.SIAK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SICHERHEITSAKADEMIE

.SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis

Blasi, Walter (2014):

Datensicherheit und Enträtselungskunst. Über das Verbergen und Entschlüsseln von Informationsinhalten

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (1), 62-73.

doi: 10.7396/2014_1_G

Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:

Blasi, Walter (2014). Datensicherheit und Enträtselungskunst. Über das Verbergen und Entschlüsseln von Informationsinhalten, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (1), 62-73, Online: http://dx.doi.org/10.7396/2014_1_G.

Online publiziert: 5/2014

Datensicherheit und Enträtselungskunst

Über das Verbergen und Entschlüsseln von Informationsinhalten

WALTER BLASI,
wissenschaftlicher Referent am Institut für Wissenschaft und Forschung der Sicherheitsakademie des Bundesministeriums für Inneres.

Wenn auch derzeit die Hysterie über die relativ junge Bedrohungsform von Cyberangriffen in all ihren Ausprägungen von „Crime“ bis „War“ sowie die Aufregung über Datendiebstahl und Abhörskandale die mediale Welt beherrschen und die Bevölkerung durch Sensationsberichte und Whistleblower in Unruhe versetzt wird, war es immer schon ein Grundbedürfnis des Menschen, Nachrichten so zu übermitteln, dass sie vor unbefugten Zugriffen geschützt sind. Über Jahrhunderte wurden daher Verschlüsselungstechniken entwickelt, die von einfachen Verfahren, wie Transposition und Substitution, bis hin zum Chiffrieren durch Computerprogramme reichen. Gleichzeitig haben Menschen auch immer wieder versucht, dem auf den ersten Blick unbrauchbaren Text sein Geheimnis zu entlocken und begannen sich mit Entschlüsselungstechniken zu beschäftigen. Der Wettlauf zwischen Nachrichtenschutz und „Knacken“ von Informationen war eröffnet. Österreich sollte am Beginn des 20. Jahrhunderts einen bedeutenden Platz auf dem Sektor der Kryptologie (Lehre von Geheimschriften) einnehmen, wobei sich zunächst der diplomatische Bereich gegenüber dem Militär überlegen zeigte – so war man, was die Verfahren zum Brechen von Chiffren betraf, das ständig betrieben wurde, auf dem aktuellen Wissensstand. In dem vorliegenden Artikel soll vor allem jener zwei Personen gedacht werden, die bereits in der Monarchie bzw. in der Ersten Republik – unter anderem im Innenministerium – tätig waren und sich durch diverse Publikationen internationale Anerkennung als Fachleute erwerben konnten. Das Ende des Ersten Weltkrieges im Jahre 1918 sollte schließlich einen Bruch im (militärischen) Chiffrewesen markieren, denn die bis dahin verwendeten umständlichen und unsicheren manuellen Verschlüsselungsverfahren wurden durch maschinelle Rotor-Verschlüsselungsmaschinen (wie z.B. der „Enigma“) ersetzt, die eine höhere kryptographische Sicherheit versprachen. In den ausgehenden 1920er bzw. 1930er Jahren konnte sich auch Österreich dem Trend zur maschinellen Verschlüsselung nicht verschließen und die später so berühmt gewordene Enigma sollte sowohl im Innen- als auch im Verteidigungsministerium Verwendung finden.

1. EINLEITUNG

„Die Sprache ist dem Menschen gegeben, um seine Gedanken zu verbergen.“ Dieses geflügelte Wort soll auf den französischen Bischof, Staatsmann und Außenminister Charles Maurice de Talleyrand zurückgehen und während einer Unterredung mit dem spanischen Gesandten Don Izquierdo im Jahre 1807 gefallen sein.[1] Gerade Politiker und Diplomaten, bei denen „die Lüge zum Beruf“ gehört (Weinrich 2013), bedienten sich verschlüsselter

Botschaften. Auf die Erkenntnis, dass „die Sprache Gedanken verberge“, wollten sie sich doch nicht verlassen. Nun soll uns hier die philosophische Betrachtung berufsspezifischer Verhaltensweisen im Umgang mit Informationen bzw. der Wahrheit nicht näher interessieren, sondern unsere Aufmerksamkeit wird vielmehr auf das Verbergen von Inhalten vor unberechtigten Dritten und die damit verbundene intellektuelle und technische Entwicklung gerichtet sein. Eine Berufsgruppe, deren Wunsch nach vertraulichen Datenübermittlungen und Datengeheimhaltung sehr stark ausgeprägt war bzw. ist, sind die Militärs. Diese waren es auch, die die Entwicklung der Datenübertragungssicherheit vorangetrieben haben bzw. noch immer vorantreiben, auch wenn Datensicherheit heute kein Privileg einer bestimmten Berufs- oder Personengruppe mehr ist (Bollak 2006, iii).

2. BEGRIFFSBESTIMMUNGEN

Zunächst sollen dem Leser noch einige grundlegende Begriffe aus dem Bereich der Kryptologie erklärt werden. Die Kryptographie beschäftigt sich mit der Entwicklung von Algorithmen zur Verschlüsselung von Informationen und die Kryptoanalyse mit der Entschlüsselung von Informationen ohne Zuhilfenahme/Kenntnis des Schlüssels. Ein Kryptosystem (auch als Chiffriersystem bezeichnet) ist jenes Verfahren, bei dem eine Eingabemenge (Klartext), gesteuert durch Parameter, in eine Ausgabemenge (Geheimtext) umgewandelt und umgekehrt der Geheimtext wieder in einen Klartext zurückgewandelt werden kann. Grundsätzlich kann man zwei Arten von Kryptosystemen unterscheiden, nämlich symmetrische und asymmetrische Systeme. Beim symmetrischen Verfahren wird mit demselben Schlüssel ver- und entschlüsselt, beim asymmetrischen dagegen kommen zwei unterschiedliche Schlüssel zur Anwendung.

