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

(10) **DE 601 29 682 T2** 2008.04.30

(12) # Übersetzung der europäischen Patentschrift

(97) **EP 1 279 249 B1**
(21) Deutsches Aktenzeichen: **601 29 682.6**
(86) PCT-Aktenzeichen: **PCT/US01/10348**
(96) Europäisches Aktenzeichen: **01 926 501.6**
(87) PCT-Veröffentlichungs-Nr.: **WO 2001/074005**
(86) PCT-Anmeldetag: **29.03.2001**
(87) Veröffentlichungstag der PCT-Anmeldung: **04.10.2001**
(97) Erstveröffentlichung durch das EPA: **29.01.2003**
(97) Veröffentlichungstag der Patenterteilung beim EPA: **01.08.2007**
(47) Veröffentlichungstag im Patentblatt: **30.04.2008**

(51) Int Cl.[8]: ***H04L 9/08*** (2006.01)
H04L 9/18 (2006.01)

(30) Unionspriorität:
193152 P **29.03.2000** **US**

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

(73) Patentinhaber:
Vadium Technology Inc., Seattle, Wash., US

(74) Vertreter:
TBK-Patent, 80336 München

(72) Erfinder:
HAMMERSMITH, Wolfgang S., Seattle, WA 98136, US

(54) Bezeichnung: **EINMALIGE PAD-VERSCHLÜSSELUNG MIT ZENTRALSCHLÜSSELDIENST UND SCHLÜSSELFÄHIGEN ZEICHEN**

Beschreibung

Gebiet der Erfindung

[0001] Die vorliegende Erfindung bezieht sich auf Verfahren zur Verschlüsselung computerlesbarer Daten, die insbesondere in Richtung Einmalverschlüsselungsverfahren verbessert sind, und die Verwendung eines eingebbaren Chiffretextzeichensatzes zum Erleichtern einer Umsetzung und Übertragung durch Personen.

Hintergrund

[0002] Vor der Einführung von Computern wurden viele Verfahren zum Verschlüsseln von Klartext in Chiffretext entwickelt, so dass eine Partei mit dem geeigneten Schlüssel die Nachricht entschlüsseln konnte, um sie im Klartext zu betrachten. Diese Verfahren wurden typischerweise durch Menschen mit Stift und Papier ausgeführt, und wurden später zur Verwendung mit Telegraph und Fernschreiber angepasst.

[0003] Ist der zur Verschlüsselung und Entschlüsselung verwendete Schlüssel so lang wie die Nachricht, wird dies als „Einmalverschlüsselungs-" (OTP)-Verschlüsselungsverfahren bezeichnet, und ist der Schlüssel kürzer als die Nachricht, so dass der Schlüssel, bzw. eine Ableitung des Schlüssels zwei- oder mehrmals verwendet werden muss, wird dies als „Wiederholungsschlüssel"-Verschlüsselungsverfahren bezeichnet.

[0004] Zu Beginn der Entwicklung von Computern war der Speicher zur Speicherung von Verschlüsselungsschlüsseln teuer und schwierig zu handhaben. Der Schlüssel für einen Einmalverschlüsselungsschlüssel muss so lang wie die Nachricht sein und darf nur einmal verwendet werden. Demzufolge wurden Wiederholungsschlüssel gegenüber Einmalverschlüsselungsschlüsseln bevorzugt, da sie viel kürzer sind, typischerweise hundert- oder tausendmal kürzer, und wiederverwendet werden können. Ein populäres Wiederholungsschlüsselverfahren, das als Verschlüsselung mit öffentlichem Schlüssel bekannt ist, verwendet verschiedene aber verwandte öffentliche und private Schlüssel zur Verschlüsselung und Entschlüsselung.

[0005] Bei genügend Abtastwerten von verschlüsselten Nachrichten und einem ausreichend schnellen Computer mit ausreichend großem Speicher kann jede Wiederholungsschlüsselverschlüsselung geknackt werden. Mit dem jüngsten Anstieg von Computergeschwindigkeit und Speichergröße wurden Wiederholungsschlüsselverschlüsselungsverfahren, von denen zuvor gedacht wurde, sie hätten ausreichend Sicherheit, geknackt. Das einzig bekannte Verschlüsselungsverfahren, das beweisbar unknackbar ist, ist die Einmalverschlüsselung.

[0006] Die ursprüngliche Form der Einmalverschlüsselung wurde unter Verwendung eines Schlüssels aus einer Zufallssequenz von 26 Buchstaben des Alphabets und 10 Ziffern und wenig oder keiner Zeichensetzung durchgeführt. Die Nachricht war auf den gleichen Zeichensatz wie der Schlüssel beschränkt. Zur Beschreibung des Vorgangs wird ein Zeichensatz von 38 Zeichen angenommen. Wird jedem Zeichen ein Wert im Bereich von null bis 37 zugeordnet, kann der Verschlüsselungsvorgang durch Kombinieren des ersten Zeichens der Nachricht mit dem ersten Zeichen des Zufallsschlüssels, des zweiten Zeichens der Nachricht mit dem zweiten Zeichen des Schlüssels, usw. durchgeführt werden. Der Kombinationsvorgang kann entweder eine Addition oder eine Subtraktion der Zeichenwerte auf der Basis 38 (Moduln 38) durchgeführt werden, wobei der Übertrag verworfen wird, und der Entschlüsselungsvorgang wird andersherum durchgeführt. Somit ergibt die Summe des Werts 35 plus dem Wert 5 den Wert 2. gleichermaßen ergibt der Wert 2 minus dem Wert 5 den Wert 35. Ein derartiger Einmalverschlüsselungsvorgang kann mit einer beliebigen Anzahl von Zeichen in einem Zeichensatz durchgeführt werden, vorausgesetzt der Schlüssel verwendet die gleiche Anzahl möglicher Werte wie die erlaubte Anzahl von Zeichen im Zeichensatz. Somit wird zur Verschlüsselung von Acht-Bit-Bytes, die 256 mögliche Werte haben, eine Addition (oder Subtraktion) in Moduln 256 verwendet. Beim Arbeiten mit binären Zahlen, wo die Anzahl möglicher Werte eine Potenz von 2 ist, kann der Verschlüsselungs- bzw. Entschlüsselungsvorgang sehr schnell unter Verwendung einer Exklusiv-Oder-Operation zur Erzeugung desselben Ergebnisses wie eine Moduln-Addition oder- Subtraktion ausgeführt werden.

[0007] Die Verschlüsselung einer Computerdatei von einem Megabyte erfordert einen Schlüssel von einem Megabyte, der nicht wiederverwendet werden kann. Mit der Entwicklung kostengünstiger CDs und DVDs zur Speicherung eines sehr langen Schlüssels wurde die Verwendung einer Einmalverschlüsselung für Computerkommunikationen praktikabel.

[0008] Die US-A-6 021 203 sieht ein Protokoll zur Übertragung von Nachrichten mit geringer Sicherheit und Nachrichten mit hoher Sicherheit mit einem Einmalverschlüsselungssystem vor. Gemäß einer Implementierung werden Nachrichten mit niedriger Sicherheit unter Verwendung von Zufallsbitketten entsprechend einem Einmalverschlüsselungsschema verschlüsselt. Eine Hochsicherheitsnachricht und eine Ködernachricht werden in einem Satz von Verschlüsselungsschlüsseln und Chiffretexten eingebettet, der von einem Sender zu einem Empfänger zu übertragen ist. Die Verschlüsselungsschlüssel werden über einen sicheren Kanal vom Sender zum Empfänger

übertragen, und die Chiffretexte werden über einen öffentlich zugänglichen Kanal vom Sender zum Empfänger übertragen. Der Empfänger verwendet die Verschlüsselungsschlüssel und Wissen über Schlüssel für eine Hochsicherheitsnachricht und eine Ködernachricht zum Entschlüsseln der Nachrichten niedriger Sicherheit, Extrahieren der Hochsicherheitsnachricht und/oder Ködernachricht und Entschlüsseln der Hochsicherheitsnachricht und/oder Ködernachricht. Die Bereitstellung der Ködernachricht wird sichtbar, wenn der Empfänger genötigt wird, den Schlüssel für eine angebliche Hochsicherheitsnachricht zu erkennen zu geben.

[0009] Die US-A-4 731 840 offenbart ein Verfahren zur Verschlüsselung, Übertragung und nachfolgender Entschlüsselung digitaler Verschlüsselungsdaten. Das Verfahren verwendet den Datenverschlüsselungsstandard und ist mittels eines Paars von Vorrichtungen implementiert, die jeweils zum Arbeiten entweder als Mastereinheit oder entfernte Einheit auswählbar sind. Jede Einheit enthält einen Satz von Schlüsselverschlüsselungsschlüsseln, die durch ein gemeinsames Indexsystem indiziert sind. Die Mastereinheit arbeitet auf einen Befehl von der entfernten Einheit hin zum Erzeugen eines Datenverschlüsselungsschlüssels und verschlüsselt den Datenverschlüsselungsschlüssel unter Verwendung eines vorausgewählten Schlüsselverschlüsselungsschlüssels. Der verschlüsselte Datenverschlüsselungsschlüssel und ein Indexbestimmer werden dann in die entfernte Einheit geladen, wo der Datenverschlüsselungsschlüssel zur nachfolgenden Verwendung bei der Verschlüsselung und Übertragung von Daten entschlüsselt wird. Das Herunterladen des verschlüsselten Datenverschlüsselungsschlüssels ermöglicht eine häufige Änderung von Schlüsseln, ohne dass ein manueller Eintrag oder eine Speicherung von Schlüsseln an der entfernten Einheit erforderlich wäre.

[0010] Die WO-A-99 26121 offenbart ein Datenübertragungssystem, in dem die Datenübertragungssicherheit über eine robuste Benutzerauthentifizierung und Dateiverschlüsselung sichergestellt werden kann. Beispielsweise sind Computer vorhanden, die als folgende Dienstprozessoren arbeiten: (1) einer oder mehrere Vertrauensabfrageprozessoren, (2) einer oder mehrere Annahmerückgabezertifizierungsprozessoren und/oder (3) einer oder mehrere Verschlüsselungs-/Entschlüsselungsschlüsselausgabe-, Benutzerauthentifizierungs- oder Sicherheitspolitikverwaltungsprozessoren (die nachstehend Sicherheitsserver genannt werden), die über eine aktive Verbindung mit der Kommunikationsleitung arbeiten und verfügbar sind.

[0011] Gemäß der WO-A-99 26121 kann eine Verschlüsselung mit öffentlichem Schlüssel oder eine Einmalverschlüsselung in Abhängigkeit von der Präferenz des Dienstanbieters implementiert sein. Es können Einmalschlüssel zur Verschlüsselung von Dateien vor dem Transport verwendet werden, die automatisch für jede Transaktion zwischen Sender und Empfänger von einem zuverlässigen dritten Sicherheitsserver erhalten werden. Verschlüsselte Dateien werden zusammen mit einer authentifizierten Benutzeridentität und dem "hash" ("elektronischer Fingerabdruck") der gesendeten Dateien direkt zwischen den Computern über die Kommunikationsleitung (d.h., das Internet) transportiert, ohne dass sie durch die Prozessoren oder den Sicherheitsserver gelenkt werden. Empfangene Dateien können automatisch entschlüsselt werden, wenn die Einmalverschlüsselung implementiert ist und die Empfängeridentität und Entschlüsselungsanforderung an den Sicherheitsserver mit der implementierten Sicherheitspolitik übereinstimmen.

Kurzzusammenfassung

[0012] Die Einführung des Internet erlaubt nunmehr die Verteilung umfangreicher Einmalverschlüsselungs-(OTP) Schlüssel zu einem mit einem Netz wie dem Internet verbundenen Computer. Damit ein in einem Netz verteilter Einmalverschlüsselungsschlüssel nicht abgefangen und dann zur Entschlüsselung einer Nachricht verwendet werden kann, sind die Einmalverschlüsselungs-Kommunikationsschlüssel selbst mit einem Schlüsselverschlüsselungsschlüssel verschlüsselt.

[0013] Der Schlüsselverschlüsselungsschlüssel kann ein Wiederholungsschlüssel oder auch ein Einmalschlüssel sein. Wird ein Kommunikationsschlüssel sowohl zu einem Sender als auch einem Empfänger verteilt, kann der Schlüsselverschlüsselungsschlüssel für beide Parteien identisch sein, so dass eine Person, die beide Übertragungen abfängt, einen identischen Inhalt empfängt und keine Unterschiede im Inhalt zur Unterstützung bei der Entschlüsselung des Inhalts verwenden kann. Zur Sicherstellung, dass nur eine Partei den jeweiligen verteilten Schlüssel verwenden kann, kann der Kommunikationsschlüssel alternativ mit einem eindeutigen Schlüsselverschlüsselungsschlüssel verschlüsselt sein.

