Zeitschrift: Pionier : Zeitschrift für die Übermittlungstruppen

Herausgeber: Eidg. Verband der Übermittlungstruppen; Vereinigung Schweiz. Feld-Telegraphen-Offiziere und -Unteroffiziere

Band: 50 (1977)

Heft: 7-8

Artikel: Spione haben nichts zu lachen : Computer-Datenleitungen werden chiffriert

Autor: Rimensberger, U.

DOI: https://doi.org/10.5169/seals-561171

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 02.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Spione haben nichts zu lachen: Computer-Datenleitungen werden chiffriert

U. Rimensberger, dipl. Ing. ETH, c/o GRETAG AG (Regensdorf)

Die Chiffrierung des Datenflusses zwischen Computer und Aussenstellen erfordert durch die grossen anfallenden Datenmengen die Anwendung moderner Techniken. Im nachfolgenden Artikel wird nach den grundsätzlichen Ueberlegungen zur Chiffrierung ein neues Gerät vorgestellt. Analoge Entwicklungen dazu sind zur Zeit auch auf dem militärischen Sektor im Gang.

1. Datenschutz — eine Notwendigkeit

«Wissen ist Macht» oder anders gesagt, Informationen bedeuten Macht. Diese alte Erkenntnis war schon immer Grund, Informationen vor fremdem Zugriff zu schützen. Denn deren Preisgabe oder unbemerkte Veränderung konnte eine finanzielle Einbusse, z.B. im Falle von Geschäftsinformationen, einen politischen Rückschlag wie im Fall Watergate oder sogar einen Verlust an Menschenleben im Falle von militärischen Informationen bedeuten.

Bisher war es einem Aussenstehenden allerdings nur schwer möglich, an grosse Informationsmengen zu gelangen, da diese meist stark dezentralisiert vorhanden waren. Bisher führten die Einwohnerkontrollen, die Steuerbehörden und die militärischen Kreiskommandos unabhängige, räumlich getrennte Personendossiers, die nicht einmal über ein gemeinsames Mutationswesen verfügten.

Die allgemeine Einführung von *EDV-Anlagen* und die Erstellung von *Datenbanken* bewirken aber heute eine gefährliche *Informationskonzentration.* Als Beispiel seien geplante Datenbanken erwähnt, in denen alle Informationen über jeden Bürger an zentrale Stelle zusammengetragen werden sollen.

Diese wachsende Informationskonzentration und die gleichzeitig erschreckend zunehmende *Computerkriminalität* zeigen die Notwendigkeit eines umfassenden Datenschutzes.

Durch rechtliche, gesetzliche Mittel soll nun der missbräuchlichen Informationsverwendung ein Riegel vorgeschoben werden. Zahlreiche Länder haben entsprechende Gesetze in Bearbeitung oder, wie in Deutschland, bereits verabschiedet. Die rechtlichen Massnahmen werden unter dem Begriff *Datenschutz* zusammengefasst. *Datensicherung* hingegen umfasst alle technischen Mittel zum Schutze von Informationen vor Verlust oder Manipulationen. Möglichkeiten sind die Zugriffskontrolle, räumlich getrennte Datenaufbewahrung oder eben Chiffrierung.

In den immer häufigeren *Datenfernverarbeitungssystemen* ist das Sicherheitsrisiko noch weit grösser. Beachtliche Informationsmengen verlassen den kontrollierbaren Sicherheitsbereich und werden über Miet- oder Wählleitungen oder sogar über Funkstrecken übertragen.

Auf dem Uebertragungsweg bestehen für die Informationen die drei Gefährdungen:

1. Informationsverfälschung durch Störungen
2. Informationsverlust durch Abhorch
3. Informationsveränderung durch Manipulation

Der Eingriff in eine Leitung ist, wie de jüngsten Abhörskandale zeigten, für eine kriminelle Organisation ohne grossen Aufwand und mit kleinen Investitionen möglich. Unter der sicher nicht unberechtigten Annahme, dass heute die Täter über gutes EDV-Wissen verfügen, besteht zusätzlich die grosse Gefahr einer Manipulation auf der Leitung. Als Beispiel sei das wiederholte Einspeisen einer Gutschrift auf einer Bankleitung erwähnt.

