ELEKTORACADEMYPRO

Practical Microcontroller Cryptography

From Simple Ciphers to Secure Systems

Dogan Ibrahim & Ahmet Ibrahim

elektor MEDIA & LEARNING

Practical Microcontroller Cryptography

From Simple Ciphers to Secure Systems

Dogan Ibrahim
Ahmet Ibrahim

elektor
design › share › earn

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

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

www.elektor.com
Editor: Clemens Valens
Prepress Production: D-Vision, Julian van den Berg
Printers: Ipskamp, Enschede, The Netherlands

Contents

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