[0014] Anstelle der Verteilung eines Schlüssel endlicher Länge jeweils zum Sender und Empfänger kann der Server zum Senden einer kontinuierlichen Sequenz von Schlüsseln jeweils mit eigenem Identifizierer eingerichtet sein, so dass Sender und Empfänger jeweils einen Abschnitt der Sequenz von Schlüsseln abfangen und diesen Abschnitt zur Verschlüsselung und Entschlüsselung ihrer Nachrichten verwenden können. Anhand dieses Vorgangs kann eine Sequenz von Einmalverschlüsselungsschlüsseln kontinuierlich zur Verwendung durch den Sender und Empfänger zu einer beliebigen Zeit übertragen werden, woraus sich effektiv ein nie endender

Schlüssel ergibt.

[0015] Die empfangenen Blöcke kontinuierlich übertragener Schlüssel werden bis zu ihrer Verwendung in einem Puffer gespeichert. Erfordern die Kommunikationen zwischen dem Sender und dem Empfänger nicht ausreichend Bandbreite zur Verwendung des gesamten Inhalts jedes empfangenen Blocks, wird der Rest jedes Blocks verworfen.

[0016] Werden die Einmalverschlüsselungs-Kommunikationsschlüssel auf physikalischen Medien wie CDs oder DVDs verteilt, macht die Verschlüsselung des Schlüsselmaterials den Schlüssel unbrauchbar, außer wenn eine bestimmte Kopie eines Kommunikationsprogramms mit dem geeigneten Schlüsselverschlüsselungsschlüssel zur Entschlüsselung des Kommunikationsschlüssels verwendet wird.

[0017] Ist der Kommunikationsschlüssel auf einem physikalischen Medium aufgezeichnet, werden Orte innerhalb des Schlüssels mit einer Verschiebungs- bzw. Offset-Nummer identifiziert, anstelle den Kommunikationsschlüssel in Blöcke mit einem Identifizierer für jeden Block aufzubrechen, so dass der Schlüssel ab Beginn jedes Blocks verwendet werden kann. Die Offsetnummer ist als Metadaten-Header für die verschlüsselte Nachricht enthalten, um den Startpunkt innerhalb des Schlüssels zur Entschlüsselung der Nachricht anzugeben.

[0018] Gleichermaßen enthält der Metadaten-Header eine Identifizierung des Schlüssels zur Erleichterung des Übereinstimmungsvergleichs des Schlüssels mit der Nachricht am Empfängercomputersystem. Der Metadaten-Header enthält auch eine Länge und einen Fehlerüberprüfungscode, die beide für die Überprüfung auf Fehler in der verschlüsselten Nachricht verwendet werden.

[0019] Wird ein Schlüssel endlicher Länge verwendet, ob er nun auf physikalischen Medien oder über Kommunikation über ein Netz empfangen wird, wird vor der Verschlüsselung die Länge der Nachricht mit der Länge des Schlüssels verglichen, um sicherzustellen, dass der Schlüssel lang genug ist, um den Verschlüsselungsvorgang abzuschließen.

[0020] Moderne westliche Zeichensätze enthalten mehr als 90 Zeichen, wobei Klein- und Großbuchstaben, Ziffern, Symbole und Interpunktionszeichen enthalten sind. Die Zeichen, die die Verwendung einer Umschalttaste auf einer Standardtastatur erfordern, sind unbequem in der Verwendung, und Zeichen, die schwer zu unterscheiden sind, wie null und 0, sind für den menschlichen Leser mehrdeutig. Ist der Chiffretext durch einen Menschen einzugeben oder durch einen Menschen als Anbindung im Übertragungsvorgang zu sprechen, ist es demnach von Vorteil, einen begrenzten Zeichensatz zu verwenden, der entweder Groß- oder Kleinbuchstaben enthält und nur jene zusätzlichen Symbole, die ohne Verwendung der Umschalttaste eingegeben werden können und leicht visuell zu unterscheiden sind. Dieser wird als eingebbarer Chiffretext-Zeichensatz bezeichnet.

[0021] Gemäß einem Ausführungsbeispiel besteht dieser Zeichensatz aus den 26 Großbuchstaben des westlichen Alphabets. Gemäß einem anderen Ausführungsbeispiel besteht er aus diesen Buchstaben plus sechs der Ziffern zum Ausbilden eines Satzes von 32 Zeichen. Ein Zeichensatz mit 32 Zeichen hat bestimmte Vorteile, da 32 eine Potenz von 2 ist, was binäre Operationen erleichtert.

[0022] Zur Verwendung des eingebbaren Chiffretext-Zeichensatzes zur Übertragung von Nachrichten, von denen beinahe alle einen Zeichensatz verwenden, der mehr als 32 Zeichen erlaubt, werden manche Klartextzeichen anhand von zwei Chiffretextzeichen dargestellt. Zum Minimieren der Anzahl von Chiffretextzeichen werden die üblichsten 22 oder 26 Klartextzeichen jeweils mit einem Chiffretextzeichen dargestellt, während alle anderen mit zwei Chiffretextzeichen dargestellt werden.

[0023] Der bevorzugte Einmalschlüssel zur Verschlüsselung in den eingebbaren Chiffretextzeichensatz besteht aus einer Zufallssequenz von Bytes, wobei jeder Bytewert auf die Anzahl von Werten im eingebbaren Chiffretextzeichensatz (48 oder weniger), vorzugsweise 26 oder 32 beschränkt ist. Vor der Verschlüsselung wird der Klartext auf einen Zwischentext verlängert, der lediglich die Zeichen des eingebbaren Chiffretextzeichensatzes enthält. Der Zwischentext wird dann mit der Zufallssequenz von Bytes einmal verschlüsselt, wobei die Bytewerte auf die Anzahl von Zeichen im Zeichensatz beschränkt sind. Obwohl die möglichen Bytewerte auf weniger als alle 256 möglichen Werte beschränkt sind, kann der Einmalverschlüsselungs-Kommunikationsschlüssel auch für eine binäre Verschlüsselung in einen Chiffretext mit allen 256 möglichen Werten verwendet werden, so dass jeder Schlüssel eine duale Verwendung erfährt.

[0024] Da die Sicherheit in Frage gestellt wäre, wenn ein Einmalverschlüsselungsschlüssel zweimal verwendet wird, wird die Schlüsselidentifikationsnummer für jeden Schlüssel halbpermanent in eine Datei im Computersystem geschrieben, und diese Datei wird überprüft, wenn ein Schlüssel installiert wird, um sicherzustellen, dass er nicht zuvor bereits installiert wurde. Im Windows-Betriebssystem ist diese Datei als Registerdatenbank bekannt. Zum Löschen dieser halbpermanenten Aufzeichnung muss das Betriebssystem auf dem Computersystem vollkommen neu installiert werden, oder ein bestimmtes Programm muss gestartet werden, um den zuvor installierten Schlüssel aus der Registerdatenbank zu

löschen, wie durch die Verwendung des von Windows bereitgestellten Wartungsprogramms REGEDIT.EXE.

[0025] Das offenbarte Clientcomputerverschlüsselungs- und Entschlüsselungscomputerprogramm kann mit beliebigen anderen Computerdateien jedes beliebigen Dateityps arbeiten. Es kann Ordner einschließlich aller Unterordner und Dateien verschlüsseln. Die Steuerung kann in der Benutzerschnittstelle für einen Wordprozessor enthalten sein, so dass eine Verschlüsselungstaste auf der Benutzerschnittstelle des Wordprozessors erscheint, zusammen mit einer Entschlüsselungstaste, und dies ist auch für andere Programme möglich. Wird eine angezeigte Information ausgewählt und die Verschlüsselungstaste gedrückt, wird das angezeigte Material verschlüsselt. Umfasst das Programm den eingebbaren Chiffretextzeichensatz-Modus, werden die verschlüsselten Informationen im bevorzugten Zeichensatz angezeigt. Wird der binäre Verschlüsselungsmodus ausgewählt, werden die verschlüsselten Informationen mit Kästchensymbolen angezeigt, die nicht-anzeigbare Zeichen darstellen, oder mit welchen anzeigbaren Zeichen auch immer die verschlüsselten Bytewerte dargestellt werden sollen.

Kurzbeschreibung der Zeichnungen

[0026] Fig. 1 zeigt den Vorgang der Erzeugung von Einmalverschlüsselungs-Kommunikationsschlüsseln und der Verteilung dieser zu Benutzern, ob anhand eines Computernetzes oder auf einer Disk.

[0027] Fig. 2 zeigt das Schlüsselverwaltungsfenster für jeden Benutzer.

[0028] Fig. 3 zeigt, wie der eingebbare Chiffretextzeichensatz verwendet wird.

[0029] Fig. 4 zeigt zusätzliche Einzelheiten über die Verteilung von Einmalverschlüsselungs-Kommunikationsschlüsseln durch einen Server.

[0030] Fig. 5 zeigt, wie die Verschlüsselung durch einen einzelnen Benutzer zur sicheren Speicherung sicherer Informationen verwendet werden kann, die nur durch diesen Benutzer abzurufen sind.

[0031] Fig. 6 zeigt separate sichere Kommunikationen unter drei Unterstationen.

[0032] Fig. 7 zeigt sichere Kommunikationen, auf die alle vier Parteien zugreifen können.

Ausführliche Beschreibung

[0033] In der folgenden Beschreibung bezieht sich „Klartext" auf die ursprünglichen nicht verschlüsselten Datenbytes, ob es sich nun um Zeichen, Symbole oder binäre Bytes handelt, Microsoft Word 2000™ wird Word 2000 genannt, und Microsoft Windows 98™ und Microsoft Windows 2000™ werden jeweils Windows 98 und Windows 2000 genannt.

[0034] Das bevorzugte Ausführungsbeispiel der Erfindung umfasst ein Computerprogramm, das in der Microsoft Windows 98- und der Windows 2000-Umgebung auf einem IBM-kompatiblen Personalcomputer arbeitet, der eine Verschlüsselung und Entschlüsselung unter Verwendung einer Einmalverschlüsselung (OTP) durchführt, die der strengen Version eines Einmalverschlüsselungsalgorithmus entspricht, um die Erzeugung eines Chiffretexts sicherzustellen, der nicht geknackt werden kann.

[0035] Das Programm verschlüsselt und entschlüsselt eine beliebige Nachricht oder einen beliebigen Datensatz, einschließlich

1. allen durch Windows 98- und Windows 2000-Programme erzeugten Dateien einschließlich eines beliebigen Typs von Bilddateien und Exceldateien,
2. Untersektionen eines Word 2000- Dokuments im Dokument durch Hinzufügen von „Verschlüsselungs"- und „Entschlüsselungs"-Tasten zu einer Symbolleiste in Word 2000,
3. Windowsordnern und deren Dateiinhalte bis auf ein beliebiges Unterordnerniveau, wobei eine verschlüsselte Datei für die gesamte Hierarchie erzeugt wird. Bei der Entschlüsselung werden die Hierarchie und ihre Dateiinhalte als perfekte Kopie ihrer ursprünglichen Struktur neu angeordnet,
4. Text oder Chiffretextinhalte der Windowszwischenablage in der Zwischenablage selbst. Unter Verwendung der Zwischenablage kann das Programm verschlüsselte oder entschlüsselte Textinformationen im RAM halten und sie in eine E-Mail oder ein anderes Windowsprogramm ohne Speichern dieser Informationen auf einer Disk einfügen. Dies verhindert Elektronenmikroskopmedienabtastungen und andere Verfahren am Erfassen gelöschter Informationen in den tiefen Schichten magnetischer Speichermedien wie einem Festplattenlaufwerk,
5. Textnachrichten, die in das Textfenster des Programms eingegeben werden.

[0036] Das Programm weist vollständige Dateisicherungs- und Ladefähigkeiten auf und kann verschlüsselte und entschlüsselte Dateien auf beliebigen Computerspeichermedien sichern.

Schlüssel zur Verschlüsselung und Entschlüsselung

[0037] Wie in Fig. 1 gezeigt werden zwei übereinstimmende OTP-Schlüssel **5** & **6**, **4** & **7** durch einen zentralen Schlüsseldienst **1** erzeugt und jeweils zu jedem Teilnehmer **2** & **3** zur Verwendung verteilt. Die Schlüssel **4**, **5**, **6**, **7** sind auf CDs, DVD-ROMs oder

anderen Computerspeichermedien gespeichert. Übereinstimmende Schlüssel müssen im Besitz des Empfängers und des Senders sein, um die Datei oder den Text zu verschlüsseln und zu entschlüsseln. Jeder Abschnitt jedes Schlüssels wird einmal für eine Verschlüsselung verwendet, und zur Sicherstellung der Sicherheit, nur einmal. Ersatzschlüssel können vom Hersteller gekauft werden, der eine zentrale Quelle von OTP-Schlüsseln bereitstellt, oder unter Verwendung eines Zufallszahlengenerators durch den Benutzer mit Lizenz vom Hersteller erzeugt werden. Schlüssel-CDs und -DVD-ROMS können kopiergeschützt sein.

[0038] Die Schlüssel können entsprechend den Bedürfnissen des Client und der Kapazität der Speichermedien eine beliebige Länge haben. Schlüsselmaterial wird vorzugsweise anhand eines im Handel erhältlichen Zufallszahlengenerators erzeugt, der SG100 genannt wird, und von Protego in Schweden hergestellt wird.