Nach diesen Betrachtungen überrascht es nicht, dass das deutsche Datenschutzgesetz ausdrücklich Sicherungsmassnahmen beim Datentransport verlangt. In der Schweiz existiert noch keine gesetzliche Richtlinie. Der Anwender trägt alleine die Verantwortung, die in seinem Falle angebrachten Sicherungsmassnahmen ergriffen zu haben.

2. Datensicherung durch Chiffrierung

Den Gefährdungen auf einer Uebertragungsstrecke kann mit den folgenden Mitteln begegnet werden:

1. Fehlersicherung
2. Chiffrierung
3. Authentifizierung

Die Chiffrierung, welche im weiteren allein betrachtet werden soll, bietet zuverlässigen Schutz vor Informationsverlust durch Abhorch, kann aber gleichzeitig auch die Informationsverfälschung durch Störungen oder betrügerische Manipulationen verunmöglichen.

Grundsätzlich können zwei Arten der Chiffrierung unterschieden werden:

— kontinuierliche Chiffrierung (stream ciphering)

— Blockchiffrierung

2.1 Kontinuierliche Chiffrierung

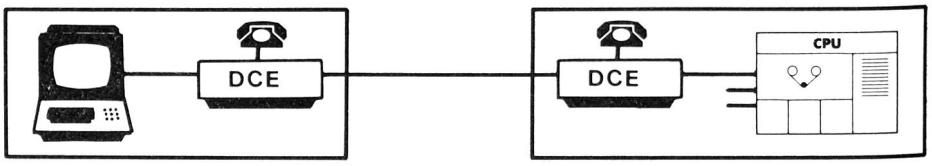
Das Prinzip der kontinuierlichen Chiffrierung, wie es heute in praktisch allen Chiffriergeräten für Regierungsanwendungen verwendet wird, lässt sich am anschaulichsten erläutern anhand des Verfahrens mit Zufallslochstreifen.

Mit Hilfe eines Zufallsgenerators werden zwei gleiche Lochstreifen gestanzt, welche eine echte Zufallsfolge enthalten. Eine solche Folge kann z. B. folgendermassen aussehen:

1+.)&()81&TBFKR%92+JHT73/ . . . . . .

Soll nun eine Meldung, die als Lochstreifen vorliegt, chiffriert werden, wird sie beim Sender bitweise mit dem Programm des Zufallslochstreifen *addiert.* Die gemischte Folge, welche entsprechend auch zufällig ist, kann auf irgend einem Medium übertragen werden. Nur der berechtigte Empfänger, der den selben Zufallslochstreifen besitzt, kann durch *Subtraktion* wieder die ursprüngliche Meldung zurückgewinnen.

Dieses Verfahren ist absolut sicher und lässt sich auch mit mathematischen Methoden nicht brechen. Der laufende Nachschub von Zufallslochstreifen würde aber, speziell bei schneller Datenübertragung, ein beachtliches Transportproblem darstellen. Aus diesem Grunde werden in heutigen kontinuierlichen Chiffriersystemen die Zufallslochstreifen durch *Chiffrierrechner* ersetzt. Diese erzeugen beim Sender und Empfänger die gleichen, jetzt aber pseudozufälligen Chiffrierfolgen. Unter «pseudozufällig» wird verstanden, dass sich die anscheinend zufällige Impulsfolge nach einer gewissen Länge, der Periode, wiederholt. Ist diese ausreichend lang, was heute ab mindestens 10^{50} Bit der Fall ist, ist ein



Figur 1: Klassische Anordnung einer Computeranlage: Links das Terminal mit dem Uebertragungsmodem DCE, rechts die zentrale Rechnungsanlage mit dem zweiten Modem DCE.

solches System *praktisch unbrechbar,* selbst bei Einsatz schneller Grossrechner. Damit sich der gleiche Chiffrierrechner von mehreren Benützern verwenden lässt, muss sich der Rechenprozess resp. das Bildungsgesetz der resultierenden Zufallsfolge durch Einstellen eines geheimen Schlüssels verändern lassen. Die Mannigfaltigkeit des Schlüssels bestimmt dann wesentlich die Sicherheit des Systems.
Zuätzliche Massnahmen müssen ergriffen werden, damit nicht aufeinanderfolgende Meldungen mit dem gleichen Abschnitt des Chiffrierprogramms chiffriert werden.

