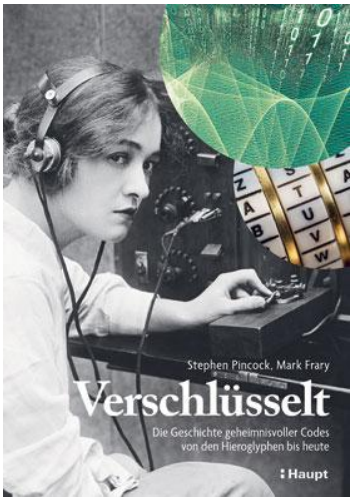
NN: Rezension des Buches **Verschlüsselt. Die Geschichte geheimnisvoller Codes von den Hieroglyphen bis heute, von Stephen Pincock und Mark Ferry. Haupt Verlag Bern 2023**



„Im 21. Jahrhundert ist digitale Verschlüsselung Teil des Alltags. Jedes Mal, wenn wir mit dem Handy telefonieren, einen Film schauen oder Online-Bankgeschäfte tätigen, bedienen wir uns einen hochentwickelten Form der computergestützten Verschlüsselung und sorgen so dafür, dass die neugierigen Augen und Ohren anderer außen vorbleiben.“ (S. 8)

Mit diesen zwei Sätzen beginnt das sehr interessante Buch. Jedoch beim Lesen dieser Sätze mußte der Rezensent schmunzeln. Warum? Die erste Frage an die Autoren in einem ausgedachten Zwiegespräch war: Haben Sie schon mal was von der NSA gehört, das gleich einer Krake die Welt umspannt und alles ausspioniert, was ausspioniert werden kann?

Ein prominentes Beispiel dieser Krake war die Ex-Kanzlerin Angela Merkel, welche von ihren „Freunden“ aus dem Land der unmöglichen Beschränktheiten (also den USA) ausspioniert wurde, ihr Handy abgehört. Und obwohl ihr „Freund“ Obama, mit dem sie so manches Wangenküsschen austauschte, versicherte, daß dieses Ablauschen eingestellt werde, lief die Überwachung weiter. Das zur Glaubwürdigkeit von US-Präsidenten.

Ein weiteres prominentes Beispiel ist Huawei, eine Technologie, die den US-Konzernen ein giftiger Dorn im Auge ist. Die Behauptung, US-Bürger könnten bei Benutzung dieser Technologie abgehört werden, gleicht einem Treppenwitz der Geschichte.

Darüber hinaus, und das ärgert den US-Konzernen am meisten, arbeiten die auf Huawei basierenden neuen Smartphones nicht mehr mit Android, dem weitverbreiteten westlichen Smartphone-Operating System (OS) neben Apples iOS, sondern mit einem eigenen, von den Chinesen notgedrungen als Alternative entwickelten OS, bei dem die Abhörtechniken der westlichen Nachrichtendienste folglich nutzlos sind. Hinzu komme, daß das chinesische OS auch mit einer von chinesischen Entwicklern perfektionierten Suchmaschine arbeitet – und nicht mit Google, das voller offener Hintertüren für US- und andere westliche Spionagedienste ist.

So sehr wir auch ausspioniert werden, können Techniken entwickelt werden, die dies eindämmen bis blockieren (siehe Tor Browser und DuckDuckGo).

Und schon sind wir bei dem Hauptthema des Buches: bei den Codes und Chiffren.

Mit ausgewiesener Sachkenntnis zeigen uns die Autoren, welche Geschichte dahinter steckt, wann erstmalig Codes und Chiffren benutzt wurden, und – das nichts sicher ist (was die Autoren in den beiden o. g. Einführungssätzen für nicht möglich hielten).

Nahezu jedes Wort hat seine Negation: Ja, Nein, Und, Oder.

Demnach: Chiffrieren, De-Chiffrieren, Codieren, De-Codieren. Was in der Praxis mehrfach bewiesen wurde.

Es war immer eine Frage der Zeit, wann benutzte Codes, besonders Mehrfach-Verschlüsselungen usw. geknackt wurden.

Die Ursprünge der Verschlüsselung geht weit in die Geschichte zurück. Die Autoren verorten den „Beginn“ im sog. Alten Ägypten. Und so setzte sich die Verschlüsselung von Nachrichten fort bis in die Gegenwart.