Wie bereits vorhin erwähnt, gibt es zwei bzw. drei Grundprinzipien zum Verschlüsseln von Nachrichten. Die Transposition (auch Versetzung oder Verwürfelung genannt) und die monoalphabetische bzw. die polyalphabetische Substitution. Bei der Transposition werden die Klarzeichen nach fix vereinbarten Regeln umgeordnet (permutiert). Als monoalphabetische Substitution bezeichnet man ein System, bei dem jedes einzelne Klarzeichen durch ein Chiffratzeichen ersetzt wird. Die Chiffratzeichen werden, gesteuert durch den Schlüssel, einem Chiffratalphabet entnommen. Die Weiterentwicklung der eben beschriebenen Verschlüsselungsart ist die polyalphabetische Substitution. Bei diesem Verfahren wird jeweils ein Klartextzeichen durch ein neues ersetzt, wobei die polyalphabetische Substitution zusätzlich von der Position des Zeichens im Text abhängig ist. Wie bereits der Name andeutet, kommen bei diesem Verschlüsselungsverfahren mehrere Chiffratalphabete zum Einsatz.

Die Sicherheit eines Chiffrensystems kann nur durch den gezielten Versuch des Knackens überprüft werden, um mögliche Schwächen aufzudecken. Lange Zeit versuchte man die Sicherheit eines Chiffrensystems mittels Geheimhaltung des zu Grunde liegenden Systems zu erreichen, was sich als falsch herausstellen sollte. Die Sicherheit des Chiffrensystems sollte einzig und alleine in der Wahl des Schlüssels beruhen, mit dem man den Klartext in einen Geheimtext umwandeln möchte (Blasi 2013, 1).

3. DIE KRYPTOLOGIE IM ÜBERBLICK

Für alle Verschlüsselungsarten lässt sich die Methodik in folgendem Satz zusammenfassen: „Verändere die Information nach vereinbarten Regeln so, dass der Uneingeweihte, der a priori als Unbefugter (Opponent, Gegner) anzusehen ist und die

Regeln nicht oder nur teilweise kennt, die Information nicht gewinnen und nützen kann“ (Horak et al. 2003, 3). Die Kryptologie kann man in der Zeitrechnung bis weit vor Christus zurückverfolgen. 600 v.Chr. erfolgte in Palästina die Textverschlüsselung mittels der Atbas(c)h-Chiffre, die auf dem hebräischen Alphabet beruhte. Es handelte sich um ein monoalphabetisches Substitutionsverfahren, das nur eine geringe kryptographische Sicherheit bot. Ebenfalls eine sehr alte Verschlüsselungsmethode stellte die Skytale von Sparta dar. Um an die geheimen Daten zu gelangen, mussten der Sender und der Empfänger eine so genannte Skytale besitzen. Dies waren zwei Zylinder mit dem gleichen Radius. Nach dem Abrollen des Pergamentstreifens mit dem Text (das Beschreiben erfolgte am Zylinder) war dieser nicht mehr ohne weiteres lesbar. Um den Originaltext wieder lesbar zu machen, musste der Streifen um einen Zylinder mit dem gleichen Durchmesser gewickelt werden. Im römischen Reich war die Caesar-Chiffre zur Nachrichtenverschlüsselung gebräuchlich. Dieses war ein einfaches symmetrisches Verschlüsselungsverfahren, das auf der monographischen und monoalphabetischen Substitution basierte und keine große Sicherheit vor Entschlüsselung bot. Zwischen 500 und 1400 n.Chr. begann in Europa die „Dunkle Zeit der Kryptographie“. Sie wurde nämlich der Schwarzen Magie zugeordnet und dadurch ging viel Wissen darüber verloren. Im Gegensatz dazu blühte die Kryptographie im persischen Raum auf und im arabischen Raum erschienen mehrere Publikationen darüber. 1466 veröffentlichte Leon Battista Alberti, der „Vater der Kryptographie“, sein Buch „Modus scribendi in ziferas“, in dem erstmals die von ihm erfundenen Chiffrierscheiben Erwähnung fanden. Im 16. Jahrhundert erschien im deutschsprachigen Raum das erste gedruckte Buch über Kryptologie. 1586 wurde das Buch „Traicte de Chiffres“ des französischen Diplomaten Blaise de Vigenère veröffentlicht. Der von ihm entwickelte Code ist der bekannteste unter allen polyalphabetischen Algorithmen. 1795 entwickelte Thomas Jefferson den ersten Chiffrierzylinder mit der Bezeichnung „Wheel-Cypher“. Der Offizier Friedrich Kasiski entwickelte einen Test zur Bestimmung der Schlüsselwortlänge der Vigenère-Chiffre anhand statistischer Analysen der Abstände sich wiederholender Buchstabengruppen. Dieser Test gilt als Klassiker der Kryptoanalyse. 1881 brachte der Österreicher Eduard Fleissner von Wostrowitz ein Buch mit dem Titel „Handbuch der Kryptographie“ heraus. Zwei Jahre später erschien „La Cryptographie militaire“ von Auguste Kerckhoffs von Nieuwenhof, das als Meilenstein in der Kryptographie der Telegrafenzeit gilt (Bollak 2006, 12–15).

Bisher ging es darum, papierene Nachrichten zu verschlüsseln bzw. zu entschlüsseln. Etwa 1895 begann sich der italienische Ingenieur und Physiker Guglielmo Marchese Marconi mit der drahtlosen Übertragung von Radiowellen zu beschäftigen. Um 1900 gelang durch seine Erfindung die drahtlose Überbrückung des Ärmelkanals und jene des Nordatlantiks. Die Möglichkeit der drahtlosen Übermittlung von Nachrichten hatte neben vielen Vorteilen auch einen schwerwiegenden Nachteil: Sie waren abhörbar und bedurften eines besonderen Schutzes. Diesen Schutz konnte das Verschlüsseln bieten, was wiederum dem Chiffrewesen zu großer Bedeutung verhalf (Horak 2011, 2 f).