[0039] Das Programm arbeitet mit Schlüsseln von beliebigen Computerspeichermedien einschließlich sehr großen Speicherarrays („Very Large Storage Arrays", VLSA). Allerdings ist es aus Sicherheitsgründen nicht empfehlenswert, dass die Programmschlüssel auf der Festplatte eines mit einem nicht sicheren Netz verbundenen Computers installiert werden. Bei großen Schlüsseldatenbanken verwaltet ein dedizierter Server die VLSA wie nachstehend beschrieben, der eine Teilnehmerdatenbank steuert, der sicherer Kommunikationssystem- oder SCS-Server genannt wird.

Programmfunktionen

[0040] Das Programm arbeitet in zwei Hauptbetriebsarten: einem rein binären Modus, in dem der Chiffretext von einem Menschen nicht lesbar ist, und einem eingebbaren Chiffretextmodus, in dem der resultierende Chiffretext die 26 Großbuchstaben des westlichen Alphabets bzw. die 26 Buchstaben plus 6 Ziffern für insgesamt 32 Zeichen umfasst. Da der binäre Verschlüsselungsvorgang sehr einfach ist, ist der Programmkern zur Verschlüsselung von Sprache und Echtzeitvideokommunikationen auf einem heutigen Windows 98- oder Windows 2000- Computer schnell genug. Der durch das Programm verschlüsselte ursprüngliche Klartext wird nicht zerstört oder in keinerlei Weise modifiziert und bleibt an seinem ursprünglichen Ort.

[0041] Das Programm platziert ein Icon in der Windowssystemablage, das dem Benutzer über ein Aufklappmenü das Öffnen des Hauptprogrammfensters, die Verschlüsselung oder Entschlüsselung des Inhalts der Windowszwischenablage oder das Schließen des Programms ermöglicht. Das Systemablageicon bleibt in der Systemablage und wird bei jedem Starten des Computers geladen.

[0042] Wie in Fig. 2 gezeigt zeigt das Programm ein Schlüsselverwaltungsfenster **20** an, in dem die Schlüsselverwendung durch das Programm verfolgt und für den Benutzer angezeigt wird. Gelangen Schlüssel an das Ende ihrer Verwendung, wie es durch einen „verbleibende Schlüssel-Indikator" in einer Statusleiste und dem „verbleibende Datenindikator **21**" im Schlüsselverwaltungsfenster für jeden Schlüssel angezeigt wird, werden sie durch den Benutzer gelöscht und niemals wieder verwendet. Das Programm erlaubt keine Verschlüsselung, wenn der ausgewählte Schlüssel nicht groß genug ist, um die angeforderte Verschlüsselungsmenge zu handhaben. Das Statusleistenfenster von verbleibenden Schlüsseln zeigt die gesamte Anzahl von im ausgewählten Schlüssel übrigen Bytes an. Ein Statusleistenfenster „aktueller Schlüssel" zeigt einem Benutzer einen vergebenen Namen oder die Schlüsselidentifikationsnummer des ausgewählten Schlüssels an, wenn kein von einem Benutzer vergebener Name zugeordnet wurde. Mehrere Schlüssel können auf einer CD oder anderen Speichermedien gespeichert werden, die alle über das Schlüsselverwaltungsfenster des Programms verwaltet werden. Auf diese Weise können verschiedene Kommunikationssystemtypen anhand eines einfachen Zwei-Stationensystems in einem komplexeren System implementiert werden.

Textverschlüsselungszeichensatz

[0043] Während der Textverschlüsselung im eingebbaren Chiffretextmodus wandelt das Programm alle Zeichen, einschließlich aller Interpunktionszeichen und nicht druckbarer Zeichen in ASCII-Großbuchstaben A bis Z um, woraus sich ein Chiffretext ergibt, der für Menschen einfach zu lesen und schnell auf einer Tastatur eingebbar ist. Wie in Fig. 3 gezeigt erleichtert dieser verringerte Zeichensatz eine nicht computerbezogene Umsetzung von Chiffretext wie durch Eingeben des Chiffretexts von Druckmedien in einen Computer, wie von Faxvorlagen und anderen Papierbriefen. Dies dient auch der Genauigkeit bei der Übertragung von Chiffretext über Sprache, Morsecode und andere nicht computerbezogene Verfahren der Übertragung. Durch Verwendung von entweder Groß- oder Kleinbuchstaben muss keine Umschalttaste gedrückt werden. Großbuchstaben sind für das Auge leichter zu unterscheiden als Kleinbuchstaben. 26 verschiedene Zeichen sind für einen Menschen einfacher zu unterscheiden und zu bearbeiten als 52 verschiedene Groß- und Kleinbuchstaben oder 62 alphanumerische oder 94 mögliche Zeichen auf der Computerstandardtastatur.

[0044] Damit jede Anzeige des Chiffretexts auf einem Standardcomputer die geeigneten Zeichen angibt, verwendet der eingebbare Chiffretext gemäß dem bevorzugten Ausführungsbeispiel die regulären

8-Bit-ASCII-Werte.

[0045] Werden allerdings lediglich 26 Zeichen in binären Zahlen dargestellt, sind lediglich 5 Bits erforderlich. Mit 5 Bits können insgesamt 32 Zeichen dargestellt werden, also 6 zusätzliche Zeichen, ohne dass der Chiffretext länger wird. Auch wenn alle möglichen Werte von 5-Bit-Binärzahlen für den Chiffretext verwendet werden, können die Zufallszahlen zur Verschlüsselung erzeugt werden, indem eine lange Kette von Zufallsbits, jeweils 5 Bits auf einmal, verwendet und dann anhand einer Nachschlagetabelle in bevorzugte 8-Bit-Darstellungen umgewandelt wird, wodurch eine beliebige Quelle für Zufallsbits effizient verwendet werden kann, vorausgesetzt, dass sowohl der Sender als auch der Empfänger auf die gleiche Quelle von Zufallsbinärbits zugreifen können.

[0046] Um aus der Verwendung von 32 Zeichen im Chiffretext-Zeichensatz einen Vorteil zu ziehen, fügt ein alternatives Ausführungsbeispiel der Erfindung 6 weitere Zeichen hinzu. Die bevorzugten Zeichen sind 6 der 10 arabischen Zahlen, da sie auf allen Tastaturen zu finden sind und Darstellungen im Morsecode haben. Beliebige 6 aus den 10 sind geeignet, jedoch sind die bevorzugten 6 die Zahlen 2-7. 0 ist zu vermeiden, da es zu sehr wie 0 aussieht. 1 ist zu vermeiden, da es sehr wie I und L und I aussieht. Bei einer Verwischung oder Verschmierung können 6, 8, und 9 schwierig zu unterscheiden sein. Für einen Menschen ist es sehr einfach, verschmierte Zeichen zu interpretieren, wenn er weiß, dass sie auf einen bestimmten Satz beschränkt sind, und der mögliche Bereich der Zahlen ist sehr einfach für einen Benutzer zu beschreiben, wenn der Bereich kontinuierlich ist. Aus diesem Grund wird der Bereich 2-7 bevorzugt.

[0047] Ob nun 26 Zeichen oder 32 Zeichen oder ein beliebiger leicht eingegebener Zeichensatz bis zu 48 Zeichen verwendet wird, der in einen Standardcomputer leicht eingegeben werden kann, ohne die Umschalttaste zu verwenden, wird der Zeichensatz hier als eingebbarer Chiffretextzeichensatz bezeichnet.

[0048] Da es lediglich 26 bis 48 Zeichen im eingebbaren Chiffretextzeichensatz gibt, erfordert die resultierende Verringerung jedes Standardzeichensatzes in den eingebbaren Chiffretextzeichensatz, dass viele Zeichen durch zwei der eingebbaren Zeichen dargestellt werden, woraus sich eine größere Anzahl von Chiffretextzeichen als Klartextzeichen ergibt. Wird ein Satz aus 32 Zeichen verwendet, werden alle Kleinbuchstaben mit einem Eins-zu-eins-Verhältnis zu einem zufälligem Chiffretextzeichen verschlüsselt. Alle Nicht-Kleinbuchstaben, einschließlich Großbuchstaben mit Akzenten werden durch zwei Zufallssymbole des Chiffretextes dargestellt. Dieses Verfahren hilft bei der Verringerung der Chiffretexterweiterung, da die meisten Nachrichten hauptsächlich aus Kleinbuchstaben bestehen. Mit dem Verfahren der Eins-zu-eins-Verwendung für 26 der möglichen Zeichen und der Zwei-zu-eins-Verwendung für alle anderen möglichen Zeichen beträgt die Anzahl der darstellbaren Zeichen 26 + 32 × 32 × 32 × 32 = 1,048,602, was zur Darstellung aller bekannten Zeichen in allen Alphabeten einschließlich chinesischer Wortzeichen ausreicht.

[0049] Bei dem Ausführungsbeispiel, das 26 Zeichen verwendet, ist den ersten 22 Kleinbuchstaben des Alphabets a bis v eine Eins-zu-eins-Beziehung mit dem Chiffretext gegeben, und allen verbleibenden Zeichen, einschließlich w, x, y und z werden durch zwei Zeichen des Chiffretextes dargestellt. Dies ermöglicht eine Darstellung von insgesamt 22 + 26 × 26 × 26 × 26 = 456,998 Zeichen, was immer noch zur Darstellung aller bekannten Zeichen in allen bekannten Sprachen ausreicht.

[0050] Ein Algorithmus zur Erzeugung dieser manchmal Eins-zu-eins- und manchmal Zwei-zu-eins-Beziehung kann wie folgt implementiert werden. Zuerst wird ein Zwischentext durch Ersetzen jedes von a bis v verschiedenen Zeichens (a-z im 32-Zeichensatzausführungsbeispiel) erzeugt, wobei eine Zwei-Zeichen-Darstellung beginnend mit W, X, Y oder Z (2-7 im 32-Zeichensatzausführungsbeispiel) durchgeführt wird. Dies reduziert alle Zeichen im Klartext auf den erlaubten Zeichensatz. Dann wird die Einmalverschlüsselung auf die übliche Weise durch Ersetzen jedes der 26 oder 32 Zeichen im Zwischentext mit einem anderen der 26 oder 32 Zeichen durchgeführt, die zufällig durch Kombination mit dem nächsten der 26 oder 32 Zeichen im Schlüssel erzeugt werden.

[0051] Im Textmodus bietet das Programm dem Benutzer eine Option zur Verringerung der Größe der Ausgabedateien unter Verwendung eines Kompressionsalgorithmus ohne Verlust. Bei Anwendung dieser Option wird das Volumen der ausgegebenen Chiffredateien des Programms vor der Speicherung automatisch erheblich verringert. Der bevorzugte Algorithmus wird vom Verteiler der PKZip Software, PK Ware, Inc., http://www.pkware.com lizenziert. Da jedes Zeichen des Chiffretexts durch 8 Bits dargestellt wird, und es nur 26 oder 32 verschiedene Zeichen im Textmodus-Chiffretext aus möglichen 256 8-Bit-Zeichen gibt, ist im Textmodus ein großer Umfang einer verlustlosen Kompression möglich. Da der Chiffretext im Binärmodus vollkommen zufällig ist und alle möglichen Bytewerte verwendet werden, ist keine Kompression möglich.

Nicht zufällig erhaltener Schlüssel

[0052] Zur Verwendung mit Text besteht der Chiffretext wie vorstehend beschrieben aus 26 oder 32 Zeichen. Demnach sollte der Schlüssel zur Verwendung im Einmal-Verschlüsselungsvorgang lediglich diese

26 oder 32 Zeichen umfassen, wobei die Auftrittshäufigkeit jedes Zeichens vollkommen zufällig ist. Bei dem Ausführungsbeispiel mit 32 Zeichen kann dies durch Beginnen mit einer langen Kette zufälliger Bits bewirkt werden, wobei jeweils 5 auf einmal genommen werden. Ist die ursprüngliche Kette zufällig, wird jedes 5-Bit-Byte zufällig jeden der 32 möglichen Werte enthalten. Zur Darstellung der 32 eingebbaren Zeichen unter Verwendung von 8-Bit-ASCII-Werten wandelt eine Nachschlagetabelle diese schnell in ASCII um. Bei dem Ausführungsbeispiel mit 32 Zeichen kann demnach das gleiche Schlüsselmaterial sowohl für die Textverschlüsselung, wobei der Schlüssel mit 5 Bits auf einmal verwendet wird, als auch für eine binäre Verschlüsselung verwendet werden, wobei 8 Bits auf einmal verwendet werden, wobei die Schlüssel im Textmodus länger halten. Alternativ dazu kann bei dem Ausführungsbeispiel mit 26 Zeichen oder dem Ausführungsbeispiel mit 32 Zeichen eine Sequenz zufälliger Bytes auf lediglich 26 oder 32 Zeichen unter Verwendung eines Zufallbytegenerators (oder durch die Verwendung von 8 zufälligen Bits auf einmal, was das Gleiche ist) und Herauswerfen aller Bytes verringert werden, die von den 26 oder 32 Bytes verschieden sind, die Zeichen innerhalb des Satzes darstellen.

