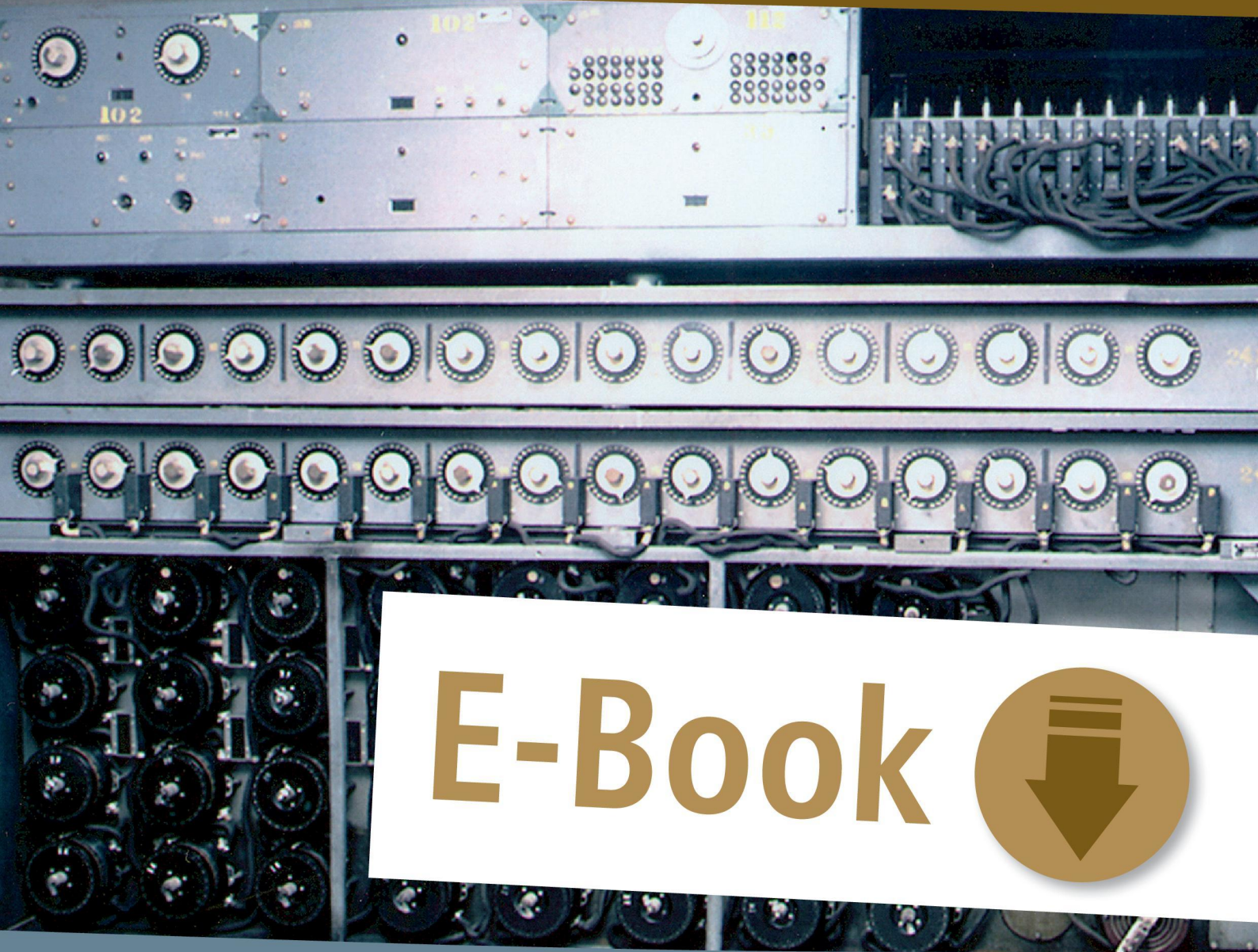


mit
Programmieraufgaben
auf CD-ROM

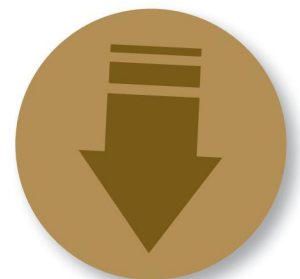
GYMNASIUM

Informatik konkret: Kryptografie

Klasse 9–12



E-Book



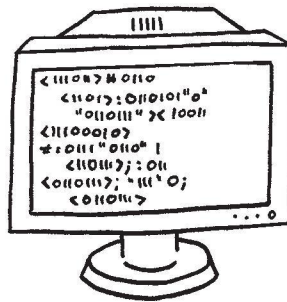
Verschlüsselungen und Codes · Hintergrundwissen und Übungsaufgaben

Alexander Haag

AOL
verlag

Alexander Haag

Informatik konkret: Kryptografie



AOL
verlag

Bildnachweis

Cover: Turing-Bombe (US-Version) © Wikipedia

S. 9: Julius Caesar © Andreas Wahra/Wikipedia

S. 18: Deckblatt der „Beale Papers“ © Wikipedia

S. 20: Amerikanische Unabhängigkeitserklärung © Wikipedia

S. 22: Enigma I © OS/Wikipedia (CC BY-SA 3.0)

S. 24: Marian Rejewski © Wikipedia; Quelle: Stanisław Strumph Wojtkiewicz (1978).
Sekret Enigmy. Warschau: Iskry. (ohne ISBN)

S. 27: Enigma-Walzen © Bon Lord/Wikipedia (CC BY-SA 3.0)

S. 29: Turing-Bombe © Magnus Manske/Wikipedia (CC BY-SA 3.0)

Creative Commons – Lizenzvereinbarung:

CC BY-SA 3.0 – Creative Commons Attribution-ShareAlike 3.0 Unported;
siehe: <http://creativecommons.org/licenses/by-sa/3.0/deed.de>

Impressum

Informatik konkret: Kryptografie



Alexander Haag unterrichtet seit vier Jahren am Albert-Einstein-Gymnasium in Ravensburg die Fächer Mathematik und Informatik.

© 2012 AOL-Verlag, Buxtehude