1917 wurde von den Amerikanern Edward S. Vernam und Joseph Mauborgne das „One-Time-Pad“ (OTP, auch Vernam-Chiffre genannt) erfunden. Es gilt als perfektes Kryptosystem. Bei einem solchen gibt es mindestens so viele Schlüssel wie

Klartexte und jeder Schlüssel darf nur einmal verwendet werden. Die Sicherheit des OTP basiert auf der wirklichen Zufälligkeit des Schlüssels. In jedem Algorithmus stellt sich nach einer bestimmten Periodenlänge eine Gesetzmäßigkeit ein. Aus diesem Grund griff man nicht auf mathematische Mittel zurück, sondern der Schlüssel wurde ausgewürfelt. Ein Kernproblem bestand darin, den Schlüssel zwischen den Kommunikationsteilnehmern sicher auszutauschen. Unter einem klassischen OTP verstand man eine sehr lange Folge eines absolut zufälligen Schlüssels, der zur einfacheren Handhabung in einem kleinen Buch abgedruckt war. Weitere Nachteile: Die Schlüssellänge musste genau der Textlänge entsprechen und jeder Schlüssel durfte nur einmal verwendet werden. Aus diesem Grund entwickelte man Rotor-Maschinen (und in späterer Folge Computerprogramme und spezielle Hardware), die eine „pseudo" Zufallsfolge automatisch generierten (pseudo deshalb, da eine Folge, die nach einem bestimmten Algorithmus generiert wird, keine komplett zufällige Folge mehr sein kann). 1923 erfolgte auf dem internationalen Postkongress die Vorstellung der vom deutschen Ingenieur Arthur Scherbius entwickelten und wohl berühmtesten Rotormaschine, der Enigma, die von ihm weltweit vermarktet wurde (Bollak 2006, 12–15).

4. DIE KRYPTOLOGEN ANDREAS FIGL UND SIEGFRIED TÜRKEL

Nach diesem Überblick sei an dieser Stelle an zwei Österreicher erinnert, die sich um die kryptologische Forschung verdient gemacht haben. Andreas Figl, der „Altmeister der österreichischen Enträtselungskunst und kryptographischen Wissenschaft", wurde 1873 in Wien geboren und absolvierte die Offiziersausbildung an den Infanterie-Kadettenschulen in Wien und Triest. 1893 wurde er zum Leutnant befördert. Als Hauptmann erlitt er im Dienst einen Unfall, der eine Sehbehinderung am rechten Auge nach sich zog. 1910 wurde Figl aus diesem Grunde in den Ruhestand versetzt, jedoch bereits eineinhalb Jahre später reaktiviert und in das Evidenzbüro des Generalstabes berufen, wo er seine Karriere als Dechiffrieroffizier und Chiffrierspezialist startete (Horak et al. 2003, 19). Im diplomatischen Bereich hatte man sich lange vor dem Militär in Österreich-Ungarn mit dem Brechen von Codes befasst. Durch den Einsatz der drahtlosen Kommunikation erfolgte auch im Generalstab, der sich bis dahin kaum mit Dechiffrieren auseinandergesetzt hatte, zu Beginn des 20. Jahrhunderts ein Umdenken. Allerdings zeigte die Diplomatie den Militärs die kalte Schulter, als es um die Unterstützung beim Aufbau von Dechiffrierkapazitäten ging. Der Leiter des militärischen Nachrichtendienstes, Oberst August Urbanski von Ostrymiecz, griff daraufhin zur Selbsthilfe. Er gründete eine eigene Chiffregruppe und holte Andreas Figl als künftigen Fachmann ins Evidenzbüro. Der Autodidakt Figl musste sich das kryptographische Wissen erst mühsam aneignen, wobei die vorhandenen veralteten Unterlagen wenig hilfreich waren. Aus dem Truppenoffizier wurde schließlich ein international anerkannter Chiffrierexperte, der bis zu seinem Lebensende von diesem Fachgebiet gefesselt blieb. Den Höhepunkt seines Schaffens erlebte er mit Sicherheit im Ersten Weltkrieg (Horak 2011, 3 f). Die von Figl entworfene und umgesetzte Chiffrierorganisation war äußerst erfolgreich – sowohl bei den eigenen Chiffriersystemen als auch beim Brechen gegnerischer Meldungen. Figl selbst war an der Italienfront erfolgreich im Einsatz und überall als hervorragender Spezialist respektiert und dennoch sollten gegen Kriegsende die ersten Neider auf den Plan treten (Horak 2011, 38).

Nach dem Kriegsende erlebte er die Auflösung des Evidenzbüros und den Übergang in die „Bewaffnete Macht“ des neuen Staates Österreich. Im Zuge der Reduzierung an Militärpersonen wurde Figl zusammen mit einigen Kameraden aus dem Chiffrebereich bei der Bundespolizeidirektion Wien eingeteilt (Horak 2011, 39). Mitte 1922 wurde Figl in das Außenministerium versetzt (BPD Wien/ Amtsbibliothek 1923). In der Bundespolizeidirektion aber kreuzten sich die Wege des Juristen und Rechtsanwaltes sowie wissenschaftlichen Leiters des Kriminalistischen Institutes und Vorstandes des Kriminalistischen Laboratoriums der Wiener Polizeidirektion, Siegfried Carl Türkel, mit jenen Figls. Der 1875 geborene Türkel beschränkte sich während seines Studiums nicht nur auf juristische Fächer, sondern beschäftigte sich auch mit Medizin (insbesonders der Psychiatrie), Psychologie, Physik und Chemie. Ihm wohnten wie Figl autodidaktische Züge inne und im Bestreben, sein umfassendes kriminologisches und kriminalistisches Wissen weiterzugeben, gründete Türkel 1922 mit Hilfe des Wiener Polizeipräsidenten Johannes Schober das Kriminalistische Laboratorium, das der Anwendung wissenschaftlicher Methoden bei der Erforschung krimineller Tatbestände dienen sollte. Im Herbst 1924 konnte Schober seinen seit 1919 gehegten Herzenswunsch erfüllen, nämlich das Kriminalistische Institut mit Türkels Unterstützung ins Leben zu rufen, das der kriminologischen Ausbildung juristisch gebildeter Wiener Polizeibeamten dienen sollte. Türkel führte das Institut zu größtem Ansehen im In- und Ausland (Öffentliche Sicherheit 1933, 4). Er war auch Mitbegründer der „Académie Internationale de Criminalistique“ im Jahre 1929 mit Sitz in Wien. Auch schriftstellerisch war Türkel tätig. Neben zahlreichen Aufsätzen über kriminologische Themen in der Tagespresse und in Fachzeitschriften hat er eine ganze Reihe wissenschaftlicher Werke als Statistiker, Kriminalpsychiater und Kriminaltechniker herausgegeben, u.a. auch im Rahmen der „Wissenschaftlichen Veröffentlichungen des Kriminalistischen Laboratoriums“ der Bundespolizeidirektion Wien (Öffentliche Sicherheit 1933, 4).

