Buchreview

"Entzifferte Geheimnisse - Methoden und Maximen der Kryptologie"

von F.L. Bauer

Springer, 2007

ISBN: 978-3-540-67931-8

Denise Reinert

2009-11-15

1 Worum es in dem Buch geht

Wie der Untertitel bereits verrät, behandelt das Buch Entzifferte Geheimnisse verschiedene Methoden und Maximen der Kryptologie.

Das Buch selbst ist in zwei Teile aufgeteilt: Kryptografie und Kryptanalyse.

Der erste Teil des Buches gibt einen Überblick über die Kryptografie als solche und stellt verschiedene Verschlüsselungsverfahren, deren Funktionsweise und Hintergründe dar. Einleitend werden historische Persönlichkeiten aus den verschiedensten Bereichen vorgestellt, die sich in der Kryptografie einen Namen gemacht haben.

In Kapitel 1 (Einleitender Überblick) stellt der Autor Kryptografie und Steganografie vor. Dabei werden steganographische und kryptologische Methoden schematisch klassifiziert und anhand historischer Beispiele anschaulich erläutert.

Kapitel 2 (Aufgabe und Methoden der Kryptographie) gibt einen kurzen Überblick über Die Kryptographie an sich. Nach einem kurzen historischen Überblick, in dem die Aufgaben der Kryptografie beschrieben werden, werden in den folgenden Abschnitten alle für die Kryptografie notwendigen Grundlagen (Klartext, Ver- und Entschlüsselung, Zeichenvorräte, Schlüssel) vorgestellt und mathematisch definiert.

In Kapitel 3 (Chiffrierschritte: einfache Substitution) werden auf Substitution basierende Verfahren vorgestellt. Dabei wird sowohl auf unipartite als auch multipartite einfache Substitutionen, sowie der Sonderfall der Permutation eingegangen. Jedes der Verfahren wird sowohl mathematisch beschrieben als auch anhand eines anschaulichen Beispiels konkret erläutert.

Kapitel 4 (Chiffrierschritte: Polygrafische Substitution und Codierung) erweitert das vorangehende Kapitel um polygraphische Chiffrierung, so werden Bigramme, Tomographische Verfahren und Trigramme eingeführt. Wie im vorhergehenden Kapitel werden die Verfahren zunächst theoretisch beschrieben, dann werden die Funktionsweise und die einzelnen Rechenschritte anhand eines Beispiels anschaulich erläutert. Die Beispiele sind um historische Informationen ergänzt, so dass der Leser nachvollziehen kann, in welchem Zusammenhang die Verfahren entwickelt und eingesetzt wurden.

Das folgende Kapitel 5 (Chiffrierschritte: Lineare Substitution) führt zunächst die Grundlagen der linearen (affinen) Substitution als Spezialfall der polygrafischen Substitution ein und betrachtet dann ausführlich verschiedene Fälle (involutorische, homogene und inhomogene, binäre sowie zerfallende lineare Substitution).

In Kapitel 6 (Chiffrierschritte: Transposition) werden Transpositionschiffren eingeführt. Dabei werden zunächst die Grundlagen der Transposition erläutert, die dann anhand einfacher Verfahren praktisch dargestellt und in den folgenden Abschnitten vertieft werden. Ergänzend wird im letzten Abschnitt auf Anagramme, deren Funktionsweise und deren Bedeutung im Laufe der Geschichte eingegangen.

Nachdem in den ersten Kapiteln monoalphabetische Chiffren beschrieben wurden, wird in Kapitel 7 (Polyalphabetische Chiffrierung: Begleitende und unabhängige Aspekte) die polyalphabetische Chiffrierung vorgestellt. Zunächst werden auch hier die theoretischen Grundlagen sowie potenzierte, verschobene und rotierte Alphabete erläutert und anhand praktischer Beispiele verdeutlicht, zudem werden bekannte Chiffren wie Vigenère, Beaufort und unabhängige Alphabete (Porta, Bazeries) mit ihrem historischen Hintergrund vorgestellt. Ergänzt wird das Kapitel durch den Abschnitt Rotor-Maschinen, in dem mechanische Lösungen wie die Enigma ausführlich erläutert werden.

Kapitel 8 (Polyalphabetische Chiffrierung: Schlüssel) befasst sich mit der Erzeugung und Verwaltung von Schlüsseln für polyalphabetische Chiffren. In Anlehnung an Kapitel 7 ist auch hier ein Abschnitt maschinellen Lösungen gewidmet, wobei auch die Enigma wieder aufgegriffen wird. Ein weiterer Abschnitt ist dem One-Time-Pad gewidmet.

In Kapitel 9 (Komposition von Chiffrierverfahren) werden Vorteile und Risiken der Komposition verschiedener Verschlüsselungsverfahren betrachtet. Dabei werden zunächst in einem Abschnitt die erforderlichen Gruppeneigenschaften von Chiffrierungen erläutert. Nach verschiedenen Beispielen für mögliche Kombinationen und möglicher dadurch entstehender Problematiken, werden die Verschlüsselungsverfahren DES und IDEA vorgestellt.