AAP Lehrerfachverlage GmbH
Alle Rechte vorbehalten.

Postfach 1656 · 21606 Buxtehude
Fon (04161) 749 60-60 · Fax (04161) 749 60-50
info@aol-verlag.de · www.aol-verlag.de

Redaktion: Daniel Marquardt
Layout/Satz: Satzpunkt Ursula Ewert GmbH,
Bayreuth
Illustrationen: MouseDesign MedienAG, Zeven

ISBN: 978-3-403-40042-4

Das Werk als Ganzes sowie in seinen Teilen unterliegt dem deutschen Urheberrecht. Der Erwerber des Werkes ist berechtigt, das Werk als Ganzes oder in seinen Teilen für den eigenen Gebrauch und den Einsatz im Unterricht zu nutzen. Die Nutzung ist nur für den genannten Zweck gestattet, nicht jedoch für einen weiteren kommerziellen Gebrauch, für die Weiterleitung an Dritte oder für die Veröffentlichung im Internet oder in Intranets. Eine über den genannten Zweck hinausgehende Nutzung bedarf in jedem Fall der vorherigen schriftlichen Zustimmung des Verlages.

Die AAP Lehrerfachverlage GmbH kann für die Inhalte externer Sites, die Sie mittels eines Links oder sonstiger Hinweise erreichen, keine Verantwortung übernehmen. Ferner haftet die AAP Lehrerfachverlage GmbH nicht für direkte oder indirekte Schäden (inkl. entgangener Gewinne), die auf Informationen zurückgeführt werden können, die auf diesen externen Websites stehen.

Engagiert unterrichten. Natürlich lernen.