Da die kontinuierliche Chiffrierung bitweise erfolgt, ist sie völlig *transparent* und reduziert die Nutzbitrate im wesentlichen nicht. Entscheidend ist weiter, dass sich *Uebertragungsfehler nicht verschleppen.* Durch das ständige Vorhandensein von Chiffrat auf der Leitung lässt sich nicht einmal feststellen, ob überhaupt eine Meldung vorhanden ist (traffic flow security).

Kontinuierliche Chiffriersysteme haben sich im militärischen und diplomatischen Einsatz selbst unter extremsten Bedingungen seit langer Zeit bewährt.

2.2 Blockchiffrierung

Die Blockchiffrierung, welche in letzter Zeit hauptsächlich in den USA diskutiert wird, beruht auf einem grundlegend anderen Prinzip, das im folgenden leicht vereinfacht dargestellt werden soll:
Liegt eine Meldung vor, die chiffriert werden soll, wird diese in einzelne Blöcke konstanter Länge aufgeteilt. Anschliessend werden innerhalb der einzelnen Blöcke die einzelnen Bits durch eine Permutation vertauscht.

Die Art der Permutation wird auch hier durch einen Schlüssel bestimmt. Die Blockchiffrierung hat allerdings für die gesicherte Datenübertragung offensichtliche Mängel:

— Fehler auf der Uebertragungsstrecke *vervielfachen* sich.
— Die einzelnen Blocks können vertauscht, weggelassen oder mehrmals hintereinander eingefügt werden (Manipulation).

Der letzte Nachteil lässt sich durch Verkettung der einzelnen Blöcke untereinander beheben. Dadurch würde sich aber durch die mehrmalige Uebertragung der gleichen Bits der *Durchfluss vermindern.* Die Blockchiffrierung kann wohl eingesetzt werden innerhalb des Sicherheitsbereiches eines Rechenzentrums zum Schutze von kurzzeitig gespeicherten Daten bei kleineren Sicherheitsanforderungen; für den Schutz einer Datenübertragungsstrecke eignet sie sich aber kaum.

3. Datenchiffriergerät GRETACODER 515

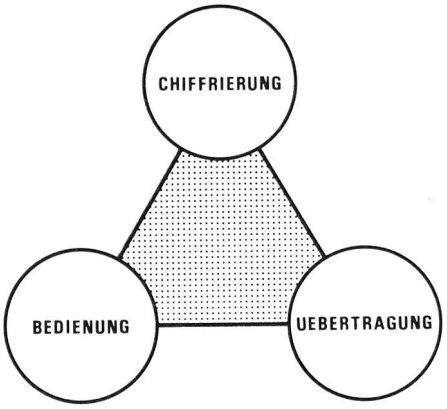
Aufgrund der vorgängigen Ueberlegungen und dank der über 25jährigen Erfahrung im Bau von on-line-Chiffriergeräten hat die GRETAG das Datenchiffriergerät GRETACODER 515 entwickelt, das auf dem Prinzip der *kontinuierlichen Chiffrierung* beruht.

