

⑤

Int. Cl. 2:

H04L 9/02

⑩ BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT



1  
B  
3  
DT 978 034 C1

⑪

# Patentschrift 9 78 034

⑫

Aktenzeichen: P 9 78 034.1-31

⑬

Anmeldetag: 19. 7. 61

⑭

Offenlegungstag: —

⑮

Bekanntmachungstag: —

⑯

Ausgabetag: 22. 4. 76

⑳

Unionspriorität:

⑳ ㉑ ㉒

㉔

Bezeichnung:

Verfahren zur nachträglichen Einschaltung von Nachrichtenempfängern  
in eine laufende, verschlüsselte Nachrichten in binär kodierter Form  
übertragende Sendung

㉕

Patentiert für:

Dr.-Ing. Rudolf Hell GmbH, 2300 Kiel

㉖

Erfinder:

Hell, Rudolf, Dr.-Ing.; Koll, Roman, Dipl.-Ing.; 2300 Kiel

㉗

Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:  
Nichts ermittelt

152

Nummer: 9 78 034  
Int. Cl.: H 04 L 9/02  
Bekanntmachungstag: 22. April 1976

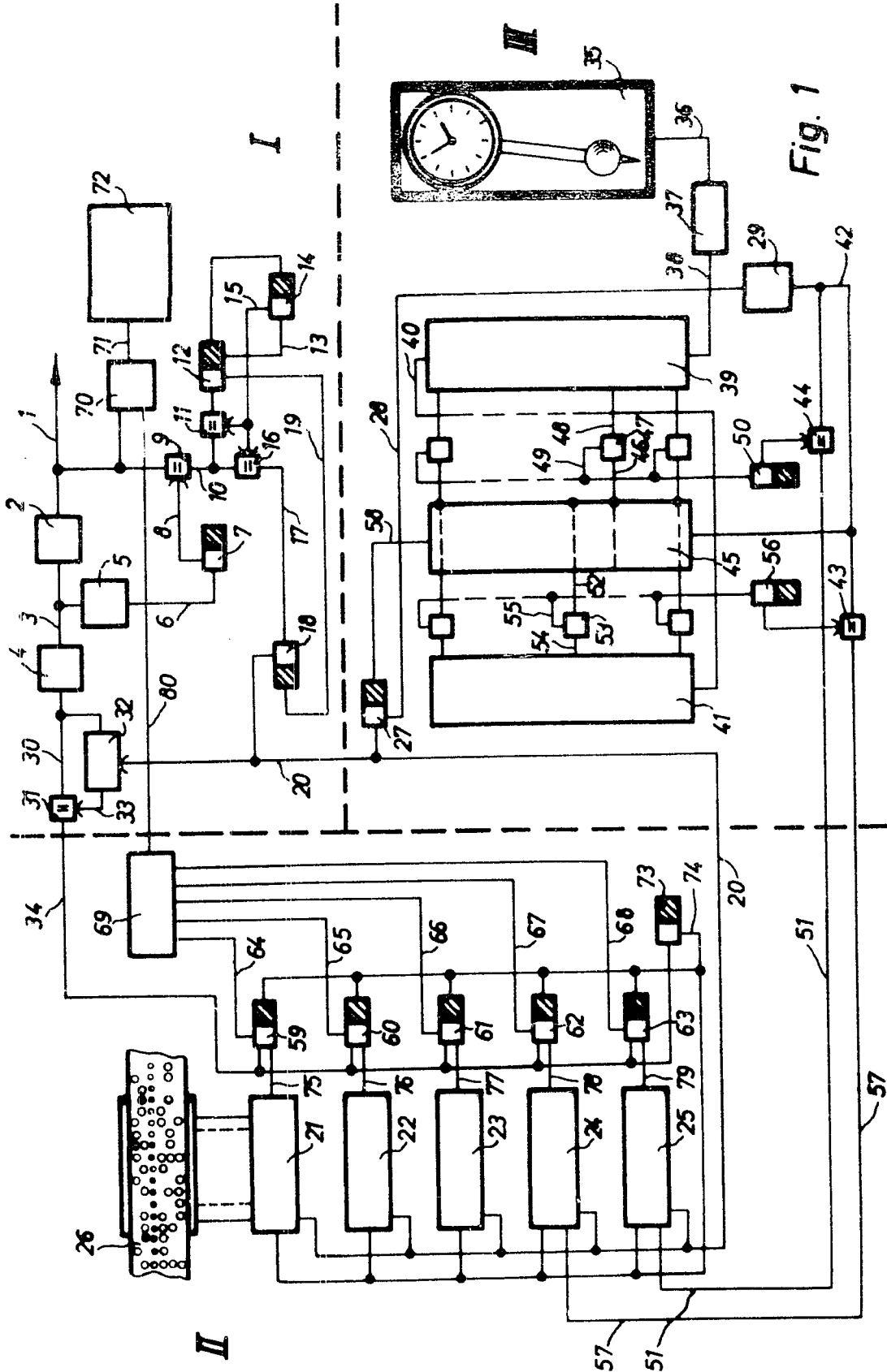


Fig. 1

## Patentansprüche:

1. Verfahren zur nachträglichen Einschaltung von Nachrichtenempfängern in eine laufende, verschlüsselte Nachrichten in binär kodierter Form übertragende Sendung, dadurch gekennzeichnet, daß nach im Verhältnis zur gesamten Übertragungszeit kurzen, periodischen Zeitabständen vom Sender ein besonderes, nicht zur Aufzeichnung eines Nachrichtenelements bestimmtes Signal ausgesendet wird, welches sowohl im Sender als auch bei den Empfängern die Einstellung eines neuen, bisher noch nicht verwendeten Abschnitts des Schlüsselablaufs veranlaßt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Einstellung eines neuen Schlüsselabschnitts des Schlüsselablaufs beim Sender und bei allen Empfängern durch lokale Zeitlaufwerke in periodischen Zeitabständen laufend vorbereitet wird, daß der Sender innerhalb dieser Vorbereitungsperioden, vorzugsweise in deren Mitten, durch Aussendung (oder Unterdrückung) des besonderen Signals bei sich selbst und bei den teilnehmenden Empfängern die Einstellung des neuen Schlüsselabschnitts vollendet, die Schlüsselimpulserzeugung von dieser neuen Anfangsstellung aus neu startet und daß anschließend die Übertragung der verschlüsselten Nachricht fortgesetzt wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß beim Fernschreibbetrieb der Sender die Übertragung verschlüsselter Nachrichten kurzzeitig unterbricht, daß er durch Aussendung eines besonderen Signals sich selbst und die an der Übertragung verschlüsselter Nachrichten bereits teilnehmenden Empfänger auf Klarbetrieb umschaltet, daß er sodann durch Aussendung einer bestimmten Buchstabengruppe im Klartext bei sich selbst und bei allen, auch bei den neu hinzukommenden Empfängern, die Umschaltung auf Verschlüsselungsbetrieb, die Einstellung eines neuen Schlüsselabschnitts und den Neustart aller Schlüsselimpulsgeneratoren bewirkt und daß anschließend die Übertragung verschlüsselter Nachrichten fortgesetzt wird.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß das besondere Signal in der Unterdrückung eines bestimmten Betriebssignals, z. B. des Stoppschrittes eines Fernschreibzeichens, besteht.

5. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß das besondere Signal in der Aussendung einer bestimmten, verschlüsselt übertragenen Buchstabengruppe besteht.

6. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die bestimmte, im Klartext übertragene Buchstabengruppe aus zwei Untergruppen besteht, deren erste aus gleichbleibenden Buchstaben zum Zweck der Umschaltung auf Verschlüsselungsbetrieb und deren zweite aus mit jeder Neueinstellung der Schlüsselabschnitte wechselnden Buchstaben zusammengesetzt ist.

7. Vorrichtung zur Durchführung des Verfahrens nach Anspruch 2, gekennzeichnet durch ein an sich bekanntes Zeitschaltwerk, vorzugsweise einen Chronometer, der in periodischen Zeitabständen Impulse abgibt, durch zwei vermittelte des Zeitschaltwerks gesteuerte Zähler, deren erster gleiche kleinere Zeitabschnitte (Minuten) und deren zweiter

gleiche Vielfache dieser Abschnitte (Stunden) zählt und speichert, durch einen vermittelte eines Impuls-generators gesteuerten Suchzähler, welcher periodisch die Ordnungszahlen der gespeicherten Zeitabschnitte abfragt und den angetroffenen Ordnungszahlen gleiche Anzahlen von Impulsen auf zwei Ringzähler des Schlüsselimpuls-generators zu dessen Neueinstellung gibt.

Die Erfindung betrifft Verfahren zur nachträglichen Einschaltung von Nachrichtenempfängern in eine laufende, verschlüsselte Nachrichten in binär kodierter Form übertragende Sendung.

Bei der Übertragung verschlüsselter Nachrichten besteht eine Schwierigkeit darin, daß sich befugte Nachrichtenempfänger nicht ohne weiteres nachträglich in eine laufende Übertragung einschalten können, weil kein Gleichlauf des Schlüsselablaufs bei ihnen und beim Sender besteht und auch nicht ohne besondere Maßnahmen, die Gegenstand der Erfindung sind, hergestellt werden kann.

Bei einem Übertragungsbetrieb, wie er bei einer Nachrichtenanlage besteht, bei welcher von einer zentralen Stelle aus gesendet und an vielen anderen Stellen empfangen wird (z. B. Konferenzschaltungen), besteht keinerlei Rückmeldemöglichkeit vom Empfänger zum Sender, wodurch z. B. der Empfänger einen Neustart der Schlüsselgeräte anfordern könnte. Bei einem Übertragungsbetrieb, wie er z. B. beim Wetterkartendienst mit Faksimilensendern oder beim Börsen- oder Wirtschaftsnachrichtendienst mit Fernschreibsendern besteht, ist es jedoch erwünscht, daß sich einzelne Teilnehmer, die sich nur für einzelne bestimmte Sendungen interessieren und die ihre Empfänger zu den übrigen Zeiten für andere Zwecke benötigen, nachträglich in eine laufende Übertragung verschlüsselter Nachrichten einschalten können. Dabei ist es nicht erforderlich, daß dies zu jedem beliebigen Zeitpunkt möglich ist. Es genügt vielmehr, wenn die Einschaltung zu bestimmten Zeitpunkten, deren Zeitabstände klein gegenüber der gesamten Übertragungszeit sind, geschehen kann. Wichtig ist dabei nur, daß diesen Zeitpunkten genau definierte neue Schlüsselabgangspunkte zugeordnet sind und daß sich nicht Teile des Schlüsselablaufs wiederholen, damit sogenannte phasengleiche Sprünge vermieden werden.

Erfindungsgemäß geschieht dies in der Weise, daß nach im Verhältnis zur gesamten Übertragungszeit kurzen, periodischen Zeitabständen vom Sender ein besonderes Signal ausgesendet wird, das bei den Empfängern nicht zur Aufzeichnung eines Nachrichtenelements bestimmt ist und welches sowohl im Sender als auch bei den Empfängern die Einstellung eines neuen, bisher noch nicht verwendeten Abschnitts des Schlüsselablaufs veranlaßt.

Die gleichen Schlüsselimpulsfolgen beim Sender und bei den vom ersten Start der Schlüsselimpulsgeneratoren ab empfangenden Empfängern laufen eine gewisse Zeit lang, z. B. einige Minuten, ab und machen dann plötzlich einen Sprung zu einer anderen Stelle des Schlüsselimpulsablaufs, welche räumlich in der Schlüsselperiode nicht notwendigerweise hinter der Stelle liegen muß, von der aus der Sprung erfolgt, sondern auch vor ihr liegen kann, jedoch derart, daß sich räumlich unmittelbar hintereinander liegende Schlüsselabschnitte

4

3

9 78 034

4

te zwischen Sprungstellen niemals überlappen. Die Einstellung neuer Startstellen im Schlüsselablauf wird entweder durch lokale Zeitlaufwerke in periodischen Zeitabständen laufend vorbereitet und durch ein besonderes Signal vom Sender ausgelöst, oder sie wird vom Sender unmittelbar vorgenommen. Der Sprung im Schlüsselablauf, der vom Sender veranlaßt wird, ist für den neu hinzukommenden Empfänger das Auslösekriterium für den ersten Start seines Schlüsselimpuls-  
generators und für die bereits am Betrieb teilnehmenden Empfänger das Kriterium für einen Neustart ihrer Schlüsselgeneratoren von den gleichen eingestellten Sprungstellen aus.

Die neue Startstelle im Schlüsselimpulsablauf des Senders und der Empfänger wird beispielsweise durch lokale Schaltungen mit nachgeschalteten Zählwerken eingestellt. Es ist aber auch möglich, die Neueinstellung des Schlüsselimpulsablaufs durch den Sender beispielsweise durch ein Codewort vorzunehmen. Das erstere Verfahren ist für den Faksimilebetrieb und für den Fernschreibbetrieb mit Springschreibern geeignet, während das letztere nur für den Fernschreibbetrieb in Betracht kommt, da ein Faksimileempfänger nicht für Fernschreibzeichen empfänglich ist.

Als Anwendungsbeispiel möge zunächst auf die Übertragung verschlüsselter Faksimileinformationen eingegangen werden, wobei Schriftzeichen oder Strichzeichnungen ohne Halbtöne bildelementeweise übertragen werden, die Information also in binärer Form vorliegt, da es nur die Signale »Schwarz« und »Weiß« gibt. Von einer zentralen Stelle aus werden Nachrichten, z. B. Wetterkarten, verschlüsselt gesendet. Die Sendungen laufen längere Zeit — oft mehrere Stunden —, und es werden während dieser Zeit Karten verschiedenen Inhalts übertragen. Manche Teilnehmer interessieren sich für die einen, manche für andere Karten. Die Zeiten aber, zu welchen die verschiedenen Karten übertragen werden, sind bekannt. So möge z. B. ab 8 Uhr eine Karte über die Temperatur- und Luftfeuchtigkeitslage, ab 9 Uhr eine über die Windverhältnisse in Bodennähe und ab 10 Uhr eine über die Wetterlage in größeren Höhen übertragen werden usf.

