No. 130

CYBERSECURITY

Encryption Basics

How encryption, hashing and keys protect your data



oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 130

Encryption Basics

How encryption, hashing and keys protect your data

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Encryption Basics

How encryption, hashing and keys protect your data

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Product, protocol and company names mentioned in this book are trademarks of their respective owners. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 What encryption is 5
2 Goals of cryptography 6
3 Keys 7
4 A short history 8
5 Symmetric encryption 9
6 Asymmetric encryption 10
7 Hybrid encryption 11
8 Randomness 12
9 Encoding, encryption and hashing 13
10 Authenticated encryption 14

PART II · HASHES AND SIGNATURES

11 Hashing 16
12 Password storage 17
13 Message authentication codes 18
14 Digital signatures 19
15 Certificates 20
16 Public key infrastructure 21
17 Shorter certificate lifetimes 22
18 Code signing 23

PART III · ENCRYPTION IN PRACTICE

19 TLS 25
20 HTTPS 26
21 Where encryption is used 27
22 Encryption at rest 28
23 Encryption in the cloud 29

FREE SAMPLE · ojayo.com

24 End-to-end encryption 30
25 Email encryption 31
26 VPNs 32
27 Key management 33
28 Secrets management 34
29 Choosing algorithms 35

PART IV · THE FUTURE AND PRACTICE

30 Quantum computing and cryptography 37
31 Post-quantum cryptography 38
32 Crypto agility 39
33 Common mistakes 40
34 Law and policy 41
35 A worked example 42
36 Careers 43
37 A learning path 44
38 Summary 45
Checklists 46
Glossary 47
Further reading 48

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Encryption scrambles data so only people with the right key can read it. It protects your online banking, messages, passwords, cloud files and almost everything else on the internet, usually without you noticing.

This book explains encryption and related cryptography for beginners: symmetric and asymmetric encryption, hashing, password storage, digital signatures, certificates, TLS, key management and the coming move to post-quantum cryptography. It uses plain language and small, tested Python examples, and it covers current practice as of late 2026.

What this book covers

- What cryptography provides and the main building blocks.
- Symmetric, asymmetric and hybrid encryption.
- Hashing, password storage, MACs and signatures.
- Certificates, PKI, TLS and HTTPS.
- Encryption at rest, end-to-end encryption and key management.
- Common mistakes and post-quantum cryptography.

Who this book is for

- **Beginners** in IT and security.
- **Developers** who use cryptography libraries.
- **Managers** making decisions about data protection.

FREE SAMPLE · ojayo.com

How the book is organized

- **Part I — Foundations** (Chapters 1–10): what encryption is, goals, keys, history, symmetric and asymmetric encryption, hybrid encryption, randomness, encoding versus encryption, and authenticated encryption.
- **Part II — Hashes and signatures** (Chapters 11–18): hashing, password storage, MACs, signatures, certificates, PKI, certificate lifetimes and code signing.
- **Part III — Encryption in practice** (Chapters 19–29): TLS, HTTPS, data at rest, cloud, end-to-end messaging, email, VPNs, key management, secrets management and choosing algorithms.
- **Part IV — The future and practice** (Chapters 30–38): quantum computing, post-quantum cryptography, crypto agility, mistakes, law and policy, a worked example, careers and a learning path.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical advice you can use straight away.

IN PRACTICE
How an idea looks in real systems.

WATCH OUT
Common mistakes and risks.

KEY IDEA
The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on screens

Screens are **simplified illustrations**, not real browser or product screens.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters introduce the core ideas of encryption: keys, symmetric and asymmetric methods, and how they combine.

FREE SAMPLE · ojayo.com

CHAPTER 1

What encryption is

Encryption hides data from anyone without the key.

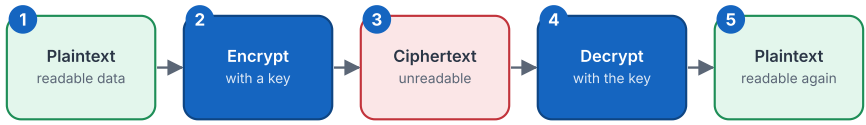


Figure 1.1 Encryption in one picture

The key matters most

Modern encryption algorithms are public; their security depends on keeping the **key** secret. This principle, known as Kerckhoffs's principle, means anyone can study an algorithm for weaknesses while data stays safe.

> **KEY IDEA**
> Use well-known, public algorithms and protect the keys.

FREE SAMPLE · ojayo.com

CHAPTER 2

Goals of cryptography

Cryptography does more than hide data.

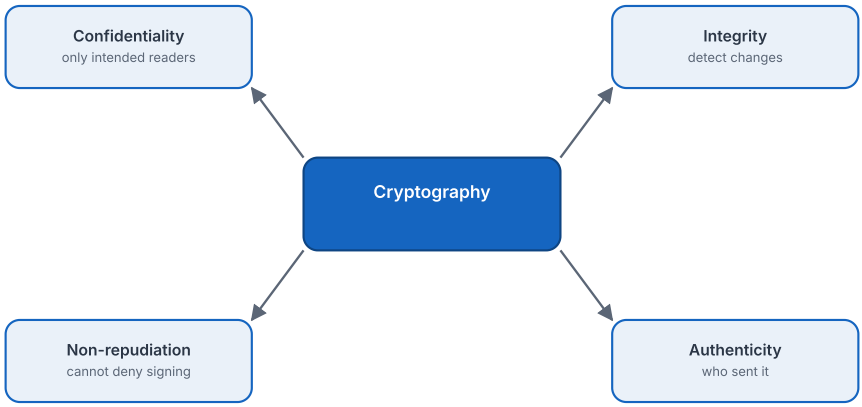


Figure 2.1 What cryptography provides

Different tools for different goals

Encryption gives confidentiality; hashes and MACs give integrity; signatures give authenticity and non-repudiation. Real systems combine them.

FREE SAMPLE · ojayo.com

CHAPTER 3

Keys

Keys are long random numbers.

A key is a long random value. A 128-bit key has about 3.4 x 10^38 possibilities, far too many to try by brute force with classical computers. Longer keys give more margin; 256-bit symmetric keys are common for long-term protection.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics (you are reading this)
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Encryption Basics

Enjoyed it? The full book has 53 pages and 38 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.