3.1 Anwendungen

Der GRETACODER 515 wird eingesetzt zur Chiffrierung von Datenübertragungsstrecken bei Banken, Industrie und öffentlichen Diensten. Die Chiffrierung von Faksimile-Uebertragungen ist jedoch ebenso möglich wie der Schutz von gespeicherten Daten.
Das Gerät arbeitet mit allen Modems im Geschwindigkeitsbereich von 0—20 kbit/s zusammen. Asynchrone Terminals und Fernschreiber mit dem CCITT-Alphabet Nr. 5 sowie alle synchronen Terminals und Rechner können mit dem GRETACODER 515 verbunden werden. Die normierte Schnittstelle V.24 ermöglicht das schnelle, einfache Einfügen des Chiffriergerätes zwischen Datenendeinheit und -übertragungseinheit.
Das Chiffrieren von Vollduplex und Halbduplexverbindungen ist mit dem gleichen Gerät möglich. Durch interne Programmiermöglichkeiten lässt sich das Gerät, analog zu einem Modem, an jeden Anwendungsfall anpassen.
die gewünschte Schlüsselnummer auswählen; alle andern Funktionen wie Synchronisation usw. werden vom Gerät vollautomatisch ausgeführt. Leuchtdioden zeigen den jeweiligen Zustand an. Im Falle eines Unterbruches kann mit Hilfe der eingebauten Selbsttesteinrichtung ein Fehler rasch eingegrenzt werden.

Uebertragungssicherheit

Die langjährige Erfahrung der GRETAG im Bau von on-line-Chiffriersystemen für Kurzwellen-Funkverbindungen zeigt sich auch in der aussergewöhnlichen Uebertragungssicherheit des GRETACODER 515. Die synchrone Datenübertragung schützt vor möglichen Störungen. Die Synchronisation mittels Korrelation garantiert selbst bei Fehlerraten von 10^{-3} eine Synchronisierwahrscheinlichkeit von 99,99 %. Der automatisch erzeugte Zusatzschlüssel, eine weitere wichtige Information, wird sogar dreimal übertragen und mittels Majoritätsentscheid ausgewählt. Nach einem Leitungsunterbruch startet das Gerät selbst und synchronisiert automatisch neu ein.
Der vollelektronische Aufbau mit integrierten Schaltkreisen gewährleistet eine hohe Lebensdauer und einen unterbruchsfreien Betrieb.



Figur 3: Nur das Zusammenwirken der drei Säulen führt zu Sicherheit bei der Datenübertragung

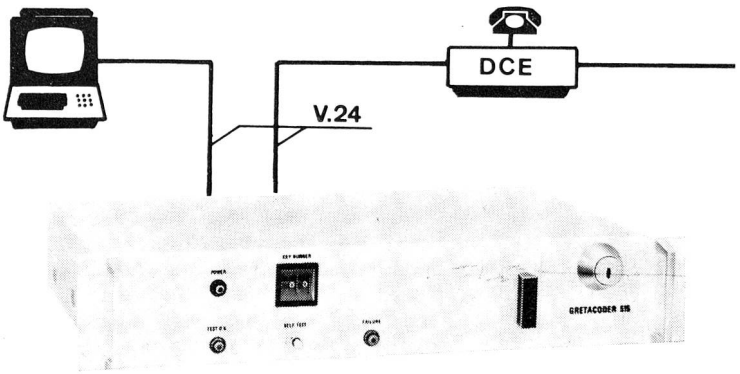


Bild 2: Das Chiffriergerät wird zwischen Terminal und Modem geschaltet.

3.2 Sicherheit

Die Sicherheit eines on-line-Chiffriersystems beruht auf den drei Säulen Chiffriersicherheit, Bedienungssicherheit und Uebertragungssicherheit. Nur durch das Zusammenwirken aller drei Faktoren ist eine zuverlässige Uebertragung gesichert.

Bedienungssicherheit

Für den Einsatz im zivilen Datenübertragungsbereich hat GRETAG ein neues Gerätekonzept entwickelt. Der GRETACODER 515 ist ausgelegt für einen *unbedienten Dauerbetrieb,* es stellt an das Bedienungspersonal keine Anforderungen. Der Operateur muss nur das Gerät einschalten und

