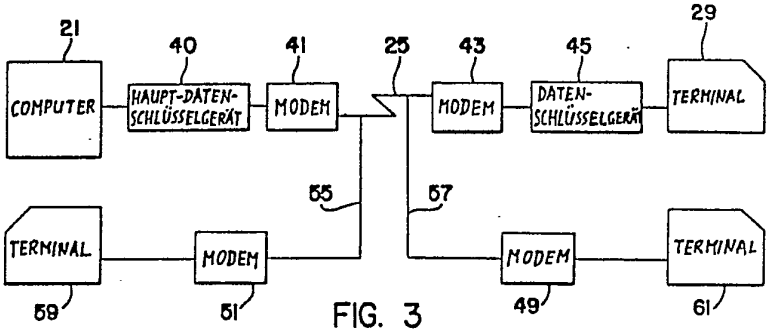


FIG. 3

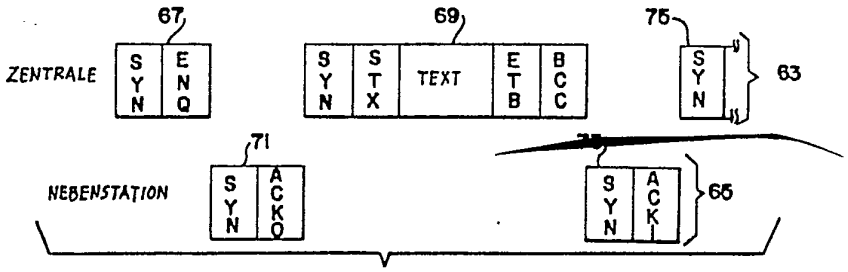


FIG. 4

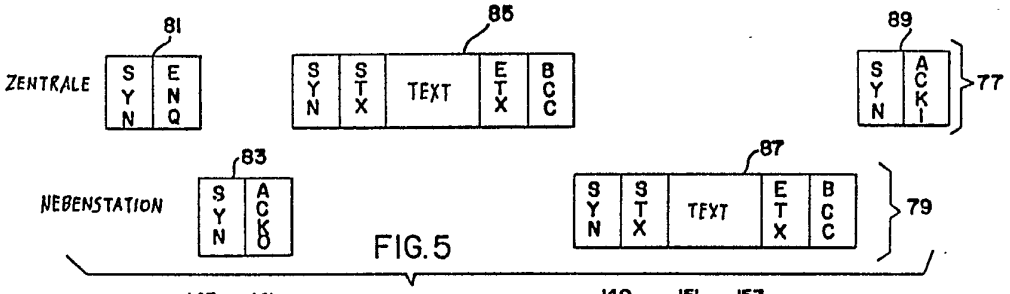


FIG. 5

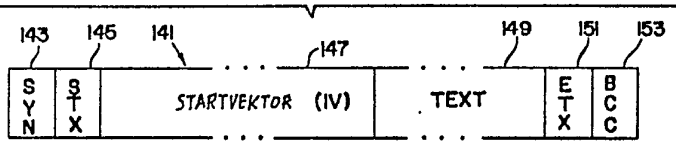


FIG. 8

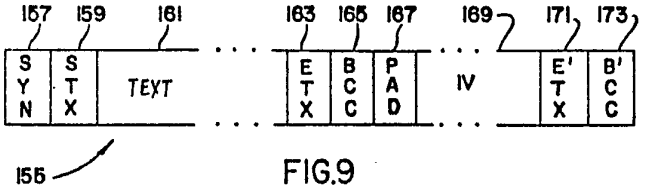


FIG.9

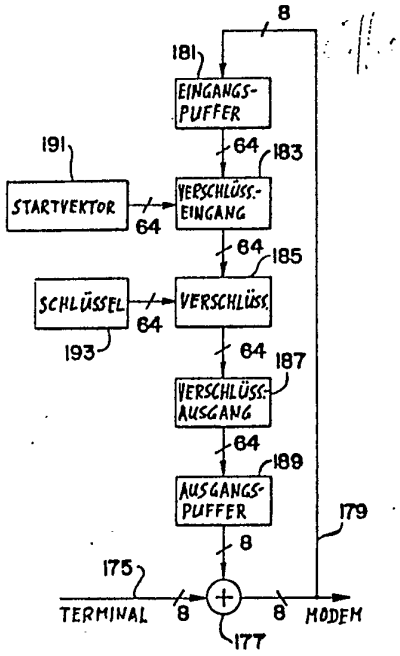


FIG. 10