[0053] Werden allerdings lediglich CDs oder andere Schlüsselmedien mit zufälligen Schlüsseln an die Benutzer zur Verwendung mit dem Programm verteilt, können die Medien mit einem beliebigen Verschlüsselungsprogramm als Quelle von Zufallszeichen oder Zufallszahlen verwendet werden. Gleichermaßen kann das Programm mit einer beliebigen Quelle von Zufallszeichen oder -Zahlen verwendet werden. Aus Geschäftsgründen wird bevorzugt, dass das Programm lediglich mit einer autorisierten CD verwendbar ist, und die CDs nur mit einem autorisierten Programm verwendbar sind. Daher wird der Schlüssel, bevor er auf der Disk aufgezeichnet wird, durch einen reversiblen Algorithmus verarbeitet, der aus dem Schlüssel nicht länger eine Zufallssequenz aus Zeichen macht. Da der auf dem Schlüsselmedium aufgezeichnete Schlüssel nicht zufällig ist, kann er für die Verschlüsselung nicht verwendet werden, ohne ihn durch den umgekehrten Algorithmus laufen zu lassen, um ihn wieder zufällig zu machen. Dieser Vorgang des Beginnens mit einem zufälligen Schlüssel, der dann nicht-zufällig gemacht wird, und dann zum Verwendungszeitpunkt wieder zufällig gemacht wird, kann leicht mit einer Eins-zu-eins-Beziehung zwischen 8-Bit-Bytes des ursprünglichen Schlüssels aus 26 oder 32 Zeichen und 8-Bit-Bytes des Schlüssels in der nicht-zufälligen Form bewirkt werden, da die nicht-zufällige Form beliebige der 256 möglichen Werte für jedes Byte verwenden kann.

[0054] Um jeden Kommunikationsschlüssel vor seiner Aufzeichnung auf der CD oder DVD oder einem anderen Medium nicht zufällig zu machen, können verschiedene Algorithmen verwendet werden. Ein geeignetes Verfahren besteht in der Verschlüsselung jedes Schlüssels mit einem Wiederholungsschlüssel-Verschlüsselungschlüssel durch Exklusiv-Oder-Verknüpfung des Kommunikationsschlüssels mit einer Kette von Bytes, die immer wieder verwendet wird. Die Kette aus Bytes ist vorzugsweise zwischen 1000 Bytes und 50000 Bytes lang, und ist als Datei gespeichert. Erreicht der Exklusiv-Oder-Verknüpfungsvorgang das Ende der Bytekette, wird der Dateizeiger an den Beginn der Datei rückgesetzt und die Kette aus Bytes wird wieder verwendet, bis die Datei den Indikator End of File erreicht. Jede Wiederholungsverschlüsselung kann verwendet werden, wie Vernam, Autokey oder DES.

[0055] Mit einer Wiederholungsschlüsselverschleierung der rohen Schlüsseldaten kann der Kommunikationsschlüssel nicht auf übliche Weise vom Benutzer gelesen oder modifiziert oder kopiert und als Verschlüsselungsprogramm des Wettbewerbers verwendet werden. Liest das Programm eine Schlüsseldatei, verwendet es seinen eigenen eingebauten Schlüsselverschlüsselungsschlüssel zum Entschlüsseln der Abschnitte des Schlüssels, die es verwenden wird. Bei einer Version des Programms ist der Schlüsselverschlüsselungsschlüssel in jeder Programminstanz und in jedem Moment jedes erzeugten Schlüssels identisch, so dass alle Programme zusammen arbeiten und alle Schlüssel für diese Version mit allen Programmen arbeiten.

Verwendung der Schlüssel für eine binäre Verschlüsselung

[0056] Die vom Benutzer wählbare binäre Verschlüsselungsoption des Programms verwendet den eingebbaren Chiffretextzeichensatz nicht, da eine Sprach- und Videoverschlüsselung einen Umfang haben, der eine manuelle Eingabe nicht praktikabel macht. Stattdessen verwendet sie alle 256 möglichen 8-Bit-Bytes im Chiffretext zur Darstellung der 8-Bit-Bytes des ursprünglichen Materials. Im binären Verschlüsselungsmodus des Programms gibt es eine direkte Beziehung zwischen jedem Schlüssel-Byte und jedem Klartext-Byte, woraus sich eine Eins-zu-eins-Beziehung zwischen Schlüsselbytes und Klartextbytes ergibt.

[0057] Bei Versionen des Programms, die sowohl eine eingebbare Chiffretextverschlüsselung als auch eine binäre Verschlüsselung ausführen können, kann der gleiche Schlüssel, der für die eingebbare Chiffretextverschlüsselung verwendet wird, für die binäre Verschlüsselung verwendet werden. Wird der Schlüssel für die Verschlüsselung mit 26 Zeichen verwendet, verwendet der Verschlüsselungsvorgang einen Algorithmus für eine Addition auf der Basis 26 und verwirft den Übertrag (Moduln 26-Addition) mit einer Umwandlung in den binären Raum, um den

Klartext mit dem Schlüssel zu kombinieren und den Chiffretext zu erhalten. Bei der binären Verschlüsselung ist der Vorgang viel schneller, da die Moduln-Addition binär durchgeführt werden kann, indem einfach eine Exklusiv-Oder-Verknüpfung (XOR) bei dem Klartext und dem Schlüssel zur Erzeugung des Chiffretexts bitweise ausgeführt wird. Da der Schlüssel lediglich die 8-Bit-Werte der 26 ASCII-Zeichen enthält, hat jedes Byte den gleichen Wert an zwei der Bitpositionen. Daher ist der Schlüssel hinsichtlich der Bits in jedem Byte nicht vollständig zufällig und zwei Bits jedes Bytes im Chiffretext können einfach entschlüsselt werden. Allerdings sind die Werte jedes Bytes im Schüssel auf Bytestufe zufällig und die verbleibenden Bits können nicht entschlüsselt werden. Daher kann der Schlüssel für eine binäre Verschlüsselung sowie für eine eingebbare Chiffretextverschlüsselung ohne Kompromiss hinsichtlich der Sicherheit verwendet werden, und die binäre Verschlüsselung läuft so schnell wie mit einem Schlüssel für alle möglichen Bytewerte.

Schlüsseldiskinhalt

[0058] Jedes Speichermedium mit einem oder mehreren Schlüsseln wird mit einer 32-Byte-Disk-ID identifiziert, die ein globaler eindeutiger Identifizierer (GUID) aus lediglich den Zeichen ist, die in einem Dateinamen in allen üblichen Datensystemen erlaubt sind (58 Zeichen in Microsoftsystemen, wobei nicht zwischen Groß- und Kleinbuchstaben unterschieden wird). Vorzugsweise wird jede GUID mit einer algorithmischen Beziehung zwischen aufeinanderfolgenden Zeichen an Stelle einer zufälligen Beziehung erzeugt. Jeder Benutzer, der Schlüsseldisks erzeugen darf, erhält ein Schlüsselgeneratorprogramm, das eine eindeutige Disk-ID-GUID für jede Disk während des Schlüsselerzeugungsvorgangs erzeugt. Die Disk-ID wird in einem Speichermedium in einer Datei gespeichert, die den gleichen 32-Byte-Namen wie der Dateiinhalt hat.

[0059] Bei einem Ausführungsbeispiel der Erfindung wird der von Microsoft veröffentlichte GUID-Erzeugungsalgorithmus angewendet. Obwohl es theoretisch möglich ist, dass zwei verschiedene Kopien dieses Programms zwei GUIDs erzeugen, die identisch sind, sind die Wahrscheinlichkeiten sehr gering und gering genug. Das GUID-Erzeugungssystem von Microsoft verwendet alphanumerische Zeichen mit geschweiften Klammern und Strichen als Satzzeichen. Zur Verwendung als Disk-ID werden die vom Microsoft-Algorithmus erzeugten geschweiften Klammern und Striche entfernt.

[0060] Bei einem anderen Ausführungsbeispiel sind die für die GUID verwendeten Zeichen die bevorzugten 32 eingebbaren Chiffretextzeichen (A-Z + 2-7), um das Lesen und die Eingabe durch Menschen zu erleichtern. Um sicherzustellen, dass keine zwei GUIDs gleich sind, sind die letzten 4 Zeichen der 32-Zeichen-GUID zum Identifizieren des Herstellers der bestimmten Disk reserviert, was eine Identifizierung von 1,048,576 möglichen Herstellern (32 × 32 × 32 × 32) erlaubt. Die ersten 28 Zeichen werden von einem Programm gefüllt, das nie dieselbe Nummer zweimal erzeugt, bis alle möglichen Nummern verwendet worden sind (32^{28})

[0061] Informationen über jeden Schlüssel auf den Speichermedien bestehen aus den folgenden Daten, die als Inhalt einer großen Datei gespeichert sind, wobei ein Dateilayoutformat verwendet wird, das für das betreffende Medium erforderlich ist:

1. Die ersten 32 8-Bit-Bytes stellen eine Schlüsselidentifizierungsnummer (KIN) dar, die ein globaler eindeutiger Identifizierer (GUID) ist, wobei die gleichen Zeichen verwendet werden, die in einer Disk-ID erlaubt sind, wie vorstehend beschrieben. Gemäß einem Ausführungsbeispiel identifizieren die letzen vier Zeichen wiederum den Hersteller des Schlüssels. Der Einfachheit halber wird eine Wiederholungsschlüsselverschlüsselung bei dem gesamten Inhalt der Schlüsseldatei angewendet, die die KIN enthält. Ist der Schlüssel auf einer Disk gespeichert, wird die Schlüsselidentifizierungsnummer in Nicht-Wiederholungsschlüssel-verschlüsselter Form in die Dateibelegungstabelle als Dateiname im Datensystem auf dem Medium kopiert.
2. Bei einem Ausführungsbeispiel wird die Disk-ID als die zweiten 32 Bytes gespeichert, damit das Kopieren der Inhalte der Schlüsselmedien auf andere Medien, die Neuinstallierung und Neuverwendung schwierig wird.
3. Der Schlüssel selbst, der eine lange Sequenz aus 26- oder 32-Zeichen-Bytes ist, die zur Verschlüsselung des ursprünglichen Materials verwendet werden, wird in Wiederholungsschlüssel-verschlüsselter Form gespeichert.

[0062] Vorzugsweise füllt ein Schlüssel (einschließlich der Schlüsselidentifizierungsnummer) oder ein Paar von Schlüsseln, einer zur Verschlüsselung und einer zur Entschlüsselung, das gesamte Medium, üblicherweise eine CD oder DVD, abgesehen von der Disk-ID-Datei. Allerdings kann eine beliebige Anzahl von Schlüsseln auf einem Speichermedium gespeichert werden, jeder als Datei mittels eines bei dem Medium verwendeten Dateiorganisationsverfahrens.

[0063] Der Schlüsseldateiname besteht aus der KIN wie vorstehend beschrieben gefolgt von einer Dateierweiterung .ENC für den Verschlüsselungsschlüssel oder .DEC für den Entschlüsselungsschlüssel. Es folgt ein Beispiel einer GUID, die für die KIN verwendet wird, und des Dateinamens für das Schlüsselpaar:

3AA91601F83211D49D6A0008C7A23A01.ENC
3AA91601F83211D49D6A0008C7A23A01.DEC

[0064] Wird ein Schlüssel auf einem Computersystem installiert, werden seine Offsetnummer (der Ort in der Schlüsseldatei, wo der verwendbare Abschnitt des Schlüssels beginnt, der zu Beginn das 33. Byte ist, das der Anfangs-32-Byte-KIN folgt), Größe, Name und Disk-ID in der residenten Registerdatenbank des Computers gespeichert. Diese Registerdatenbank-Einträge bleiben solange im System, wie das Programm installiert ist, und Schlüsselinformationen aus dem Schlüsselnamen, der Disk-ID und dem Offset bleiben in der Registerdatenbank, nachdem das Programm deinstalliert ist, für den Fall, dass das Programm in Zukunft wieder im System installiert wird. Ein bestimmter Deinstalliervorgang, der von der Standarddeinstalliereinrichtung des Programms verschieden ist, ist zum Entfernen der residenten Registerdatenbank-Daten erforderlich. Das Verbleiben der Registerdatenbank-Daten nach einer Deinstallierung des Programms hilft bei der Verhinderung einer unbeabsichtigten Wiederverwendung der Schlüssel, sollte eine andere Instanz des Programms zu einem späteren Zeitpunkt installiert werden.

[0065] Natürlich kann jedes Verschlüsselungssystem absichtlich missbraucht werden, was in einer Umgehung der Sicherheit resultiert. Es gibt keine technische Einrichtung, die verhindert, dass ein Paar von CDs oder andere Schlüsselmedien, die denselben Schlüssel enthalten, auf einem zweiten Paar von Computersystemen wiederverwendet werden, die den Schlüssel zuvor nicht verwendet hatten. Da dies die Sicherheit sowohl für den ersten als auch den zweiten Benutzer in Frage stellt, wenn ein Angreifer Kopien einer großen Anzahl an Nachrichten auffängt, wo derselbe Schlüssel verwendet wurde, was eine Analyse für tiefgehende Angriffe erleichtert, haben die Benutzer einen starken Antrieb, CDs oder andere Speichermedien mit verwendeten Schlüsseln zu zerstören.