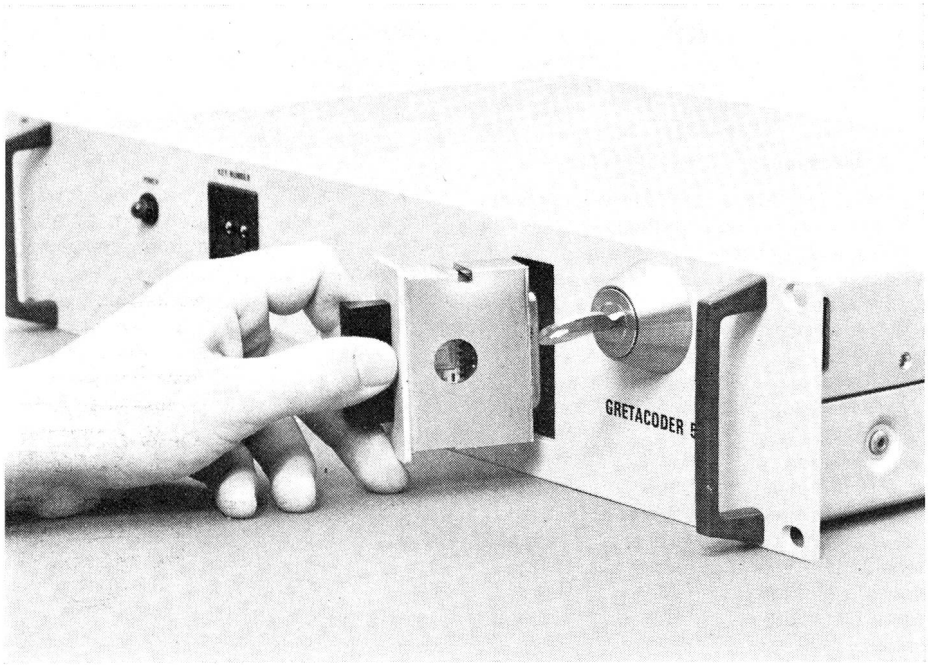


Bild 4: Die geheimen Schlüsselelemente, der Verknüpfungsschlüssel und 30 verschiedene Grundschlüssel werden vom Sicherheitsbeauftragten in einem Einschub programmiert, welcher im Gerät eingeschlossen wird.

Chiffriersicherheit

Wie in Abschnitt 2 erläutert wurde, beruht die Chiffriersicherheit einerseits auf der Periode, anderseits auf der Schlüsselmannigfaltigkeit des verwendeten Chiffrierrechners. Im GRETACODER 515 beträgt die Periode bei der grössten Uebertragungsgeschwindigkeit mindestens 15^{14} Jahre. Wie alle anderen GRETAG-Chiffriergeräte verfügt auch der GRETACODER 515 über drei verschiedene, unabhängige Schlüsselelemente:

1. Der geheime *Grundschlüssel* mit einer Mannigfaltigkeit von $> 10^{19}$
2. der geheime *Verknüpfungsschlüssel* mit einer zusätzlichen Mannigfaltigkeit von $> 10^{38}$
3. der *Zusatzschlüssel,* der verhindert, dass zweimal dieselbe Chiffrierfolge verwendet wird und der bei jeder Synchronisation Startstellung und Rechengesetz der Chiffrierrechner verändert.

Die geheimen Schlüsselelemente, der Verknüpfungsschlüssel und 30 verschiedene Grundschlüssel werden vom Sicherheitsbeauftragten in einem kleinen Einschub programmiert, welcher im Gerät eingeschlossen wird.
Der Operateur braucht somit den geheimen Schlüssel nicht zu kennen; er stellt lediglich eine Adresse ein. Da die Schlüssel auf dem automatischen GRETAG Programmiergerät erzeugt werden, braucht nicht einmal der Sicherheitsbeauftragte den Inhalt des geheimen Einschubes zu kennen. Da der Grundschlüssel zirka alle ein bis zwei Wochen gewechselt werden soll, muss der Einschub nur alle ein bis zwei Jahre einmal neu programmiert werden.
Ueberwachungsschaltungen kontrollieren zusätzlich laufend das Chiffrierprogramm. Sollte der Chiffrierrechner einmal ausfallen, unterbrechen sie automatisch die Uebertragung und betätigen die Alarmanzeige.

