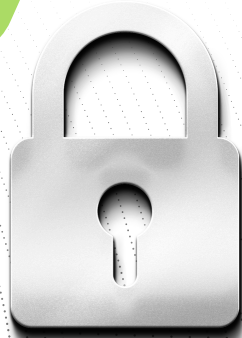


SOEBIT Cybersecurity Cryptography Foundation (SCCF)

2 days edition
Course Overview



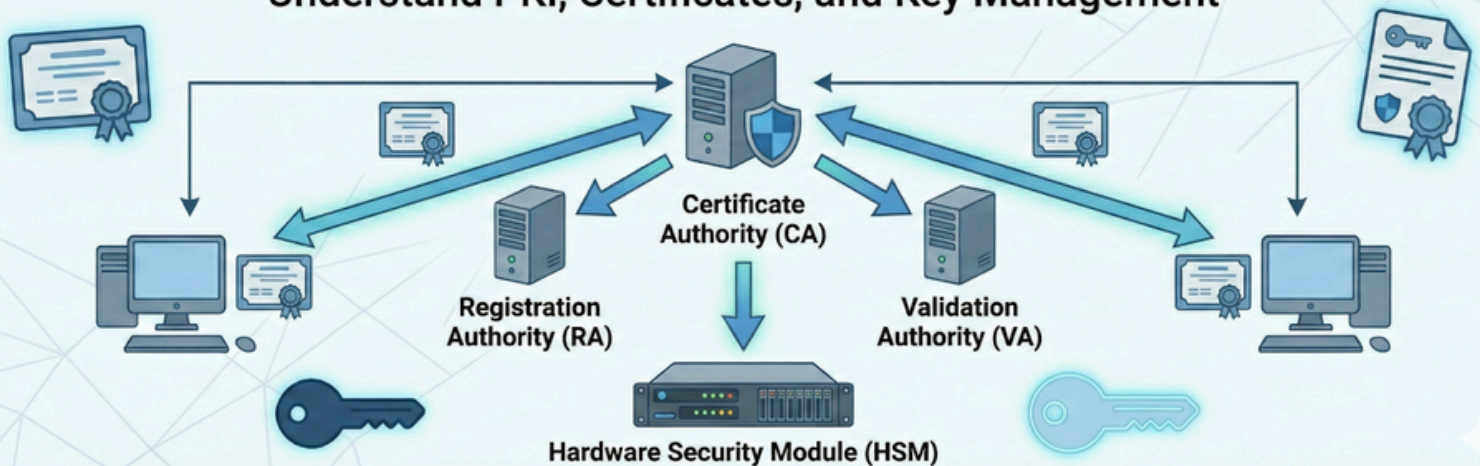
The Cryptography Foundation training course delivers a comprehensive and practical introduction to the principles, technologies, and real-world applications of cryptographic systems used across today's digital enterprises, while also building awareness of emerging shifts such as post-quantum cryptography. This course covers widely used encryption algorithms, secure communication mechanisms, and critical cryptographic infrastructures, including Public Key Infrastructure (PKI), digital certificates, certificate lifecycle management, cryptographic key management, and Hardware Security Modules (HSMs), as well as their use across on-premises and cloud environments.

Participants develop a strong foundation in how cryptography enables secure communication, establishes trust and identity, protects sensitive information throughout its lifecycle, and supports regulatory and compliance requirements. The course also examines cryptographic risks, threat scenarios, protocol weaknesses, governance challenges, and common implementation failures that frequently lead to security breaches, operational disruption, and compliance violations.

By the end of this program, learners gain a well-rounded understanding of how cryptographic controls are designed, implemented, managed, and evaluated in modern enterprise environments, enabling them to support informed security decisions and strengthen organizational cryptographic posture.

CRYPTOGRAPHY FOUNDATION

Understand PKI, Certificates, and Key Management



Why should you attend?

As organizations increasingly depend on encryption to protect data, communications, cloud services, and critical infrastructure, cryptography has become a core security capability across both technical and leadership roles. Cryptographic controls now underpin secure communications, digital identity, enterprise trust models, regulatory compliance, and emerging data protection requirements.

Poorly implemented or mismanaged cryptographic controls—such as weak key handling, expired certificates, insecure configurations, unclear ownership responsibilities, and fragmented governance—frequently result in data breaches, service outages, regulatory penalties, and reputational damage. This course enables you to clearly understand how cryptographic systems operate in real-world environments, where they commonly fail, and how organizations can manage cryptographic risks effectively while building awareness and readiness for post-quantum challenges in a rapidly evolving technology landscape.

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, cryptography, and digital trust
- Managers and technical leads responsible for security strategy, cryptographic governance, and risk decisions
- IT and information security professionals working with encryption, PKI, and secure communications
- System architects and engineers involved in secure system design, cloud architecture, and trust-based security models
- Risk, audit, and compliance professionals assessing cryptographic controls, regulatory alignment, data protection requirements, and emerging post-quantum considerations
- 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 cryptographic technologies used across classical, modern, and post-quantum cryptography.
- Explain how cryptography enables secure communication, digital trust, identity, and data protection
- Apply practical knowledge of PKI, digital certificates, trust models, and secure communication mechanisms
- Understand certificate lifecycle management and cryptographic key management processes
- Identify weaknesses, misconfigurations, and risks in cryptographic implementations across on-premises and cloud systems
- Understand governance, compliance, regulatory expectations, and emerging considerations such as post-quantum cryptography



Key Skills Gained

- Cryptographic risk awareness and threat understanding
- Secure communication and protocol fundamentals
- PKI, certificate, identity, and trust model understanding
- Cryptographic key lifecycle management principles
- Enterprise HSM and cloud-based cryptographic service usage concepts
- Awareness of post-quantum cryptography impacts and future cryptographic risks
- Cryptography-driven compliance alignment

Career Benefits

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

- Support secure technology and architecture decisions
- Strengthen daily operations related to cryptography, certificates, and key management
- Improve organizational cryptographic governance and compliance alignment
- Reduce encryption-related security and compliance risks
- Build awareness for future cryptographic challenges, including post-quantum considerations

Prerequisites

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

Course agenda

Day 1

- 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
- Practical Cryptographic Assessment Scenarios

Day 2

- Secure Communication Protocols
- Identity, Trust, and Digital Identity Foundations
- Introduction to Post-Quantum Cryptography (PQC)
- Cryptography in Modern Enterprise Architectures
- Cryptography in Cloud & Managed Security Services
- Modern Cryptographic Threats & Attack Scenarios
- Cryptography, Compliance & Regulations
- Course Wrap-Up & Key Takeaways



SOEBIT Cybersecurity Cryptography Foundation (SCCF)