Der verschlüsselte Faksimilebetrieb geht nun in der Weise vor sich, daß vor Beginn des eigentlichen Übertragungsbetriebs die Schlüsselgeräte gestartet werden. Dies geschieht beispielsweise dadurch, daß der Sender zunächst ein Vorsignal aussendet, durch welches die Taktgeneratoren derjenigen Empfänger, welche bereits eine erste Übertragung empfangen wollen, mit dem Taktgenerator des Senders synchronisiert werden. Dann werden die Schlüsselgeräte durch ein charakteristisches Merkmal, z. B. durch Aufhören des Vorsignals, durch Einsetzen eines Nachsignals oder etwas ähnliches, gestartet. Durch dieses charakteristische Merkmal laufen die Schlüsselimpulsgeneratoren aller Empfänger von einer bestimmten gleichen Stelle aus an und bleiben auch im Gleichlauf, weil ihre synchron arbeitenden Taktgeber den Takt für den Schlüsselimpulsablauf liefern. Anschließend oder zu einem beliebigen späteren Zeitpunkt werden die Faksimileempfänger durch den Faksimilesender eingephaset und gestartet. Vom Zeitpunkt des Starts der Schlüsselimpulsgeneratoren an befinden sich Schlüssel- oder Geheimsignale auf dem Übertragungsweg. Sie bestehen aus der Trägerfrequenz, welche durch die Schlüsselimpulse oder durch die Geheimimpulse aufgetastet wird. Zur laufenden starren Synchronisierung der Taktgeneratoren der Empfänger mit dem Taktgenerator des Senders wird

aus den empfangenen Schlüssel- oder Geheimsignalen des Senders die Trägerfrequenz herausgesiebt. Durch deren synchronisierenden Einfluß bleiben die Empfänger mit dem Sender in Gleichlauf, und ihre Schlüsselimpuls-  
generatoren erzeugen mit dem Sender gleiche Schlüsselimpulsfolgen, welche durch Mischung mit den Geheimimpulsfolgen zum Entschlüsseln verwendet werden.

Will nun ein bisher nicht am Empfang beteiligter be-  
fugter Teilnehmer in die Verbindung eintreten, so empfängt er durch Einschaltung seines Gerätes die Schlüssel- oder Geheimsignale, ohne sie jedoch zunächst entschlüsseln zu können. Die Geheimsignale enthalten aber die Trägerfrequenz, und diese wird dazu benutzt, den Taktgenerator des Empfängers mit dem Taktgenerator des Senders zu synchronisieren. Von nun an wird der Taktgenerator des Empfängers in Synchronismus und Phasengleichheit mit dem Taktgenerator des Senders gehalten.

Da Sender und Empfänger für einen gewissen Betriebsabschnitt, z. B. für einen ganzen Tag, gleiche Schlüssel vereinbart haben, kommt es darauf an, daß der sich später einschaltende Empfänger die gerade ablaufende Stelle der Schlüsselimpulsfolge genau erwischt. Bekannt ist die Anzahl der Schlüsselimpulse pro Sekunde. Deshalb ist auch, wenn zu einer bestimmten Uhrzeit der Schlüsselablauf gestartet wurde, zu einer bestimmten späteren Uhrzeit des Betriebstages eine bestimmte Stelle der Schlüsselimpulsfolge erreicht. Es liegt der Gedanke nahe, eine später in die Übertragung eintretende Empfangsstelle durch lokale Chronometer anzuschalten. Leider ist dieser Weg nicht gangbar, weil die Schlüsselimpulsfolge ja auch an der Empfangsstelle vom Beginn des Starts des senderseitigen Schlüsselimpuls-  
generators ab bis zu dem interessierenden Zeitpunkt abgelaufen sein müßte. Das aber setzte gleichzeitigen Start der Schlüsselimpulsgeneratoren beim Sender und bei den Empfängern voraus. Wenn zwischen Sender und Empfänger zum Zeitpunkt dieses gleichzeitigen Starts keine Verbindung besteht, müßte die Einschaltung durch den Chronometer mit einer Genauigkeit von  $\pm 0,1$  msec erfolgen, und diese Genauigkeit müßte auch während der gesamten Übertragungszeit beibehalten werden. Mit normalen Chronometern ist dies jedoch nicht annähernd erreichbar.

Für die Verschlüsselung von Nachrichten, die in binärer oder binär kodierter Form vorliegen, wie z. B. Faksimileinformationen, Fernschreib- und Morsezeichen oder Sprache, die nach dem Verfahren der Puls-Code-Modulation übertragen wird, werden unregelmäßige Folgen aus gleich langen Impulsen zweier verschiedener Amplituden, deren eine meistens Null ist, verwendet. Diese Schlüsselimpulse, die taktgleich mit den Klarimpulsen angeleert werden müssen, werden paarweise mit den gleichzeitig anliegenden Klarimpulsen gemäß den Vernamschen Vorzeichenregeln gemischt, welche besagen, daß die Mischung zweier Impulse gleicher Amplitude Impulse der einen, verschiedener Amplitude Impulse der anderen Amplitude ergibt, wofür es zwei gleichwertige Zuordnungsmöglichkeiten gibt.

Schlüsselimpulsfolgen werden im allgemeinen mit Hilfe von Zufallsgeneratoren erzeugt. Solche Schlüsselimpulsfolgen mit zufälliger Verteilung der Schlüsselimpulse sind aperiodisch und können grundsätzlich nicht in einer zweiten gleichen Apparatur reproduziert werden, da ihre Erzeugung eben auf Zufall beruht und einmalig ist. Die derart erzeugten Schlüsselimpulse werden meistens, zu Fünfer-Kombinationen zusammenge-

faßt, in einen Papierstreifen in Form von entsprechenden Lochkombinationen gestanzt und damit gespeichert. Diese Lochstreifen werden kopiert und die Kopien an die Chiffrierteilnehmer verteilt. Mit Hilfe solcher Lochstreifen und eines Mischgerätes werden noch heute Fernschreibnachrichten verschlüsselt. Wenn solche Lochstreifen einige Zeit ausreichen sollen, nehmen sie unangenehm große Längen an, insbesondere, wenn mit ihrer Hilfe nicht Fernschreibzeichen, sondern Faksimilezeichen verschlüsselt werden sollen. Während der Lochstreifenverbrauch beim Fernschreibbetrieb mit 50 Impulsen pro Sekunde (50 Baud), also mit 10 Impulskombinationen pro Sekunde, noch in erträglichen Grenzen bleibt, wird er beim Faksimilebetrieb mit der 40fachen Impulsfrequenz, weil 2000 Bildpunkte pro Sekunde verschlüsselt werden müssen, unerträglich groß.

Da es aus Gründen des Versandes, der Aufbewahrung und der Geheimhaltung sehr mißlich ist, dicke Lochstreifenrollen herzustellen, hat man schon vor längerer Zeit Verlängerungsverfahren erdacht, welche von einem verhältnismäßig sehr kurzen, etwa 25 bis 100 Lochkombinationen in zufälliger Verteilung enthaltenen aperiodischen Urlochstreifen ausgehen, aus welchem Schlüsselimpulsfolgen mit sehr großen Perioden abgeleitet werden. Man kann dabei erreichen, daß diese verlängerten periodischen Folgen in ihrer Struktur, d. h. in der angenäherten Gleichverteilung der beiden Impulse, weitgehend den aperiodischen zufallsverteilten Impulsfolgen gleichen und daß ihre Perioden so groß sind, daß sie für Unbefugte nicht zu erkennen sind. Der Vorteil dieser Verlängerungsverfahren liegt auf der Hand: An Stelle dicker Lochstreifenrollen wird ein höchstens 25 cm langer Urlochstreifen hergestellt, von dem außerdem keine Kopien verschickt zu werden brauchen, sondern dessen Inhalt chiffriert an die Chiffrierteilnehmer übertragen werden kann und aus dem durch gleiche lokale Verlängerungsapparaturen die gleichen Schlüsselimpulsfolgen abgeleitet werden.

Der Hauptgrund aber, weshalb Lochstreifen für die Schlüsselimpulserzeugung für den vorliegenden Zweck nicht unmittelbar verwendet werden können, besteht darin, daß es technisch unmöglich ist, einen Sprung im Schlüsselablauf durch einen plötzlichen Transport des Lochstreifens um Meter, Dekameter oder womöglich Hektometer vorzunehmen.

Grundsätzlich gibt es zwei Arten von Verlängerungsverfahren, nämlich die rekurrenten, wobei die Erzeugung des folgenden Schlüsselimpulses die Kenntnis vorangegangener Schlüsselimpulse voraussetzt, und die nichtrekurrenten. Auf die letzteren möge etwas näher eingegangen werden, weil sie für das Verständnis der späteren Darlegungen unerlässlich sind.

Man denke sich einen Lochstreifen, dessen fünf Lochreihen (parallel zur Längsausdehnung des Streifens) verschiedene Anzahlen von Löchern und Nichtlöchern aufweisen, deren keine zwei einen gemeinschaftlichen Teiler haben, also z. B. die Anzahlen 25, 27, 67, 71, 73, so daß er an seinem einen Ende treppenförmig abgestuft erscheint.

Diesen Lochstreifen denke man sich in die fünf Lochreihen zerschnitten und diese einzeln zu Ringen zusammengeklebt. Werden nun diese fünf Lochringe, bei denen es keinen Anfang und kein Ende mehr gibt, durch irgendwelche Verdrehungen in eine relative Anfangslage (Anfangskonfiguration) zueinander gebracht und durch fünf in einer Geraden quer zu den Ringen angeordnete Abtastvorrichtungen gleichzeitig, mit gleicher Schrittgeschwindigkeit und periodisch abgetastet,

so ergeben sich an den Ausgängen der Abtastvorrichtungen dauernd wechselnde Impulskombinationen. Durch die unterschiedlichen Umfangslängen der Ringe tritt beim zyklischen Abtasten im Verlauf der Zeit eine zunehmende relative Verschiebung der Ringe zueinander ein. Wegen der Teilerfremdheit der Anzahlen von Löchern und Nichtlöchern in den einzelnen Ringen wird eine gewisse Anfangskonfiguration der Ringe, mit der die Abtastung begonnen würde, nach einer Anzahl von Schritten wieder erreicht, die gleich dem Produkt der Anzahlen der Löcher und Nichtlöcher der fünf Ringe ist, also im Beispielsfall nach

$$25 \cdot 27 \cdot 67 \cdot 71 \cdot 73 = 324\,401\,175$$

Schritten. Diese Zahl ist die Periode des Ringsystems, d. h. die Periode der verlängerten Impulskombinationsfolge. Die Anzahl der möglichen relativen Anfangsstellungen (Konfigurationen) der Ringe zueinander ist ebenso groß.

Die abgetasteten Impulskombinationen werden durch einen Parallel-Serien-Umwandler jeweils in zeitliche Folgen von je fünf Impulsen umgewandelt, die zum Verschlüsseln verwendet werden. Aus jeder abgetasteten Impulskombination kann aber auch durch Mischung der fünf Impulse miteinander nach den Vernamschen Vorzeichenregeln ein einziger Impuls gewonnen werden. Die Impulserzeugung ist in diesem Falle fünfmal weniger ergiebig. Es ist aber auch möglich, den abgetasteten Impulskombinationen noch auf viele andere Weisen einzelne Schlüsselimpulse zuzuordnen, worauf aber nicht näher eingegangen werden soll. Die Ableitung eines Schlüsselimpulses aus je fünf Schlüsselimpulsen nach irgendeiner Regel verkompliziert aber die Verschlüsselung und erschwert eine unbefugte Entschlüsselung.

Bei der Fernschreibverschlüsselung kann man, wie beschrieben, vorgehen. Für die Faksimileverschlüsselung oder für die Sprachverschlüsselung hingegen sind die durch elektromechanische (Fühler) oder elektrooptische (Photozellen) Abtastvorrichtungen erzielbaren Abtastgeschwindigkeiten der Lochringe bei weitem nicht ausreichend. Bei der Faksimileverschlüsselung, bei der, wie bereits erwähnt, 2000 Bildpunkte pro Sekunde verschlüsselt werden müssen, würde dies eine relative Transportgeschwindigkeit der Ringe zu den Abtastvorrichtungen von 5 m/sec erfordern. Aber auch eine plötzliche Änderung der relativen Anfangsstellung der Ringe zueinander entsprechend den geforderten Sprüngen im Schlüsselablauf ist technisch nicht durchführbar.

Zur Umgehung dieser mechanischen Schwierigkeiten wird in bekannter Weise auf mechanisch bewegte Teile des Schlüsselimpulsgenerators völlig verzichtet und die Abtastung rein elektronisch vorgenommen.

Zu diesem Zwecke wird mit Hilfe eines kurzen, sogenannten Urlochstreifens, dessen eines Ende nicht mehr treppenförmig abgestuft zu sein braucht, eine Kontaktbank programmiert, deren Kontakte wie die Löcher eines voll ausgestanzten Lochstreifens angeordnet sind. Auf die Kontaktstifte der Kontaktbank wird der Urlochstreifen gelegt und auf diesen eine dünne, elektrisch leitende Metallfolie, welche zusammen mit dem Lochstreifen durch einen Weichgummiklotz auf die Kontaktstifte gepreßt wird. Die Metallfolie wird dabei durch die Löcher des Urlochstreifens etwas hindurchgedrückt und gibt Kontakt mit den darunter befindlichen Kontaktstiften. Diese nehmen das Potential der Folie an, während diejenigen Kontaktstifte, die durch das Lochstreifenpapier abgedeckt sind, ein anderes Po-

tential haben. Auf diese Weise sind die Löcher und Nichtlöcher des Urlochstreifens in Form von zwei verschiedenen Potentialen der zugeordneten Kontaktstifte der Kontaktbank programmiert. Die fünf Kontaktreihen (parallel zur Längenausdehnung der Kontaktbank) werden nun durch fünf elektronische Ringzähler synchron und periodisch abgetastet, beginnend mit einer beliebig einstellbaren Kontaktkonfiguration quer zu den Kontaktreihen. Dabei haben die fünf Ringzähler verschiedene Zählerperioden, deren keine zwei einen gemeinschaftlichen Teiler haben und deren größte nicht größer als die Anzahl der Kontaktstifte einer Kontaktreihe ist, die der Länge des eingelegten Lochstreifens entspricht.

