Faysal Aziz

Cryptography and Security

Knights of the cyber-world

FA-0145

Cybersecurity

Introduction

Course Title: Cryptography for Computing and Security

Introduction

This is an **exploratory one-day or comprehensive two-day** workshop designed to demystify the complex world of cryptography and hardware security modules (HSM). In today's digital era, the importance of securing information cannot be overstated. As cyber threats evolve, understanding the principles of cryptography and the role of HSMs in safeguarding data is crucial for anyone involved in computing and security.

This course is tailored to provide you with a solid foundation in the concepts, mathematics*, and applications of cryptography, along with an in-depth* exploration of HSM technology. Whether you're a developer, a security professional, or just a tech enthusiast, this training will arm you with the knowledge and skills to enhance your cybersecurity measures.

Learning outcomes

By the end of this workshop, participants will be able to:

- Understand the fundamental concepts and terminologies of cryptography.
- Identify different types of cryptographic algorithms and their applications.
- Grasp the basic mathematical principles underlying cryptographic algorithms.*
- Comprehend the significance of key management and cryptographic protocols.
- Gain insights into symmetric and asymmetric encryption methods.
- Understand the role and functionality of HSMs in securing cryptographic keys and managing digital identities.

- Apply cryptographic principles to real-world scenarios for enhancing data security.*

Prerequisites

Participants are expected to have:

- Basic understanding of computing principles.
- Familiarity with general concepts of digital security.
- Comfort with mathematical reasoning.

Training outline

1. Introduction to Cryptography

Overview of Cryptography

1. Definition and significance in digital security
2. Historical perspective

Terminologies and Concepts

1. Plain text, cipher text, encryption, decryption
2. Key, algorithm, protocol

Purpose and Applications

1. Confidentiality, integrity, authentication, non-repudiation
2. Applications in digital communications, e-commerce, digital signatures

2. Types of Cryptographic Systems

Symmetric-Key Cryptography

1. Concept and operation
2. Block ciphers vs. stream ciphers
3. Examples: AES, DES

Asymmetric-Key Cryptography

1. Concept and operation
2. Public and private keys
3. Examples: RSA, ECC

Hash Functions

1. Concept and application
2. Properties of cryptographic hash functions

3. Examples: SHA-256, MD5 (discussion on vulnerabilities)

3. Mathematical Foundations of Cryptography*

Basic Mathematical Concepts

1. Modular arithmetic, prime numbers, greatest common divisor

Principles Underlying Asymmetric Cryptography

1. Finite fields and elliptic curves

Introduction to Cryptanalysis

1. Basic techniques and historical examples
2. The significance of computational hardness

4. Key Management and Cryptographic Protocols

Key Lifecycle Management

1. Generation, distribution, storage, rotation, and destruction

Public Key Infrastructure (PKI)

1. Certificates and certificate authorities
2. Digital signatures

Cryptographic Protocols

1. Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
2. Secure Shell (SSH)
3. Blockchain basics and cryptographic applications

5. Introduction to Hardware Security Modules (HSM)

Role of HSM in Cryptography

1. Definition and importance
2. Physical and logical security features

Types of HSMs

1. USB, PCI, network-attached

Use Cases and Applications

1. Key generation and storage
2. Digital signing and encryption
3. Payment systems and digital identities

6. Implementing Cryptography with HSM*

Integrating HSMs into IT Infrastructure

1. Compatibility and interoperability
2. Best practices for deployment and management

HSM Configuration and Operation

1. Initial setup, backup, and recovery
2. Performance optimization

Security Considerations and Compliance

1. Regulatory standards and compliance (e.g., FIPS 140-2, PCI DSS)
2. Auditing and logging

7. Practical Applications and Case Studies*

Real-World Cryptography

1. Encrypting a database
2. Secure communication protocols

HSM in Action

1. Case studies of HSM deployment
2. Lessons learned and best practices

8. Closing Session*

Review and Q&A

1. Recap of key concepts
2. Open floor for questions and discussion

Next Steps and Resources

1. Further learning resources
2. Communities and forums for ongoing support

*Items marked with an asterisk are only available for the 2-day comprehensive fundamental course.

© 2026 Faysal Aziz · Kuala Lumpur