Abenteuer Kryptologie

Reinhard Wobst; "Abenteuer Kryptologie"; Addison-Wesley; ISBN 3-8273-1193-4; 360 S. + CD-ROM (ca. 25 MB); öS 510,—

Martin Schönhacker

Ist das Sparschwein doch sicherer als eine Bankomatkarte mit PIN-Code?

Nun, man könnte beinahe zum Sparschwein tendieren, wenn man liest, daß es eigentlich nur eine einzige restlos sichere Verschlüsselungsmethode gibt (und der PIN-Code ist ja nichts anderes als ein Schlüssel), nämlich das sogenannte "One-Time-Pad". Dabei verwendet man den Schlüssel nur ein einziges Mal, und zwar einen möglichst zufälligen. Der drastische Vorschlag im Buch:

"Zeichnen Sie auf, was ein unzuverlässiger Geigerzähler während einer Fahrt über holprige Straßen von einer radioaktiven Probe im Fahrzeug mißt, und überlagern Sie anschließend diesen Datenstrom mit dem digitalisierten Rauschen eines Wasserfalles sowie dem Blöken eines Schafes: Da gibt jeder Geheimdienst auf."

Glücklicherweise sind die übrigen Verfahren, die das vorliegende Buch beschreibt, etwas näher an der täglichen Praxis — obwohl obige Aussage natürlich richtig ist.

"Methoden, Risiken und Nutzen der Datenverschlüsselung" lautet der Untertitel des gleichermaßen umfassenden wie verständlich geschriebenen Werkes. Von historischen Codierungsverfahren bis zu verschlüsselter Datenübertragung am Internet, von der deutschen "Enigma" im 2. Weltkrieg (übrigens mit einer klar verständlichen Beschreibung, was selten vorkommt) bis zu den im Bankbereich eingesetzten "Chipkarten" werden die wichtigsten Bereiche der Kryptologie abgedeckt.

Weil ein guter Kryptologe nach Aussage des Autors nicht nur über die Verwendung kryptologischer Verfahren, sondern auch über das unbefugte "Knacken" von Codes Bescheid wissen muß, gibt es immer auch Gedanken und konkrete Methoden zur Kryptanalyse. Gerade auch durch diese Überlegungen lernt man beim Lesen eine ganze Menge über gängige Codierfehler sowie Art und Grad der Anfälligkeit verschiedener Codes.

Die beiliegende CD-ROM enthält zwar eine für dieses Medium relativ bescheidene Datenmenge, aber dafür handelt es sich zum Teil um echte Perlen, die der Autor zusammengestellt hat. Man findet Quelltexte für die Implementierung diverser Codierverfahren, aber auch für deren (unbefugte) Entschlüsselung. Außerdem sind zahlreiche weiterführende Texte enthalten, wie etwa lange geheimgehaltene Details über die "Enigma".

Alles in allem handelt es sich um ein gelungenes Buch mit vielen wertvollen Referenzen, das als Einführung und auch zum Nachschlagen empfohlen werden kann. Details und ein Inhaltsverzeichnis sind bei `http://www.addison-wesley.de/` verfügbar.

➢

MTB-Seite mit Schaltflächen für die Erstellung von Balkendiagrammen in Abhängigkeit der Jahreszahlen und vielen weiteren grafischen Elementen, z.B.:

- gewählte Jahreszahl erscheint in der Titelzeile der Grafik
- Tabelle für die Zahlenwerte (analog zur Grafik) wird ausgegeben
- optisches Hervorheben des gedrückten Buttons durch Schatteneffekt

Analoge MTB-Seite mit Schaltflächen für die Erstellung von Liniendiagrammen mit weiteren grafischen Elementen, z.B.:

- transparente Schaltflächen für die Auswahl verschiedener Kurven
- Anzeigefeld für die Diagramm-Werte, die mit der Maus in der Graphik abgetastet werden können
- Legende zum Diagramm

MTB-Seite mit Schaltflächen für die Erstellung von Tortendiagrammen mit weiteren interaktiven Benutzerfunktionen, z.B.:

- Buttons in den Farben der Sektoren, die auf Mausklick, entsprechend dem Diagrammwert in die Höhe wachsen
- Aufleuchten der einzelnen Sektoren beim Überfahren der entsprechenden Elemente in der Legende

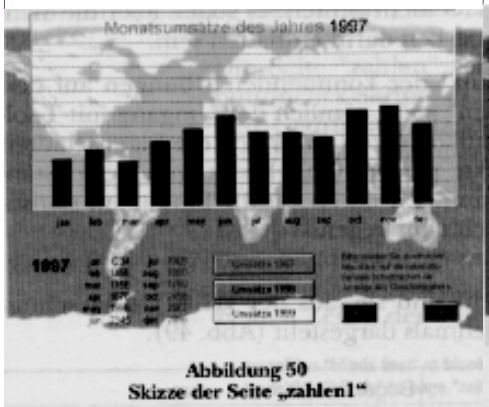

Abbildung 50
Skizze der Seite „zahlen1"

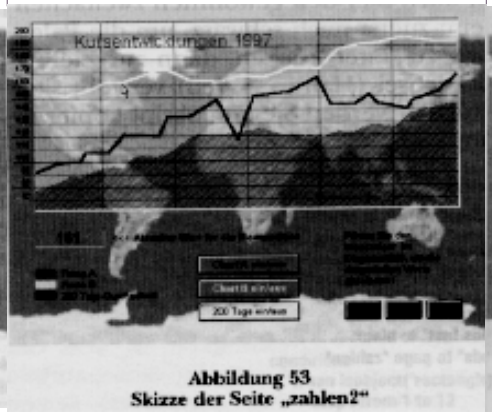

Abbildung 53
Skizze der Seite „zahlen2"

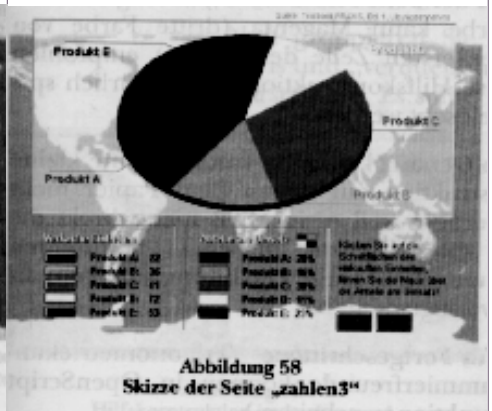

Abbildung 58
Skizze der Seite „zahlen3"