Es ist klar, daß es bei dieser rein elektronisch arbeitenden Vorrichtung leicht möglich ist, eine Änderung der abzutastenden Anfangskontaktkonfigurationen der Kontaktstifte quer zu den Kontaktreihen zum Zweck der geforderten Sprünge im Schlüsselablauf in Bruchteilen einer Millisekunde durch entsprechende Kommandos an die Ringzähler herbeizuführen. Außerdem ist eine beträchtliche Steigerung der Abtastgeschwindigkeit möglich.

In der Gesamtperiode des Ringzähler-systems ist eine Anzahl von Unterperioden enthalten, nach deren Ablauf sich gewisse Teilkombinationen der abgetasteten Potentialkombinationen (von zwei Elementen zur fünften Klasse) wiederholen. Zunächst einmal sind die Zählerperioden selbst, im Beispielfalle die bereits erwähnten Perioden 25, 27, 67, 71, 73, Unterperioden, und zwar die kleinsten. Weiter gibt es zehn verschiedene Unterperioden, die aus dem Produkt je zweier Zählerperioden bestehen. Nach Ablauf jeder dieser Unterperioden wiederholen sich jeweils gewisse »Zweier-Teilkombinationen« der Ausgangs-Fünfer-Kombination der beiden Potentiale. Ferner gibt es ebenfalls zehn verschiedene Unterperioden, die aus dem Produkt je dreier Zählerperioden bestehen. Nach Ablauf jeder dieser Unterperioden wiederholen sich jeweils gewisse »Dreier-Teilkombinationen« der gewählten Ausgangskombination. Schließlich gibt es fünf verschiedene Unterperioden, die aus dem Produkt je vierer Zählerperioden bestehen. Nach Ablauf jeder dieser Unterperioden, die die größten nach der Gesamtperiode sind, wiederholen sich jeweils gewisse »Vierer-Teilkombinationen« der gewählten Anfangskombination.

Eine Unterperiode teilt die gesamte Schlüsselperiode in eine Anzahl Schlüsselabschnitte, die gleich dem Quotienten aus Gesamtperiode und Unterperiode ist. Die Anzahlen der Potentialkombinationen, die diese Schlüsselabschnitte enthalten, sind einander gleich und gleich der Unterperiode. Aneinandergrenzende Schlüsselabschnitte überlappen sich dabei niemals. Bildet man nun eine Unterperiode aus dem Produkt dreier der fünf Zählerperioden und eine zweite Unterperiode aus dem Produkt der beiden übrigen Zählerperioden, so wird die gesamte Schlüsselperiode in so viele Schlüsselabschnitte von jeweils der Länge des Produktes der drei Zählerperioden eingeteilt, wie das Produkt der beiden übrigen Zählerperioden beträgt. Auf das erwähnte Zahlenbeispiel angewendet, bedeutet dies, daß die aus dem Produkt aller Zählerperioden gebildete Gesamtperiode, nämlich  $324 \cdot 401 \cdot 175$ , durch das Produkt der beiden Zählerperioden 25 und 27 in 675 gleich lange Schlüsselabschnitte eingeteilt wird, deren jeder

$$67 \cdot 71 \cdot 73 = 347 \cdot 261$$

Kombinationen enthält. Werden zum Verschlüsseln von Faksimileinformationen 2000 Kombinationen pro

Sekunde benötigt, so beträgt die Laufzeit eines Unterperiodenabschnittes  $347 \cdot 261 : 2000 = 173,6$  sec. also fast 3 Minuten.

Nimmt man an, daß die Periode einer Schlüsselbestückung für einen ganzen Betriebstag, also 24 Stunden, ausreichen soll, und nimmt man zweckmäßigerweise auch die Unterteilung einer Stunde in 24 Teile, d. h. in Zeitabschnitte zu je 2,5 Minuten, vor, so ist eine recht günstige Voreinstellmöglichkeit für den Schlüssel gefunden. Von der Zählerperiode 25 werden nur 24 Schritte verwendet, und zwar je einer für die 24 Stunden des Tages, und von der Zählerperiode 27 werden ebenfalls nur 24 Schritte benutzt, und zwar je einer für die 2,5 Minuten langen Zeitabschnitte einer Stunde. Es wurde oben eine Laufzeit von 173,6 sec für einen Schlüsselabschnitt bei Verwendung der Zählerperioden 25 und 27 errechnet. Es bleibt demnach ein zeitlicher Sicherheitsüberschuß von  $173,6 - 150 = 23,6$  sec übrig

Die Weiterschaltung des Schlüsselablaufs, d. h. die Einstellung der Sprungstellen, geht nun in der folgenden Weise vor sich:

Vor dem Start des Schlüsselimpuls-generators werden alle Ringzähler auf Null gestellt, was irgendeiner Anfangskonfiguration von fünf Kontaktstiften aus den fünf Kontaktreihen entsprechen möge, beispielsweise jeweils der erste Kontakt aus jeder Kontaktreihe an einem Ende der Kontaktbank. Alle fünf Zähler beginnen gleichzeitig, synchron und periodisch mit der Taktfrequenz 2000 Hz zu zählen und tasten dabei die ange-troffenen Kontaktpotentiale ab. Nach Ablauf von 2,5 Minuten, währenddessen sie 300 000 Potentialkombinationen — den Unterperiodenabschnitt — abgetastet haben, werden sie alle auf Null gestellt, und der Zähler mit der Periode 27 wird auf die Zählstellung »1« gestellt. Daraufhin werden alle Zähler von dieser neuer Startstelle an von neuem gestartet, und sie laufen wieder 2,5 Minuten lang, woraufhin sie wieder alle auf Null gestellt werden, der Zähler mit der Periode 27 jedoch auf »2« gestellt wird. Alle 2,5 Minuten wird dieser Zähler um eine Zählstellung weitergestellt, nachdem jedes Mal vorher alle Zähler auf Null gestellt wurden, bis er nach Ablauf von einer Stunde die Zählstellung »24« erreicht hat. Wieder werden alle Zähler auf Null gestellt dieses Mal jedoch der Zähler mit der Periode 25 auf »1«. Nach Ablauf von weiteren 2,5 Minuten werden beide Zähler mit den Perioden 27 und 25 auf »1« gestellt, nach Ablauf von weiteren 2,5 Minuten der Zähler mit der Periode 27 auf »2« und der Zähler mit der Periode 25 auf »1«, usf. Der Zähler mit der Periode 27 wird also alle 2,5 Minuten und der Zähler mit der Periode 25 jede Stunde um eine Zählstellung weitergestellt bis nach Ablauf von 24 Stunden beide Zähler die Zählstellung »24« erreicht haben. Jetzt ist die gesamte Schlüsselperiode abgelaufen, wobei, wie bereits erwähnt, die Schlüsselabschnitte nicht voll ausgenutzt und  $675 - 576 = 99$  Abschnitte überhaupt nicht verwendet wurden. Diese auf die beschriebene Weise alle 2,5 Minuten neu eingestellten Schlüsselabschnitte folgen nun zwar zeitlich, aber keineswegs räumlich in der gesamten Schlüsselperiode unmittelbar aufeinander sondern sind anscheinend regellos über die gesamte Schlüsselperiode verteilt. Markiert man sich in dieser alle Sprungstellen, so erkennt man, daß diese äquidistant sind und daß sich räumlich aufeinanderfolgende Schlüsselabschnitte niemals überlappen, daß mithin eine mehrfache Verwendung gleicher Schlüsselabschnitte ausgeschlossen ist.

Das alle 2,5 Minuten erfolgende »auf Null stellen«

aller Zähler und das Weiterschalten des Zählers mit der Periode 27 um einen Zählschritt sowie das jede Stunde erfolgende Weiterschalten des Zählers mit der Periode 25 um einen Zählschritt wird durch eine Schaltuhr, die alle 2,5 Minuten einen Impuls abgibt, veranlaßt. Diese Impulse geben den Takt für zwei Hilfszähler mit je der Zählperiode 24, von denen der eine die 2,5-Minuten-Abschnitte und der andere die vollen Stunden zählt. Bei jedem Zählschritt stellt der eine dieser beiden Hilfszähler durch Abgabe eines Impulses den einen Abtastzähler mit der Periode 27 und der andere den zweiten Abtastzähler mit der Periode 25 jeweils auf Null und unmittelbar darauf um eine Zählstellung gegenüber der zuletzt innegehabten weiter.

Das beschriebene, etwas kompliziert und nicht systematisch erscheinende Verfahren der Weiterstellung der Abtastzähler wurde deshalb gewählt, weil es mit einem Minimum an unterscheidbaren Kommandos an das Ringzählersystem auskommt. Dies ist dann von Bedeutung, wenn die Weiterstellung der Abtastzähler nicht durch eine lokale Schaltuhr, sondern, wie beim Fernschreibbetrieb möglich, durch vom Sender übertragene kurze Codeworte veranlaßt wird, wobei keine uferlosen Möglichkeiten an Kommandokombinationen zur Verfügung stehen.

Für den Verschlüsselungsbetrieb mit Fernschreibern kann das gleiche Verfahren, wie am Beispiel der Faksimileverschlüsselung beschrieben, verwendet werden. Im Gegensatz zum stetig arbeitenden Faksimilebetrieb, wobei die Schlüsselimpulse im regelmäßigen Takt erzeugt werden müssen, werden die Schlüsselimpulsgeneratoren beim Fernschreibbetrieb gemäß dem Start-Stop-Prinzip der Springschreiber intermittierend betrieben, indem mit jedem Startschritt eines Fernschreibzeichens der Schlüsselimpulsgenerator ein-, und mit jedem Stoppschritt wieder ausgeschaltet wird, und zwischen Start- und Stoppschritt jeweils fünf Schlüsselimpulse erzeugt werden.

Wegen der geringen Informationsmenge (bit/sec), die vom Fernschreiber pro Sekunde übertragen wird, ist der Verbrauch an Schlüsselimpulsen pro Sekunde sehr viel geringer als beim Faksimilebetrieb. Bei der Übertragungsgeschwindigkeit von 7,14 Fernschreibzeichen pro Sekunde (50 Baud) werden 50 Schlüsselimpulse pro Sekunde benötigt, also vierzigmal weniger als beim Faksimilebetrieb. Auch beim Fernschreibbetrieb sollen die Zeitabschnitte, nach welchen jeweils das Eintreten eines Empfängers in eine laufende Übertragung möglich ist, also eine Weiterstellung des Schlüssels vorgenommen wird, 2,5 Minuten betragen, obwohl natürlich auch kürzere Zeitintervalle von beispielsweise einer Minute möglich wären, entsprechend der im Durchschnitt kürzeren Übertragungsdauer eines Fernschreibens gegenüber der einer Wetterkarte. Bei dem angenommenen Zeitintervall von 2,5 Minuten für die Schlüsselfortschaltung werden für die einzelnen Schlüsselabschnitte mindestens  $150 \cdot 50 = 7500$  Schlüsselimpulse benötigt, für einen ganzen Tag also mindestens

$$7500 \cdot 24 \cdot 24 = 4\,320\,00 \text{ Schlüsselimpulse.}$$

Daher können die Zählerperioden der fünf Abtastzähler viel kleiner als beim Faksimilebetrieb sein. Diese mögen beispielsweise 17, 19, 24, 25, 29 betragen. Zahlen, deren keine zwei einen gemeinschaftlichen Teiler haben. Die Gesamtperiode des Ringzählersystems beträgt dann  $17 \cdot 19 \cdot 24 \cdot 25 \cdot 29 = 5\,620\,200$  Schritte, ist also ausreichend groß.

Entsprechend dem beschriebenen Beispiel für die

Faksimileverschlüsselung wird auch hier die aus den Produkt aller Zählerperioden gebildete gesamte Schlüsselperiode durch das Produkt der beiden Zählerperioden 24 und 25 in 600 Schlüsselabschnitte, die je

$$5 \quad 17 \cdot 19 \cdot 29 = 9367 \text{ Impulskombinationen}$$

umfassen, eingeteilt. Diese für die 2,5-Minuten-Abschnitte ebenfalls reichlich bemessene Anzahl von Impulskombinationen hat eine Laufzeit vor

$$10 \quad 9367 : 50 = 187,3 \text{ sec.}$$

Es besteht also ein zeitlicher Sicherheitsüberschuß von  $187,3 - 150 = 37,3$  sec.

Auch hier werden zur sprunghaften Fortschaltung des Schlüssels nur die beiden Zähler mit den Zählerperioden 24 und 25 periodisch um je einen Zählschritt weitergestellt, und zwar der erste alle 2,5 Minuten und der zweite jede volle Stunde, von welcher letzterem die Zählstellung »25« jedoch nicht benutzt wird. Die übrigen drei Zähler werden alle 2,5 Minuten immer wieder auf Null gestellt, bleiben also an der Voreinstellung des Schlüssels unbeteiligt.