Möglicherweise entschloss sich Figl durch den Kontakt mit Türkel, der selbst einige Werke zur Kryptographie verfasste, schriftstellerisch tätig zu werden. Von 1919 bis 1922 verfasste Figl mehrere Fachschriften, von denen nur „Chiffre und Radio“ in Druckform erschien (Horak 2005, 224). 1924 wurden die „Die Kryptographischen Erinnerungen aus dem Weltkriege“ fertig gestellt. Sein Hauptwerk, „Systeme des Chiffrierens“, vermutlich bereits 1920 begonnen, erschien 1926 (Figl 1926) und sollte für einen handfesten Skandal sorgen (Horak 2011, xi f). Das aufwändige Buch mit 45 Beilagen und beweglichen „Schiebern“ erschien in der Reihe der „Wissenschaftlichen Veröffentlichungen des Kriminalistischen Laboratoriums“ von Siegfried Türkel, was sicherlich kein Zufall war. Figl arbeitete gleichzeitig schon am zweiten Buch, den „Systemen des Dechiffrierens“, das er im zweiten Kapitel des ersten Bandes bereits ankündigte (Horak 2005, 231). Nur, es sollte nie erscheinen. Die Herausgabe wurde durch jene Dienststelle verhindert, in der Figl tätig war (Chiffrengruppe des Bundeskanzleramtes, Auswärtige Angelegenheiten). Zunächst reagierte sein Vorgesetzter auf die Veröffentlichung des ersten Buches mit Entsetzen; ebenso das Bundesministerium für Heerwesen. Figl löste damit eine „Lawine bürokratischer Exzesse an Unwissenheit, Überheblichkeit und Wichtigmacherei“ aus (O-Ton Horak). Offenbar war das eine oder andere von ihm mit allen Vorzügen und Schwächen beschriebene Verfahren noch in behörd-

licher Verwendung. Statt nach neuen, sicheren Methoden zu suchen, dürfte man gehofft haben, die Schwachstellen der in Gebrauch stehenden Verfahren geheim halten zu können. Die Schwächen waren in der Fachwelt sicherlich bekannt und werden kaum erst durch Figls Buch offenkundig geworden sein (Horak 2005, 233). Der gemaßregelte Autor wurde jedenfalls mit einem faktischen Publikationsverbot über Kryptographie belegt („[…] mir auf Lebensdauer untersagt, Werke über Kryptographie ohne Erlaubnis unserer Regierung zu veröffentlichen"). 1927 wurde Figl noch einmal darüber belehrt, dass er „das Manuskript in keiner Weise, weder im Innoch im Auslande, auch nicht unter einem Pseudonym oder durch einen Strohmann" verwerten dürfe (Horak 2005, 250).

Was nun das „skandalträchtige" Buch betrifft, beschrieb Figl viele alte und sowohl bekannte als auch weniger bekannte Chiffrierverfahren mit ihren Vor- und Nachteilen sowie ihren Schwächen mit wissenschaftlicher Präzision. Im militärischen Bereich übte der Autor sehr wohl Selbstzensur und beschrieb nur solche Verfahren, die auf historischen Vorbildern aufbauten und aus diesem Grund als fragwürdig und unsicher gelten mussten (Horak 2005, 232).

Vielleicht haben die Arbeiten Figls auch Türkel inspiriert, neben seinen Fachgebieten auch über Kryptographie zu publizieren, oder stand hinter so mancher Passage, die Türkel verfasste, vielleicht Figl? Durchaus denkbar, denn so hätte sich für Ersteren die Möglichkeit geboten, das Publikationsverbot „zu umgehen". 1924 wurde von Türkel die 16-seitige Broschüre „Morsezeichen und Geheimschrift" als Sonderabdruck veröffentlicht (Türkel 1924). 1926 folgte die Publikation „Morse- und Morseähnliche Zeichen als Grundlage der Überchiffrierung" (Türkel 1926), die sich an den Kriminalisten wandte, damit er die weniger „für den diplomatischen, militärischen und kommerziellen Verkehr" geeigneten Methoden kennenlerne. Das Buch „Chiffrieren mit Geräten und Maschinen" erschien dann 1927 (Türkel 1927) und zwei Jahre später kam die Broschüre „Kryptographische Parerga (Vom Chiffrieren und Dechiffrieren)" (Türkel 1929) heraus. Bis auf die erste Broschüre wurden alle Publikationen in der Reihe der „Wissenschaftlichen Veröffentlichungen des Kriminalistischen Laboratoriums" verlegt. Von Schwierigkeiten, wie man sie Figl bereitet hat, ist bei Türkels kryptographischen Werken nichts bekannt. Seine Zielgruppe waren Kriminalisten und seine Ausführungen entsprangen der kryptographischen Kasuistik, wenn es auch zwangsläufig zu Überschneidungen mit Figls Darstellungen kommen musste (z.B. beschreiben beide die Enigma, Türkel allerdings viel ausführlicher als Figl). 1933 verstarb Türkel dann unerwartet (Öffentliche Sicherheit 1933, 4).

