

SOEBIT Cybersecurity Cryptography Foundation (SCCF)

1 day edition
Course Overview



The Cryptography Foundation (SCCF) training course delivers a comprehensive and practical introduction to the principles, techniques, and real-world applications of classical and modern cryptography. This course covers widely used encryption algorithms and explores critical cryptographic infrastructures used in modern enterprises, including Public Key Infrastructure (PKI), digital certificates, certificate lifecycle management, cryptographic key management, and Hardware Security Modules (HSMs). Participants develop a strong foundation in how cryptography enables secure communication, protects sensitive information, and supports regulatory compliance. The course also addresses cryptographic risks, vulnerabilities, and common implementation failures that often lead to security breaches and compliance violations.

By the end of this program, learners gain the knowledge required to evaluate cryptographic implementations, support secure technology decisions, and strengthen organizational security posture.

Course agenda

- Introduction to Cryptography
- Classical and Modern Encryption Algorithms
- Cryptographic Risks and Common Failures
- Public Key Infrastructure (PKI) Fundamentals
- Digital Certificates and Certificate Lifecycle Management
- Cryptographic Key Management Concepts
- Hardware Security Module (HSM) Fundamentals



Why should you attend?

As organizations increasingly depend on encryption to protect data, communications, and critical infrastructure, cryptography has become a core security capability across both technical and leadership roles.

Poorly implemented or mismanaged cryptographic controls — such as weak key handling, expired certificates, and insecure configurations — frequently result in data breaches, service outages, regulatory penalties, and reputational damage. This course enables you to clearly understand how modern encryption systems operate, where they commonly fail, and how organizations can manage cryptographic risks effectively in real-world environments.

Who should attend?

This course is ideal for professionals across technical and non-technical roles, including:

- Students, beginners, and early-career professionals building a foundation in cybersecurity
- Managers and technical leads responsible for security strategy and risk decisions
- IT and information security professionals working with encryption, PKI, and secure communications
- System architects and engineers involved in secure system design
- Risk, audit, and compliance professionals assessing cryptographic controls
- Anyone responsible for protecting sensitive data and ensuring secure technology implementations

What You Will Learn

By completing this course, you will be able to:

- Understand fundamental concepts of classical and modern cryptography
- Explain how cryptography enables secure communication and data protection
- Apply practical knowledge of PKI, digital certificates, and trust models
- Understand certificate lifecycle management and cryptographic key management processes
- Identify weaknesses and vulnerabilities in cryptographic implementations
- Connect cryptographic controls with regulatory and compliance requirements

Key Skills Gained

- Cryptographic risk awareness
- Secure communication fundamentals
- PKI and certificate management understanding
- Key lifecycle management principles
- Enterprise HSM usage concepts
- Cryptography-driven compliance alignment

Career Benefits

After completing this course, you will be better prepared to:

- Support secure technology and architecture decisions
- Strengthen daily security operations
- Improve organizational cryptographic governance
- Reduce encryption-related security and compliance risks

Prerequisites

- No prior cryptography or security experience is required.
- This course is designed for beginners and professionals from diverse backgrounds.