Es mag noch erwähnt werden, daß es auf dem beschriebenen bekannten Schlüsselverlängerungsverfahren beruhende Schlüsselimpulsgeneratoren gibt, die nicht regelmäßig mit jeder Taktzeit einen Schlüsselimpuls oder eine Schlüsselimpulskombination erzeugen, sondern welche zeitlich völlig unregelmäßig Schlüsselimpulse oder -kombinationen liefern, so daß sich diese zeitweise sehr häufen oder sehr spärlich auftreten können. In diesem Falle muß die Schlüsselimpulserzeugung mit einer vielfach höheren mittleren Erzeugungsgeschwindigkeit betrieben werden, als sie tatsächlich benötigt wird. Der Schlüsselimpulsgenerator wird dann intermittierend betrieben. Nur der erste von mehreren innerhalb einer Taktzeit erzeugten Schlüsselimpulsen wird zum Verschlüsseln verwendet, nach dessen Erzeugung der Generator sofort wieder abgeschaltet und mit Beginn der nächsten Taktzeit sogleich wieder eingeschaltet wird. Der Schlüsselimpulsgenerator steht also größtenteils still. Da der erste dieser während einer Taktzeit gelieferten Schlüsselimpulse zu einem beliebigen, nicht bekannten Zeitpunkt innerhalb der Taktzeit auftreten kann, kann er erst in der nächsten Taktzeit zum Verschlüsseln verwendet werden. Dieser intermittierende Betrieb erfordert eine Zwischenspeicherung der Schlüsselimpulse mit Hilfe zweier Wechselspeicherelemente, dessen eines für die geradzahigen, und dessen anderes für die ungeradzahigen Schlüsselimpulse dient.

Bei der Verschlüsselung von Sprache, die nach dem Verfahren der Puls-Code-Modulation (PCM) übertragen wird, ist die pro Sekunde benötigte Anzahl von Schlüsselimpulsen noch erheblich größer als bei der Faksimileverschlüsselung, und ein geeigneter Schlüsselimpulsgenerator kann nur rein elektronisch arbeiten.

Bei der Übertragung von Sprache wird das tonfrequente Frequenzband bekanntlich auf 3000 Hz beschnitten, wobei noch Silbenverständlichkeit erzielt wird. Bei der Puls-Code-Modulation wird das stetige Sprachsignal mit einer Frequenz abgefragt, die mindestens das Doppelte der Bandbreite beträgt (um den Bedingungen des Shannonschen Abtasttheorems der Nachrichtentechnik zu genügen), also mindestens 6000mal pro Sekunde. Werden diese diskreten Signalproben quantisiert und die Signalquanten in einem fünfstelligen Binärkode kodiert, damit 32 verschiedene Amplitudenstufen, d. h. Lautstärken, unterschieden werden können, so kommt man auf eine Impulsfrequenz von 30 kHz. Zur Verschlüsselung der Codeimpulskombina-

tionen müssen daher 30 000 Schlüsselimpulse pro Sekunde zur Verfügung stehen.

Wählt man als Fortschalteperiode für den Schlüssel das Zeitintervall von einer Minute, so müssen pro Minute mindestens

$$30\ 00 \cdot 60 = 1,8 \cdot 10^6 \text{ Schlüsselimpulse}$$

erzeugt werden, pro Stunde also

$$1,8 \cdot 10^6 \cdot 60 = 1,08 \cdot 10^8$$

und pro Tag

$$1,08 \cdot 10^8 \cdot 24 = 2,592 \cdot 10^9 \text{ Schlüsselimpulse.}$$

Wählt man für die fünf Zähler etwa die Zählerperioden 25, 61, 133, 137, 139, deren keine zwei einen gemeinschaftlichen Teiler haben und was einer Urlochstreifen gleich lange von rund 35 cm entspricht, so beträgt die gesamte Schlüsselperiode rund  $3,86 \cdot 10^9$ , ist also reichlich bemessen. Durch das Produkt der beiden Zählerperioden 25 und 61 wird die gesamte Schlüsselperiode in 1525 gleichlange Schlüsselabschnitte unterteilt, deren jeder

$$133 \cdot 137 \cdot 139 \sim 2,53 \cdot 10^6 \text{ Kombinationen}$$

enthält. Diese, für die 1-Minuten-Abschnitte ebenfalls ausreichend bemessene Anzahl von Impulskombinationen hat eine Laufzeit von rund

$$2,53 \cdot 10^6 : 3 \cdot 10^4 \sim 84 \text{ sec.}$$

Es bleibt also ein zeitlicher Sicherheitsüberschuß von 24 sec übrig.

Für die sprunghafte Fortschaltung des Schlüssels werden nur die beiden Zähler mit den Zählerperioden 61 und 25 periodisch um je einen Zählschritt weitergestellt, und zwar der erste jede Minute und der zweite jede Stunde, wobei jedoch die Zählstellungen »61« und »25« nicht verwendet werden. Die übrigen drei Zähler werden jede Minute immer wieder auf Null gestellt, bleiben also an der Fortschaltung des Schlüssels unbetieilt.

Auf diese Weise kann sich ein später in eine Telefonverbindung eintretender befugter Abhörer von Nachrichten jede Minute in die Verbindung einschalten.

Die sprunghafte Fortschaltung des Schlüssels kann sowohl durch lokale Schaltuhren als auch durch vom Sender übertragene Codeworte vorgenommen werden. In den Zeichnungen wird die Erfindung an Hand von Ausführungsbeispielen näher erläutert.

Fig. 1 zeigt eine Faksimileempfangsanlage mit Schaltuhr;

Fig. 2 zeigt eine Fernschreiberempfangsanlage mit Schaltuhr;

Fig. 3 zeigt eine Fernschreiberempfangsanlage, bei der die Schlüsselvoreinstellung mittels eines Codewortes übertragen wird.

Die Wirkungsweise einer Faksimileempfangsanlage mit Schaltuhr ist in Fig. 1 dargestellt.

Die Anlage besteht aus drei Bauteilen, nämlich dem Hauptteil I, welcher das Faksimilegerät mit den Steuerorganen enthält, den Schlüsselimpulsgenerator II, welcher die fünf Urpotentialfolgen, gespeichert in dem Urlochstreifen 26, enthält, aus denen die Schlüsselimpulsfolge mit großer Periode gewonnen wird, und schließlich das Zeitschaltwerk III, welches die Voreinstellung der Abtastzähler mit den Zählerperioden 25 und 27 bewirkt.

Es sei zunächst unterschieden zwischen einem ersten Start der Anlage und dem der Erfindung entsprechen-

den Fall des nachträglichen Einschaltens eines Empfängers in eine ablaufende Faksimileübertragung. Vor deren Beginn ist die Schlüsselverbindung zwischen Sender und Empfänger herzustellen. Zu diesem Zwecke gibt der Sender zunächst ein Vorsignal über die Fernleitung 1 zum Empfänger. Dieses Vorsignal hat erstens den Zweck, den Empfänger durch Aufhebung einer aus dem Filter 2 bestehenden Sperrung, welche ihn vor Fehlstarts durch Störgeräusche schützt, empfangsbereit zu machen, und zweitens, den Taktgenerator 4, durch welchen der Funktionsablauf des Empfängers gesteuert wird, in Phase mit dem Taktgenerator des Senders zu bringen. Das Vorsignal in Leitung 1 gelangt über das Filter 2 und die Leitung 3 zum Taktgenerator 4. Das Bandfilter 2 läßt nur die Trägerfrequenz hindurch, außerdem wirkt es zeitverzögernd, so daß die Empfangsspannung etwas verspätet an die Leitung 3 gelangt. Diese Spannung gelangt auch über den Gleichrichter 5, über die Leitung 6 zum Schalter 7, welcher in Arbeitsstellung geht und über die Leitung 8 das Tor 9 öffnet. Dadurch gelangt die noch bestehende Spannung des Vorsignals von Leitung 1 über das Tor 9 zur Leitung 10 und über das Tor 11 auch zum Schalter 12, welcher in Arbeitsstellung geht. Dabei entsteht ein Impuls an Leitung 19, der zum Schalter 18 führt und ihn in die Ruhestellung bringt, falls er sich nicht bereits in dieser Stellung befindet. Eine weitere Wirkung erfolgt zunächst nicht.

Nach Aufhören des Vorsignals fällt der Schalter 12 mit etwa 20 msec Verzögerung ab. Dabei entsteht ein Impuls an Leitung 13, welcher den Schalter 14 in Arbeitsstellung bringt. Dieser sperrt über die Leitung 15 das Tor 11 und öffnet das Tor 16. Ein kurze Zeit später auftretendes Nachsignal von bestimmter Dauer (8 Taktzeiten = 4 msec) findet das Tor 9 noch geöffnet vor, da der Schalter 7 eine große Zeitverzögerung hat, und gelangt über Leitung 10 und Tor 16 zur Leitung 17 und zum Schalter 18, welcher in Arbeitsstellung geht. Über die Leitung 20 gelangt Spannung an die fünf Ringzähler 21 bis 25, welche den fünf Lochreihen des Urlochstreifens 26 zugeordnet sind, und bringt diese in ihre Null-Stellungen. Die Spannung an Leitung 20 bringt außerdem den Schalter 27 im Zeitschaltwerk III in Arbeitsstellung, welcher über die Leitung 28 den Impulsgenerator 29 einschaltet und damit die Voreinstellung der Ringzähler 21 bis 25 im Schlüsselimpuls-generator II einleitet. Bis diese vollendet ist, muß der Beginn der Schlüsselerzeugung verzögert werden. Deshalb ist das Tor 31 noch gesperrt und verhindert zunächst, daß die Taktimpulse von Leitung 30 zum Schlüsselimpuls-generator II gelangen. Acht Taktzeiten später, als durch die Umschaltung des Schalters 18 über Leitung 20 Einschaltenspannung an den Zähler 32 gelangt ist, tritt Spannung an dessen Ausgang 33 auf, durch welche das Tor 31 geöffnet wird. Der neunte und alle weiteren Taktimpulse gelangen über Leitung 34 zum Schlüsselimpuls-generator II, welcher dadurch mit der Erzeugung der Schlüsselimpulsfolge beginnt.

Unabhängig von allen bisher beschriebenen Vorgängen, also auch unabhängig von der Einschaltung des Hauptteiles I und des Schlüsselimpulsgenerators II, spielt sich während des Zeitraumes von einem Tag im Zeitschaltwerk III, welches in dauerndem Betriebszustand ist, folgender Vorgang ab:

Der Chronometer 35 gibt nach jeder halben Minute über die Leitung 36 einen Impuls an, den Zähler 37, welcher nach jedem fünften Schritt einen Impuls über die Leitung 38 an den Einstellzähler 39 gibt. Dieser



13

schaltet, von seiner Null-Stellung ausgehend, mit jedem Impuls um einen Schritt weiter, wobei er nacheinander an alle seine Ausgänge Spannung legt. Der Einstellzähler 39 hat 24 Zählstufen, und, da er nach je 2,5 Minuten um einen Schritt weiterschaltet, ist nach einer Stunde ein voller Durchlauf vollendet. Angenommen, der Anfangszeitpunkt dieses Vorganges sei die Zeit 0.00 Uhr. Dann ist der erste Durchlauf nach dem 24. Schritt zur Zeit 1.00 Uhr erreicht.

In diesem Augenblick entsteht ein Impuls an der Leitung 40, welcher zum Eingang des Einstellzählers 41 gelangt und ihn in die erste Zählstellung schaltet. Der Einstellzähler 39 beginnt mit dem 25. Impuls an der Leitung 38 seinen zweiten Durchlauf, bis er nach insgesamt 48 Zählschritten seine Endstellung zum zweiten Mal erreicht hat. Damit geht auch zum zweiten Mal ein Impuls über die Leitung 40 an den Einstellzähler 41, welcher in die zweite Zählstellung geht. Dies geschieht zur Zeit 2.00 Uhr. Entsprechend der Uhrzeit des Tages stehen also die Einstellzähler 41 und 39 in bestimmten Zählstellungen, und zwar so, daß die Ordnungsnummer der Stellung des Zählers 41 die Tagesstunde, und die Ordnungsnummer der Stellung des Zählers 39 den 2,5-Minuten-Abschnitt dieser Stunde angibt. Die Stellung der Einstellzähler 39 und 41 ist maßgebend für die Startstellung des Schlüsselimpulsgenerators II. Während der acht Taktzeiten des Nachsignals erfolgt seine Voreinstellung entsprechend der Stellungen der Einstellzähler 39 und 41. Wie diese Voreinstellung vor sich geht, wird später erläutert. Mit dem neunten Taktimpuls nach Beginn des Nachsignals beginnt die Erzeugung der Schlüsselimpulse. Diese werden vom Schlüsselimpulsgenerator II über Leitung 80 zum zweiten Eingang des Mischgerätes 70 geliefert, dort mit den über Leitung 1 empfangenen Geheimimpulsen gemischt, und die gewonnenen Klarimpulse werden zum Faksimilegerät 72 geliefert und von diesem aufgezeichnet.

Angenommen, ein Empfänger, welcher bisher nicht an der Übertragung teilgenommen hat, will eine ab 10.30 Uhr übertragene Nachricht empfangen. Zu diesem Zwecke schaltet er gegen 10.20 Uhr sein Gerät ein. Der Teilnehmer empfängt zunächst Geheimsignale, welche aber nicht entschlüsselt werden können, da noch kein Gleichlauf des empfängerseitigen mit dem senderseitigen Schlüsselablauf besteht. Durch das Filter 2 wird der Träger ausgesiebt, und über die Leitung 3 wird der Taktgenerator 4 des Empfängers synchronisiert. Ferner ist über den Gleichrichter 5 und die Leitung 6 der Schalter 7 eingeschaltet und dadurch das Tor 9 geöffnet, wodurch die Geheimsignale auch an Leitung 10 über das Tor 11 auch an den Schalter 12 gelangen. Der Schalter 12 geht in Arbeitsstellung und gibt dabei einen Impuls über Leitung 19 an den Schalter 18, der dadurch in die Ruhestellung zurückgeht. Schalter 12 bleibt zunächst in Arbeitsstellung stehen. Die Wirkung ist die gleiche wie die des Vorsignals beim ersten Start des Schlüsselablaufes.