5. DES RÄTSELS LÖSUNG – DIE ENIGMA IN ÖSTERREICH

Nach dem Ersten Weltkrieg lösten maschinelle Verschlüsselungsverfahren die inzwischen veralteten, umständlichen und unsicheren manuellen Methoden ab. Die maschinellen Verfahren versprachen eine einfachere Handhabung und eine verbesserte kryptographische Sicherheit. Als der Erfinder der Enigma gilt der deutsche Ingenieur Arthur Scherbius, dessen erstes Patent von 1918 stammt. Er war allerdings nicht der Einzige, der die Idee des Rotor-Prinzips zur Verschlüsselung von Texten hatte. Neben ihm meldeten ein Amerikaner, ein Niederländer und ein Schwede ihre Ideen ebenfalls zum Patent an. 1923 wurde zur Fertigung der Enigma die Chiffriermaschinen Aktiengesellschaft in Berlin gegründet. Die Enigma war zunächst als ziviles Chiffriersystem konzipiert und

wurde auf Messen zum Kauf angeboten. Ende der 1920er Jahre zeigten militärische Stellen verstärkt Interesse an der Maschine, so dass sie bald darauf vom zivilen Markt verschwand. Da im Zuge der Aufrüstung der deutschen Wehrmacht durch das nationalsozialistische Regime auch ein zuverlässiges Verschlüsselungssystem benötigt wurde, begann die Erfolgsstory der Enigma, deren Produktionszahl auf etwa 100.000 Stück geschätzt wird. Als Scherbius sie 1918 zum Patent angemeldet hatte, konnte sie zu Recht als unknackbar bezeichnet werden. Die auf einer polyalphabetischen Verschlüsselungsbasis arbeitende Enigma war durch die damals üblichen manuellen, hauptsächlich linguistisch gestützten Entzifferungsmethoden unangreifbar und blieb das auch bis in die 1930er Jahre, also mehr als zehn Jahre lang. Spielfilme, die vor dem Hintergrund des U-Boot-Krieges spielen, sorgten dafür, dass der Ruhm der Enigma für die Nachwelt erhalten blieb.[2]

In der Ersten Republik entschlossen sich sowohl das österreichische Innenministerium als auch das Bundesministerium für Heerwesen, die Enigmas anzuschaffen. Leider haben sich die Akten über die Beschaffung im Innenministerium nicht erhalten. Das Interesse dieses Ressorts an einer solchen Maschine geht auf das Jahr 1934 zurück (ÖStA/AdR, BKA-Inneres, Zl. 222154/GD1/34, Enigma, Chiffriermaschinen). 1935 erfolgte offenbar die Verteilung der Enigmas[3] und damit enden auch schon die Informationen, die man den Indices entnehmen kann. Interessant ist noch, dass der Entwurf einer „Funkordnung für den österreichischen Polizeifunk", der etwa um 1930 verfasst wurde, die Durchführung des Chiffredienstes mit einer „E-Maschine" (offenbar ist die Enigma gemeint) vorsah. In der endgültigen Fassung wurde dieser Absatz dann jedoch gestrichen. Das könnte darauf hindeuten, dass der Ankauf von Enigmas zu einem früheren Zeitpunkt (siehe dazu Bundesministerium für Heerwesen) geplant war, als er dann tatsächlich erfolgte (ÖStA/AdR, BKA-Inneres, Funkwesen, Entwurf einer Funkordnung für den österreichischen Polizeidienst).

Die Akten des Bundesministeriums für Heerwesen über die Enigma haben sich dagegen erhalten. Daraus ist zu entnehmen, dass das Bundesheer bereits im März 1928 mit der Erprobung dieser Maschine (sie wurde als „26teilige Glühlampen-Chiffriermaschine" bezeichnet) begann. Zwei Stück davon wurden an die Funkhorchzentrale geliefert, die u.a. meldete, „dass in annehmbarer Zeit ein unbefugtes Dechiffrieren fast unmöglich ist". Der Erprobungsbericht vermerkt auch, dass der Aufbau der Maschine mit diesen Walzen derart ist, „dass wohl nach Ausspruch von Fachmännern ein Dechiffrieren nach langen Versuchen möglich erscheint, jedoch nicht sehr wahrscheinlich ist. Es bietet ja der häufige Wechsel des Schlüsselwortes auch genügend Gewähr, um das Dechiffrieren fast unmöglich zu machen" (ÖStA/AdR, BMfHW, GschZl. 36275-6/28, Bestellung von Chiffriermaschinen Enigma). Zur Beurteilung der Enigma wurde neben einem namentlich nicht genannten Bundesbeamten der Chiffreabteilung auch der in Ungnade gefallene Figl herangezogen. Beide beschäftigten „sich längere Zeit mit der Maschine" und ihr Urteil wurde als maßgebend angesehen. Figl und sein Kollege kamen zur Überzeugung, dass diese Chiffriermaschine „nach dem heutigen Stande sehr gut und speziell für militärische Zwecke besonders geeignet" wäre. Allerdings wiesen sie darauf hin, dass es in einigen Jahren gelingen könnte, eine Maschine zu konstruieren, die ein Dechiffrieren von durch die Enigma erstellten Chiffrentexte in annehmbarer Zeit durchführen könnte. Die Stärke der Enigma wurde von allen

Fachleuten in der Geheimhaltung der Walzenschaltung sowie in der Verfügbarkeit von Reservewalzen zwecks Auswechslung des Chiffrenmechanismus gesehen (ÖStA/AdR, BMfHW, GschZl. 19929-6/28). Im Juli 1928 erfolgte die Bestellung von zehn Enigmas (Modell A 27) zum damaligen Preis von 1.044,- Schilling (ÖStA/AdR, BMfHW, GschZl. 36275-6/28, Bestellung von Chiffriermaschinen „Enigma"). Für die Übernahme war die Telegraphenzeugsanstalt zuständig, was am 11. September 1928 geschah. Empfänger der Chiffriermaschinen (mit den Herstellungsnummern A 805 bis A 814) waren die Telegraphenfachschule (besorgte den Chiffreverkehr für das Heeresministerium), die Brigade-Telegraphenkompanien und die Heeresverwaltungsstelle Klagenfurt (ÖStA/AdR, BMfHW, GschZl. 44.404-6/28, Enigma Chiffriermaschinen – Ausgabe).

