

Practical Microcontroller Cryptography

From Simple Ciphers to Secure Systems



Dogan Ibrahim & Ahmet Ibrahim

Practical Microcontroller Cryptography

From Simple Ciphers to
Secure Systems



Dogan Ibrahim
Ahmet Ibrahim

● This is an Elektor Publication. Elektor is the media brand of
Elektor International Media B.V.
PO Box 11, NL-6114-ZG Susteren, The Netherlands
Phone: +31 46 4389444

● All rights reserved. No part of this book may be reproduced in any material form, including photocopying, or storing in any medium by electronic means and whether or not transiently or incidentally to some other use of this publication, without the written permission of the copyright holder except in accordance with the provisions of the Copyright Designs and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency Ltd., 90 Tottenham Court Road, London, England W1P 9HE. Applications for the copyright holder's permission to reproduce any part of the publication should be addressed to the publishers.

● **Declaration**

The author and publisher have made every effort to ensure the accuracy of the information contained in this book. They do not assume, or hereby disclaim, any liability to any party for any loss or damage caused by errors or omissions in this book, whether such errors or omissions result from negligence, accident, or any other cause.

● **ISBN 978-3-89576-716-6** Print
ISBN 978-3-89576-717-3 eBook

● © Copyright 2026 Elektor International Media
www.elektor.com
Editor: Clemens Valens
Prepress Production: D-Vision, Julian van den Berg
Printers: Ipskamp, Enschede, The Netherlands

Elektor is the world's leading source of essential technical information and electronics products for pro engineers, electronics designers, and the companies seeking to engage them. Each day, our international team develops and delivers high-quality content - via a variety of media channels (including magazines, video, digital media, and social media) in several languages - relating to electronics design and DIY electronics. www.elektormagazine.com

Contents

Preface	8
Chapter 1 • Foundations of Cryptography	10
1.1 Overview	10
1.2 Mathematical foundations of cryptography	11
1.2.1 Number theory	12
1.2.2 Modular arithmetic	12
1.2.3 Prime numbers	12
1.2.4 Finite fields	13
1.3 History of Cryptography	13
1.3.1 Transposition Ciphers	13
1.3.1.1 Spartan Scytale	13
1.3.2 Substitution Ciphers	14
1.3.2.1 Hebrew Atbash Cipher	14
1.3.2.2 Caesar Cipher	18
1.3.2.3 ROT13 Cipher	23
1.3.2.4 Alberti Cipher Disk	24
1.3.2.5 Vigenère Cipher	25
1.3.2.6 Affine Cipher	31
1.3.2.7 Polybius Cipher	38
1.3.2.8 Playfair Cipher	45
1.3.2.9 Beaufort Cipher	47
1.3.2.10 Ottoman Codebooks	54
1.3.2.11 One-Time Pad Cipher	60
1.3.2.12 Bacon's cipher	67
1.3.2.13 Aristocrat cipher	68
1.4 Summary	69
Chapter 2 • Hacking Simple Ciphers and Passwords	70
2.1 Introduction	70
2.2 The Brute-Force attack	70
2.2.1 Hacking the Caesar cipher using Brute-Force attack	70

- 2.2.2 Hacking a password or a small text using brute-force 76
- 2.2.3 Guessing a password – Using the Arduino Uno 78
- 2.2.4 Guessing a password – Using the ESP32 80
- 2.2.5 Guessing a password – Using the Raspberry Pi Pico 80
- 2.2.6 Guessing a password – Using the Raspberry Pi 5 82
- 2.3 Frequency analysis 84
- 2.4 Man in the middle attacks. 88
- Chapter 3 • Random Number Generation. 89**
- 3.1 Overview 89
- 3.2 Pseudorandom number generation using C/C++ 89
- 3.2.1 Using the Arduino Uno and ESP32 with C/C++. 90
- 3.2.2 Using the Raspberry Pi Pico with MicroPython. 92
- 3.3 True random number generation using C/C++ 94
- 3.3.1 Using the Arduino Uno R4 Minima and WiFi 94
- 3.3.2 Using the ESP32. 94
- 3.4 True random number generation using the Raspberry Pi 5 96
- Chapter 4 • Symmetric Key Cryptography 99**
- 4.1 Overview 99
- 4.2 Block ciphers 100
- 4.3 The DES Cryptography 100
- 4.3.1 Triple DES 102
- 4.3.2 DES Examples – Arduino Uno 102
- 4.3.3 DES examples – DES on Raspberry Pi Pico. 112
- 4.3.4 DES on ESP32 117
- 4.3.5 DES on Raspberry Pi 5 117
- 4.4 The AES Algorithm. 124
- 4.4.1 AES Examples 126
- 4.5 The ChaCha20 Cipher 151
- 4.6 Memory and speed constraints of microcontrollers. 153
- 4.6.1 The Arduino family 154
- 4.6.2 The ESP32 family 155
- 4.6.3 The Raspberry Pi Pico 156

