Understanding Cryptography

A Textbook for Students and Practitioners

Foreword by Bart Preneel

Prof Dr Ing Christof Paar Chair for Embedded Security

Department of Electrical Engineering and Information Sciences

Ruhr Universita t Bochum 0 Bochum

escrypt GmbH Embedded Security Zentrum fu r IT Sicherheit

ISBN 9 6 6 e ISBN 9 6 3 DOI 0 6 3

Springer Heidelberg Dordrecht London New York

ACM Computing Classification E 3 K K

Library of Congress Control Number 47 c Springer Verlag Berlin Heidelberg

This work is subject to copyright All rights are reserved whether the whole or part of the material is concerned specifically the rights of translation reprinting reuse of illustrations recitation broadcasting reproduction on microfilm or in any other way and storage in data banks Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9 in its current version and permission for use must always be obtained from Springer Violations are liable to prosecution under the German Copyright Law

The use of general descriptive names registered names trademarks etc in this publication does not imply even in the absence of a specific statement that such names are exempt from the relevant protective laws and regulations and therefore free for general use

Cover design KuenkelLopka GmbH Printed on acid free paper

Springer is part of Springer Science Business Media www springer com

Flora Maja Noah and Sarah as well as to

While writing this book we noticed that for some reason the names of our spouses and children are limited to five letters As far as we know this has no cryptographic relevance

Academic research in cryptology started in the mid s today it is a mature re search discipline with an established professional organization IACR International Association for Cryptologic Research thousands of researchers and dozens of in ternational conferences Every year more than a thousand scientific papers are pub lished on cryptology and its applications

Until the s cryptography was almost exclusively found in diplomatic mili tary and government applications During the s the financial and telecommuni cations industries deployed hardware cryptographic devices The first mass market cryptographic application was the digital mobile phone system of the late s Today everyone uses cryptography on a daily basis Examples include unlocking a car or garage door with a remote control device connecting to a wireless LAN buying goods with a credit or debit card in a brick and mortar store or on the Inter net installing a software update making a phone call via voice over IP or paying for a ride on a public transport system There is no doubt that emerging application areas such as e health car telematics and smart buildings will make cryptography even more ubiquitous

Cryptology is a fascinating discipline at the intersection of computer science mathematics and electrical engineering As cryptology is moving fast it is hard to keep up with all the developments During the last 25 years the theoretical foun dations of the area have been strengthened we now have a solid understanding of security definitions and of ways to prove constructions secure Also in the area of applied cryptography we witness very fast developments old algorithms are broken and withdrawn and new algorithms and protocols emerge

While several excellent textbooks on cryptology have been published in the last decade they tend to focus on readers with a strong mathematical background More over the exciting new developments and advanced protocols form a temptation to add ever more fancy material It is the great merit of this textbook that it restricts itself to those topics that are relevant to practitioners today Moreover the mathe matical background and formalism is limited to what is strictly necessary and it is introduced exactly in the place where it is needed This less is more approach is very suitable to address the needs of newcomers in the field as they get introduced

step by step to the basic concepts and judiciously chosen algorithms and protocols Each chapter contains very helpful pointers to further reading for those who want to expand and deepen their knowledge

Overall I am very pleased that the authors have succeeded in creating a highly valuable introduction to the subject of applied cryptography I hope that it can serve as a guide for practitioners to build more secure systems based on cryptography and as a stepping stone for future researchers to explore the exciting world of cryptog raphy and its applications

Leuven August Bart Preneel

Cryptography has crept into everything from Web browsers and e mail programs to cell phones bank cards cars and even into medical implants In the near fu ture we will see many new exciting applications for cryptography such as radio frequency identification RFID tags for anti counterfeiting or car to car commu nications we ve worked on securing both of these applications This is quite a change from the past where cryptography had been traditionally confined to very specific applications especially government communications and banking systems As a consequence of the pervasiveness of crypto algorithms an increasing number of people must understand how they work and how they can be applied in prac tice This book addresses this issue by providing a comprehensive introduction to modern applied cryptography that is equally suited for students and practitioners in industry

Our book provides the reader with a deep understanding of how modern cryp tographic schemes work We introduce the necessary mathematical concepts in a way that is accessible for every reader with a minimum background in college level calculus It is thus equally well suited as a textbook for undergraduate or begin ning graduate classes or as a reference book for practicing engineers and computer scientists who are interested in a solid understanding of modern cryptography

The book has many features that make it a unique source for practitioners and stu dents We focused on practical relevance by introducing most crypto algorithms that are used in modern real world applications For every crypto scheme up to date se curity estimations and key length recommendations are given We also discuss the important issue of software and hardware implementation for every algorithm In addition to crypto algorithms we introduce topics such as important cryptographic protocols modes of operation security services and key establishment techniques Many very timely topics e g lightweight ciphers which are optimized for con strained applications such as RFID tags or smart cards or new modes of operations are also contained in the book

A discussion section at the end of each chapter with annotated references pro vides plenty of material for further reading For classroom use these sections are

an excellent source for course projects In particular when used as a textbook the companion website for the book is highly recommended

Readers will find many ideas for course projects links to open source software test vectors and much more information on contemporary cryptography In addition links to video lectures are provided

The material in this book has evolved over many years and is classroom proven We ve taught it both as a course for beginning graduate students and advanced un dergraduate students and as a pure undergraduate course for students majoring in our IT security programs We found that one can teach most of the book content in a two semester course with 90 minutes of lecture time plus 45 minutes of help session with exercises per week total of 10 ECTS credits In a typical US style three credit course or in a one semester European course some of the material should be omitted Here are some reasonable choices for a one semester course

Curriculum 1 Focus on the application of cryptography e g in a computer sci ence or electrical engineering program This crypto course is a good addition to courses in computer networks or more advanced security courses Sect