Cryptography and Data Encryption Fundamentals Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Cryptography and Data Encryption Fundamentals Training Course is engineered to equip professionals with the in-depth knowledge and Hands-on Skills required to implement robust defensive measures. As global regulations like GDPR Compliance and the looming threat of Quantum Computing intensify the need for advanced protection, understanding the bedrock of information security encryption is paramount. We bridge the gap between theoretical Cryptographic Algorithms and real-world application, focusing on critical areas such as Secure Key Management, End-to-End Encryption, and the principles of the Zero Trust Architecture.

This course delves into both Symmetric and Asymmetric Encryption techniques, providing a clear pathway to securing data at Rest and in Transit across complex, modern infrastructures including Cloud Environments. Participants will master protocols like TLS/SSL, understand Digital Signatures for Data Integrity, and explore cutting-edge trends like Post-Quantum Cryptography (PQC) and Homomorphic Encryption. By focusing on practical Vulnerability Analysis and proven Threat Mitigation strategies, this course ensures you can design, deploy, and audit Enterprise-level Data Protection solutions, safeguarding sensitive PII and achieving comprehensive Data Privacy.

Programme Curriculum

Cryptography and Data Encryption Fundamentals Training Course

Introduction

Cryptography and Data Encryption Fundamentals Training Course is engineered to equip professionals with the in-depth knowledge and Hands-on Skills required to implement robust defensive measures. As global regulations like GDPR Compliance and the looming threat of Quantum Computing intensify the need for advanced protection, understanding the bedrock of information security encryption is paramount. We bridge the

gap between theoretical Cryptographic Algorithms and real-world application, focusing on critical areas such as Secure Key Management, End-to-End Encryption, and the principles of the Zero Trust Architecture.

This course delves into both Symmetric and Asymmetric Encryption techniques, providing a clear pathway to securing data at Rest and in Transit across complex, modern infrastructures including Cloud Environments. Participants will master protocols like TLS/SSL, understand Digital Signatures for Data Integrity, and explore cutting-edge trends like Post-Quantum Cryptography (PQC) and Homomorphic Encryption. By focusing on practical Vulnerability Analysis and proven Threat Mitigation strategies, this course ensures you can design, deploy, and audit Enterprise-level Data Protection solutions, safeguarding sensitive PII and achieving comprehensive Data Privacy.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Differentiate between Symmetric and Asymmetric Cryptography and their optimal use cases.
2. Implement industry-leading Advanced Encryption Standard for Data at Rest.
3. Apply and troubleshoot Transport Layer Security protocols for Data in Transit.
4. Master best practices for Cryptographic Key Management including rotation and storage using HSMs.
5. Analyze vulnerabilities and enforce Crypto-Agility in existing IT infrastructure.
6. Explain the foundational mathematics behind Elliptic Curve Cryptography (ECC) and RSA.
7. Design End-to-End Encryption systems for secure messaging and cloud applications.
8. Utilize Hashing Algorithms and Digital Signatures to ensure Data Integrity and Non-Repudiation.
9. Assess the impact of Quantum Computing and strategize for Post-Quantum Cryptography (PQC) migration.
10. Integrate encryption solutions to meet GDPR, HIPAA, and PCI DSS Compliance requirements.
11. Explore the application of Homomorphic Encryption for Privacy-Preserving Computation.
12. Conduct a basic Cryptographic Audit and Vulnerability Analysis of a system.
13. Implement Zero Trust principles using robust Multi-Factor Authentication (MFA) and encryption.

Target Audience

1. Cybersecurity Analysts and Security Engineers
2. IT/Network Administrators responsible for security infrastructure
3. Software Developers and Architects building secure applications
4. Data Protection Officers (DPOs) and Compliance Managers
5. Cloud Security Professionals managing data in AWS, Azure, or GCP
6. Information Security (InfoSec) Consultants and Auditors
7. System Administrators and DevOps Engineers
8. Technical Managers needing a deep understanding of Data Privacy solutions

Course Modules

Module 1: Cryptographic Foundations and Primitives

- The three pillars of security.
- Understanding Symmetric Ciphers.
- Introduction to Asymmetric Cryptography and Public Key Infrastructure

- The role of Hash Functions in digital security and Data Integrity.
- Case Study: The WannaCry Ransomware attack and its dependency on flawed encryption/key management, demonstrating the catastrophic failure of poor system-wide cryptography.

Module 2: Symmetric and Asymmetric Algorithms in Depth

- Detailed analysis of the Advanced Encryption Standard.
- The mathematics and security of RSA
- Understanding Elliptic Curve Cryptography for performance and mobile security.
- The Diffie-Hellman and Elliptic Curve Diffie-Hellman key exchange protocols.
- Case Study: Target?ÇÖs 2013 Data Breach, exploring how the lack of proper network segmentation and point-of-sale data encryption exposed millions of customer records.

Module 3: Key Management and Public Key Infrastructure

- Best practices for Secure Key Generation, Distribution, and Rotation.
- Implementing Hardware Security Modules for root of trust.
- Designing and maintaining a robust PKI including CAs, certificates, and revocation.
- Managing keys in Cloud Environments
- Case Study: The Equifax Breach, focusing on how the failure to patch a known TLS/SSL vulnerability led to massive data exfiltration.

Module 4: Secure Communications and Network Protocols

- In-depth look at TLS/SSL Handshake Process and protocol versions
- Configuration of secure VPNs using IPsec and TLS-based VPNs.
- Implementing End-to-End Encryption for messaging and email.
- Securing DNS queries using DNS-over-HTTPS and DNS-over-TLS
- Case Study: Analyzing the Heartbleed Vulnerability, a critical flaw in OpenSSL that compromised private keys and sensitive data across the internet.

Module 5: Data Integrity, Authentication, and Non-Repudiation

- Using Message Authentication Codes and HMACs.
- Creating and verifying Digital Signatures for document and software authentication.
- Understanding the role of Hashing in password storage and file integrity verification.
- Implementing Digital Certificates for device and user authentication.
- Case Study: A Software Supply Chain Attack, detailing how compromised or stolen digital signatures were used to distribute malicious code undetected.

Module 6: Advanced and Emerging Cryptographic Concepts

- The threat of Shor?ÇÖs and Grover?ÇÖs Algorithms on current public-key cryptography.
- Introduction to Post-Quantum Cryptography and NIST PQC Standardization.
- Exploring Homomorphic Encryption for computation on encrypted data.
- Basics of Zero-Knowledge Proofs and their applications in blockchain and privacy.
- Case Study: Microsoft?ÇÖs PQC Roadmap and Migration Strategy, showcasing a large enterprise's planned transition to Quantum-Safe Algorithms like CRYSTALS-Dilithium and CRYSTALS-Kyber.

Module 7: Data Protection and Compliance Frameworks

- Mapping encryption techniques to meet GDPR

- PCI DSS requirements for encrypting Cardholder Data at rest and in transit.
- HIPAA security rules for protecting Electronic Protected Health Information.
- Designing an encryption strategy for a Zero Trust security model.
- Case Study: The Capital One Cloud Breach, emphasizing the importance of correctly configuring cloud data encryption services and access controls to maintain compliance.

Module 8: Cryptography Implementation and Auditing

- Practical implementation of file and disk encryption tools
- Performing a Cryptographic Audit to identify weak algorithms or key length deficiencies.
- Setting up and managing encrypted volumes and containers on-premises and in the cloud.
- Developing an incident response plan for a Key Compromise scenario.
- Case Study: A successful implementation of End-to-End Encryption by a global messaging platform, discussing the technical challenges and security benefits of E2EE on a massive scale.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com