

## Geleitwort

Erst kürzlich beschäftigte sich ein Artikel auf der Titelseite der New York Times mit dem Brechen geheimer Codes der irakischen Regierung durch die US-Geheimdienste. Welches andere Thema der Informationswissenschaften kann behaupten, so direkt eine Rolle in der Weltpolitik zu spielen? Vielleicht rührt hierher die Faszination, welche die Kryptologie – die Wissenschaft der geheimen Botschaften – auf viele Menschen ausübt. Die Faszination dieses Themas war auch mein Beweggrund, mich im Jahr 1994 der Kryptologie zuzuwenden. Meine Erfahrung seither ist allerdings, dass eine klassische Einführung in die Kryptologie mit einer gehörigen Portion Theorie – insbesondere der reinen Mathematik – einhergeht. Obwohl ich selber seit 10 Jahren Kryptologie auf diese Weise unterrichte, war mir schon seit langem bewusst, dass für viele besonders »aufregende« Aspekte der Kryptologie ein solch mathematisches Vorgehen nicht notwendig ist.

Herrn Klaus Schmech ist es nun mit diesem Buch in hervorragender Weise geglückt, die interessantesten Aspekte der Kryptologie in ebenso verständlicher wie fesselnder Weise darzustellen. In den ersten beiden Teilen des Buches wird ein Bogen gespannt, der von der Verschlüsselung im amerikanischen Bürgerkrieg bis hin zum Codebrechen im Kalten Krieg reicht. Natürlich darf eine spannende Behandlung des Brechens der berühmten Enigma nicht fehlen. Auch weniger bekannte Begebenheiten, wie die Erfolge der deutschen Codebrecher im Zweiten Weltkrieg oder Kryptologie in der DDR, werden in interessanter Weise dargestellt.

Die Enigma darf nicht fehlen

Im nächsten Teil des Buches gelingt Herrn Schmech das Meisterstück, die überaus spannende Geschichte der modernen Datensicherheit seit den siebziger Jahren bildhaft und sehr interessant ohne theoretische Überlast darzustellen. Die Themen sind hier ebenso vielfältig wie die Bedeutung der Verschlüsselung in unserem täglichen Leben geworden ist: Von der Entstehungsgeschichte der bekanntesten Verschlüsselungssoftware PGP über das deutsche Signaturgesetz bis hin zur Quantenkryptographie, die schon in einigen Jahren einsatzbereit sein kann, werden hier zahlreiche Themen in fesselnder Weise aufbereitet.

Besonders gefällt mir, dass neben der historischen Bedeutung von (oft zu schwachen) Codes auch der technische Hintergrund ohne mathematischen Ballast beschrieben wird. Alles in allem ein Buch, welches einen nicht mehr loslässt und das ich vom Laien bis zum Datensicherheitsexperten jedem empfehlen kann!

Prof. Dr.-Ing. Christof Paar  
Inhaber des Lehrstuhls für Kommunikationssicherheit  
Ruhr-Universität Bochum  
Bochum, im Dezember 2007

**Lesehinweise** Wenn Sie an technischen Einzelheiten interessiert sind, dann lesen Sie bitte die in den einzelnen Kapiteln angeordneten Boxen (im Titel durch »Box:« gekennzeichnet). Alle Glossarbegriffe alphabetisch sortiert finden Sie am Ende des Buches.

Wenn Sie den spannenden Lesefluss *nicht* unterbrechen möchten, dann überspringen Sie die Boxen.

Die schönsten Fotos finden Sie im Anhang nochmals in Farbe wiedergegeben.

Ihr W3L-Verlag