Kapitel 10 (Öffentliche Chiffrierschlüssel) führt nach den symmetrischen Verfahren nun die asymmetrischen Verschlüsselungs- und Signaturverfahren ein. Dabei wird auch auf auf die mathematischen Probleme eingegangen, die den aktuellen Verfahren zugrunde liegen. Dieser wird durch einen kurzen Abschnitt zur Zeitabschätzung von Berechnungen ergänzt. Als praktisches Beispiel wird RSA vorgestellt, wobei auch die gängigen Angriffe kurz erläutert werden.

Kapitel 11 (Chiffriersicherheit) schließt den ersten Teil des Buches (Kryptografie) ab und leitet in den zweiten Teil des Buches (Kryptanalyse) über. Dabei werden verschiedene Fehler aufgegriffen, die bei der Chiffrierung von Nachrichten passieren können und anschaulich anhand historischer Gegebenheiten dargestellt. Zudem werden Regeln und Hinweise für den Umgang mit kryptografischen Verfahren gegeben. Im letzten Abschnitt wird auf den politischen Interessenkonflikt zwischen Bürgern und Staat im Bezug auf die Verwendung von Verschlüsselungssystemen eingegangen.

Im Anhang an den ersten Teil des Buches finden sich Fotografien von Chiffriergeräten aus verschiedenen Epochen, vom antiken Griechenland bis zu modernen Hochgeschwindigkeitsrechnern.

Der zweite Teil des Buches befasst sich mit Kryptanalyse und beginnt mit einem einleitenden Text über Ziel, Vorgehen und Geschichte der Kryptanalyse, also des Brechens Kryptografischer Verfahren.

Kapitel 12 (Ausschöpfung der kombinatorischen Komplexität) stellt das einfachste Verfahren der Kryptanalyse dar: die erschöpfende Suche. Dabei wird zunächst jeweils die Komplexität der im Buch zuvor vorgestellten Chiffren gezeigt. Außerdem finden sich praktische Hinweise zur Durchführung eines Exhaustationsverfahrens und zu dessen Mechanisierung.

In Kapitel 13 (Anatomie der Sprache: Muster) werden verschiedene Ansätze zur Mustererkennung vorgestellt. Dabei wird sowohl auf Muster innerhalb einzelner Wörter, als auch insbesondere im historischen Kontext auf Muster innerhalb von Nachrichten eingegangen.

Die einfache Mustersuche aus dem vorigen Kapitel wird in Kapitel 14 (Polyalphabetischer Fall: Wahrscheinliche Wörter) auf polyalphabetische Chiffren ausgedehnt. Dabei wird das Konzept der negativen Mustersuche erläutert, hinzu kommen weitere Methoden wie die von de Viaris, Friedman und die Isomorpie-Methode.

Kapitel 15 (Anatomie der Sprache: Häufigkeit) befasst sich mit verschiedenen Methoden der Häufigkeitsanalyse. Dabei wird auf das Vorkommen von Buchstaben- und Buchstabengruppen in unterschiedlichen Sprachen sowie auf kombinierte Vorgehensweisen eingegangen. Zudem beinhaltet das Kapitel eine Vielzahl an Statistiken zur Auswertung von Texten.

Kapitel 16 (Kappa und Chi) vertieft die Möglichkeiten zur Analyse von symmetrischen Chiffren um relative Häufigkeiten wie die Zeichenkoinzidenz (Kappa), sowie die Koeffizienten Chi und Psi zur Ermittlung der Sprache eines Textes aus dem Chiffrat.

In Kapitel 17 (Periodenanalyse) werden die zuvor beschriebenen Verfahren (Kappa, Chi und Psi) auf periodische polyalphabetische Chiffren angewendet, um Abschätzungen zur Periodenlänge zu erhalten. Neben einem Abschnitt über maschinelle Kryptanalyse wird hier auch der Kasiski-Test vorgestellt.

Kapitel 18 (Zurechtrücken begleitender Alphabete) widmet sich dem Problem, bei einer bekannten Periodenlänge eines polyalphabetischen Geheimtextes die verschiedenen Alphabete auf ein Referenzalphabet zu reduzieren. Dabei werden die zuvor erläuterten Verfahren zur Häufigkeitsanalyse anhand von praktischen Beispielen eingesetzt. Abschließend wird auf die Rekonstruktion des Schlüssels eingegangen.

In Kapitel 19 (Kompromittierung) wird einer der Chiffrierfehler aus Kapitel 11 aufgegriffen und die aus der Kompromittierung einer Chiffre resultierenden Möglichkeiten für methodische Angriffe beschrieben. Darunter verschiedene Varianten für die Superimposition (also Überlagerung) von Klartexten sowie die Indikatorverdopplung und die Erzeugung von Rückkoppelplänen erläutert.