35 mm-Flakpanzer Gepard Oerlikon-Contraves

Der 35 mm-Flakpanzer Oerlikon-Contraves wird in Serie unter Lizenz der Firmengruppe Oerlikon-Contraves durch die Firma Krauss-Maffei, München, für die *Streitkräfte der Bundesrepublik Deutschland,* von *Belgien* und der *Niederlande* produziert.
Der 35 mm-Flakpanzer Oerlikon-Contraves ist ein in jeder Hinsicht autonomes *Fliegerabwehrsystem,* ausgerüstet mit einem sehr präzisen Feuerleitsystem mit *Such-* und *Zielfolgeradar* (Typ B2: Siemens, Typ CA-1: Signaal), einem *Contraves-Feuerleitcomputer,* Periskopen für optische Zielerfassung- und Verfolgung sowie verschiedenen anderen Teil-Systemen und bewaffnet mit zwei *automatischen 35 mm-Oerlikon-Flakkanonen* mit grosser Feuerleistung. Die hervorragenden Eigenschaften der 35 mm-Fliegerabwehrkanone und der 35 mm-Munition, kombiniert mit der präzisen Zielverfolgung des Feuerleitsystems, verleihen dem Flakpanzer eine grosse taktische Wirksamkeit und Abschussleistung bei jedem Wetter, Tag und Nacht. Dank dem gepanzerten Turm, der ABC-gefilterten Belüftungsanlage und dem Leopard-Kampfpanzer-Fahrgestell sind *grosse Mobilität und Ueberlebens-Chance* gewährleistet.
Streitkräfte anderer Länder wünschen, den Turm des 35 mm-Flakpanzers auf das Fahrgestell ihres eigenen Kampfpanzers aufzusetzen. Die konstruktive Aufteilung des 35 mm-Flakpanzers in Turm, Energieversorgungsanlage und Fahrgestell erlaubt es, dieses Fliegerabwehrsystem in nahezu alle anderen Kampfpanzer-Fahrgestelle wie diejenigen des M 48, M 60, Pz 68 und Chieftain zu integrieren. Damit kann Oerlikon-Contraves dem weltweiten Interesse anderer Streitkräfte am 35 mm-Flakpanzer weitgehend entsprechen.

NATEL

Die Einführung des Nationalen Autotelefonnetzes — welches die veralteten Regionalnetze ablösen wird — erfordert die Errichtung von zusätzlichen Relaisstationen. Zum Bau einer solchen Station auf dem Schauenberg bei Winterthur ist letzthin bei den zuständigen Behörden das Gesuch zur Erteilung der Baubewilligung eingereicht worden. Wie nun bekannt geworden ist, entsteht in der regionalen Oeffentlichkeit gegen das Vorhaben Opposition.

Fernmeldeunternehmen bilden Exportgemeinschaft

Die SWISSCOM ist eine Exportgemeinschaft schweizerischer Fernmeldeunternehmen. Zu den Initianten und Gründungsmitgliedern gehören die Autophon AG, die Cablex SA, Chr. Gfeller AG, Hasler AG, Sodeco-Saia SA und die Zellweger-Uster AG. Durch gemeinsames Auftreten und Koordination der Exportbemühungen soll die Schlagkraft der Schweizer Fernmeldeindustrie im hart umkämpften internationalen Telekommunikationsgeschäft vergrössert werden. Die Schweizer Fernmeldeindustrie hat ihre Leistungen im In- und Ausland unter Beweis gestellt. In der Schweiz wurde zusammen mit der Schweizerischen PTT eines der besten Fernmeldenetze der Welt aufgebaut. Dieses «Know-how» und den guten Ruf will die SWISSCOM nutzen; durch das gemeinsame Vorgehen können unter Ausnützung des Ingenieurpotentials auch grössere und komplexere Projekte in Angriff genommen werden.
Die verstärkten Exportbemühungen sollen dazu beitragen, den durch Rezession und geringeren Bedarf im Inland bedingten Geschäftsrückgang in der schweizerischen Fernmeldeindustrie aufzufangen, und im weltweit zunehmenden Fernmeldegeschäft grösseren Chancen zu sichern.