

Drei Anekdoten der historischen Kryptographie

# IDEENKLAU UND DEUTSCHES LIEDGUT

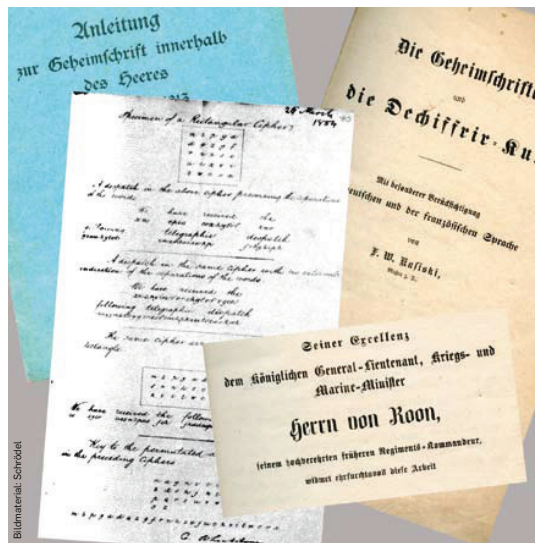
Die Geschichte der Kryptographie ist eine Geschichte voller Missverständnisse. Dem einen gelingt ein Durchbruch nach Jahrhunderten, keiner merkt es und dann war doch schon einer schneller. Ein anderer erfindet eine fast virtuos anmutende Ver-

schlüsselung, zeigt sie einem Freund und prompt wird sie nach diesem benannt. Und wieder andere zeigen, dass sogar Minister lernfähig sind, wenn auch auf Raten und ohne Erfolg. Drei Anekdoten zur Verschlüsselung von Tobias Schrödel.

## VIGENÈRE UND KASISKI

Als um 1540 Blaise de Vigenère nach Vorarbeit von Porta die nach ihm benannte Verschlüsselungsmethode beschrieb, dachte er an eine sichere Geheimschrift, die bis in alle Ewigkeit halten würde. Freilich ist eine Ewigkeit im ebenfalls ewigen Wettstreit der Kryptographen mit den Kryptoanalytikern ein hohes Ziel. Nichtsdestotrotz sollte die Vigenère-Verschlüsselung so lange als sicher gelten, wie keine andere zuvor und bis heute auch keine danach. Erst 1864 nämlich, also mehr als 300 Jahre später, entdeckte der deutsche Major a.D. Friedrich Wilhelm Kasiski eine Schwäche darin und beschrieb diese in einem Büchlein, von dem er im Eigenverlag ein paar Dutzend drucken ließ. Im Vorwort grüßt er freundlich den Kriegsminister und ließ diesem sein famoses Werk auch gleich per Post zustellen. Das würde Orden hageln am Ende seiner Laufbahn, dessen war sich Kasiski sicher. Die Vigenère-Verschlüsselung war beim ausländischen Militär, gerade bei den Franzosen, noch immer im Einsatz, abgefangene Depeschen unlesbar und Kasiskis Entdeckung ein vielleicht entscheidender Vorteil, falls es Krieg gäbe. Kriegsminister von Roon erkannte die Tragweite

von Kasiskis Entdeckung jedoch nicht. Es ist nicht einmal belegt, dass er das Buch überhaupt gelesen hat. Friedrich Kasiski konnte sich über eine derartige Kurzsichtigkeit des Ministers, noch dazu ein Preuße wie er selbst, nur maßlos ärgern, ließ fortan das Deciffrieren sein und widmete sich den Rest seines Lebens der Archäologie. Zum Glück erfuhr er niemals, dass man im Nachlass des umtriebigen britischen Erfinders Charles Babbage Aufzeichnungen fand, die belegen, dass dieser bereits zehn Jahre vor Kasiski die gleiche Schwachstelle gefunden, aber aus Faulheit nie veröffentlicht hatte. Kasiski hätte sich an einer seiner Ausgrabungsstätten wohl gleich selbst mit eingegraben. Zwar existiert die gefundene Schwachstelle nur bei langen Texten, in Universitäten wird dem Major a.D. trotzdem gehuldigt, wenn vom Kasiski-Test die Rede ist. Die letzte Bastion von Vigenère fiel erst nach rund 450 Jahren im März 2008. Seitdem können auch kurze Chiffren gebrochen werden. Details zur Vigenère Verschlüsselung und den Methoden sie zu knacken stehen im Internet, siehe Linkslage. Tobias Schrödel



Dienstanweisung „Anleitung zur Geheimschrift innerhalb des Heeres“ in der Ausgabe von 1913 (links oben). Darüber eine Kopie der handschriftlichen Beschreibung der als „Playfair-Chiffre“ bezeichneten Verschlüsselung, datiert auf März 1854 und von ihrem Erfinder Charles Wheatstone unterzeichnet. Rechts das Titelblatt von Friedrich Wilhelm Kasiskis Buch über das Entziffern einer Vigenère-Verschlüsselung mit darüber gelegter Widmung der Folgeseite an den damaligen Kriegsminister.