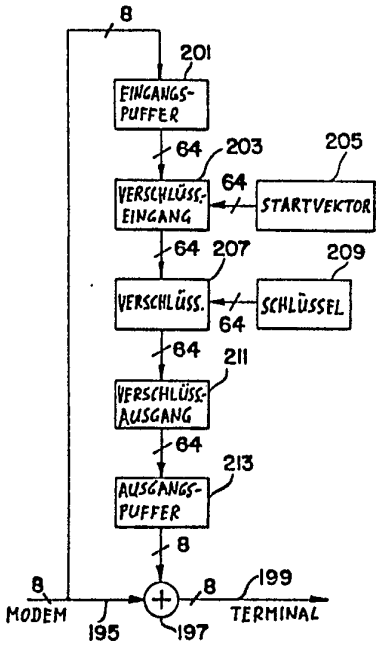


FIG. 11

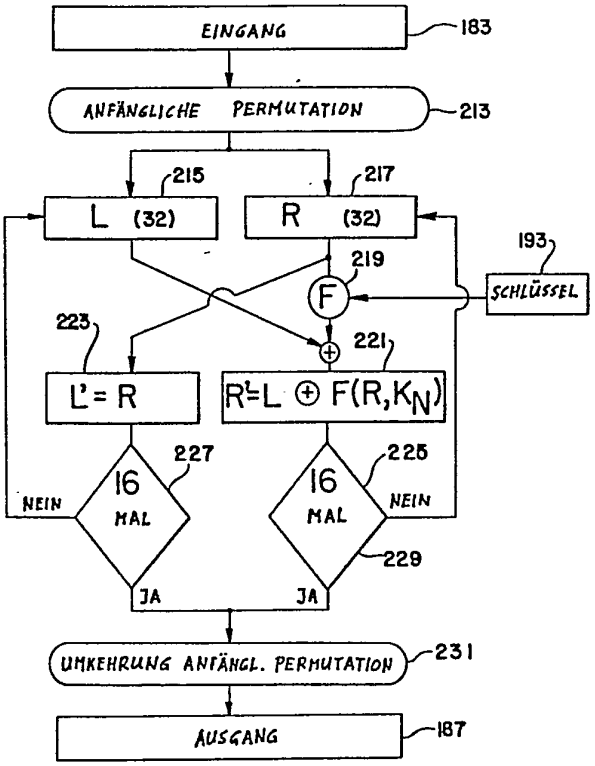

EINGANG
183
ANFÄNGLICHE PERMUTATION
213
215
217
L (32)
R (32)
193
219
F
SCHLÜSSEL
223
221
L' = R
R' = L ⊕ F(R,K_N)
227
225
16 MAL
NEIN
16 MAL
NEIN
229
JA
JA
UMKEHRUNG ANFÄNGL. PERMUTATION
231
AUSGANG
187