Man braucht kein Prophet zu sein, um vorherzusagen, dass es dann tatsächlich gelang, die Enigma zu knacken. Der maschinellen Verschlüsselung konnte durch eine maschinelle Entzifferung sehr wohl begegnet werden. Die Geschichte der Entzifferung der Enigma begann 1932, als ein für die Franzosen spionierender Deutscher Unterlagen wie Schlüsseltafeln, Gebrauchs- und Schlüsselanleitung verriet. Der in der polnischen Dechiffrierstelle arbeitende Mathematiker Marian Rejewski sollte der Erste sein, dem ein Einbruch in die Enigma mit Hilfe einer legal gekauften kommerziellen Maschine (Modell D) gelang, während Briten und Franzosen diese Maschine weiterhin für nicht knackbar hielten. Rejewski gab nicht auf und arbeitete mit zwei Kollegen weiter an der Entschlüsselung der Enigma. 1938 konnten die Deutschen mit Hilfe einer Änderung der Verfahrenstechnik und der Einführung weiterer Walzen die Enigma wieder sicher machen. Mit dem Wissen der polnischen Codebrecher ausgestattet, starteten bei Ausbruch des Zweiten Weltkrieges britische Kryptoanalytiker in Bletchley Park einen erneuten Angriff auf die Enigma. Mit Hilfe einer speziellen elektromechanischen Maschine (Turing-Bombe) und einem hohen Personaleinsatz von bis zu 14.000 Frauen und Männern gelang es, die mehr als 200 Trilliarden Verschlüsselungsmöglichkeiten drastisch zu reduzieren. So konnten die Alliierten ab 1940 die von der deutschen Luftwaffe und dem Heer verschlüsselten Nachrichten mitlesen. Zäher sollte sich die Entschlüsselung der Enigma der U-Boote der deutschen Kriegsmarine erweisen, weil diese eine wesentlich stärkere Verschlüsselung durch die Geheimhaltung der Anzahl der im Walzensatz verwendeten Walzen hatte. Dies gelang erst mit der Erbeutung von Marine-Enigmas einschließlich der Arbeitsunterlagen aus versenkten deutschen U-Booten. Danach sollten die U-Boote der deutschen Kriegsmarine nie mehr sicher sein.[4]

6. DIE MODERNE KRYPTOGRAPHIE – VON DER GEHEIMNISKRÄMEREI ZUR MATHEMATISCHEN WISSENSCHAFT

Die Blütezeit der Rotor- und Verschlüsselungsmaschinen war zwischen 1920 und 1970; aus der Zeit des Kalten Krieges seien hier für die NATO die „KL-7" (1952 unter anderem auch von der National Security Agency [NSA] in Dienst gestellt) und für den Warschauer Pakt die „Fialka" als bedeutende Vertreter genannt. Mit der Entwicklung von elektromechanischen Maschinen (siehe Turing-Bombe) konnten jedoch die Berechnungen vielfach automatisiert und daher wesentlich beschleunigt werden. Diese Vorläufer der Computer wiesen für Kryptographie und Kryptoanalyse einen neuen Weg in Richtung Mathematik. Den Durchbruch schaffte Claude E. Shannon im Jahre 1949 mit seiner bahnbrechenden Arbeit „The Commu-

nication Theory of Secrecy Systems“ über Informationstheorie und legte damit den mathematischen Grundstein für die moderne Kryptographie. Zusammen mit dem Kerckhoffs'schen Prinzip[5] gehörte damit der Begriff einer „Geheimwissenschaft“ endgültig der Vergangenheit an und mit dem Aufkommen von Computern ab 1970 wurde es gängige Praxis, Kryptoverfahren zur offenen wissenschaftlichen Diskussion zu stellen[6].

Die moderne Kryptographie hat vier Hauptziele zum Schutz von Information:

1. Vertraulichkeit: unberechtigte Personen dürfen nichts über den Inhalt der Daten erfahren,
2. Integrität: die Daten müssen nachweislich vollständig und unverändert sein,
3. Authentizität: die Herkunft bzw. Urheberschaft der Daten muss nachweisbar sein,
4. Verbindlichkeit: die Urheberschaft darf nicht abstreitbar sein; ein Sender darf nicht im Nachhinein leugnen können, der Verfasser einer Nachricht zu sein.

Der erste Punkt wird grundsätzlich durch Verschlüsselung erreicht. Für die anderen Punkte eignen sich digitale Signaturen zusammen mit Hashwerten (etwa mittels Streufunktion). In der Kryptologie, vor allem bei der Entwicklung von Kryptosystemen, haben folgende Maximen große Bedeutung erlangt:

1. Unterschätze nie deinen Gegner (kann im wahrsten Sinne des Wortes den Kopf kosten).
2. Nur der Kryptoanalytiker, wenn überhaupt jemand, kann die kryptoanalytische Sicherheit eines Chiffrierverfahrens beurteilen (der Laie wiegt sich durch kompliziert wirkende Mechanismen eines Kryptosystems in Sicherheit).
3. Gehe davon aus, dass der Gegner das verwendete System kennt (der Gegner kann sich immer auf verschiedenste Weise Kenntnis von einem System verschaffen und kompromittierte Schlüssel lassen sich wesentlich einfacher austauschen als kompromittierte Systeme).

Mit der Anerkennung des Kerckhoffs' schen Prinzips wurde versucht, die Darstellung von kryptologischen Verfahren zu vereinheitlichen. Dafür erwies sich die Sprache der Mathematik als besonders geeignet. Je besser die Verschlüsselungssysteme mathematisch modelliert werden konnten, desto aussagekräftigere Resultate konnten gewonnen werden.

