Der Kampf gegen die Geheimcodes

Autor(en): **[s.n.]**

Objekttyp: **Article**

Zeitschrift: **Pionier : Zeitschrift für die Übermittlungstruppen**

Band (Jahr): **24 (1951)**

Heft 1

PDF erstellt am: **22.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-559970

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

genauer umschrieben wird. Die Erfahrung zeigte, dass die Pressevertreter im allgemeinen keinen grossen Gebrauch von der Möglichkeit machten, die Reportage mitzuhören —, ihnen war eher daran gelegen, von verschiedenen Punkten Listen der ersten Läufer mit den Durchgangszeiten zu erhalten, ohne dass Wert auf sofortige Übermittlung gelegt wurde. Solche Listen lassen sich aber vielleicht auch durch den internen Funkdienst zusammenstellen und übermitteln. Die Reportagen für das Publikum können sich somit darauf konzentrieren, einige Kilometer vor Wil und einige Kilometer vor Frauenfeld eine Vorschau über den Stand des Rennens zu geben, was auch mit festen Stationen möglich ist. Damit könnte das wartende Publikum unterhalten, die Spannung auf den kommenden Durchmarsch gesteigert, und so dem Veranstalter eine gute propagandistische Unterstützung geboten werden. Nun, wir werden ja nächstes Jahr sehen.

Für uns Fünkeler und Telephönler war die Übung lehrreich, zumal die wenigsten Teilnehmer zuvor Gelegenheit hatten, ausgiebig mit der TLD zu arbeiten und ihre Finessen kennenzulernen. Die Erfahrung zeigt, dass nicht alles, was im Kopfhörer intern gut verständlich ist, sich ohne weiteres auch zur Verstärkung auf Grosslautsprecheranlagen eignet. MG

Der Kampf gegen die Geheimcodes

Mit einem neuen Modell der amerikanischen Elektronengehirne ist es gelungen, Geheimcodes und chiffrierte Texte in kurzer Zeit zu entschlüsseln. Diese Rechenmaschine, die elfstellige Zahlen in Bruchteilen einer Sekunde dividieren und multiplizieren kann, tastet die in jedem Geheimtext regelmässig wiederkehrenden Buchstabengruppen blitzschnell ab und hilft so, dem Inhalt auf die Spur zu kommen.

Die Verschlüsselung von Nachrichten und die Entzifferung von Geheimcodes ist auf vielen Gebieten von entscheidender Bedeutung. Während der Ardennenoffensive, im Dezember 1944, stiess Skorzeny mit 2000 Mann in amerikanischen Uniformen, mit Jeeps und Sherman-Panzern, in den Rücken der alliierten Front. Sie verdrehten Richtungsschilder, zerschnitten Kabel, bauten Strassensperren und richteten die grösste Verwirrung an. Die Deutschen sprachen perfekten amerikanischen Slang; ihre Ausrüstung war von der Lucky Strike bis zum Soldbuch echt. Und die ganze Aktion war so gründlich vorbereitet, dass der US-Geheimdienst trotz zahlloser Strassenkontrollen tagelang im Dunkeln tappte. Schliesslich wurde in einem der Panzer ein deutsches Code-Buch entdeckt, mit dem sich die Amerikaner sofort in Skorzenys Funkverkehr einschalteten. Kurz darauf waren die meisten Störtrupps gefasst.

Heute arbeiten nicht nur viele Firmen, Industrieunternehmen und Grossbanken, sondern auch die Verbrecherbanden und Schmuggelorganisationen mit Codebüchern und Chiffriermaschinen. Im Dienste der «Interpol» (Internationale Polizeikommission) tauschen täglich 15 Funkstationen von London und Lissabon bis Triest und Helsinki ihre Nachrichten im Geheimcode aus. In der Diplomatie ist die Verwendung von Geheimsprachen für vertrauliche Mitteilungen ja seit jeher üblich gewesen.