FIG. 12

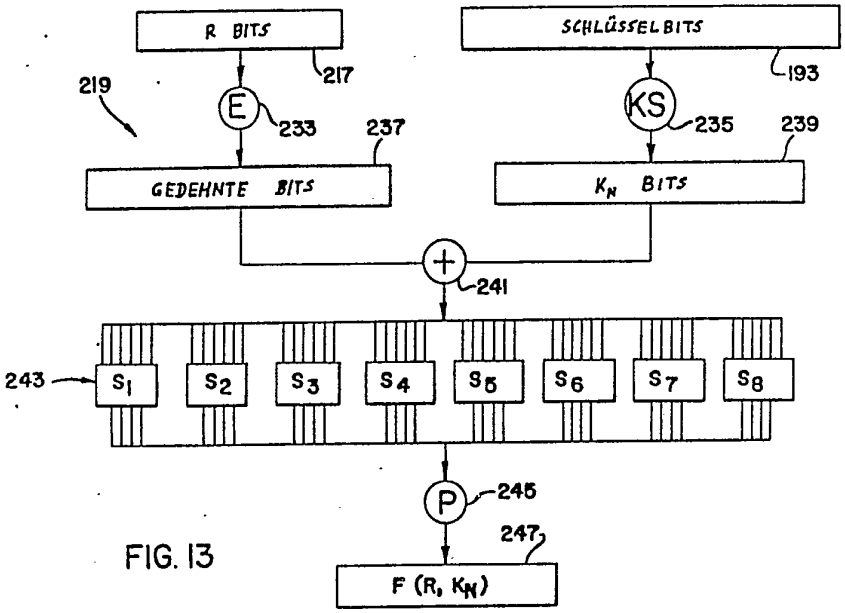

R BITS
217
SCHLÜSSEL BITS
193
219
E
233
237
KS
235
239
GEDEHNTE BITS
K_N BITS
241
243
S1
S2
S3
S4
S5
S6
S7
S8
P
245
247
F (R, K_N)