Der Uhrzeit 10.20 Uhr entsprechend steht der Einstellzähler 41 in seiner 10. und der Einstellzähler 39 in seiner 8. Stellung. Da die Weiterschaltung durch die Schaltuhr alle 2,5 Minuten erfolgt, stehen die Einstellzähler 41 und 39 in diesen Stellungen von 10.20 bis 10.22.30 Uhr. Es werde angenommen, daß der Sender um 10.21.15 Uhr seinen Schlüsselimpulsgenerator erneuert startet, d. h. etwa in der Mitte der durch das Zeitschaltwerk bestimmten Zeitabschnitte. Dies ist zweckmäßig, damit nicht die Gefahr besteht, daß Zeitunge-

nauigkeiten zwischen den Chronometern der einzelnen Stellen oder in den Neustartintervallen zu Fehlern führen.

Zum Zwecke des Neustartes unterbricht der Sender die Übertragung für etwa 50 msec. Dadurch fällt der Schalter 12, dessen Verzögerungszeit etwa 30 msec beträgt, ab und gibt über die Leitung 13 einen Impuls an den Schalter 14. Dieser geht in Arbeitsstellung, wodurch an Leitung 15 Spannung gelangt, welche das Tor 11 sperrt und das Tor 16 öffnet. Durch diesen Vorgang ist zunächst der Zustand erreicht, den alle vor diesem neu in die Verbindung eintretenden Empfänger bereits angenommen haben. Das nach einer Lücke von etwa 50 msec wieder einsetzende Nachsignal von acht Taktzeiten (= 4 msec) Dauer gelangt über die Leitung 17 zu dem Schalter 18, welcher in Arbeitsstellung geht. Der Schalter 18 legt Spannung an die Leitung 20, durch welche, wie bereits beschrieben, die Ringzähler 21 bis 25 in die Null-Stellung gebracht werden. Ferner geht der Schalter 27 in Arbeitsstellung und schaltet über die Leitung 28 den Impulsgenerator 29 ein. Schließlich wird durch die Spannung an der Leitung 20 der Verzögerungszähler 32 eingeschaltet, welcher nach acht Taktimpulsen seine Endstellung erreicht und über die Leitung 33 das Tor 31 öffnet.

Beim Sender und bei allen Empfängern, also auch bei den neu hinzugekommenen und sogar bei allen, welche die Möglichkeit haben, zu einem selbst gewählten späteren Zeitpunkt in die Verbindung einzutreten, stehen die Einstellzähler 41 und 39 in gleichen Stellungen, nämlich in der zehnten und achten. Bei allen in Betrieb befindlichen Anlagen gelangen von dem Impulsgenerator 29 Impulse der Frequenz 50 kHz zur Leitung 42 und weiter über die Tore 43 und 44 zu den Ringzählern 24 und 25. Diese schalten mit jedem Impuls um einen Schritt weiter. Gleichzeitig gelangen diese Impulse von der Leitung 42 auch zu dem Suchzähler 45. Dieser schaltet von seiner Null-Stellung aus schrittweise weiter und legt dabei nacheinander an alle seine Ausgänge Spannung. Nach acht Schritten entsteht Spannung an seinem Ausgang 46, welcher mit dem Und-Tor 47 verbunden ist. An dem zweiten Steuereingang dieses Tores, nämlich an Leitung 48, liegt Spannung, die vom Einstellzähler 39 geliefert wird. Durch das Auftreten von Spannung an seinen beiden Eingängen ist die Durchlaßbedingung für das Und-Tor 47 erfüllt, so daß Spannung an die Leitung 49 gelangt und der Schalter 50 in die Arbeitsstellung bringt. Damit wird das Tor 44 gesperrt, so daß fortan keine Impulse mehr an den Ringzähler 25 gelangen. Er bleibt in seiner achten Stellung zunächst stehen. Der Suchzähler 45 schaltet weiter und legt während seines zehnten Schrittes an seinen Ausgang, nämlich an Leitung 52, Spannung. Damit ist auch die Durchlaßbedingung für das Tor 53 erfüllt, denn der zweite Steuereingang dieses Tores, das ist der zehnte Ausgang des Einstellzählers 41, Leitung 54, führt ebenfalls Spannung. Es gelangt deshalb auch Spannung an die Leitung 55, wodurch der Schalter 56 in Arbeitsstellung geht und das Tor 43 sperrt. Dadurch gelangen keine Impulse mehr zur Leitung 57 und zum Ringzähler 24, so daß auch dieser nach zehn Schritten stehenbleibt. Der Suchzähler 45 schaltet inzwischen weiter und gibt nach einem vollen Durchlauf, also nach 24 Schritten, an die Leitung 58 Spannung, welche den Schalter 27 in die Ruhestellung zurückbringt. Damit verschwindet die Spannung an der Leitung 28, und der Impulsgenerator 29 wird angehalten.

Der Einstellvorgang der Ringzähler dauert höch-

10

15

9 78 034

16

stens 2,4 msec. Er ist also beendet, bevor der Zähler 32 seinen achten Zähler Schritt vollendet hat, was nach 4 msec geschehen ist. Zu diesem Zeitpunkt stehen die Ringzähler 21, 22, 23 in der Null-Stellung, der Zähler 24, der Stundenzahl entsprechend, in Stellung »10« und Zähler 25, der Minutenzahl entsprechend, in Stellung »8«. Da der Beginn des Nachsignals, das ist der Beginn der Takterzeugung, der Zeitnullpunkt des Schlüsselimpulsablaufes ist, beginnt die Erzeugung der Schlüsselimpulsfolge mit dem neunten Taktimpuls. Dieser passiert als erster das Tor 31 und gelangt an die Leitung 34. Die Ausgänge 75 bis 79 der Ringzähler 21 bis 25 werden durch den Urlochstreifen 26 gesteuert und nehmen unregelmäßig wechselnd positive und negative Potentiale an. Diejenigen Ringzähler, welche zufällig positive Ausgangsspannung haben, bereiten die Schalter 59 bis 63 vor. Durch den Taktimpuls an der Leitung 34 schalten die vorbereiteten Schalter um, während die nichtvorbereiteten in der Ruhestellung bleiben. Entsprechend dieser Umschaltung gelangt Spannung an die Leitungen 64 bis 68 oder nicht. In der Mehrfach-Überlagerungsstufe 69 wird aus dieser Spannungsconfiguration durch mehrfache Überlagerung ein positiver oder negativer Schlüsselimpuls gewonnen, welcher dem zweiten Eingang, Leitung 80, der Mischstufe 70 zugeführt wird und dort mit dem über die Fernleitung 1 an dem ersten Eingang der Mischstufe 70 gelangenden Geheimimpuls gemischt wird. Der entschlüsselte Klarimpuls geht über die Leitung 71 zum Faksimilegerät 72 und wird dort als Punkt oder Lücke aufgezeichnet.

Noch vor Ablauf der ersten Taktzeit müssen die Speicherschalter 59 bis 63 in die Ruhestellung gebracht, und alle Ringzähler 21 bis 25 um einen Schritt weiterschaltet werden. Zu diesem Zwecke war durch den ersten Taktimpuls an Leitung 34 auch der monostabile Schalter 73 umgeschaltet worden. Seine Schaltzeit ist so bemessen, daß er, bevor der zweite Taktimpuls an Leitung 34 auftritt, selbsttätig in die Ruhelage zurückkehrt. Dabei entsteht an Leitung 74 ein Impuls, welcher diese notwendige Rückschaltung der Speicherschalter und Weiterschaltung der Ringzähler vornimmt. Durch die Weiterschaltung der Ringzähler entstehen entsprechend den durch sie abgetasteten Potentialkonfigurationen andere Spannungsconfigurationen an den Leitungen 75 bis 79, wodurch andere der Schalter 59 bis 63 vorbereitet werden. Der nun folgende zweite Taktimpuls bringt die vorbereiteten Speicherschalter in Arbeitsstellung. Entsprechend der Konfiguration der eingeschalteten Schalter wird in der Mehrfach-Überlagerungsstufe 69 erneut ein Schlüsselimpuls gewonnen und an die Mischstufe 70 weitergeleitet, während gleichzeitig der Schalter 73 eingeschaltet wird. Bei seinem Rückschalten kurz vor Ende der zweiten Taktzeit bringt er die Speicherschalter in Ruhestellung, schaltet die Ringzähler um einen Schritt weiter und stellt so den dritten Schlüsselimpuls bereit. Dieser Vorgang läuft sinngemäß weiter. Die Übertragung der verschlüsselten Nachricht geht ordnungsgemäß vor sich, und auch der neu hinzugekommene Empfänger nimmt an der Übertragung teil. Da die ihn interessierende Nachricht um 10.30 Uhr beginnt, ist er früh genug in die Verbindung eingetreten.

Der beschriebene Vorgang — Unterbrechung der Übertragung, Rück- und Neueinstellung der Ringzähler in den Schlüsselimpulsgeneratoren und neuer Start — dauert insgesamt etwa 54 msec. Dies ist eine Unterbrechungszeit, die keine nennenswerte Störung in der Faksimileübertragung zur Folge hat. Bei einer normalen

Aufzeichnungsgeschwindigkeit von 40 cm pro Sekunde würde diese Lücke in der Übertragung einen punktierten Strich von etwa 2 cm Länge auf dem übertragenen Faksimilogramm verursachen. Dieser punktierte Strich entsteht deshalb, weil die Schlüsselimpulse vom Sender ausbleiben und die Faksimilegeräte aller Empfänger während dieser Zeit selbst erzeugte Schlüsselimpulse aufzeichnen. Diese kleine Störung tritt verhältnismäßig selten auf, und zwar in Abständen von 2,5 Minuten. Dies bedeutet, daß auf einer Bildfläche vom Format DIN A 5 einmal ein solcher Störstrich auftritt. Es besteht aber die Möglichkeit, diese Störung dadurch zu beseitigen, daß der Neustart in eine Lücke der Faksimileübertragung verlegt wird.

Beim Sender ist die Bildvorlage auf eine Trommel aufgespannt, wobei die beiden gegenüberliegenden Bildkanten durch Spangen festgehalten werden. Der Abtastlichtpunkt überläuft bei jeder Trommelumdrehung diese für die Bildübertragung tote Zone einmal. Da sich die Trommel wenigstens einmal pro Sekunde dreht, besteht in jeder Sekunde wenigstens einmal die Möglichkeit, ohne Störung der Bildübertragung die Verschlüsselungsgeräte neu zu starten. Dies geht so vor sich, daß der Sender in Abständen von 2,5 Minuten die Kommandosignale für die Neustarte auslöst, daß ein solches Signal aber durch eine Kupplung mit der Trommelbewegung des Faksimilesenders bis zur nächstfolgenden Übertragungslücke verzögert wird. Diese Verzögerung von maximal 1 sec ist bedeutungslos gegenüber dem früher errechneten zeitlichen Sicherheitsüberschuß von 23,6 sec, um den ein Schlüsselabschnitt maximal länger laufen kann, als normalerweise erforderlich ist.

Ein zweites Ausführungsbeispiel, welches eine Fernschreiberempfangsanlage mit Schaltuhr betrifft, ist in Fig. 2 dargestellt. Die Übertragungsanlage möge, ebenso wie in der Anlage nach Fig. 1, aus einer zentralen Sendestelle und vielen empfangenden Stellen bestehen. In die vom zentralen Sender laufend übermittelte Nachrichtensendung sollen sich einzelne Empfänger nachträglich einschalten können.

Auch diese Anlage besteht aus drei Bauteilen, nämlich dem Hauptteil I, welcher die Steuerorgane für den Betrieb der Fernschreibmaschine und Einrichtungen für den Empfang der Kommandosignale enthält, ferner dem Schlüsselimpulsgenerator II und dem Zeitschaltwerk III. Die Bauteile II und III sind die gleichen, wie die in Fig. 1 beschrieben. Deshalb sind auch die einzelnen Bauelemente des Bauteils II in beiden Figuren mit den gleichen Bezugswahlen numeriert, und der Bauteil III ist aus Platzgründen nur als Block gezeichnet.

Der Teilnehmer, welcher in eine ablaufende geheime Nachrichtenübertragung eintreten will, schaltet seine Empfangsanlage ein, welche sich zunächst im Betriebszustand »Klarbetrieb« befindet. Sie empfängt zwar geheime Nachrichten, ohne sie aber entschlüsseln zu können. Die Fernschreibmaschine der Anlage soll deshalb zunächst noch nicht eingeschaltet werden. Während der ersten empfangenen Geheimsignale, insbesondere, wenn diese mittels Lochstreifenbetrieb maschinell gesendet werden, ist möglicherweise der Gleichlauf der Fernschreibmaschinen von Sender und Empfänger noch nicht vorhanden, da die empfangende Anlage nicht sofort die Startschritte der Zeichenkombinationen erkennen kann. Während der Übertragung einiger Fernschreibzeichen stellt sich der Gleichlauf jedoch selbsttätig ein.