Chiffretextinhalte

[0066] Der Körper des durch das Programm erzeugten Chiffretexts enthält die folgenden Headerinformationen (Metadaten):
|KIN|Offset|Länge|CRC|binär/Text|

[0067] Die KIN identifiziert den Schlüssel, der zur Erzeugung der Nachricht verwendet wurde. Der Offset stellt den Startort vom Beginn des verwendbaren Schlüssels (der KIN im 32. Byte folgt) für das Programm zum Beginnen der Entschlüsselung dar. Die Länge der verschlüsselten Nachricht wird zum Erleichtern einer Fehlerüberprüfung durch einfachen Vergleich der beobachteten Länge der Nachricht mit dieser Zahl verwendet. CRC ist eine Prüfsumme des Chiffretexts, die bei der Fehlererfassung verwendet wird. Die binär/Textbestimmung weist das Empfangsprogramm an, ob es im binären Modus oder eingebbaren Chiffretextmodus entschlüsseln soll.

[0068] Da Offset in der Nachricht jeweils identifiziert, wo das Programm mit dem Entschlüsseln der Nachricht innerhalb des bestimmten Schlüssels beginnen muss, können die verschlüsselten Nachrichten in einer beliebigen Reihenfolge entschlüsselt werden, anders als bei der herkömmlichen Einmalverschlüsselung, bei der verschlüsselte Nachrichten in der Reihenfolge entschlüsselt werden müssen, in der sie verschlüsselt wurden, um einen geeigneten Index im Entschlüsselungsschlüssel zu bewahren.

[0069] CRC (Prüfsummenvorgang) verwendet einen Algorithmus, der einen Ersatz, eine Subtraktion oder Addition eines einzelnen Zeichens in einem Feld von Hundertmillionen Zeichen erfassen kann. Obwohl ein Fehler, der ein Zeichen in ein anderes tauscht, üblicherweise belanglos ist, macht eine Änderung der Länge durch Subtrahieren oder Addieren selbst eines Zeichens die Nachricht durch jede Einrichtung unentschlüsselbar. Das Programm wird daher am Entschlüsseln von Chiffretext gehindert, wenn ein einzelnes Zeichen hinzugefügt oder subtrahiert ist, also ist eine Überprüfung hinsichtlich einer Eins-zu-eins-Zeichenentsprechung bei der Programmentwicklung zwingend. Ersetzungen sind am harmlosesten, da sie sich lediglich auf ein oder zwei Zeichen im Klartext auswirken. Allerdings findet der CRC-Algorithmus diese genauso.

Programmablauf

[0070] Unter Verwendung der Funktionen, auf die über das Schlüsselverwaltungsfenster zugegriffen werden kann, wie in Fig. 2 gezeigt, kann jeder auf dem Medium gespeicherte Schlüssel folgendes sein:

1. Installiert. Die Installieren-Taste **22** registriert die Disk-ID-Nummer in der Windows-Registerdatenbank (oder einer ähnlichen Registerdatenbank für ein anderes Betriebssystem) zusammen mit der Wiederholungsschlüsselentschlüsselten Schlüsselidentifizierungsnummer und Schlüsselverwendungsinformationen und zeigt Schlüsselinformationen im Schlüsselverwaltungsfenster **20** an. Kann die Schlüssel-CD nicht installiert werden oder enthält sie keine gültige Disk-ID, informiert eine Nachricht den Benutzer, dass keine Installation stattfinden kann.
2. Ausgewählt zur Verwendung. Die Verschlüsselung wird mit dem mittels der Auswählen-Taste **23** ausgewählten Schlüssel ausgeführt.
3. Importiert von einem anderen System zusammen mit Verwendungsdaten. Die Verwendungsdaten werden zum Sicherstellen verwendet, dass die verwendeten Abschnitte des importierten Schlüssels nicht wiederverwendet werden. Die Verwendungsdaten können über ein Netz importiert oder aus einer Diskette mittels der Importieren-Taste **24** gelesen werden.
4. Exportiert in ein anderes System zusammen mit Verwendungsdaten. Die Verwendungsdaten

liefern dem Empfangssystem die Informationen, die es braucht, um sicherzustellen, dass keine Schlüsselwiederverwendung auftritt. Die Verwendungsdaten können mittels der Exportieren-Taste **25** über ein Netz exportiert oder auf einer Diskette gesichert werden.

5. Umbenannt mittels eines von einem Benutzer vergebenen Namens. Für den anfänglichen Schlüsselnamen zeigt das Schlüsselverwaltungsfenster eine Kopie der Wiederholungsschlüssel-entschlüsselten Schlüsselidentifizierungsnummer an (die auch im Schlüsselverwaltungsfenster **20** zwei Zeilen unter der Schlüsselidentifizierungsnummer angezeigt wird). Mit einem Rechtsklick auf den Schlüsselnamen erscheint ein Menü, das dem Benutzer die Umbenennung des Schlüssels in einen bevorzugten Namen, wie „Jim's Office" oder „Seattle Center" ermöglicht. Wird der ursprüngliche Schlüsselname oder Dateiname durch den Benutzer mit einer beabsichtigten Neuinstallierung eines verwendeten Schlüssels modifiziert, verhindert die eingebettete KIN eine Schlüsselwiederverwendung durch Vergleichen der Wiederholungsschlüssel-entschlüsselten KIN jedes neuen Schlüssels mit der KIN zuvor installierter Schlüssel, die in der Registerdatenbank des Computers aufgelistet sind. Eine Installation wird nicht erlaubt, wenn es eine Übereinstimmung gibt. Weder der Schlüsselname noch der Schlüsseldateiname werden bei dem Vergleich verwendet. Die KIN wird immer zum Identifizieren des Schlüssels verwendet, ungeachtet von Änderungen des Schlüsselnamens oder des Schlüsseldateinamens durch den Benutzer.

6. Gelöscht. Wurde ein Schlüssel einmal durch Drücken der Löschen-Taste **26** gelöscht, kann der Schlüssel während der Lebensdauer der Programminstallation auf dem Computer auf diesem Computer nicht wiederverwendet werden. Das Löschen eines Schlüssels aktualisiert die Windows-Registerdatenbank zum Angeben, dass der Schlüssel insgesamt verwendet wurde, durch Diebstahl beeinträchtigt wurde, beschädigt oder auf andere Weise untauglich gemacht wurde.

[0071] Die Umbenennung eines Schlüssels in einen freundlichen Namen erleichtert dem Benutzer die Entscheidung, welcher Schlüssel auszuwählen ist. Zur Auswahl eines Schlüssels klickt der Benutzer auf den Namen des Schlüssels im Schlüsselverwaltungsfenster und drückt die "Auswählen"-Taste. Ist der ausgewählte Schlüssel auf der aktuell installierten CD oder einem anderen Schlüsselspeichermedium nicht vorhanden, fordert das Programm den Benutzer auf, das geeignete Medium einzufügen. Die Anforderung wird wiederholt, bis das Medium mit dem ausgewählten Schlüssel installiert oder der Auswahlvorgang abgebrochen wird.

[0072] Ist der Schlüssel installiert, wird die KIN durch das Programm gelesen, mit dem Wiederholungsschlüssel entschlüsselt und entsprechend dem Algorithmus zur Erzeugung einer GUID als gültige GUID authentifiziert. Die GUID wird zur Sicherstellung überprüft, dass sie lediglich erlaubte Zeichen enthält. GUIDs werden mittels einer algorithmischen Beziehung zwischen aufeinanderfolgenden Zeichen anstelle einer zufälligen Beziehung erzeugt, und diese Beziehung wird verifiziert. Ist die KIN verifiziert, wird sie im Schlüsselverwaltungsfenster **20** im Abschnitt für diesen Schlüssel angezeigt. Ist die KIN nicht korrekt oder fehlt sie, erlaubt das Programm die Installierung des zugehörigen Schlüssels nicht.

[0073] Das Programm zeigt eine Dialogbox mit allgemeinen Optionen an, die nachstehend beschriebene, vom Benutzer auswählbare Optionen enthalten.

[0074] „Programm im Hintergrund laufen lassen, wenn Windows startet": diese Optionen platziert ein Icon für das Programm in der Systemablage für einen einfachen Zugriff auf Verschlüsselungs- und Entschlüsselungsfunktionen und als alternative Art und Weise zum Öffnen des Hauptprogramms.

[0075] „Zipdatei für verschlüsselte Dateien und Ordner erzeugen": diese Funktion wandelt Dateien automatisch in ein Standard-Zip-Dateiformat als letzten Schritt der Verschlüsselung um. Dies macht die Datei kleiner, was eine Übertragung über das Netz viel schneller macht.

[0076] „Wizards zur Verschlüsselung und Entschlüsselung von Dateien verwenden": diese Option öffnet hilfreiche Wizards bzw. Helfer, um den Benutzer bei der Verschlüsselung und Entschlüsselung von Datei und Ordnern anzuweisen.

[0077] „Schnelle Verschlüsselung und Entschlüsselung": diese Option öffnet einfache Dialogboxen für erfahrene Benutzer zum Entschlüsseln und Verschlüsseln von Dateien.

Direkter Kommunikationsmodus

[0078] Das Programm kann für eine direkte Kommunikation zwischen zwei Punkten verwendet werden, wenn beide Orte identische Schlüssel haben. Dies wird direkter Kommunikationsmodus genannt. Eine Kommunikation zwischen zwei Orten, einem Ort A und einem Ort B in der nachstehenden Tabelle stellt den grundlegendsten Weg dar, wie das Programm funktioniert.

Ort A	Ort B
A Verschlüsselungsschlüssel	= B Entschlüsselungsschlüssel
A Entschlüsselungsschlüssel	= B Verschlüsselungsschlüssel

[0079] Der „A Verschlüsselungsschlüssel" ist hinsichtlich des Schlüsselinhalts mit dem „B Entschlüsselungsschlüssel" identisch. Der „A Entschlüsselungsschlüssel" ist hinsichtlich des Schlüsselinhalts mit dem „B Verschlüsselungsschlüssel" identisch. Am Ort A wird der A Verschlüsselungsschlüsselbetrag verfolgt und durch das Programm gespeichert, und am Ort B geschieht das gleiche für den B Entschlüsselungsschlüssel. Wenn der Ort B eine Nachricht vom Ort A empfängt, wird der B Entschlüsselungsschlüssel zum Entschlüsseln der Nachricht beginnend an dem durch den Nachrichtenheader angegebenen Offset verwendet.

[0080] Die Entschlüsselungsschlüssel können immer wieder verwendet werden, wenn der Empfänger eine bestimmte verschlüsselte Nachricht lesen möchte, ohne die Sicherheit zu beeinträchtigen, da die Nachricht und der Schlüsselinhalt durch die in dem Schlüssel eingebettete KIN und die in dem Nachrichtenheader eingebetteten KIN- und Offsetdaten miteinander verknüpft sind. Der zur Verschlüsselung einer bestimmten Nachricht verwendete Schlüssel wird nie mehr wieder für eine andere Nachricht verwendet, so dass es keine Einschränkung hinsichtlich der Anzahl gibt, wie oft eine verschlüsselte Nachricht entschlüsselt werden kann. Dies ist ein großer Vorteil für Leute, die große und kleine Mengen von Nachrichten in öffentlichen Speicherzentren wie Driveway und ähnlichen Onlineunternehmen speichern müssen. Die verschlüsselten Nachrichten können heruntergeladen und so oft entschlüsselt werden, wie der Benutzer dies wünscht, ohne dass es eine Schlüsselverwendungsbeschränkung gibt.

[0081] Der Verschlüsselungsschlüssel an beiden Stationen ist verbrauchbar, was heißt, dass beim Aussenden von Nachrichten der Verschlüsselungsschlüssel verwendet wird, bis er für die Verschlüsselung einer weiteren Nachricht zu klein ist. Das Programm informiert den Benutzer dann, dass der verbleibende Verschlüsselungsschlüssel zu klein für die aktuelle Nachricht ist und fordert den Benutzer auf, einen anderen Schlüssel auszuwählen oder zu installieren. Dagegen wird der Entschlüsselungsschlüssel so oft wie gewünscht verwendet und muss aufbewahrt werden, bis die gespeicherten verschlüsselten Nachrichten nie mehr wieder entschlüsselt werden müssen.

[0082] Das Ausmaß des verbleibenden Verschlüsselungsschlüssels für den ausgewählten Schlüssel wird in der Programmstatusleiste zusammen mit dem Schlüsseldateinamen oder vom Benutzer zugewiesenen Namen angezeigt.

[0083] Beliebige zwei Stationen können kommunizieren, bis ihre Verschlüsselungsschlüssel aufgebraucht sind, zu welchem Zeitpunkt sie einen neuen Schlüsselsatz installieren und erneut beginnen. Schlüsselsätze können 650 MB für jeden Schlüssel auf einem Paar von CDs, 8 Gigabytes auf einer DVD-ROM und eine beliebige Größe auf ausreichend großen Speichermedien haben.