Auffallend, wenn auch nicht explizit von den Autoren genannt, ist die Tatsache, daß das Verschlüsseln nur Sinn hat, wenn es Menschen gibt, denen diese verschlüsselten Nachrichten nicht zugedacht sind. Das ist in diesem Fall der jeweilige Feind.

Und wer war dieser Feind? Zum einen der Herrscher in einem anderen Land, mit dem man im Clinch lag (z. B. durch Krieg); zum anderen der Gegner innerhalb derselben Gesellschaft, sprich in einer von der Existenz von Klassen geprägten Gesellschaft.

Das Verheimlichen von Wissen, so die Hypothese, ist nur denkbar und sinnvoll innerhalb von durch Klassenkampf geprägten Gesellschaften.

Eine Gesellschaft, welche auf Offenheit und Solidarität aufgebaut ist, braucht keine Verschlüsselung. Hier muß gegenüber den Massen immer die Wahrheit gesagt werden. Denn nur die Wahrheit, so grausam sie auch sein kann, gebiert die Lösung von Problemen.

Leider geht den Autoren diese Phantasie ab. Sie können sich, so scheint es, partout keine Gesellschaft vorstellen, die der Geheimnisse entbehren kann.

Es ist daher nicht verwunderlich, wenn die Autoren sagen: „*eine menschliche Gesellschaft ohne Geheimnisse kann man sich kaum vorstellen ...*“ (S. 11)

Auch wenn die Autoren dieser Phantasie entbehren, ist es dennoch nützlich, sich der Geschichte der Kryptologie zu bemächtigen.

Es ist schon erstaunlich, welche Phantasie Menschen in den letzten 4000 bis 5000 Jahren aufwandten, um Wissen in ein Geheimnis zu verwandeln. Im sog. Alten Ägypten waren es die Schreibkundigen, „*die historische Berichte in die Steine großer Bauwerke meißelten.*“ (S. 11)

Das Buch liefert diverse Beispiele der Codierung und De-Codierung; bei Letzterem also die Analyse. Wer sich demnach mit der De-Codierung befassen will, sollte ein mathematisch-logisches Verständnis haben.

Nehmen wir ein Beispiel gleich zu Beginn des Buches (S. 16 f.): *Substitutionschiffren*

Der Geschichtsschreiber Polybios (* um 200 v. Chr. in Megalopolis auf der Peloponnes; † um 120 v. Chr. vermutlich auf der Peloponnes) entwickelte in einem Gitternetz von 5 × 5 Quadraten die Buchstaben des Alphabets:

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Hier ergibt der Buchstabe c die Zahl 13.

Durch entsprechende Verschiebung der Buchstaben entstehen neue Wörter.

Hier ein einfaches Beispiel auf S. 17 des Buches:

FIAEVI XLI MHIW SJ QEVGL

Zahl der verschobenen Stellen	Möglicher Klartext
0	FIAEVI XLI
1	EHZDUH WKH
2	DGYCTG UIF
4	BEWARE THE

„*Die Entschlüsselung des restlichen Textes zeigt, dass die Nachricht ‚Beware the Ides of March‘*[1] *(Hüte dich vor den Iden des März) lautet.*“ (S. 17)

[1] „Anmerkung des Haupt Verlags: Stephen Pincock und Mark Ferry haben dieses Buch im Original auf Englisch verfasst. Die Beispieltexte in dieser Ausgabe wurden auf Englisch belassen, damit die Codeanalysen möglichst nachvollziehbar bleiben. Natürlich lassen sich die Prinzipien auf Texte in deutscher Sprache übertragen.“ (S. 17)

Es sei erwähnt, daß diese Art der Verschlüsselung relativ leicht entzifferbar ist.

Doch in dem Maße, wie eine Verkomplizierung stattfand, erhöhte sich der Aufwand für die Entschlüsselung.

Ein historisch sehr bekanntes Beispiel ist das durch die deutschen Faschisten im Krieg eingesetzte Chiffrier-Maschine Enigma. Dieser Name sollte Programm sein: Enigma = griechisch αἴνιγμα aínigma, deutsch Rätsel. Nur wie schon genannt, ist es eine Frage der Zeit, wann dieses Rätsel geknackt sein wird.