Die empfangenen Nachrichtensignale gelangen von

der Fernleitung 1 zum ersten Eingang des Mischgerätes 70. Der zweite Eingang, Leitung 81, ist ohne Spannung, da der Schlüsselimpulsgenerator II noch außer Betrieb ist. Die Signale gehen deshalb durch das Mischgerät hindurch, ohne entschlüsselt zu werden, d. h., die Signale haben an der Ausgangsleitung 99 des Mischgerätes positive, Signallücken dagegen negative Spannung zur Folge. Die Signale an Leitung 1 gelangen ferner an den bistabilen Schalter 82. Durch den Startschritt eines empfangenen Fernschreibzeichens geht Schalter 82 in die Arbeitsstellung. Dadurch entsteht Spannung an Leitung 83, welche den Taktgenerator 84 in Tätigkeit setzt. Dieser liefert nadelförmige Taktimpulse der Frequenz von 50 Hz. Das ist die gleiche Frequenz, mit welcher die einzelnen Zeichenschritte der Fernschreibzeichen gesendet werden. Die Taktimpulse gelangen über die Leitung 85 zum Zähler 86. Dieser hat sieben Zählstellungen, welche den sieben Zeichenschritten eines Fernschreibzeichens entsprechen; das sind der Startschritt, fünf Informationsschritte und der Stoppschritt. Durch die Taktimpulse gesteuert, legt der Zähler 86 nacheinander an seine sieben Ausgänge Spannung. Die Zeiten, während welcher Spannung an den Ausgängen liegt, sind mit hinreichender Genauigkeit zeitgleich mit den einzelnen Schritten der empfangenen Fernschreibzeichen. Während des Startschrittes liegt Spannung am ersten Ausgang, nämlich an Leitung 87. Beim ersten Informationsschritt liegt Spannung am zweiten Ausgang 88, beim zweiten Informationsschritt an Ausgang 89, bis schließlich beim siebenten Schritt des Fernschreibzeichens, dem Stoppschritt, der siebente bzw. nullte Ausgang des Zählers Spannung führt. Dieser Zählerausgang ist, ebenso wie der erste Ausgang, mit Leitung 87 verbunden. Sie führt zum Steuereingang des Tores 172. Während des Start- und des Stoppschrittes liegt Spannung an Leitung 87, durch welche das Tor 172 gesperrt wird, so daß keine Schlüsselimpulse zum Mischgerät gelangen. Von den sieben Schritten der Fernschreibzeichen werden nämlich nur die fünf Informationsschritte verschlüsselt, während Start- und Stoppschritt als reine Betriebssignale unverschlüsselt übertragen werden. Mit Erreichen des siebenten Schrittes entsteht auch ein Impuls an Leitung 93, wodurch der Schalter 82 wieder in die Ruhestellung gebracht wird. Dadurch wird Leitung 83 stromlos, und der Taktgenerator 84 bleibt stehen. Der Impuls an Leitung 93 stellt alle während der abgelaufenen Übertragung in Arbeitsstellung befindlichen Speicherschalter 105 bis 109 in die Ruhestellung. Der siebente Schritt ist gleichzeitig Ruhestellung des Zählers 86, in welcher er verharret, bis ein neues Fernschreibzeichen empfangen wird.

Jedes weitere empfangene Fernschreibzeichen bringt auf die gleiche Weise durch seinen Startschritt den Schalter 82 zum Wiederansprechen, wodurch der Taktgenerator 84 und der Zähler 86 erneut sieben Schritte machen und beim Erreichen des siebenten Schrittes durch die Rückschaltung des Schalters 82 sich selbsttätig wieder abschalten. Die dabei an den Leitungen 88 bis 92 nacheinander entstehenden Spannungen werden den Steuereingängen der Tore 94 bis 98 zugeführt. Die Tore werden dabei nacheinander durchlässig. Der Ausgang des Mischgerätes 70 ist mit den Eingängen dieser Tore durch die Leitung 99 verbunden. Es gelangt jedesmal dann Spannung durch eines der geöffneten Tore 94 bis 98, wenn der zugeordnete Informationsschritt des Fernschreibzeichens gerade positiv ist.

Solange der Schlüsselimpulsgenerator II noch nicht in Betrieb ist, was vorläufig angenommen wird, gelangt

die Spannung des ersten Informationsschrittes von der Fernleitung 1 ohne Veränderung ihres Informationswertes über das Mischgerät 70 zur Leitung 99 und damit an die Eingänge der Tore 94 bis 98. Der erste Informationsschritt des Fernschreibzeichens  $+ - + + -$ , welches beispielsweise empfangen werden soll, ist positiv und steht auch als positive Spannung an Leitung 99 und an den Eingängen der Tore 94 bis 98 zur Verfügung. Da, wie erwähnt, während des ersten Informationsschrittes das Tor 94 geöffnet ist, gelangt die Spannung über das Tor 94 und die Leitung 100 zum Speicherschalter 105. Die Speicherschalter sind bistabile Schalter mit zwei Eingängen, welche durch einen Spannungsimpuls an einem Eingang eine bestimmte von zwei möglichen Lagen annehmen und durch einen Spannungsimpuls an dem anderen Eingang in die inverse Lage umgeschaltet werden. Der Schalter 105 geht in die Arbeitsstellung, und dadurch wechselt die Polarität an seinen Ausgangsleitungen 110 und 115. Die Leitung 115, bisher positiv, wird negativ, und die Leitung 110, bisher negativ, wird positiv. Der zweite Informationsschritt, während dessen Dauer das Tor 95 geöffnet ist, ist Signallücke. Es liegt also keine Spannung an Leitung 1, und deshalb ist auch die Leitung 99 spannungslos. Es gelangt keine Spannung an die Leitung 101, so daß der Speicherschalter 106 in Ruhe bleibt. Während des dritten Informationsschrittes, währenddessen das Tor 96 geöffnet ist, liegt wieder Signal an der Leitung 1 und positive Spannung an der Leitung 99. Sie gelangt über das geöffnete Tor 96 zum Speicherschalter 107, welcher in die Arbeitsstellung geht. Die Potentiale an seinen Ausgangsleitungen 112 und 117 wechseln. Die Leitung 112 wird positiv und Leitung 117 negativ. Auf die gleiche Weise geht während des vierten Informationsschrittes der Speicherschalter 108 in Arbeitsstellung, da der vierte Informationsschritt positiv ist. Der Speicherschalter 109 aber bleibt in Ruhe, da der fünfte Informationsschritt negativ, und die Leitung 99 spannungslos ist.

Das im Beispielsfalle gewählte Fernschreibzeichen  $+ - + + -$  entspricht dem Schriftzeichen *F*. Dieses Zeichen hat für den Empfänger jedoch keine Bedeutung und bleibt ohne Wirkung, d. h., es wird weder entschlüsselt noch geschrieben. Das gleiche geschieht mit weiteren empfangenen Fernschreibzeichen. Das Tor 173 bleibt gesperrt, so daß keine Fernschreibzeichen vom Fernschreiber 163 geschrieben werden. Das Empfangsgerät steht in Wartestellung bis zu einem bestimmten Zeitpunkt, in dem vom Sender Kommandosignale zum Eintritt in die verschlüsselte Nachrichtenübertragung gegeben werden.

Damit der neu hinzukommende Teilnehmer diese Kommandosignale auswerten kann, müssen diese im Klartext übermittelt werden. Der Sender und auch alle bereits an der Sendung teilnehmenden Partner müssen deshalb zunächst auf Klarbetrieb umgeschaltet werden. Das Kommando für die Umschaltung auf Klarbetrieb wird vom sendenden Teilnehmer gegeben.

Eine Möglichkeit, dies zu tun, besteht darin, daß eine Buchstabengruppe (Codewort) verschlüsselt gesendet wird, wodurch bei den Empfängern mittels einer selektiv auf diese Buchstabengruppe ansprechenden Einrichtung alle an der Verschlüsselungsübertragung teilnehmenden Empfänger in Klarbetrieb umgeschaltet werden. Die Umschaltung auf Klarbetrieb kann auch durch ein anderes charakteristisches Signal erfolgen. Es könnte z. B. dadurch geschehen, daß der Ruhebetrriebszustand der Verbindungsleitung für eine oder mehrere

Fernschreibzeichenlängen unterbrochen wird. Durch das Ausbleiben des Stoppschrittes eines oder mehrerer Fernschreibzeichen kann an den Empfangsstellen leicht ein Kriterium für die Umschaltung auf Klarbetrieb gewonnen werden. Welche der beiden genannten Arten im einzelnen Falle zweckmäßiger ist, ist von den Betriebsverhältnissen abhängig, vor allem von der Art des Übertragungsweges, d. h. ob Funkt oder Draht. Im Ausführungsbeispiel wird die Umschaltung auf Klarbetrieb durch die Aussendung einer Buchstabengruppe (Code-  
word) gewählt.

Nachdem alle Empfänger auf Klarbetrieb umgeschaltet worden sind, gibt der Sender im Klartext eine weitere Buchstabengruppe als Umschaltekommando, durch welche alle Empfänger, einschließlich der neu hinzukommenden, auf den verschlüsselten Betrieb umgeschaltet werden. Bei jedem dieser Neustarte beginnt der Schlüsselimpulsgenerator II, wie aus dem ersten Ausführungsbeispiel bekannt ist, von einer neuen Stelle der Schlüsselimpulsfolge an zu laufen. Die Startstelle des Impulsgenerators, von dem aus neu gestartet werden soll, wird durch das Zeitschaltwerk III, wie aus dem ersten Ausführungsbeispiel ebenfalls bekannt ist, vorbereitet.

Die Buchstabengruppe für die Umschaltung auf Klarbetrieb möge beispielsweise  $Q X V K$  sein, und für die Umschaltung auf Schlüsselbetrieb mögen die Buchstaben  $Q X V S$  vorgesehen sein. Die Buchstabengruppen für die Umschaltekommandos bestehen aus je vier Buchstaben. Diese verhältnismäßig große Buchstabenanzahl ist deshalb gewählt, damit fehlerhafte Umschaltungen vom Schlüssel- auf Klarbetrieb bzw. umgekehrt weitestgehend ausgeschaltet werden. Um eine weitere Sicherheit gegen Fehlumschaltungen zu haben, wird noch gefordert, daß die zur Umschaltung bestimmten Buchstaben einer Gruppe zeitlich unmittelbar aufeinanderfolgen.

Es sei angenommen, daß eine Übertragung verschlüsselter Nachrichten abläuft. Über die Fernleitung I kommen die Impulse der geheimen Fernschreibzeichen an, gelangen zum Eingang des Mischgerätes 70, wo sie mit den vom Schlüsselimpulsgenerator II über die Leitung 80, das Tor 172 und die Leitung 81 zugeleiteten Schlüsselimpulsen gemischt werden. Durch diese Mischung verschwinden die Schlüsselimpulse, und es stehen an der Ausgangsleitung 99 des Mischgerätes 70 Klarimpulse zur Verfügung. Sie gelangen über das Tor 173 und die Leitung 72 zum Fernschreiber 163 und werden dort aufgezeichnet.

Will der Sender neu hinzukommenden Teilnehmern die Möglichkeit geben, in die Sendung einzutreten, so muß er also zunächst durch die Aussendung der Buchstaben  $Q X V K$  das Umschaltekommando geben. Als ersten Buchstabe sendet er also  $Q$ , das ist das Fernschreibzeichen  $+++ - +$ . Entsprechend der bereits oben gegebenen Beschreibung gehen die Schalter 105, 106, 107 und 109 in Arbeitsstellung, während Schalter 108 in Ruhestellung bleibt. Dadurch erhalten die Leitungen 110, 111, 112 und 114, welche mit denjenigen Ausgängen der Speicherschalter verbunden sind, welche im Ruhezustand negativ sind, positives Potential. Bis zu diesem Zeitpunkt floß Strom vom Plus-Pol einer Stromquelle über den Widerstand 120, die Leitung 121 und über die parallelliegenden Dioden 122, 123, 124 und 126 zu den Leitungen 110, 111, 112 und 114, welche bisher negatives Potential führten. Durch den Spannungsabfall am Widerstand 120 wurde auch der Leitung 121 negatives Potential aufgedrückt. Durch das

Positivwerden der Leitungen 110, 111, 112 und 114 ist der Strom über den Widerstand 120 unterbrochen, und das Potential an Leitung 121 wird ebenfalls positiv. Dadurch schaltet der Schalter 127 um und legt Spannung an die Leitung 128. Der Schalter 127 ist ein monostabiler Schalter, welcher nach einer Zeit, die nur wenig größer als die Zeit ist, welche ein Fernschreibzeichen zur Übertragung benötigt, in Arbeitsstellung bleibt, dann aber automatisch in die Ruhestellung zurückgeht.

Unmittelbar auf die Übertragung des Buchstabens  $Q$  muß die Übertragung des Buchstabens  $X$  folgen, der durch das Fernschreibzeichen  $- + + +$  dargestellt wird. Entsprechend dieser Zeichenelementkombination schalten die Speicherschalter 105, 107, 108 und 109 um, wodurch die negative Spannung an den Kathoden der Dioden 132, 134, 135 und 136 verschwindet. Die Dioden werden damit undurchlässig. Damit wird auch die Leitung 131 positiv, weil kein Strom mehr über den Widerstand 130 fließt und kein Spannungsabfall mehr an ihm auftritt. Der Schalter 137 geht in die Arbeitsstellung und legt dabei an die Leitung 138 positive Spannung. Der Schalter 137 ist monostabil, ebenso wie Schalter 127. Auch seine Schaltzeit beträgt nur wenig mehr als die Übertragungszeit eines Fernschreibzeichens. Zu erwähnen ist noch, daß die Leitung 131 nur deshalb positiv werden kann, weil und solange sich der Schalter 127 in Betriebsstellung befindet und Leitung 128 positiv ist. Sonst flösse Strom über den Widerstand 130, die Leitung 131 und die Diode 129 zur negativen Seite des Schalters 127. Durch den Spannungsabfall am Widerstand 130 könnte deshalb die Leitung 131 nicht positiv werden, und der Schalter 137 bliebe in Ruhe. Da aber, wie bereits erwähnt, die Betriebszeit des monostabilen Schalters 127 nur wenig mehr als die Übertragungszeit eines Fernschreibzeichens beträgt, kann der Schalter 137 umschalten, wenn nur der Buchstabe  $X$  unmittelbar auf den Buchstaben  $Q$  folgt.

Unmittelbar auf den Buchstaben  $X$  wiederum muß die Zeichenelementkombination  $- + + +$  des Buchstabens  $V$  folgen. Dadurch gehen die Schalter 106 bis 109 in Arbeitsstellung. Die Dioden 143 bis 146 werden stromlos, und die Leitung 141 wird positiv. Die Abhängigkeit vom Schalter 137 besteht über die Diode 139 in der Leitung 138. Nur so lange der Schalter 137 umgeschaltet und die Leitung 138 positiv ist, kann auch die Leitung 141 positiv werden. Dadurch geht auch der Schalter 147 in Arbeitsstellung und legt positive Spannung an die Leitung 148.