SCS-Server-Kommunikationen

[0084] Der sichere Kommunikationssystemserver ermöglicht direkte verschlüsselte Kommunikationen zwischen zwei oder mehr Leuten, die physikalisch keine Schlüssel austauschen können. Wie in **Fig. 1** gezeigt, erhält normalerweise eine der Parteien, die kommunizieren möchte, einen übereinstimmenden Satz von der zentralen Quelle und liefert eine Schlüssel-CD oder ein anderes Speichermedium zu der anderen und beginnt mit der Kommunikation. Manchmal ist eine körperliche Lieferung einer Schlüsseldisk von einer Quelle zur ersten Partei oder einer der beiden zu der zweiten Partei nicht möglich. In diesem Fall kann die Schlüsselzustellung gemäß **Fig. 1** durch elektronische Kommunikationen wie in **Fig. 4** gezeigt bewirkt werden.

[0085] Wenn zwei oder mehr Leute an dem in **Fig. 4** gezeigten SCS Dienst teilnehmen, erhalten diese jeweils eine CD oder ein größeres Speichermedium mit dem Programm und einem SCS-Schlüsselverschlüsselungsschlüssel, der ihnen das Herunterladen von Kommunikationsschlüsseln vom SCS-Verteilungszentrum ermöglicht. Die Kommunikationsschlüssel, die heruntergeladen werden, werden mit dem SCS-Schlüsselverschlüsselungsschlüssel verschlüsselt, so dass lediglich eine Partei mit dem SCS-Schlüsselverschlüsselungsschlüssel den Kommunikationsschlüssel für die Verschlüsselung oder Entschlüsselung verwenden kann. Eine Verschlüsselung mit dem SCS-Schlüssel enthält keine KIN. Da die Kommunikationsschlüssel mit den SCS-Schlüsseln verschlüsselt sind, ist keine weitere Wiederholungsschlüsselverschleierung wie vorstehend beschrieben erforderlich. Nachdem jede Partei ihre Kopie des Paars der Kommunikationsschlüssel heruntergeladen und entschlüsselt hat, verwenden die involvierten Parteien dann die Kommunikationsschlüssel zum direkten Kommunizieren miteinander ohne ihre verschlüsselten Nachrichten durch das SCS-Verteilungszentrum zu schicken.

[0086] Dies verbessert die Privatsphäre, da die Schlüssel nach dem Herunterladen vom SCS-Verteilungszentrum in der SCS-Datenbank zerstört werden. Die SCS-Datenbank hält keine Kopien der heruntergeladenen Kommunikationsschlüssel, wenn dies nicht vom Eigentümer des Schlüsselabonnements gefordert wird. Eine Kommunikation zwischen den Teilnehmern unter Verwendung der heruntergeladenen Schlüssel findet über eine andere Verbindung statt, üblicherweise über ihre eigenen Telefonleitungen oder Satellitensysteme oder das Internet, wie in **Fig. 4** gezeigt.

[0087] Wie in Fig. 4 gezeigt, wird die Erfassung von Schlüsseln durch den folgenden Vorgang oder eine Abwandlung dieses Vorgangs gesteuert. Teilnehmer A **42** fordert einen Kommunikationsschlüsselsatz eines Teilnehmers B an. Damit das SCS-Verteilungszentrum **41** einen Kommunikationsschlüsselsatz des Teilnehmers B ausgibt, muss der Austausch vom Teilnehmer B **43** zuvor bewilligt werden. Nach der Zustimmung lädt der Teilnehmer A dann den Schlüsselsatz des Teilnehmers B herunter und der Teilnehmer B kann den Schlüsselsatz des Teilnehmers A herunterladen. Dann findet eine Kommunikation direkt zwischen dem Teilnehmer A und dem Teilnehmer B außerhalb des SCS-Verteilungszentrums statt.

[0088] Das SCS-Verteilungszentrum **41** zerstört seine Kopien der Kommunikationsschlüssel, wenn sie zu den Teilnehmern gesendet werden, wenn es nicht ausdrücklich angewiesen wird, dies nicht zu tun. Auf eine Benutzeranforderung hin archivierte Schlüssel werden in einem separaten SCS-Verteilungszentrumserver einen vorbestimmten Zeitabschnitt lang auf Kosten des Benutzers aufbewahrt.

[0089] Wie vorstehend angeführt werden die Kommunikationsschlüssel selbst vor ihrer Übertragung durch den Server durch einen SCS-Schlüsselverschlüsselungsschlüssel verschlüsselt, der zu jedem Teilnehmer an dem SCS-Dienst zum Zeitpunkt der Teilnahme verteilt wird. Der Kommunikationsschlüssel wird auf Anforderung erzeugt, mit dem SCS-Schlüssel verschlüsselt und dann zerstört, wenn er zu den Teilnehmern übertragen wird, die kommunizieren möchten. Die verschlüsselten Kommunikationsschlüssel werden in Paketen übertragen, die Blöcke aus 512, 1024 oder mehr sind, und jeder Block wird als durch das Programm intakt empfangen verifiziert, bevor er im SCS-Server zerstört wird, was Übertragungsfehler am Ruinieren des Schlüssels hindert. Der SCS-Schlüsselverschlüsselungsschlüssel wird zum Verschlüsseln des Kommunikationsschlüssels verwendet und verhindert, dass die Blöcke des Kommunikationsschlüssels abgefangen und durch Nichteilnehmer oder andere nicht autorisierte Teilnehmer verwendet werden. Kein anderer Teilnehmer kann einen für einen anderen Teilnehmer gedachten Kommunikationsschlüsselsatz ohne Autorisierung zwischen den Teilnehmern erhalten und verwenden. Das Programm entschlüsselt jeden Kommunikationsschlüssel, wenn er durch jeden Benutzer empfangen wird, wodurch dieser für Kommunikationen zwischen den Benutzern bereitgemacht wird.

[0090] Für eine maximale Sicherheit ist der SCS-Schlüsselverschlüsselungsschlüssel vorzugsweise ein Einmalverschlüsselungsschlüssel, der so lang wie das Paar an Kommunikationsschlüsseln ist, die herunter zu laden sind, und wird vorzugsweise körperlich auf einer CD oder DVD oder alternativ dazu über ein Herunterladen von einem Netz geliefert. Ist der im Server aufbewahrte passende SCS-Schlüsselverschlüsselungsschlüssel aufgebraucht, hat der Teilnehmer die Option einer Erneuerung der Teilnahme und des Empfangs eines neuen SCS-Schlüssels, der auf einer CD, DVD oder einem anderen entfernbaren Computerspeicherträger aufgezeichnet ist, oder über ein Herunterladen vom Netz gesendet wird.

[0091] Dieses Ausführungsbeispiel befasst sich lediglich mit der binären Verschlüsselung, so dass die Kommunikationsschlüssel vorzugsweise alle möglichen Bytewerte verwenden. Da der mit dem SCS-Schlüssel zu verschlüsselnde Klartext lediglich eine Zufallssequenz aller möglichen Bytewerte ist, ist demnach ein Verschlüsselungsverfahren unter Verwendung eines Wiederholungsschlüssels ausreichend, da der Klartext von einem Menschen oder durch einen Computer nicht erkennbar ist, wenn er erfolgreich entschlüsselt ist. Die KIN, die aus dem Dateinamen bekannt ist, ist nicht verschlüsselt. Demnach kann der SCS-Schlüssel ein Wiederholungsschlüssel für eine RSA-Verschlüsselung mit öffentlichem Schlüssel oder eine DES-Verschlüsselung oder eine Autokey-Verschlüsselung oder vieler anderer Verfahren sein, vorausgesetzt, dass jedem Paar von Kommunikationsnutzern ein anderer SCS-Schlüssel gegeben wird.

[0092] Anstatt des Herunterladens von Kommunikationsschlüsseln zum Sender und Empfänger jeweils mit einem Beginn, einer Länge und einem Ende kann der SCS-Server alternativ zum endlosen Erzeugen und Übertragen eines nie endenden Kommunikationsschlüssels zu beiden Parteien eingerichtet sein, der mit dem SCS-Schlüsselverschlüsselungsschlüssel verschlüsselt ist und in Blöcke mit einem Blockidentifizierer zu Beginn jedes Blocks unterteilt ist. Eine gewünschte Länge für jeden Block liegt zwischen 1 Kilobyte und 1 Megabyte. Ein geeigneter Identifizierer für jeden Block ist das Datum und die Zeit, zu dem er übertragen wird. Dann bestimmt eine Partei mittels einer Sicherheitseinrichtung für die andere einen Identifizierer eines Blocks (Datum und Zeit), die der Sender zum Beginnen der Verschlüsselung einer Nachricht verwenden wird, die zum Empfänger gesendet wird. Der Empfänger beginnt dann mit der Aufzeichnung des vom SCS-Server gesendeten Schlüssels beginnenden an dem Blockidentifizierer und zeichnet genug von dem nie endenden Schlüssel zur Entschlüsselung der Nachricht auf, die vom Sender empfangen wird.

[0093] Der empfangene Schlüssel und die Nachricht können beliebig lange aufbewahrt werden. Alternativ dazu kann der Schlüssel lediglich in einem flüchtigen Speicher aufbewahrt und nur lang genug zur Verwendung für die Entschlüsselung aufbewahrt werden, bevor der Schlüssel sowie die Nachricht gelöscht werden. Dann kann kein Abfänger, der eine

Kopie der Nachricht abgefangen hat, den Sender, den SCS-Server oder den Empfänger zum Aufdecken des Entschlüsselungsschlüssels zwingen, da alle Kopien davon zerstört wurden. Weder der Sender noch der SCS-Server hatten jemals eine Kopie, sondern erzeugten ihn oder verwendeten ihn unterwegs.

[0094] Der nie endende Schlüssel kann erzeugt und mit ausreichender Geschwindigkeit zu beiden Parteien gesendet werden, so dass er entschlüsselt und unterwegs zum Verschlüsseln von Echtzeitsprache oder Videokonferenzkommunikationen verwendet werden kann. Für gleichzeitige Duplexkommunikationen werden zwei nie endende Schlüssel zu jeder Partei gleichzeitig übertragen. Die Geschwindigkeit der Schlüsselerzeugung muss nur so schnell sein wie die schnellste dieser Sprach- oder Videokommunikationen. Puffer können zum Ausgleichen von Geschwindigkeitsunterschieden verwendet werden. Ist die Kommunikation langsamer als die Geschwindigkeit, mit der der Schlüssel bereitgestellt wird, kann die Verschlüsselung lediglich einen Abschnitt jedes Blocks des Schlüssels verwenden, wobei die Differenz verworfen wird.

[0095] Anstelle der immer andauernden Erzeugung und kontinuierlichen Übertragung ohne Unterbrechung kann der Schlüssel einfach über einen Zeitabschnitt erzeugt und übertragen werden, der für Sender und Empfänger ausreichend ist, wie beispielsweise acht Stunden pro Tag während der Arbeitszeit oder während eines bestimmten Zeitabschnitts von 4 oder 6 Stunden.

Archivierungsmöglichkeiten

[0096] Das Programm kann Dateien zur Speicherung auf öffentlichen Datenbanken oder lokalen Mehrfachbenutzercomputern verschlüsseln. Fig. 5 zeigt Dateien, die in einer öffentlich zugänglichen Speichereinrichtung eines beliebigen Typs **52** archiviert sind.

[0097] Alle in einer öffentlichen Speichereinrichtung aufbewahrten verschlüsselten Dateien können von jedem heruntergeladen werden, jedoch kann lediglich ein Benutzer mit einem mit diesen Dateien verbundenen Schlüssel, wie das System A **51** in Fig. 5, diese entschlüsseln und lesen. Dies beseitigt die Sorge hinsichtlich einer Dateisicherheit an der Speichereinrichtung, obwohl die Einrichtung die üblichen Standards gegen Vandalismus und andere körperliche Angriffe und Hackerangriffe beibehalten muss, die die gespeicherten verschlüsselten Dateien löschen oder ändern könnten. Wenn eine Beschädigung bestehend aus Additionen oder Subtraktionen zum Chiffretext nicht ungeschehen gemacht werden kann, ist die Datei nicht entschlüsselbar. Eine Beschädigung hinsichtlich eines Ersatzes wird auch durch das Programm erfasst und die Entschlüsselung der beschädigten Datei wird auch zurückgewiesen.

Vielseitige Kommunikationsstrukturen

[0098] Das Programm kann zum Kommunizieren zwischen mehreren Unterstationen auf verschiedene Arten eingerichtet sein. Schlüsselsätze für 3, 4, 5, 8, 10 und 20 Unterstationen oder eine beliebige Anzahl von Unterstationen können mit einer Masterstation und untereinander eingeschränkt oder offen kommunizieren.

[0099] Wie in Fig. 6 gezeigt kann das Programm sicher mit drei Unterstationen **62**, **63**, **64** kommunizieren, die untereinander nicht sicher kommunizieren können. Der Verkehr jeder Unterstation wird an der Masterstation **61** empfangen und entschlüsselt und einzelne Antworten werden von der Masterstation zu jeder Unterstation gesendet. Empfängt die Unterstation 3 Verkehr von der Unterstation 1 oder 2 fehlerhaft, kann dieser nicht entschlüsselt werden.