4.6.4 The Raspberry Pi 5	156
4.6.5 The STM32 family	157
Chapter 5 • Asymmetric Key Cryptography	159
5.1 Overview	159
5.2 Key distribution	159
5.3 Digital certificates	161
5.4 Security without digital certificate?	161
5.5 Security without public/private key	162
5.5.1 Project 1 – Key Derivation using the Raspberry Pi 5	162
5.6 Generating public/private key pair	164
5.6.1 The PEM data format.	165
5.6.2 Project 2 – RSA public/private key generation on ESP32	166
5.6.3 Project 3 – RSA public/private key generation on Raspberry Pi 5	169
5.6.4 Project 4 - Encrypt the AES-256 key using the RSA on Raspberry Pi 5	171
5.6.5 Project 5 – Decrypt the AES-256 key using the RSA on Raspberry Pi 5	173
5.7 Secure/secret communication between two parties using the AES and the RSA algorithms with public/private key exchange	175
5.7.1 Project 6 – Complete program to send/receive messages to/from the second party using the Raspberry Pi 5	176
5.7.2 Case study – Communicating secretly and securely	181
Chapter 6 • Other Topics in Cryptography	185
6.1 Overview	185
6.2 The Hash algorithms	185
6.2.1 Project 1 - SHA-256 hashing using the Arduino Uno	185
6.2.2 Project 2 - SHA-256 hashing using the ESP32	187
6.2.3 Project 3 – SHA-256 hashing using the Raspberry Pi Pico	187
6.2.4 Project 4 - SHA-256 hashing using the Raspberry Pi 5	188
6.3 The Diffie-Hellman key exchange algorithm	189
6.4 Post Quantum Cryptography	189
Appendix A – Commonly Used Cryptography Terms	191
Index	197

Preface

Cryptography is no longer confined to high-performance super computers or specialized hardware. In today's interconnected world, even the smallest devices, such as door locks, smart phones, smart heaters, and many other devices must be secure and they must be designed to protect the data they hold. At the heart of almost all of these systems we find microcontrollers or single board computers. A microcontroller is a fast digital processor which sits at the heart of a computer. Understanding how to apply cryptography using present day microcontrollers is very important for anyone who wishes to build secure, reliable and trustworthy systems.

This book describes and analyzes cryptography in the context of microcontrollers, from simple ciphers that illustrate the main principles to modern techniques such as the AES that enable practical and highly secure applications. By using the latest mathematical theory and the developed cryptography algorithms in real-world hardware, readers will discover not only how cryptography works, but also *how to make it work* in microcontroller based systems with limited processing powers and limited memories.

Why focus on **Arduino, ESP32, Raspberry Pi Pico and similar platforms**? These microcontrollers represent the spectrum of what is both easily accessible and practical. Arduino boards offer low-cost, simplicity and approachability, making them excellent tools for demonstrating fundamental ideas. ESP32, Raspberry Pi Pico and related devices, equipped with wireless connectivity (Pico W version) and dedicated security features, make it possible to deploy cryptography in modern IoT systems. Highly popular Raspberry Pi 5 is also used in some projects in the book where high performance cryptography is a requirement. Together, they all create a learning path that is both hands-on and directly relevant to today's embedded applications.

The aims of this book can be divided into three parts:

1. To introduce cryptographic concepts in a way that is intuitive and grounded in practical experimentation.
2. To demonstrate how these concepts can be implemented efficiently on popular microcontroller development systems and single board computers, with attention to real-world limitations and trade-offs.
3. To equip readers with the knowledge and skills necessary to design and build secure embedded systems, moving from classroom exercises or hobby projects toward professional applications.

The book is intended for a wide audience: students beginning their exploration of cryptography, hobbyists wanting to secure their personal projects, and engineers seeking a structured guide to embedded security. By the end of this book, readers will be able to move confidently from simple ciphers to the design of modern secure systems (e.g. the

AES), and gaining not only theoretical insight but also the practical experience of making cryptography work on the smallest of microcontroller development systems and single board computers.

Dogan Ibrahim
Ahmet Ibrahim
London, 2026