Der nach der Übertragung der Buchstabengruppe  $Q X V$  unmittelbar folgende Buchstabe  $K$  bzw.  $S$  bewirkt die Umschaltung auf Klar- bzw. Schlüsselbetrieb. Zunächst muß aber auf Klarbetrieb umgeschaltet werden, deshalb folgt der Buchstabe  $K (+ + + -)$ . Entsprechend den erwähnten Vorgängen wird die Spannung an der Leitung 151 positiv, und der Schalter 157 geht in Arbeitsstellung. Dadurch gelangt Spannung an die Leitung 158, die den Schalter 169, welcher durch eine frühere Umschaltung auf Verschlüsselungsbetrieb in Arbeitsstellung ist, in die Ruhestellung bringt. Damit verschwindet die Spannung an der Leitung 170, wodurch das Tor 31 gesperrt wird und damit die vom Generator 84 über die Leitung 85 gelieferten Taktimpulse vom Schlüsselimpulsgenerator II ferngehalten werden. Gleichzeitig wird auch das Tor 173 gesperrt, so daß keine Impulse mehr zum Fernschreiber 163 gelangen und dieser die folgenden Buchstaben nicht mitschreibt.

Die Umschaltung auf Verschlüsselungsbetrieb soll anschließend erfolgen. Deshalb sendet der Sender in

Klarschrift unmittelbar hintereinander die Buchstaben-  
gruppe  $Q X V S$ . Die Buchstaben-  
gruppe  $Q X V$  wird  
also sowohl für die Umschaltung auf Klar- als auch auf  
Verschlüsselungsbetrieb verwendet. Sie ist gleichsam  
das Schutzkommando, welches die eigentlichen Kom-  
mandos  $K$  bzw.  $S$  wirksam macht und die Empfangsan-  
lagen vor Fehlschaltungen schützt. Am Empfang  
dieser Buchstaben-  
gruppe  $Q X V S$  nehmen nun auch  
die neu hinzukommenden Teilnehmer teil, deren An-  
lagen zum Klarempfang bereit sind.

Durch die den Buchstaben  $Q X V$  folgende Zeichen-  
elementkombination des Buchstabens  $S$  wird die Lei-  
tung **161** stromlos, und der Schalter **167** geht in Arbeits-  
stellung. Damit gelangt Spannung an die Leitung **168**,  
so daß der Schalter **169** umschaltet. Über die Leitung  
**170** gelangt Spannung an das Tor **173**, welches die  
Fernschreibmaschine **163** wieder einschaltet, und ferner  
an das Tor **31**, durch welches die von nun an folgenden  
Taktimpulse wieder zum Schlüsselimpuls-generator II  
gelangen. Mit der Umschaltung des Schalters **169** ent-  
steht durch Differenzierung in dem Differenzierglied  
**171** ein Impuls an der Leitung **20**, durch welchen alle  
Ringzähler **21** bis **25** des Impuls-generators II in die  
Null-Stellung gebracht werden und gleichzeitig das  
Zeitschaltwerk III in Tätigkeit gesetzt wird, wodurch  
die Ringzähler **24** und **25** der Tageszeit entsprechend  
eingestellt werden.

Diese Einstellung des Schlüsselimpuls-generators II  
geht sehr schnell vor sich und ist mit Sicherheit beend-  
et, bevor der erste Schlüsselimpuls benötigt wird. Die  
den einzelnen Zeichenelementen des nun folgenden  
Fernschreibzeichens zugeordneten Taktimpulse gelan-  
gen vom Taktgenerator **84** über die Leitung **85** und das  
Tor **31** zur Leitung **34** des Schlüsselimpuls-generators II.  
Dadurch werden die Schalter **59** bis **63** entsprechend  
der Konstellation der Ringzähler **21** bis **25** umgeschal-  
tet oder nicht umgeschaltet. Die Übertragung der ver-  
schlüsselten Nachricht, die nun auch von den neu hinzu-  
gekommenen Teilnehmern empfangen wird, geht, wie  
oben beschrieben, ordnungsgemäß weiter. Die Unter-  
brechung des gesamten Betriebes hat nur so lange ge-  
dauert, wie die Übertragungszeit der acht Kommando-  
buchstaben beträgt, das sind etwa 1,2 Sekunden. Diese  
kurze Unterbrechung erfolgt nach verhältnismäßig lan-  
gen Zeitabständen von 2,5 Minuten und ist im Fern-  
schreibbetrieb kaum störend.

Das dritte in Fig. 3 dargestellte Ausführungsbeispiel  
bezieht sich ebenfalls auf eine Nachrichtenübertra-  
gungsanlage mit Fernschreibern. Die neue Startstellung  
der Schlüsselimpulsfolgen wird im Gegensatz zu den  
beiden bisher gezeigten Ausführungsbeispielen nicht  
durch ein Zeitschaltwerk voreingestellt, sondern durch  
den Sender ferneingestellt.

Wie an Hand der Fig. 2 beschrieben, gibt der Sen-  
der nach bestimmten Zeitabständen eine verschlüsselte  
Buchstaben-  
gruppe als Kommandosignale, durch wel-  
che alle an der geheimen Nachrichtenübertragung be-  
teiligten Teilnehmer auf Klarbetrieb umgeschaltet wer-  
den, und sendet dann anschließend eine weitere Buch-  
staben-  
gruppe im Klartext, welche für alle Teilnehmer,  
einschließlich den neu hinzukommenden, das Komman-  
do gibt, auf Schlüsselbetrieb umzuschalten. Dieses letz-  
tere Kommandosignal ist in der Ausführung nach  
Fig. 3 gegenüber der in Fig. 2 dargestellten Anlage  
um zwei Buchstaben erweitert worden, welche die  
Startstellungen der Schlüsselimpulsfolgen bestimmen.

In dem neuen Ausführungsbeispiel ist die Buchsta-  
ben-  
gruppe  $Q V X K$  für die Umschaltung auf Klarbe-

trieb, und die Gruppe  $K X V Z$  für die unmittelbar  
anschließende Umschaltung auf Schlüsselbetrieb beibe-  
halten worden. Die zusätzlichen Buchstaben wechseln  
bei jedem neuen Start der Schlüsselimpulsfolge, wei-  
5 jeder neue Start von einer anderen Stelle der Schlüssel-  
periode aus erfolgt. Die Fernschreibzeichen bestehen  
aus Kombinationen von zwei binären Zeichenelemen-  
ten zur fünften Klasse, so daß entsprechend dem Fün-  
fer-Code 32 verschiedene Zeichenelementkombinatio-  
10 nen möglich sind. Jeder von diesen wird eine natürliche  
Zahl zugeordnet, so daß die beiden zusätzlichen Buch-  
staben bestimmte Zahlen zwischen 1 und 32 darstellen  
Von den 32 möglichen werden je 24 als Zahlen für die  
Einstellung der 24 Stunden des Tages und für die  
15 2,5-Minuten-Abschnitte der einzelnen Stunden verwen-  
det. Die Verschlüsselung der übertragenen Nachricht  
beginnt erst, nachdem die beiden Buchstaben zur Ein-  
stellung der neuen Startstelle der Schlüsselimpulsfolge  
gesendet worden sind.

In der Fig. 3 sind alle mit den Nummern **81** bis **173**  
bezeichneten Bauteile die gleichen wie die in Fig. 2,  
und auch die entsprechenden Funktionsabläufe bei der  
Umschaltung auf Klarbetrieb und der anschließenden  
Rückschaltung auf Verschlüsselungsbetrieb sind die  
25 gleichen.

Nach Empfang der als Kommando für die Umschal-  
tung auf Verschlüsselung gegebenen Buchstaben-  
gruppe  $Q X V S$  gehen, wie aus der Fig. 2 bekannt ist, die  
Schalter **167** und **169** in die Arbeitsstellung. Dabei ent-  
steht Spannung an Leitung **174**, welche das Tor **202**  
öffnet. Gleichzeitig wird in dem Differenzierglied **171**  
ein Impuls gewonnen, der über die Leitung **20** zum  
Schlüsselimpuls-generator II geführt wird und die Rück-  
schaltung aller Ringzähler **21** bis **25** in die Null-Stellung  
35 bewirkt. Der Schalter **169** bleibt fortan in dieser Stel-  
lung, während der monostabile Schalter **167** nach einer  
Zeit, welche gleich der Zeit ist, die zwei Fernschreibzei-  
chen zu einer Übertragung benötigen, wieder in die Ru-  
hestellung zurückkehrt. Es bleibt also zunächst noch  
40 Spannung an Leitung **175** bestehen, wodurch das Tor  
**176** geöffnet wird.

Der Startimpuls des folgenden ersten zur Einstellung  
der Ausgangsstellung des Schlüsselimpuls-generators  
bestimmten Buchstabens, der noch unverschlüsselt  
übertragen wird, bewirkt die Umschaltung des Schal-  
ters **82**. Die fünf Informationsschritte des Fernschreib-  
zeichens dieses Buchstabens werden nacheinander in  
den Speicherschaltern **105** bis **109** gespeichert. Ihre  
Ausgangsleitungen **110** bis **114** sind an die Eingänge des  
Decodierers **177** geführt. Entsprechend der an seinem  
Eingang auftretenden Spannungskonfiguration entsteht  
an einem von 24 Ausgängen **178**...**179**... bis **180** des  
Decodierers **177** Spannung. Durch den Stopimpuls des  
Fernschreibzeichens dieses Buchstabens schaltet der  
Schalter **82** in die Ruhestellung zurück. Dabei entsteht  
an der Leitung **181** ein Impuls, welcher über das geöff-  
nete Tor **176** zur Leitung **182** gelangt. Dadurch gehen  
beide Schalter **183** und **184** in die Arbeitsstellung. Der  
Schalter **183** schaltet über die Leitung **185** den Impuls-  
generator **186** ein. Dieser liefert mit einer Frequenz  
von z. B. 10 kHz Impulse über die Leitung **187** an die  
Tore **188** und **189**. Das Tor **188** ist im Ruhezustand ge-  
öffnet und das Tor **189** gesperrt. Die Impulse von Ge-  
nerator **186** gehen also durch das Tor **188** hindurch,  
55 gelangen zur Leitung **57** und weiter zum Schlüsselim-  
puls-generator II. Dort bewirken sie, wie aus der frühe-  
ren Beschreibung bekannt, die Voreinstellung des Ring-  
zählers **24**. Die Impulse an der Leitung **187** gelangen

aber auch zum Suchzähler 190. Dieser Zähler legt, mit seinem ersten Ausgang 191 beginnend, nacheinander an alle seine Ausgänge 191 ... 192 ... bis 193 Spannung. Diese Ausgänge sind mit den Und-Toren 94 ... 95 ... bis 96 verbunden. Die zweiten Eingänge der Tore sind mit ebenso vielen Ausgängen 178 ... 179 ... bis 180 des Decodierers 177 verbunden.

Angenommen, der empfangene Buchstabe führe zu einer Spannung an dem Ausgang 179 des Decodierers 177. Damit ist das Und-Tor 195 vorbereitet. Die Impulse an der Leitung 187 schalten den Suchzähler 190 so lange weiter, bis an dessen Ausgang 192 Spannung entsteht, welche an den zweiten Eingang des Und-Tores 195 gelangt. Dadurch wird die Koinzidenzbedingung erfüllt, und das Tor 195 gibt einen Impuls an die Leitung 197. Dieser Impuls schaltet zunächst den Schalter 183 in seine Ruhestellung zurück. Damit verschwindet die Spannung an der Leitung 185, der Impulsgenerator 186 bleibt stehen und liefert keine Impulse mehr an die Leitung 187. Es gelangen deshalb auch keine weiteren Impulse mehr zum Suchzähler 190 und über die Leitung 57 zum Ringzähler 24. Der Impuls an der Leitung 197 schaltet ferner den Wechselschalter 198 in seine inverse Stellung. Dadurch tritt an der Leitung 199 Spannung auf, durch welche das Tor 188 gesperrt, und das Tor 189 geöffnet wird. Der Impuls an der Leitung 197 schließlich bringt den Suchzähler 190 in die Null-Stellung zurück.

Der zweite empfangene Einstellbuchstabe bringt den Schalter 82 erneut in Arbeitsstellung, wodurch auf bekannte Weise die Speicherschalter 105 und 109 gemäß der Zeichenelementkombination des Fernschreibzeichens des empfangenen Buchstabens umschalten oder nicht. Entsprechend dieser Spannungsconfiguration entsteht an einem bestimmten Ausgang des Decodierers 177 Spannung. Durch die Rückschaltung des Schalters 82 beim siebenten Schritt (Stopschritt) entsteht erneut ein Impuls an Leitung 181, welcher über das Tor 176 und die Leitung 182 den Schalter 183 einschaltet. Über die Leitung 185 wird der Generator 186 erneut eingeschaltet. Er liefert Taktimpulse der Frequenz 10 kHz über das nunmehr geöffnete Tor 189 zur Leitung 51 und über diese zum Ringzähler 25 des Schlüsselimpulsgenerators II. Durch diese Impulse wird der Ringzähler weitergeschaltet. Die Taktimpulse gelangen aber auch über die Leitung 187 zum Suchzähler 190. Dieser schaltet schrittweise weiter, bis er nach einer

Anzahl von Impulsen, welche der zu decodierenden Zeichenelementkombination entspricht, eines der Tore 194 bis 196 vorbereitet antrifft. Dadurch entsteht erneut ein Impuls an der Leitung 197, welcher den Schalter 183 in die Ruhestellung und den Schalter 198 in seine Ausgangslage bringt. Die Leitung 185 wird spannungslos, und der Generator 186 bleibt stehen. Es gelangen keine weiteren Impulse mehr über die Leitung 187 zum Suchzähler 190 und zum Ringzähler 25. Durch die Rückschaltung des Schalters 198 entsteht ein Impuls an der Leitung 200, welcher auch den Schalter 184 in seine Ruhestellung zurückbringt. Dadurch entsteht an der Leitung 201 ein Impuls, welcher über das Tor 202 und die Leitung 203 zum Schalter 204 gelangt und diesen einschaltet. Dadurch wiederum entsteht Spannung an der Leitung 170, durch welche die Tore 31 und 173 geöffnet werden. Mit der Umschaltung des Schalters 204 ist die Umschaltung der Anlage auf Verschlüsselungsbetrieb beendet. Alle weiter empfangenen Fernschreibzeichen, welche verschlüsselt sind, werden jetzt entschlüsselt, da die an der Leitung 85 auftretenden Taktimpulse über das Tor 31 und die Leitung 34 zum Schlüsselimpulsgenerator II gelangen.