Mit der Kryptographie, der Wissenschaft der verschlüsselten Sprache, haben sich schon die alten Griechen beschäftigt. Cäsar pflegte in seinen Geheimbriefen jeden Buchstaben durch den im Alphabet viertnächsten zu ersetzen. Später tüftelten so geniale Köpfe wie Richelieu, Napoleon und Edgar Allan Poe neue Möglichkeiten aus. Das nach einem französischen Diplomaten benannte Vigenère-System bewahrte sein Geheimnis 300 Jahre lang, bis es 1863 von dem preussischen Major Kasiski analysiert wurde. Für die kniffligen Aufgaben, welche die Chiffrierabteilung des OKW zu lösen hatte, wurden bekannte Mathematiker, Schachspieler, Ingenieure und Universitätsprofessoren herangezogen.

Grundsätzlich lassen sich alle Codemethoden aufdecken. Durch die Erfindung von Chiffriermaschinen nach dem ersten Weltkrieg wurde das aber immer schwieriger. Der von dem Schweden Hagelin konstruierte Apparat «C 38» bestand aus zwei Scheiben. Die eine nahm den Klartext auf, die andere schrieb den verschlüsselten Text. Beide waren durch ein Chiffrierrad verbunden, das sich unregelmässig drehte und auf einen bestimmten Schlüssel eingestellt werden konnte. Diese Maschine lieferte millionenfache Variationsmöglichkeiten. Sie wurde während des Krieges von den Achsenmächten wie von den Alliierten benutzt, ohne dass man eine Dechiffrierung befürchten musste. Heute werden nicht nur Schriftstücke, sondern auch Telephongespräche verschlüsselt. Bevor die Wörter über das Kabel laufen, werden sie in einen völlig unverständlichen Laut-Salat verwandelt, indem man die Schwingungszahl der einzelnen Laute verändert und sie dann vom Empfangsgerät wieder normalisieren lässt.

Durch genaues Studium kann jedoch auch das komplizierteste System durchschaut werden. Das liegt an der Eigenart der Sprache. Bestimmte Buchstabenfolgen kehren stets in der gleichen Häufigkeit wieder. Zum Beispiel tritt im Englischen unter 1000 Buchstaben das e durchschnittlich 131mal auf, und die häufigsten Konsonanten sind t, n, r, s und h. So ergeben sich bald zahlreiche Anhaltspunkte. Bei aufgefangenen Geheimbotschaften kommt es also darauf an, typische Buchstabengruppen möglichst schnell zu erkennen und tabellarisch zu ordnen. Mit Hilfe statistischer Formeln kann dann festgestellt werden, zu welcher Kategorie eine Chiffre gehört.

Bisher konnten militärische oder diplomatische Stäbe für längere Zeit mit demselben Schlüssel arbeiten, da auch die gewiegtesten Experten für die Entzifferung mechanisch chiffrierter Nachrichten mindestens ein Jahr brauchten. Eine Gefahr bestand lediglich darin, dass die wertvollen Apparate feindlichen Agenten in die Hände fielen. Zu ihrem Schutz sind deshalb von allen Regierungen die schärfsten Sicherheitsbestimmungen erlassen worden. Die Amerikaner hatten im Kriege eine Maschine, die alle Funksprüche der japanischen Regierung entschlüsselte. Wie ihnen diese Konstruktion gelang, ist bis heute geheim geblieben. Angeblich soll ein Agent direkt in der Tokioter Regierung gesessen haben. So erfuhren sie den Inhalt der Gespräche zwischen hohen japanischen und deutschen Stellen und kannten bei verschiedenen Schlachten die Stärke der feindlichen Flotte im voraus.

Der Kampf um das Verschlüsseln und Entziffern von Geheimtexten ist so alt wie der Wettstreit zwischen Angriffs- und Abwehrwaffen. Bisher hatten die Chiffriermaschinen vor ihren rechnenden und kombinierenden «Verfolgern» einen beruhigenden zeitlichen Vorsprung. Wenn dieser jetzt von den Elektronengehirnen eingeholt wird, ist es höchste Zeit, dass die Meister der Geheimschrift sich etwas Neues ausdenken.