Ein Chiffriersystem heißt theoretisch oder absolut sicher, wenn gilt: Aus einem Chiffrat soll ohne Kenntnis des Schlüssels keinerlei zusätzliche Information über den Klartext gewonnen werden können. Ein Angreifer soll nach Abfangen eines Chiffrats nicht mehr über den Klartext herausfinden können, als er ohnehin schon weiß – etwa, dass es sich um eine Nachricht in deutscher Sprache handelt. Eine zwingende Voraussetzung für absolut sichere Chiffriersysteme ist, dass es mindestens ebenso viele mögliche Schlüssel wie Klartexte gibt. Mit anderen Worten, der Schlüssel muss mindestens so lang sein wie der Klartext. Als absolut sicheres Kryptosystem gilt das bereits erwähnte „One-Time-Pad“ (auch computertauglich), das nach besagtem Prinzip arbeitet, allerdings wenig praxistauglich ist. In den meisten Fällen ist es nicht möglich, eine derart große Menge an Schlüsselmaterial zu erzeugen und zu verwalten. Die Verschlüsselung einer Festplatte z.B. würde eine zweite Festplatte gleicher Größe nur mit Schlüsselmaterial benötigen. Muss nur wenig Klartext verschlüsselt werden und ist höchste Sicherheit notwendig (wie etwa in hochrangigen Diplomatenkreisen), dann ist das OTP nach wie vor die erste Wahl.

Aber ist absolute Sicherheit tatsächlich

immer notwendig? Sollte man nicht gewisse Abstriche zu Gunsten einer einfacheren Schlüsselverwaltung in Kauf nehmen? Und ein Kryptosystem gilt praktisch als sicher, wenn es nicht gelingt, innerhalb eines vernünftigen Zeitraums ohne Kenntnis des Schlüssels den Klartext zu ermitteln.[7]

7. CHIFFRIERVERFAHREN

Die Arbeitsweise des OTP bildet die Grundlage für die Stromchiffrierverfahren (stream ciphers). Es wird zeichenweise der Klartext mit der Schlüsselfolge zum Chiffrat verknüpft. Das Herzstück dieses Verfahrens ist ein Pseudozufallsgenerator. Im Gegensatz zu Stromchiffrierverfahren wird bei Blockchiffrierverfahren der Klartext in Blöcke gleicher Länge zerlegt, die nacheinander verschlüsselt werden. Diese Verschlüsselung ist unabhängig von der Position des jeweiligen Blocks. Gleiche Klartextblöcke erzeugen immer gleiche Chiffratblöcke. Für die Sicherheit ist daher eine Mindestblocklänge erforderlich. Das bekannteste Blockchiffrierverfahren ist der 1977 publizierte „Data Encryption Standard" (DES). Der DES wurde offiziell nie gebrochen, jedoch ermöglicht die kurze Schlüssellänge immer wieder Anlass für Spekulationen in Richtung von „Brute Force"-Attacken, also Testen aller möglichen Schlüssel. Mittlerweile sind die handelsüblichen Computer bereits derart leistungsfähig, dass DES nicht mehr als sicher gilt. Im Oktober 2000 wurde in den USA der Blockchiffrieralgorithmus Rijndael als neuer „Advanced Encryption Standard" (AES) auserkoren und damit DES als Standard abgelöst.[8]

1978 wurde das so genannte RSA-Verfahren, benannt nach seinen Entwicklern Ron Rivest, Adi Shamir und Leonard Adleman, veröffentlicht. RSA ist das erste praktisch einsetzbare, bekannteste und zugleich am einfachsten zu verstehende und implementierende, asymmetrische Public-Key-Kryptosystem. Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum Entschlüsseln von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt. Der private Schlüssel wird geheim gehalten und kann nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel errechnet werden.[9]

Das von Whitfield Diffie und Martin Hellman entwickelte Schlüsselaustauschverfahren (DH-Verfahren) dient dazu, einen gemeinsamen geheimen Schlüssel (meist für einmalige Verwendung) für „Alice" und „Bob" zu erzeugen (so werden in der englischsprachigen Kryptographie A und B bezeichnet). Anders als beim RSA beruht die Sicherheit des DH-Verfahrens auf der Schwierigkeit der Berechnung von diskreten Logarithmen (diskret kann hier als ganzzahlig verstanden werden).[10]

Hybride Chiffrierverfahren sind eine Kombination aus einem symmetrischen und einem asymmetrischen Verfahren, bei denen die Vorteile beider Systeme genutzt werden. Eines der bekanntesten Beispiele ist „Pretty Good Privacy" (PGP), das 1991 von Philip R. Zimmermann entwickelt und unentgeltlich für die Öffentlichkeit freigegeben wurde. Unter Kryptographie mit Elliptischen Kurven („Elliptic Curve Cryptography", ECC) versteht man asymmetrische Kryptosysteme, die Rechenoperationen verwenden, welche auf elliptischen Kurven definiert sind. Das Prinzip wurde 1985 von Neal Koblitz und Victor S. Miller vorgeschlagen. Die diesem Verfahren zu Grunde liegende Mathematik ist sehr komplex. Digitale Signaturen eignen sich wiederum, um die Urheberschaft einer Nachricht nachweisen zu können.

8. ZUKUNFTSVISIONEN

Unter Quantenkryptographie versteht man die Anwendung von quantenphysikalischen Effekten in der Kryptographie.

Herkömmliche Operationen wie Computerberechnungen oder Übertragungen von Bits sollen durch quantenmechanische Abläufe ersetzt werden. Die Quantenkryptographie gliedert sich in die beiden Bereiche Quantenübertragung und Quantencomputer. Bei der Quantenübertragung soll Information abhörsicher versendet werden. Die Übersendung geschieht mittels Lichtteilchen oder Photonen. Die Abhörsicherheit wird in der Theorie durch die Quantenmechanikgesetze garantiert, die besagen, dass ein Photon nicht abgehört, d.h. gemessen werden kann, ohne zerstört zu werden (Heisenberg'sche Unschärferelation[11]). Quantenübertragung funktioniert in der Theorie, jedoch nicht immer in der Praxis. Die dafür zu verwendenden Geräte können sich nämlich in der Praxis anders verhalten als in der Theorie. Im April 2004 wurde übrigens weltweit erstmals ein mit Quantenkryptographie verschlüsselter Scheck vom Wiener Rathaus in eine Bankfiliale übertragen.