„*Die erste Enigma-Nachricht wurde in Bletchley Park am 20. Januar 1940 geknackt.*“ Seitdem konnten die Nachrichten der Deutschen mitgelesen werden. Interessant ist daran, daß man diesen Fakt selbstredend geheim halten mußte. Also wurde zu dieser Verschleierung eine weitere Verschleierung erfunden: „*Um die Existenz und die Erfolge von Bletchley Park geheim zu halten, erfand die britische Regierung einen Spion mit dem Decknamen Boniface und einen imaginären Agentennetzwerk im Feindesland. Boniface oder eine seiner Spione in Deutschland habe ein Gespräch zwischen hochrangigen deutschen Offizieren mitgehört oder ein geheimes Dokument in einer Mülltonne gefunden. Auf diese Weise sickerte die Informationen wieder zu den Deutschen durch, ohne dass diese erkennen konnten, dass ihr Funksignale mitgehöhrt wurden.*“ (S. 109)

Maßgeblich beteiligt an der Entschlüsselung war Alan Turing, „*einer der größten Kryptoanalytiker aller Zeiten*“ (S. 8), von dem die Autoren behaupten, daß er zur Kriegswende beigetragen soll.

Keine Frage. Die De-Codierung verschlüsselter Nachrichten während eines Krieges ist äußerst wichtig. Man erfährt relativ rechtzeitig, was der Feind geplant hat und bereit ist, auszuführen.

Von Alfred Jodl (Chef des Wehrmachtführungsstabes) stammt die Aussage, die er im Nürnberger Prozeß äußerte, daß die Nachrichten an die Ostfront schneller in Moskau gewesen wären als auf seinem Schreibtisch. Hier spielte weniger eine De-Codierung eine Rolle, sondern immer noch die klassische Variante: die Spionage. Neben der Rolle des britischen Geheimdienstes, hier in Gestalt der De-Chiffrierer, gab es direkt im OKW antifaschistische Kräfte, die sensible Nachrichten weiterleiteten.

Noch zu der Annahme der Autoren, Alan Turings Arbeit habe zur Kriegswende geführt. Nun, die tatsächliche Wende wurde letztendlich auf dem Schlachtfeld geschlagen: zuerst vor Moskau, als die Wehrmacht gestoppt und zurückgedrängt wurde, Hitler also nicht wie einst Napoleon in Moskau einmarschieren konnte.

Die nächste Etappe der Kriegswende war Stalingrad, die dritte die Kursker Panzerschlacht. *Die entscheidendsten Schlachten fanden ohnehin auf sowjetischem Territorium statt.*

Aber wie schon gesagt: die Entschlüsselung spielte damals eine große Rolle, und half zumindest den West-Alliierten.

Gedankt wurde es übrigens Alan Turing nicht, was er an Heldenhaftem leistete. Wegen seiner Homosexualität wurde er bestraft, psychiatrisch behandelt. Letztendlich, so die Annahme, beging er Selbstmord.

Das prüde England brauchte ca. ein halbes Jahrhundert, um ihn zu rehabilitieren.

Zusammenfassend ist zu sagen, daß bis auf wenige Äußerungen, mit denen der Rezensent nicht übereinstimmt, ein außerordentlich gutes Buch vorliegt, das, so ist zu hoffen, viele Leserinnen und Leser finden wird.

Der Rezensent ist übrigens davon überzeugt, daß es eines Tages eine Gesellschaft gibt, in der es nicht mehr nötig sein wird, Wissen zu verschlüsseln. Denn Wissen ist Macht.

Hier nebenbei eine Leseempfehlung: „Das Mädchen aus dem All“ von Iwan Jefremow (1957), in dem (ab Kapitel 2) zu lesen ist, wie eine Gesellschaft ausschaut, in der das Wissen und die Wahrheit Grundpfeiler einer menschlichen Gesellschaft sind, die also des Geheimnisses, der Chiffrierung, nicht mehr bedarf.

Wir sollten die Wahrheit nicht fürchten und nicht zu jener Sorte von Menschen gehören, die sich weigerten, durch Galileis Fernrohr zu schauen, um die Bestätigung seiner neuen Erkenntnisse zur Kenntnis zu nehmen.

Würden wir das Wissen eines Aristarchos von Samos, eines Kopernikus, eines Galileis, eines Keplers nicht nur verheimlichen, sondern auch noch bei Übertragungen verschlüsseln, so müssten wir immer noch annehmen, die Sonne bewege sich um die Erde.