## DEUTSCHES LIEDGUT

Das Kriegsministerium des deutschen Staatenbundes brachte 1898 eine aktualisierte Version seiner Dienstanweisung zur „Geheimschrift innerhalb des Heeres“ heraus. Die vorgestellte Verschlüsselung ähnelt dem sog. Doppelwürfel (s. Info). Diesen beschreibt Otto Leiberich, der erste Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI), noch 1999 in „Spektrum der Wissenschaft“ als unlösbar. Jedoch nur dann, so führt er aus, wenn sie richtig angewendet wird, was auch an der Wahl eines sicheren Schlüsselwortes liegt.

Rund 100 Jahre früher war das dem Kriegsministerium offenbar noch nicht so klar, denn man schrieb den Soldaten in die Anweisung: „Zum Schlüsseltext empfiehlt sich ein leicht zu behaltender Spruch oder Liedvers“. Ein Vorschlag, der heute noch jedem PC Benutzer die Haare zu Berge stehen lässt, weiß man doch, dass Hacker schon länger mögliche Schlüsselwörter ausprobieren. Und was lag damals näher, als das Liedgut der feindlichen Kameraden? Es ist daher auch gar nicht verwunderlich, dass man im nahen Ausland deutsche Funk-

sprüche und Depeschen las. Nur in Berlin wunderte man sich immer wieder über die guten Informationen, die die Nachbarstaaten über die deutschen Truppenbewegungen hatten. Eine Idee, woran das liegen könnte, hatte man wohl, aber so richtig sicher, war man sich nicht. Beweis dafür ist die Neuaufgabe der Dienst-anweisung von 1908: „Der Anfang eines Liedes ist zu vermeiden“ steht dort. 1911, es wurde nicht besser, entschied man sich, die Soldaten gar nicht erst auf die Idee mit dem Liedvers zu bringen und empfahl schlicht „einige leicht zu behaltende Worte“. Die Ausgabe von 1913 bleibt dabei. Erst vier Jahre später kam man darauf, dass Soldaten immer noch gerne singen und allen voran die französischen Kryptoanalytiker deutsche Schellackplatten auf ihren Grammophonen rotieren ließen. Sie wollten nicht mitsingen, nur den Liedtext verstehen. Nun wurde die Anweisung erneut geändert, der Zusatz lautet kurz und knapp: „Der Anfang eines Liedes ist verboten“. Général Cartier, der für die französischen Truppen den gesamten ersten Weltkrieg hindurch deutsche Verschlüsselungen knackte, berichtete später, dass es ihm half, dass sehr oft der Anfang eines Gedichtes als Schlüsselwort verwendet wurde. Nun sind Gedichte ja keine Lieder, es fehlt schließlich die Melodie. Etwas anderes hätte ich im Land der Dichter und Denker auch nicht erwartet. Vorschrift ist Vorschrift. Ausschnitte aus dem Buch, insbesondere die angesprochene Dienstanweisung im Internet: s. Linkslage. Tobias Schrödel

## DER AUTOR

Tobias Schrödel ist freiberuflicher Berater für IT Security & Awareness und arbeitet bei T-Systems als Consultant im Bereich ICT PreSales. Tipps zu historischen und aktuellen Büchern und Software zu Verschlüsselungsmethoden: s. Linkslage.

## DER DOPPELWÜRFEL

Angeblich setzen Spione beim Verschlüsseln von Texten selbst heute noch den so genannten Doppelwürfel ein, wenn sie nur Stift und Papier zur Verfügung haben oder der Einsatz einer Verschlüsselungsmaschine oder -software zu auffällig ist. Das Verfahren war Anfang des 20. Jahrhunderts auch als Nihilistenwürfel bekannt. Notwendig ist die Kenntnis eines Schlüsselwortes, unter das man den zu verschleiern Text schreibt. (a) Nehmen wir als Schlüssel RUBBITS und als Text eine Zeile aus einem Lied, welche wir unter das Lösungswort schreiben. (b) Nun sortiert man das Schlüsselwort alphabetisch und vertauscht so die Spalten. (c) Nun liest man den Text Spaltenweise aus. Mit einem neuen Schlüsselwort werden diese Schritte wiederholt, so dass aus dem einfachen Würfel, der Doppelwürfel wird. Dieser ist – angeblich – unlösbar, wenn der Würfel nicht voll gefüllt ist, also die Textlänge kein Vielfaches der Länge des Schlüsselwortes ist. Auch sollte das Schlüsselwort nicht zu erraten sein.