FIG. 13

FIG. 14

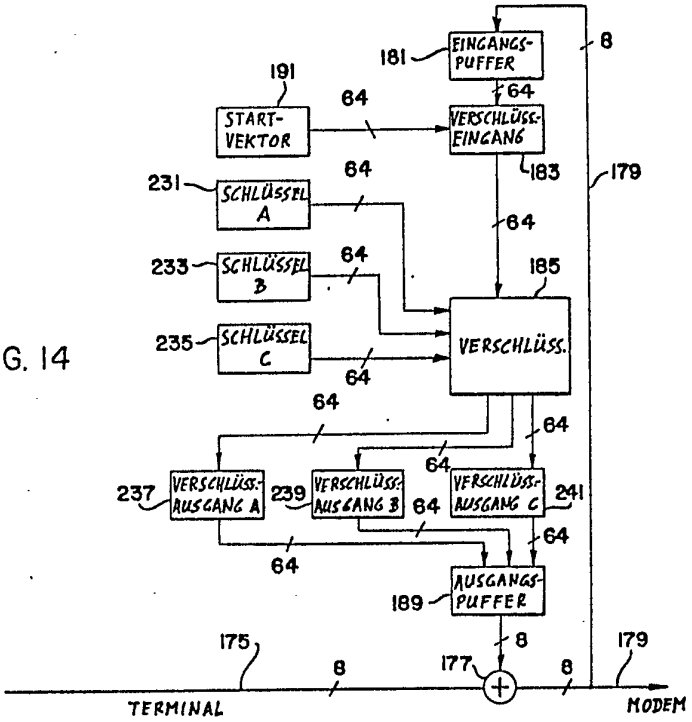


FIG. 15

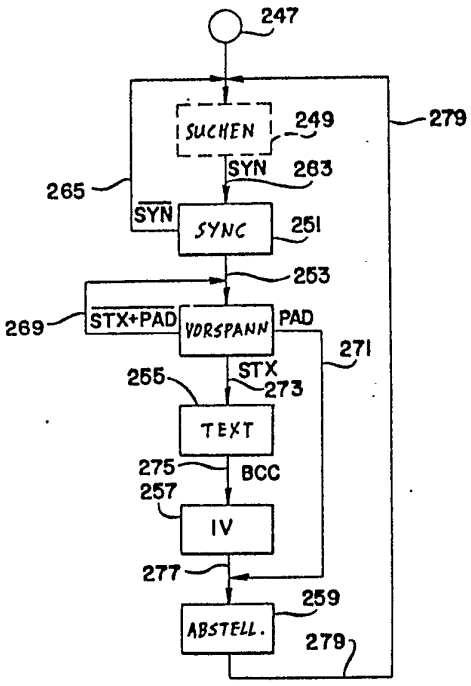
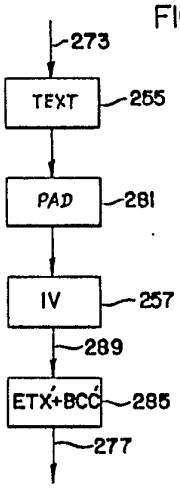