[0100] Das in Fig. 2 gezeigte Schlüsselverwaltungsfenster **20** erleichtert die Handhabung der komplexen Schlüsselanordnungen. Jeder Schlüssel kann individuell benannt werden (beispielsweise „Unterstation 1"). Dies reduziert die Schwierigkeit bei der Verwendung des geeigneten Schlüssels für eine bestimmte Station erheblich. Wählt ein Benutzer einen Schlüssel aus, der sich nicht auf der aktuell eingefügten CD befindet, fragt das Programm wie vorstehend beschrieben nach dem Einfügen der richtigen CD, wodurch mögliche Fehler bei der Schlüsselauswahl verringert werden.

[0101] Wie in Fig. 7 gezeigt können Beziehungen errichtet werden, die Unterstationen **72**, **73**, **74** die sichere Kommunikation miteinander sowie mit der Masterstation **71** ermöglichen. Diese Form der Kommunikation kann gut mit einer Forschungsgruppe funktionieren, die sich über einen weiten geographischen Bereich verstreut befindet oder innerhalb einer Firma, wo Daten in einer bestimmten Abteilung aufzubewahren sind, jedoch in einem Firmenintranet gespeichert sind. Das Programm ist zur vielseitigen Verwendung entwickelt und kann jeder Kommunikationsanforderung genügen. Beispielsweise können Abteilungsleiter mit den Abteilungschefs über eine öffentliche Datenbank oder das Intranet ohne der Gefahr der Bloßstellung kommunizieren. Abteilungsleiterberichte, die zu den Abteilungschefs gesendet werden, können von niemand anderem gelesen werden, der nicht autorisiert ist, den Abteilungschefschlüssel zu besitzen.

Authentifizierung, digitale Signaturen und biometrische Daten

[0102] Im Programmchiffretextprotokoll ist eine Authentifizierung eingebaut. Wie mit einer digitalen Signatur kann lediglich die Person im Besitz eines Schlüssels Nachrichten von der Gegenstelle entschlüsseln. Ist eine Nachricht erfolgreich mit dem Senderschlüssel entschlüsselt, erzwingt die Programmlogik die Annahme, dass sie von einer Person mit Zugang zum Senderschlüssel verschlüsselt worden sein muss. So weit das Programm betroffen ist, ist die Nachricht daher echt, ist ursprünglich vom Besitzer des Verschlüsselungsschlüssels, und daher authentifiziert. Dieser Authentifizierungsvorgang nimmt an, dass andere Variablen, die für das Programm unmöglich zu identifizieren sind, wie ein Dieb des Schlüssels, nicht aufgetreten sind. Wird die Verschlüsselungsdisk oder digitale Signatur oder der PGP-Schlüssel oder private Schlüssel eines Verschlüsselungssystems mit öffentlichem Schlüssel gestohlen, wird wie bei den meisten Formen der Authentifizierung der Dieb zum autorisierten Benutzer. Das Programm kann auch ein Passwort oder eine PIN oder biometrische Daten mit den Nachrichteninhalten verschlüsseln, wodurch eine weitere Authentifizierungsstufe hinzugefügt wird, die im nicht-knackbarem Chiffretext vorliegt.

Patentansprüche

1. Verfahren zum Bereitstellen eines Paars von Sequenzen verschlüsselter Einmalverschlüsselungs-Kommunikationsschlüssel (**5** & **6**, **4** & **7**) durch einen Server (**1**; **41**) in einem Computernetz, einer für einen Sender (**2**, **3**; **42**, **43**) und einer für einen Empfänger (**2**, **3**; **42**, **43**), mit den Schritten
a. Empfangen einer Sequenz von Zufallszahlen von einem Zufallszahlengenerator,
b. Verwenden der Sequenz von Zufallszahlen zur Erzeugung einer Sequenz von Einmalverschlüsselungs-Kommunikationsschlüsseln, die jeweils mit einem Identifizierer beginnen, und
c. Senden einer Kopie jedes Schlüssels der Schlüsselsequenz (**5** & **6**, **4** & **7**) vom Server (**1**; **41**) über das Computernetz jeweils zu einem Datensatzsender (**2**, **3**; **42**, **43**) und einem Datensatzempfänger (**2**, **3**; **42**, **43**), wobei jede Kopie mit einem Schlüsselverschlüsselungsschlüssel verschlüsselt ist.

2. Verfahren nach Anspruch 1, wobei jeder der Einmalverschlüsselungs-Kommunikationsschlüssel eine Vielzahl von Blöcken umfasst, die jeweils einen mit dem Block verbundenen Blockidentifizierer aufweisen.

3. Verfahren nach Anspruch 2, wobei die Blöcke in einem sequenziellen Strom mehr als 4 kontinuierliche Stunden lang erzeugt und gesendet werden.

4. Verfahren nach Anspruch 1, wobei das Schlüsselverschlüsselungsverfahren ein Einmalschlüsselverfahren ist.

5. Verfahren nach Anspruch 1, wobei das Schlüsselverschlüsselungsverfahren ein Wiederholungsschlüsselverfahren ist.

6. Verfahren nach Anspruch 1, wobei jeder der Einmalverschlüsselungs-Kommunikationsschlüssel mit einem Schlüsselverschlüsselungsschlüssel für den Sender verschlüsselt ist, der derselbe wie der Schlüsselverschlüsselungsschlüssel für den Empfänger ist.

7. Verfahren zur Verwendung eines Einmalverschlüsselungs-Kommunikationsschlüssels zur Verschlüsselung eines Datensatzes in einem Computer (**2**, **3**; **42**; **43**), der mit einem Computernetz verbunden ist, mit den Schritten
a. Empfangen einer Sequenz verschlüsselter Einmalverschlüsselungs-Kommunikationsschlüssel jeweils mit einem Identifizierer von einem Server (**1**; **41**) im Computernetz,
b. Entschlüsseln der Einmalverschlüsselungs-Kommunikationsschlüssel,
c. Verschlüsseln eines Datensatzes unter Verwendung eines der Einmalverschlüsselungs-Kommunikationsschlüssel,
d. Senden des verschlüsselten Datensatzes von einem mit dem Computernetz verbundenen Sender (**2**, **3**; **42**; **43**) zu einem mit dem Computernetz verbundenen Empfänger (**2**, **3**; **42**; **43**) zusammen mit dem Identifizierer für den einen der Einmalverschlüsselungs-Kommunikationsschlüssel,
e. Empfangen des verschlüsselten Datensatzes und
f. Entschlüsseln des Datensatzes unter Verwendung des einen der Einmalverschlüsselungs-Kommunikationsschlüssel.

8. Verfahren nach Anspruch 7, wobei der Einmalverschlüsselungs-Kommunikationsschlüssel zur Erzeugung eines Chiffretexts eingebbarer Zeichen oder eines binären Chiffretexts verwendet wird, wobei das Verfahren die Schritte umfasst
Empfangen einer Auswahl von einem Benutzer, ob der Datensatz in eingebbare Chiffretext-Zeichen oder in binäre Form zu verschlüsseln ist,
wenn der Benutzer eingebbare Chiffretext-Zeichen auswählt, Verwenden des Einmalverschlüsselungs-Kommunikationsschlüssels zur Verschlüsselung des Datensatzes in einen Chiffretext eingebbarer Zeichen, der aus einer Bytesequenz besteht, wobei die Bytewerte auf 48 oder weniger Werte begrenzt sind, und
wenn der Benutzer die binäre Form auswählt, Verwenden des Einmalverschlüsselungs-Kommunikationsschlüssels zur Verschlüsselung des Datensatzes in binäre Form, die aus einer Bytesequenz besteht, wobei die Bytewerte nicht begrenzt sind.

9. Verfahren nach Anspruch 7, wobei der Einmalverschlüsselungs-Kommunikationsschlüssel zur Entschlüsselung entweder eines Chiffretexts eingebbarer Zeichen oder eines binären Chiffretexts verwendet wird, wobei das Verfahren die Schritte umfasst
Empfangen einer Angabe, ob der Datensatz aus eingebbaren Chiffretext-Zeichen oder aus binärer Form zu entschlüsseln ist,
stellt die Angabe eingebbare Chiffretext-Zeichen dar, Verwenden des Einmalverschlüsselungs-Kommunikationsschlüssels zur Entschlüsselung des Datensatzes aus Chiffretext eingebbarer Zeichen, der aus einer Bytesequenz besteht, wobei die Bytewerte auf 48 oder weniger Werte begrenzt sind, und
stellt die Angabe die binäre Form dar, Verwenden des Einmalverschlüsselungs-Kommunikationsschlüssels zur Entschlüsselung des Datensatzes aus binärer Form, die aus einer Bytesequenz besteht, wobei die Bytewerte nicht begrenzt sind.

10. Verfahren nach Anspruch 7, mit den Schritten
Empfangen des verschlüsselten Datensatzes zusammen mit einem bestimmten Offset und
Entschlüsseln des Datensatzes unter Verwendung des Einmalverschlüsselungs-Kommunikationsschlüssels, wobei an einem Ort in dem Schlüssel begonnen wird, der durch den Offset bestimmt ist.

11. Verfahren nach Anspruch 7, mit den Schritten
Verwenden des Einmalverschlüsselungs-Kommunikationsschlüssels zum Verschlüsseln des Datensatzes beginnend am Offsetort im Einmalverschlüsselungs-Kommunikationsschlüssel und
Hinzufügen einer den Offsetort bestimmenden Offsetnummer zu dem Datensatz.

12. Verfahren nach Anspruch 7, mit den Schritten
Empfangen des verschlüsselten Datensatzes zusammen mit einem Identifizierer für den Einmalverschlüsselungs-Kommunikationsschlüssel,
Verwenden des Identifizierers zum Auswählen des Einmalverschlüsselungs-Kommunikationsschlüssels und
Verwenden des Kommunikationsschlüssels zur Entschlüsselung des Datensatzes.

13. Verfahren nach Anspruch 7 oder 12, wobei der Kommunikationsschlüssel eine Vielzahl von Blöcken umfasst und der Identifizierer einen mit dem Block verbundenen Blockidentifizierer umfasst.

14. Verfahren nach Anspruch 13, wobei ein Abschnitt jedes Blocks zum Verschlüsseln/Entschlüsseln des Datensatzes verwendet wird, und ein Restabschnitt jedes Blocks verworfen wird.

15. Verfahren nach Anspruch 7, wobei das Schlüsselentschlüsselungsverfahren ein Einmalschlüsselverfahren ist.

16. Verfahren nach Anspruch 7, wobei das Schlüsselentschlüsselungsverfahren ein Wiederholungsschlüsselverfahren ist.

17. Verfahren nach Anspruch 7 oder 12, wobei das Verfahren zum Verschlüsseln/Entschlüsseln des Datensatzes eine binäre Verschlüsselung/Entschlüsselung ist.

18. Verfahren nach Anspruch 7, wobei das Verfahren zur Verschlüsselung des Datensatzes einen Chiffretext mit einem eingebbaren Zeichensatz erzeugt.

19. Verfahren nach Anspruch 7 oder 12, wobei der Datensatz einen Chiffretext mit einem eingebbaren Zeichensatz umfasst und das Verfahren zur Entschlüsselung auf der Anzahl von Zeichen im Zeichensatz beruht.

20. Verfahren nach Anspruch 8, ferner mit einem Hinzufügen eines Header zu dem verschlüsselten Datensatz, der angibt, ob der Datensatz in binärer Form oder in eingebbarer Chiffretext-Zeichenform ist.

21. Verfahren nach Anspruch 9, ferner mit einem Empfangen der Angabe aus einem Header des verschlüsselten Datensatzes, der angibt, ob der Datensatz in binärer Form oder in eingebbarer Chiffretext-Zeichenform ist.

22. Verfahren nach Anspruch 8 oder 9, wobei die eingebbaren Chiffretext-Bytewerte auf 32 oder weniger Bytewerte begrenzt sind.

23. Verfahren nach Anspruch 10 oder 11, wobei der Datensatz auch eine Schlüsselidentifizierungsnummer enthält, die den Einmalverschlüsselungs-Kommunikationsschlüssel identifiziert.

24. Verfahren nach Anspruch 10 oder 11, wobei der Datensatz auch Informationen zum Überprüfen des Datensatzes auf Fehler enthält.

25. Computerprogrammprodukt mit einem Programm für eine Verarbeitungseinrichtung in einem Computernetz, mit Softwarekodeabschnitten zum Durchführen der folgenden Schritte, wenn das Programm auf der Verarbeitungseinrichtung läuft
a. Empfangen einer Sequenz von Zufallszahlen von einem Zufallszahlengenerator,
b. Verwenden der Sequenz der Zufallszahlen zur Erzeugung einer Sequenz von Einmalverschlüsselungs-Kommunikationsschlüsseln, die jeweils mit einem Identifizierer beginnen, und
c. Senden einer Kopie jedes Schlüssels der Sequenz der Schlüssel (**5** & **6**, **4** & **7**) von der Verarbeitungseinrichtung (**1**; **41**) über das Computernetz jeweils zu einem Datensatzsender (**2**, **3**; **42**, **43**) und einem Datensatzempfänger (**2**, **3**; **42**, **43**), wobei jede Kopie mit

einem Schlüsselverschlüsselungsschlüssel verschlüsselt ist,
wobei jeder Einmalverschlüsselungs-Kommunikationsschlüssel, der von der Verarbeitungseinrichtung (**1**; **41**) jeweils zum Datensatzsender (**2**, **3**; **42**, **43**) und Datensatzempfänger (**2**, **3**; **42**, **43**) zu senden ist, auf einem Paar computerlesbarer Datenträger zum Verschlüsseln/Entschlüsseln eines Datensatzes im Empfänger/Sender gespeichert ist, wobei jeder Einmalverschlüsselungs-Kommunikationsschlüssel aus einer verschlüsselten Bytesequenz besteht, die durch die Verarbeitungseinrichtung durch Zusammensetzen einer Zufallssequenz von Bytes, Verschlüsseln der Sequenz durch Ausführen eines Verschlüsselungsvorgangs mit dem Schlüsselverschlüsselungsschlüssel und Einfügen in den Träger erzeugt wird.