R	U	B	B	I	T	S
t	i	e	f	i	m	w
e	s	t	e	n	w	o
d	i	e	s	o	n	n
e	v	e	r	s	t	a
u	b	t				

B	B	I	R	S	T	U
e	f	i	t	w	m	i
t	e	n	e	o	w	s
e	s	o	d	n	n	i
e	r	s	e	a	t	v
t		u				b

eteefresnostedeuwonamwntvisb

## IDEENKLAU VON LORD PLAYFAIR

Charles Wheatstone nutzte für geschäftliche und private Korrespondenz, ebenso wie viele andere um 1850, eine einfache, weil schnelle Substitutionsmethode. Teilten die Beteiligten nicht nur geschäftliche Kontakte oder das Bett miteinander, sondern auch ein Schlüsselwort, so konnten sie damit das Alphabet sehr einfach, aber effektiv durchmischen und geheim kommunizieren. Wheatstone tauschte die Buchstaben jedoch nicht nur fest verdrahtet aus, er ordnete das gemischte Alphabet in einem 5x5 Quadrat in Spalten und Zeilen an (glücklicherweise wurde das J erst später erfunden). Aus jeweils zwei aufeinander folgenden Buch-

staben des Klartextes bildete er innerhalb dieses Quadrats die gegenüberliegenden Ecken eines gedachten Rechtecks. Die Buchstaben an den freien Ecken ergaben das verschlüsselte Buchstabenpärchen. Durch eine Häufigkeitsanalyse war dem geheimen Text nun nicht mehr zu Leibe zu rücken. Er zeigte diese geniale Idee seinem Freund Baron Lyon Playfair. Dieser genoss seine Abende in weit feinerer Gesellschaft als Wheatstone und die Hoffnung war, dass er ihm half, den Ruhm und die Ehre des britischen Empires zu erlangen. Bei einem Dinner mit Prince Albert, dem Mann von Königin Victoria, konnte Playfair auch tat-

sächlich davon berichten. Der König war derart angetan von der Sicherheit dieser einfachen Methode, dass er sogleich seinen geheimen Kabinetten auftrag, die neue „Playfair-Chiffre“ zu verwenden. Sie wird heute noch gerne unter dieser Bezeichnung in Büchern oder Vorlesungen über historische Kryptografie beschrieben. Ganz gleich, ob Lord Playfair die Namensgebung des Königs unterstützte oder sich einfach nicht traute zu widersprechen: An so etwas gehen Männerfreundschaften zu Grunde. Details zur Playfair Chiffre stehen im Internet, siehe Linkslage. Tobias Schrödel

## IMPRESSUM

Herausgeber: Pressestelle der Ruhr-Universität Bochum; Leiter: Dr. Josef König (v.i.S.d.P.); Redaktion: Meike Drießen, md; Koordination: Meike Drießen, Rainer Wojcieszynski, RZ; Redaktionsanschrift: Pressestelle der RUB, LV 3/266, 44780 Bochum, Tel.: 0234/32-26952, -22830, Fax: 0234/32-14136, Internet: http://www.ruhr-uni-bochum.de/pressestelle; Layout und Satz: bsp\_design, Babette Sponehauer, Bochum; Anzeigenverwaltung und -herstellung: vmm Wirtschaftsverlag, Maximilianstraße 9, 86150 Augsburg, Tel.: 0821/4405-0; Anzeigenschluss für Ausgabe 26 (November 2010) ist der 11.10.2010; Mediadaten: http://www.ruhr-uni-bochum.de/rubens/mediadat.htm RUBbits erscheint zweimal pro Jahr als Service-Beilage zu RUBENS, Zeitschrift der Ruhr-Universität Bochum (http://www.ruhr-uni-bochum.de/RUBbits). Namentlich gekennzeichnete Beiträge geben nicht unbedingt die Meinung der Redaktion wieder. Anfragen und Mittelungen per E-Mail: rubbits@ruhr-uni-bochum.de Auflage: 13.200

© by Dewitz, Seitzer, Partner - Peter Esser