Die Ausführungsbeispiele in den Fig. 1 bis 3 zeigen die grundsätzlichen Stromläufe der Empfangsanlagen. Die Sendeanlagen sind, was die Einrichtungen, welche die Verschlüsselung, die Voreinstellung des Schlüsselimpulsgenerators und die Mischung anbetreffen, die gleichen wie die der Empfangsanlagen. Nur die Übertragungsrichtung ist umgekehrt. Es tritt an die Stelle der Fernleitung die Sendeapparatur (Faksimilesender oder Fernschreibmaschine als Geber) und an Stelle der Empfangsapparatur (Faksimileempfänger oder Fernschreibmaschine als Empfänger) die Fernleitung. Auf eine besondere Darstellung der Schaltung der Sendestelle wird deshalb verzichtet.

Außer den für die Funktion der Verschlüsselungsübertragung wichtigen Bauelementen ist die Sendestelle zweckmäßigerweise noch mit Einrichtungen ausgerüstet, welche eine den Betriebsverhältnissen angemessene automatische Abwicklung vornehmen. Diese sind durch ein Zeitschaltwerk gesteuerte Geber, welche periodisch Kommandosignale für die Voreinstellung und Neustarte der Schlüsselimpulsgeneratoren der Empfänger aussenden. Auch auf die Darstellung dieser Einrichtungen, welche mit bekannten Mitteln leicht verwirklicht werden können, wird verzichtet.

---

Hierzu 3 Blatt Zeichnungen

---

152

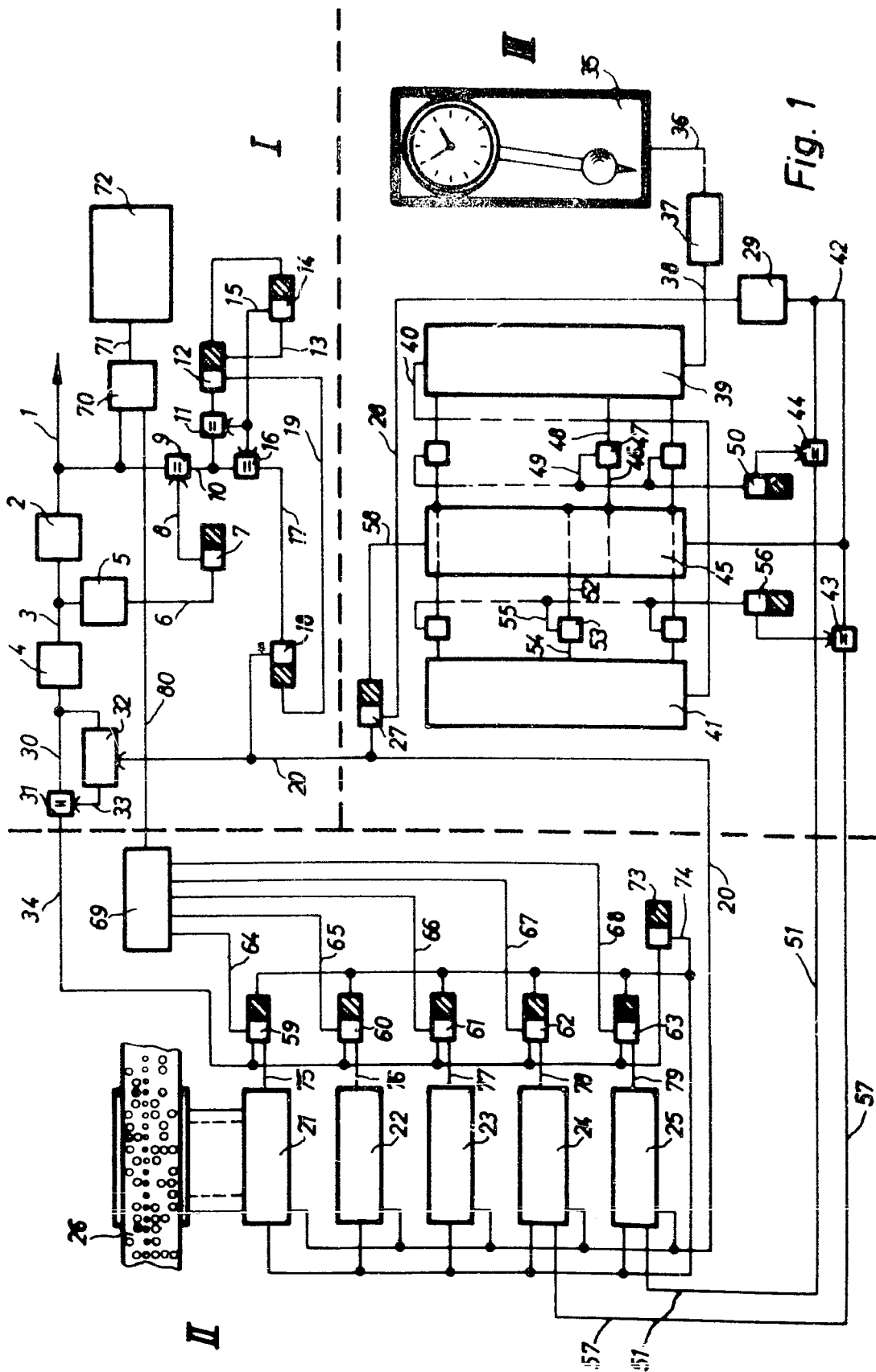


Fig. 1

16

Nummer: 9 78 034  
Int. Cl.²: H 04 L 9/02  
Bekanntmachungstag: 22. April 1976

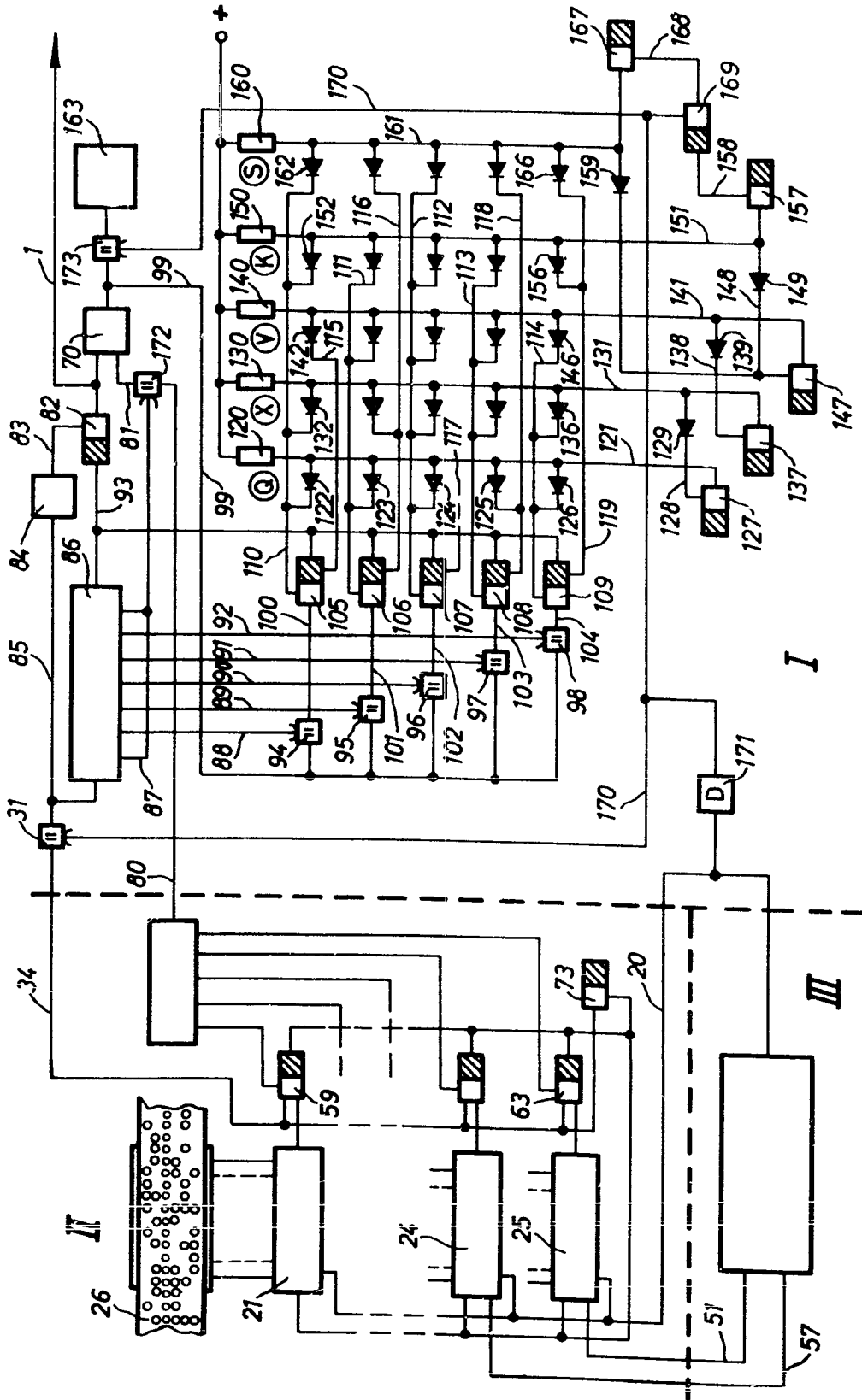


Fig. 2



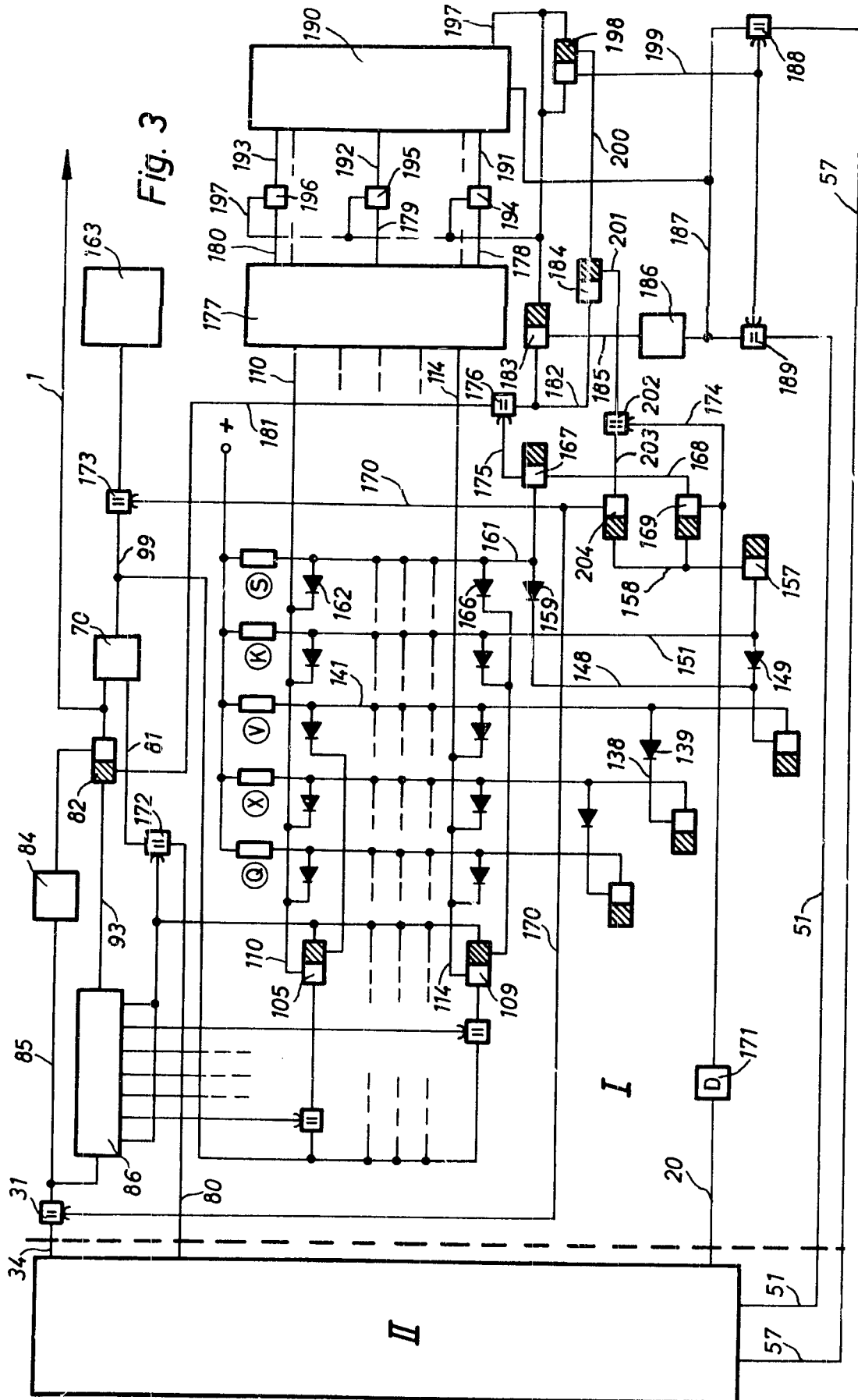


Fig. 3