26. Computerprogrammprodukt nach Anspruch 25, wobei die Träger körperliche, tragbare Datenspeicher sind.

27. Computerprogrammprodukt nach Anspruch 25, wobei die Träger Trägersignale mit elektronischen Intra-Computerkommunikationen sind.

28. Computerprogrammprodukt nach Anspruch 25, wobei jeder Kommunikationsschlüssel auf jedem Träger mit einem Schlüsselverschlüsselungsschlüssel verschlüsselt ist, der derselbe wie der Schlüsselverschlüsselungsschlüssel für den anderen Träger des Paares ist.

29. Computerprogrammprodukt nach Anspruch 25, wobei jeder Kommunikationsschlüssel auf jedem Träger mit einem Schlüsselverschlüsselungsschlüssel verschlüsselt ist, der von dem Schlüsselverschlüsselungsschlüssel für den anderen Träger des Paares verschieden ist.

30. Computerprogrammprodukt nach Anspruch 28, wobei jeder Kommunikationsschlüssel auf jedem Träger mit einem Einmalverschlüsselungsschlüssel verschlüsselt ist.

31. Computerprogrammprodukt nach Anspruch 28, wobei jeder Kommunikationsschlüssel auf jedem Träger mit einem Wiederholungsschlüssel verschlüsselt ist.

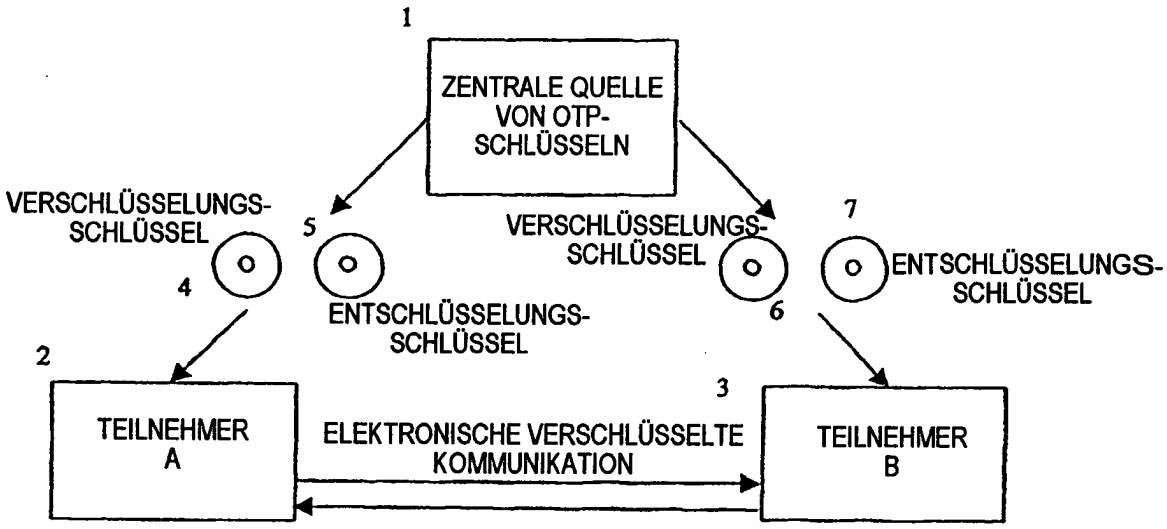
32. Computerprogrammprodukt nach Anspruch 25, wobei die Bytewerte in der Zufallssequenz von Bytes auf einen Satz von Bytewerten begrenzt sind, die weniger als alle möglichen Bytewerte enthalten, so dass der Verschlüsselungsvorgang mit dem Schlüsselverschlüsselungsschlüssel verschlüsselte Bytewerte erzeugt, die aus dem Satz herausfallen.

33. Computerprogrammprodukt nach Anspruch 25, wobei jeder Einmalverschlüsselungs-Kommunikationsschlüssel zur Erzeugung eines Chiffretexts eingebbarer Zeichen dient, der aus einer Bytesequenz besteht, die durch Zusammensetzen einer Zufallssequenz von Bytes, wobei die Bytewerte auf 48 oder weniger Werte begrenzt sind, und Einfügen einer Kopie der Bytesequenz in den Träger erzeugt wird.

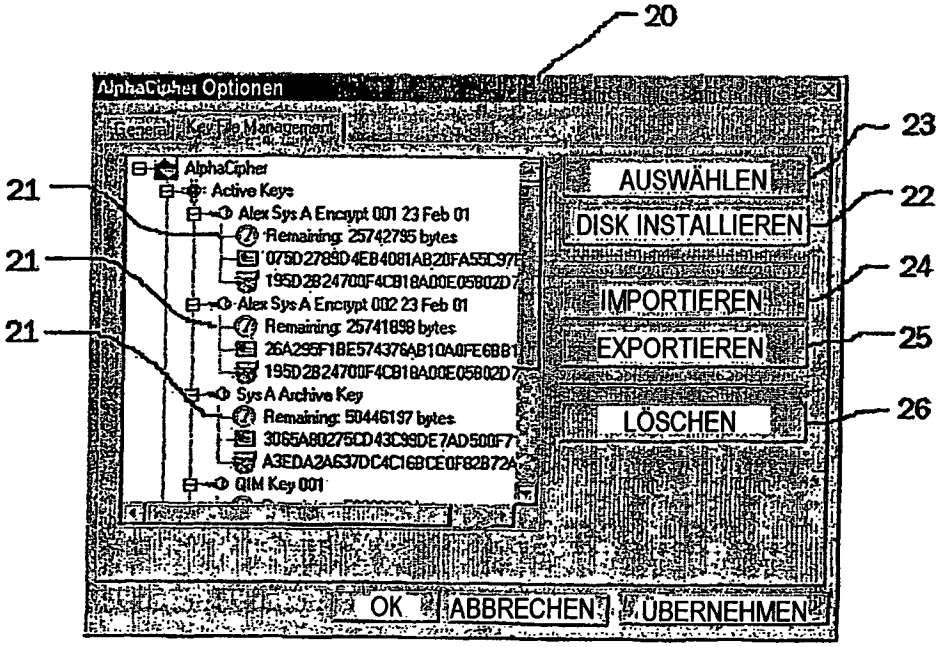
34. Computerprogrammprodukt nach Anspruch 30, wobei die Bytewerte auf 32 oder weniger Werte begrenzt sind.

Es folgen 5 Blatt Zeichnungen

Anhängende Zeichnungen



Figur 1. ZENTRALER SCHLÜSSELDIENST



Figur 2. SCHLÜSSELVERWALTUNGSFENSTER

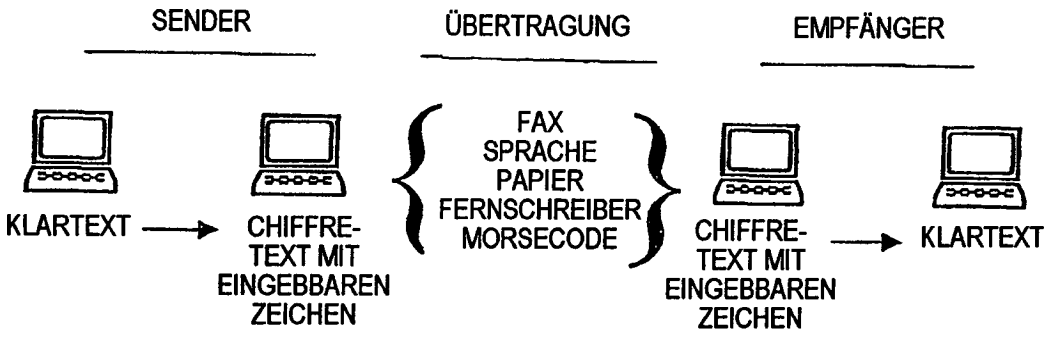
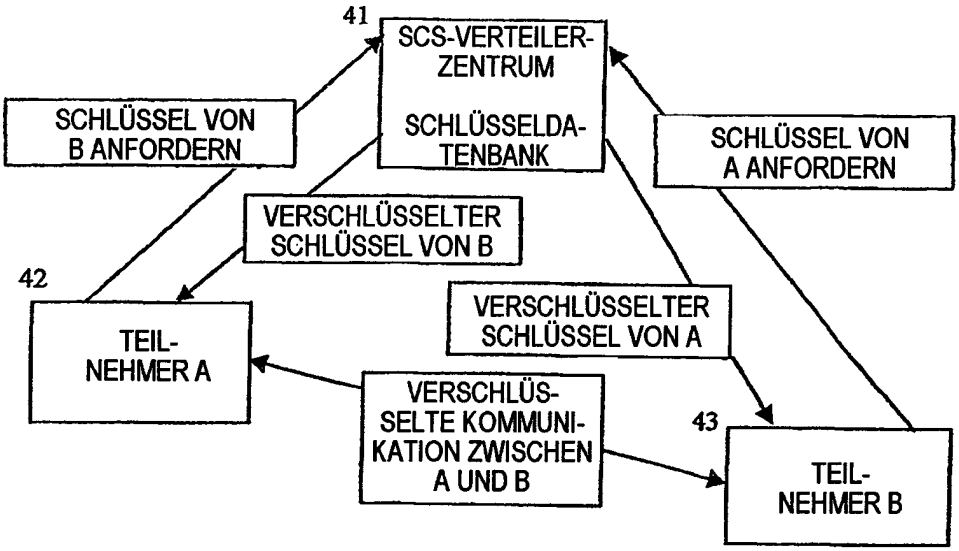
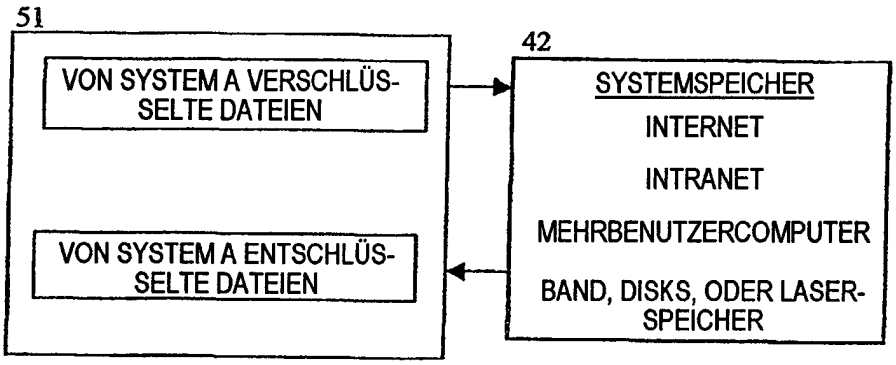


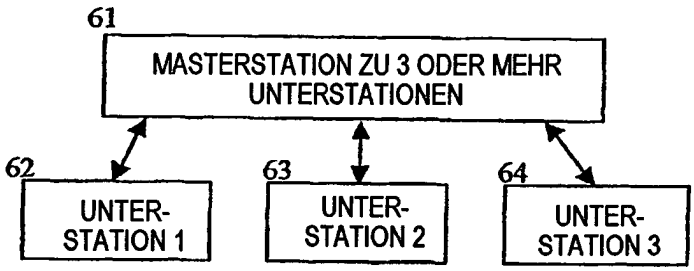
Fig. 3. VERWENDUNG EINES EINGEBBAREN CHIFFRETEXT-ZEICHENSATZES



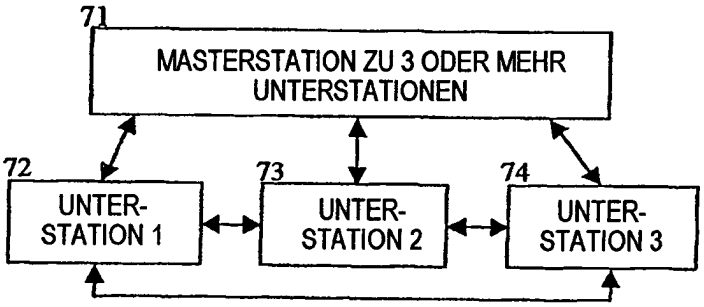
Figur 4. SCS-KOMMUNIKATIONSSYSTEM



Figur 5. DATENARCHIVIERUNGSVORGANG



Figur 6. MASTER ZU MEHREREN UNTERSTATIONEN



Figur 7. RINGVERTEILUNG