Kapitel 20 (Lineare Basisanalyse) beschreibt kurz die Analyse linearer polygraphischer Chiffren, darunter die Rekonstruktion des Schlüssels sowie eines linearen Schieberegisters.

Kapitel 21 (Anagrammieren) befasst sich recht knapp mit der Analyse von Transpositions-Chiffren.

In Kapitel 22 (Abschließende Bemerkungen) werden noch einmal geglückte Angriffe auf Chiffren im historischen Kontext aufgegriffen und die Arbeitsweise der Kryptanalysten beschrieben. Zuletzt wird auf die Bedeutung der Kryptografie und der Kryptanalyse in der Geschichte eingegangen.

Im Anhang finden sich Übersichten über die informationstheoretische Axiome und über kryptologische Geräte und Maschinen im Deutschen Museum München.

2 Zusammenfassung

Das Buch besteht aus zwei Teilen: Kryptographie und Kryptanalysis. Im ersten Teil wird eine Vielzahl von kryptographischen Verfahren beschrieben, ihre Funktionsweise mathematisch erläutert und anhand von Beispielen anschaulich dargestellt.
Der zweite Teil des Buches widmet sich der Kryptanalyse, also dem Brechen kryptographischer Verfahren, die hier ebenfalls sehr detailliert und fundiert beschrieben werden. Zusätzlich enthält das Buch eine ausführliche Geschichte der Kryptografie, der damit verbundenen Personen und ihrer Rolle in militärischen und privaten Situationen.

3 Wie ist das Buch?

Der Stil des Autors ist sehr präzise, wie es vom Autor Dr. rer. nat. Dr. ès sc. h.c. Dr.rer.nat. h.c. mult. Friedrich Bauer, Professor emeritus der Mathematik und Informatik der TU München zu erwarten ist. Die Verfahren sind korrekt und fehlerfrei beschrieben, alle Aussagen durch Literatur belegt, so dass sie ausgezeichnet für Studien- und Forschungszwecke geeignet sind.

Besonders hervorzuheben ist die durchgehende Vorgehensweise, die einzelnen Verfahren und Angriffe zunächst zu beschreiben, dann mathematisch darzustellen und sie schließlich anhand praktischer Beispiele Schritt für Schritt durchzuexerzieren, so dass der Leser die zuvor gelernte Theorie direkt in ihrer Anwendung nachvollziehen kann. Durch dieses Vorgehen lernt der Leser zudem eine Vielzahl historischer Chiffren kennen, was das Verständnis erleichtert und das Lesen (bzw. Lernen) auflockert. Auch auf die derzeit gängigen asymmetrischen Verschlüsselungsverfahren wird in dem Buch eingegangen. Zwar widmet sich diesen Verfahren nur ein kleiner Teil des Buches, jedoch sind die wichtigsten Inhalte zu Funktionsweise und Schwachstellen durchaus enthalten.

Ungewohnt für ein so mathematisch gehaltenes Buch über Kryptografie und Kryptologie ist der historische Hintergrund, der sich als roter Faden durch die Kapitel zieht. Dadurch erfährt der Leser nicht nur Funktionsweisen und Schwachstellen von Verfahren, sondern kann sich ein Bild über den gesellschaftlichen und politischen Hintergrund der Entstehung von Chiffren und Angriffen und der daran beteiligten Persönlichkeiten machen.

4 Wem würden Sie das Buch weiterempfehlen?

Dieses Buch ist für jeden empfehlenswert, der sich aus mathematischer, informationstechnischer, historischer oder sprachlicher Sicht für Kryptographie interessiert.

Dabei gibt es verschiedene Herangehensweisen, das Buch zu lesen. Durch den lebhaften Stil kann es durchaus linear als Roman gelesen werden, jedoch ist es auch als Nachschlagewerk für einzelne Bereiche geeignet.
Um das Buch in seiner Gänze nutzen zu können, ist ein Grundwissen in diskreter Mathematik hilfreich, damit die einzelnen Verfahren tatsächlich genau nachvollzogen werden können.
Jedoch ist es nicht zwingend erforderlich, das Buch vollständig zu lesen, so wird ein vorwiegend historisch interessierter Leser die mathematischen Definitionen überfliegen können, hingegen kann ein Mathematiker die Details der Kriegsgeschehnisse im 2. Weltkrieg (mit genauen Daten, Ortsangaben, Namen und Decknamen) querlesen.

Abschließend lässt sich sagen, dass es sich bei diesem Buch um spannende Literatur handelt, die in dieser Kombination selten zu finden ist.

Die Reviewerin promoviert derzeit am Insitut für die Sicherheit im E-Business (ISEB) der Ruhr-Universität Bochum, Deutschland.