FIG. 16



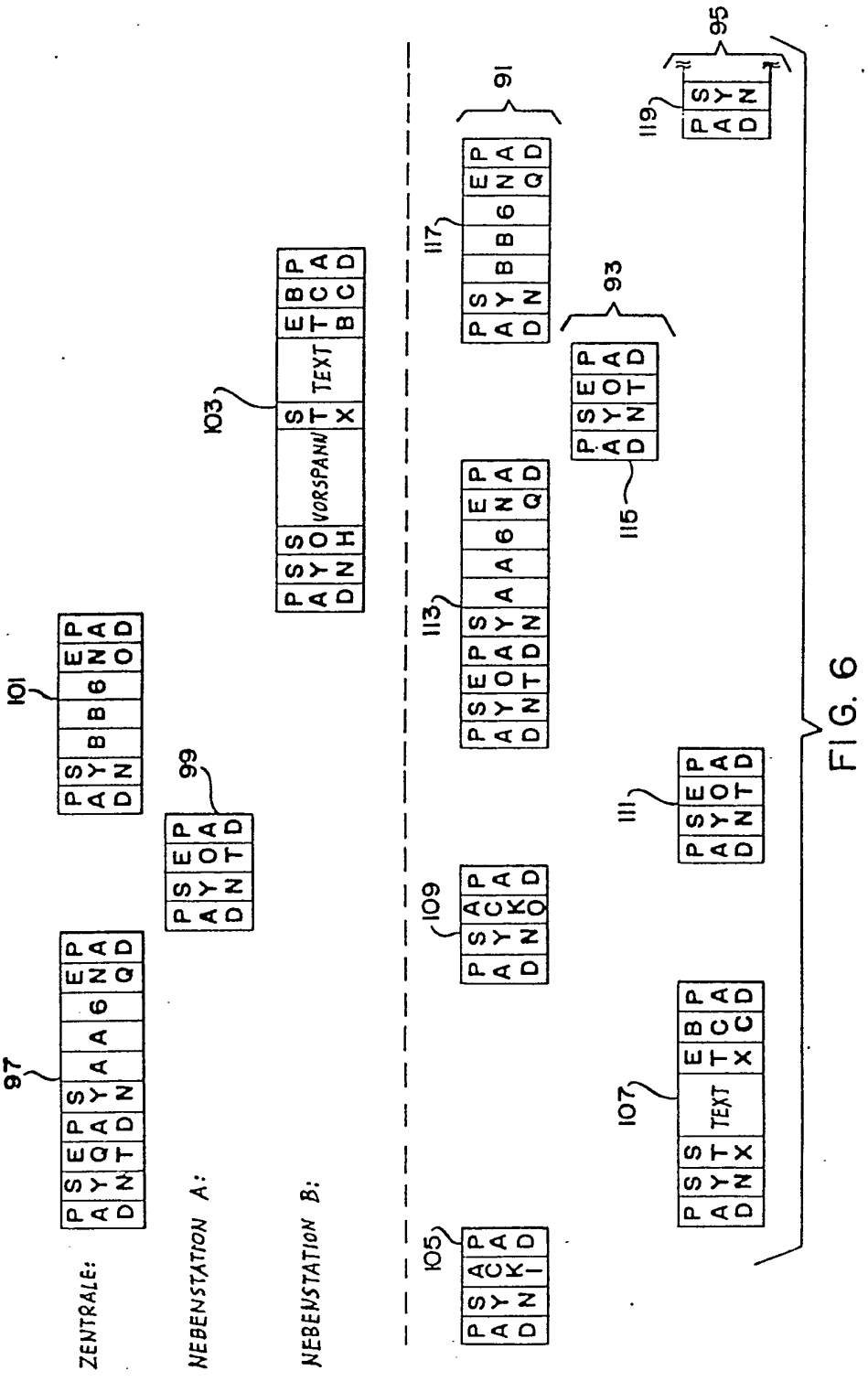

ZENTRALE:
NEBENSTATION A:
NEBENSTATION B:
VORSPANN
TEXT
97
99
101
103
105
107
109
111
113
115
117
119
91
93
95

FIG. 6

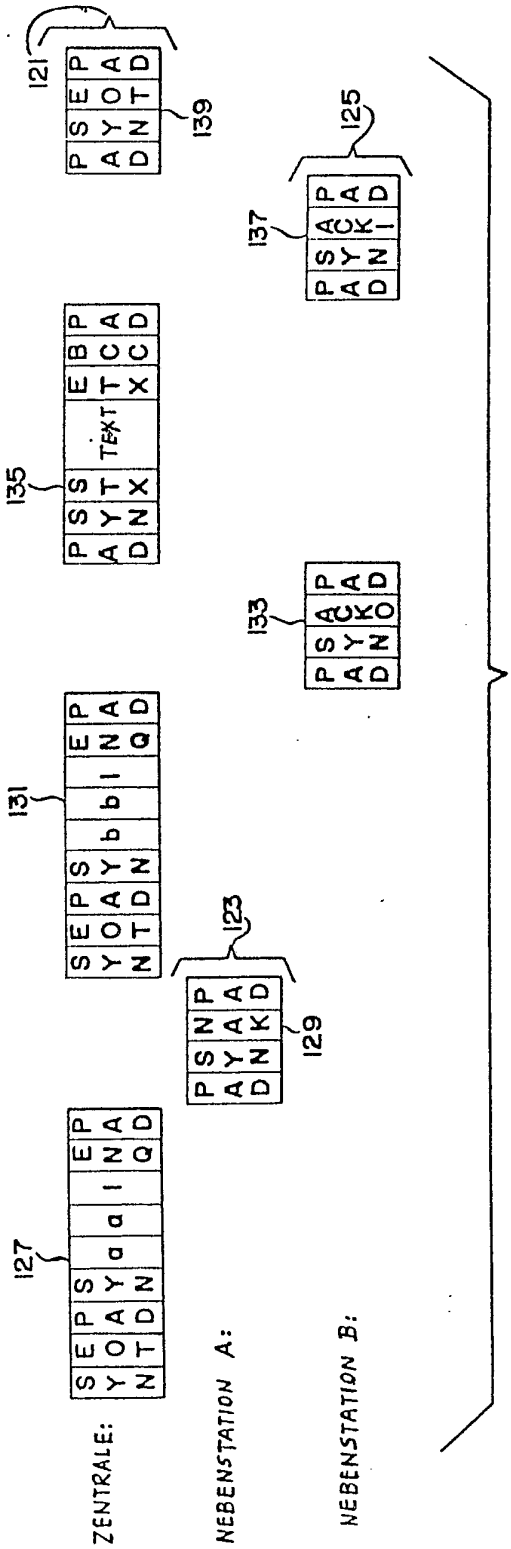

ZENTRALE:
NEBENSTATION A:
NEBENSTATION B:
TEXT
121
123
125
127
129
131
133
135
137
139

FIG. 7