AOL
verlag

Inhaltsverzeichnis

Vorwort	4
1. Steganografie	5
2. Transposition	6
Die „Gartenzaun“-Transposition	6
Die Skytale	7
3. Monoalphabetische Substitution	9
Die Caesar-Verschlüsselung & ROT13	9
Einfache monoalphabetische Substitution	11
4. Polyalphabetische Substitution	13
5. Buch-Verschlüsselung	18
6. Die Enigma	22
7. Asymmetrische Verschlüsselung	30
Lösungen	47
Hinweise zu den Inhalten der CD und zum Programm „Lazarus“	56

Vorwort

Liebe Kollegin, lieber Kollege,

die Kryptografie ist sicher nicht das grundlegendste Thema im Informatikunterricht und sie wird vielleicht in Ihrem Bildungsplan eher am Rande erwähnt. Aber sie ist ein Thema, das die Menschen seit jeher fasziniert hat – und bestimmt auch Ihre Schüler faszinieren wird. Mich hat diese Faszination gepackt, nachdem ich das Buch „Codes“ von Simon Singh gelesen hatte, und so habe ich mich dazu entschlossen, eine entsprechende Unterrichtseinheit für den Informatikunterricht zu erstellen. Diese halten Sie nun in den Händen.

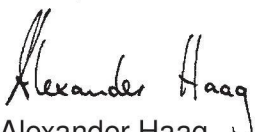
Das Heft lässt sich auf zweierlei Arten verwenden:

- Für Schüler, die noch keine Programmiersprache beherrschen, bietet es neben den umfangreichen Informationen über die in chronologischer Reihenfolge vorgestellten kryptografischen Verfahren eine Fülle von Aufgaben, bei denen Texte „von Hand“ bzw. mithilfe von kleinen Programmen, die sich auf der Begleit-CD zum Heft befinden, verschlüsselt oder entschlüsselt werden sollen. Der Lehrer muss dafür überhaupt nichts vorbereiten, die Schüler arbeiten selbstständig mit dem ausgeteilten Material und können sich anhand der Lösungen (hinten im Heft sowie auf der Begleit-CD) sogar selbst kontrollieren. Die verschlüsselten Nachrichten enthalten oft einen witzigen Spruch und sind teilweise bewusst flapsig, um die Schüler zu motivieren. Sollte Ihnen das nicht zusagen, können Sie mit den Programmen auf der Begleit-CD auch Aufgaben mit eigenen Lösungssätzen erstellen.
- Für Schüler, die bereits eine Programmiersprache (zumindest in Grundzügen) beherrschen, gibt es zusätzlich Programmieraufgaben. In diesen geht es darum, Programme zu schreiben, die die verschiedenen Codierverfahren automatisieren, sodass man nur noch die Nachricht und – falls erforderlich – ein Codewort eingeben muss und die Nachricht dann vom Computer ver- bzw. entschlüsselt wird. Auch hierbei ist der Aufwand für die Lehrperson minimal, da sich alles, was benötigt wird (inklusive Musterlösungen der Programmieraufgaben in Free Pascal!), auf der beiliegenden CD befindet.

Auf der CD finden Sie alle Aufgaben aus dem Buch, alle Lösungen zu den Aufgaben, alle Lösungen zu den Programmieraufgaben, einige grundlegende Hinweise zur Veränderung von Strings (darauf beruht fast jede Ver- bzw. Entschlüsselung) sowie eine Vielzahl an von mir geschriebenen Programmen, die bei einzelnen Aufgaben benötigt werden. Für nähere Informationen siehe Seite 56.

Die Musterlösungen zu den Programmieraufgaben wurden mit Lazarus erstellt, einer Entwicklungsumgebung, die man unter <http://sourceforge.net/projects/lazarus/files/> herunterladen kann. Die verwendete Programmiersprache – Free Pascal – entspricht bis auf winzige Details der Programmiersprache Delphi. Ein solches winziges, aber entscheidendes Detail ist, dass Free Pascal und Lazarus absolut kostenlos sind und uneingeschränkt genutzt werden können. Nach der Installation von Lazarus (Free Pascal braucht nicht extra installiert zu werden!) kann man sofort mit dem Programmieren loslegen und auch die Musterlösungen anschauen. Natürlich kann aber auch jede andere Programmiersprache verwendet werden.

Viel Spaß bei der Kryptografie wünscht Ihnen


Alexander Haag