Ein Quantencomputer (Stichwort „Zukunftsvision") kann im Gegensatz zu einem herkömmlichen Computer gewisse Probleme der Informatik und Mathematik wesentlich schneller lösen, was viele derzeitige Kryptosysteme mit einem Schlag unsicher machen würde. In der Praxis jedoch stecken die Entwicklungen noch in den Kinderschuhen und es ist nicht abzusehen, wann und ob es jemals einen brauchbaren Quantencomputer geben wird.[12]

Quantentechnologie hin oder her, im Augenblick beschäftigt eine breite Weltöffentlichkeit ohnehin eine ganz andere Sorge, nämlich in welchem Maße die NSA das gesamte Internet kontrolliert und es in eine gigantische Überwachungsplattform verwandelt wird und wie überdies jene amerikanische Behörde sogar gezielt Verschlüsselungen unterwandert, indem sie Geheimabkommen mit den Herstellern von Kryptographie-Software schließt. Wem kann man da noch trauen? (Talbot 2013, 58) Auch wenn die USA Besserung geloben, wird sich eine solche Informationsbeschaffung bzw. Ausspähung immer in irgendeiner Form wiederholen – sind doch die Staaten selbst die Auftraggeber dieser Form des Verbrechens.[13]

[1] *Man schreibt diese Aussage übrigens auch dem französischen Polizeiminister Fouché oder dem österreichischen Staatskanzler Metternich zu.*

[2] *http://www.wikipedia.org/wiki/Enigma_(Maschine), 1 F, 10 und 35.*

[3] *Freundliche Mitteilung von Heinz Placz vom ÖStA/AdR.*

[4] *http://de.wikipedia.org/wiki/Enigma_(Maschine), 10, 17–20.*

[5] *Die Sicherheit eines Kryptoverfahrens soll allein auf der Geheimhaltung des Schlüssels beruhen.*

[6] *http://de.wikipedia.org/wiki/Kryptographie.*

[7] *http://de.wikipedia.org/wiki/Kryptographie; http://de.wikipedia.org/wiki/One-Time-Pad.*

[8] *http://de.wikipedia.org/wiki/Stromverschlüsselung; http://de.wikipedia.org/wiki/Kryptographie.*

[9] *http://de.wikipedia.org/wiki/RSA-Kryptosystem.*

[10] *http://de.wikipedia.org/wiki/Kryptographie.*

[11] *Die Heisenbergsche Unschärferelation oder Unbestimmtheitsrelation (1927 von Werner Heisenberg formuliert) ist die Aussage der Quantenphysik, dass zwei komplementäre Eigenschaften eines Teilchens nicht gleichzeitig beliebig genau bestimmbar sind. Das bekannteste Beispiel für ein Paar solcher Eigenschaften sind Ort und Impuls.*

[12] *http://de.wikipedia.org/wiki/Quantenkyptographie; http://de.wikipedia.org/Quantencomputer.*

[13] *Diese Feststellung hat übrigens bereits vor 100 Jahren der „rasende Reporter"*

Egon Erwin Kisch anlässlich der aufsehenerregenden Redl-Affäre getroffen.

Quellenangaben

BPD Wien/Amtsbibliothek (1923). Nachlass Johann Schober, Karton 38/1 1923.
Österreichisches Staatsarchiv/Archiv der Republik (ÖStA/AdR), Bestand des Bundesministeriums für Heerwesen (BMfHW).
Österreichisches Staatsarchiv/Archiv der Republik (ÖStA/AdR), Bestand des Bundeskanzleramtes-Inneres (BKA-Inneres).
Blasi, Walter (2013). Chiffrierapparate des Kriegsarchivs. Manuskript für die virtuelle Erste Weltkrieg-Ausstellung des Österreichischen Staatsarchivs, Wien.
Bollak, Michael (2006). Historische Methoden der Kryptoanalyse. Diplomarbeit am Fachhochschul-Studienlehrgang Informationstechnologie und Telekommunikation, Wien.
Figl, Andreas (1926). Systeme des Chiffrierens, Graz.
Horak, Otto J. (2011). Oberst a.D. Andreas Figl und der k.u.k. Radiohorch- und Dechiffrierdienst. Die „Kryptographischen Erinnerungen", Graz.
Horak, Otto J. (2005). Andreas Figl – Leben und Werk 1873–1967, Linz.
Horak, Otto J. (2003). E. B. Fleissner und A. Figl. Zwei österreichische Pioniere der Kryptographie, ungedrucktes Manuskript.
Öffentliche Sicherheit (1933). Polizei-Rundschau der österreichischen Bundes- und Gemeindepolizei sowie Gendarmerie (5).
Talbot, D. (2013). USA „Die NSA-Spionage macht uns weniger sicher". Interview mit dem IT-Sicherheitsexperten Bruce Schneier, Technology Review, November 2013, 58–59.
Türkel, Siegfried (1924). Morsezeichen und Geheimschrift, Wien.
Türkel, Siegfried (1926). Morse- und Morseähnliche Zeichen als Grundlage der Überchiffrierung, Graz.
Türkel, Siegfried (1927). Chiffrieren mit Geräten und Maschinen. Eine Einführung in die Kryptographie, Graz.
Türkel, Siegfried (1929). Kryptographische Parerga (Vom Chiffrieren und Dechiffrieren). Kasuistisches aus der kriminalistischen Praxis, Graz.
Weinrich, Harald (2013). Wort, Text und Begriff, Online: http://www.gleichsatz.de.

Weiterführende Literatur und Links

Bauer, Friedrich L. (1997). Entzifferte Geheimnisse, Berlin.
Beker, Henry/Piper, Fred (1982). Cipher Systems, London.
Beutelspacher, Albrecht (1991). Kryptologie, Braunschweig.
Daemen, Joan/Rijmen, Vincent (2002). The Design of Rijndael, Heidelberg.
Fumy, Walter/Rieß, Hans P. (1988). Kryptographie, München.
Schneier, Bruce (1996). Applied Cryptography, New York.
Schneier, Bruce (1997). Angewandte Kryptographie, Bonn.
http://www.nord-com.net/h-g.mekelburg/kryp
http://de.wikipedia.org/wiki/Security_through_obscurity
http://de.wikipedia.org/wiki/Quantenschlüsselaustausch
http://sciencev1.orf.at/science/news/112098
http://sciencev1.orf.at/science/news/150499.html
http://de.wikipedia.org/wiki/SHA-3