uCertify

Course Outline

Cryptography And Network Security

19 May 2024

1. Course Objective
2. Pre-Assessment
3. Exercises, Quizzes, Flashcards & Glossary

   Number of Questions
4. Expert Instructor-Led Training
5. ADA Compliant & JAWS Compatible Platform
6. State of the Art Educator Tools
7. Award Winning Learning Platform (LMS)
8. Chapter & Lessons

   Syllabus

   Chapter 1: Information and Network Security Concepts

   Chapter 2: Introduction to Number Theory

   Chapter 3: Classical Encryption Techniques

   Chapter 4: Block Ciphers and the Data Encryption Standard

   Chapter 5: Finite Fields

   Chapter 6: Advanced Encryption Standard

   Chapter 7: Block Cipher Operation

   Chapter 8: Random Bit Generation and Stream Ciphers

   Chapter 9: Public-Key Cryptography and RSA

   Chapter 10: Other Public-Key Cryptosystems

   Chapter 11: Cryptographic Hash Functions

   Chapter 12: Message Authentication Codes

   Chapter 13: Digital Signatures

   Chapter 14: Lightweight Cryptography and Post-Quantum Cryptography

   Chapter 15: Cryptographic Key Management and Distribution

   Chapter 16: User Authentication

   Chapter 17: Transport-Level Security

   Chapter 18: Wireless Network Security

1. Course Objective

The Cryptography And Network Security course helps you explore the history and evolution of cryptographic techniques, including symmetric-key and public-key algorithms, hash functions, and digital signatures. The course delves into the mechanisms for secure communication over computer networks, including authentication, access control, and secure protocols such as SSL/TLS and IPsec. Additionally, you will gain an understanding of network security threats, including malware, denial-of-service attacks, and intrusion detection/prevention systems.

2. Pre-Assessment

Pre-Assessment lets you identify the areas for improvement before you start your prep. It determines what students know about a topic before it is taught and identifies areas for improvement with question assessment before beginning the course.

3. Quiz

Quizzes test your knowledge on the topics of the exam when you go through the course material. There is no limit to the number of times you can attempt it.

4. flashcards

Flashcards are effective memory-aiding tools that help you learn complex topics easily. The flashcard will help you in memorizing definitions, terminologies, key concepts, and more. There is no limit to the number of times learners can attempt these. Flashcards help master the key concepts.

5. Glossary of terms

uCertify provides detailed explanations of concepts relevant to the course through Glossary. It contains a list of frequently used terminologies along with its detailed explanation. Glossary defines the key terms.

6. Expert Instructor-Led Training

uCertify uses the content from the finest publishers and only the IT industry's finest instructors. They have a minimum of 15 years real-world experience and are subject matter experts in their fields. Unlike a live class, you can study at your own pace. This creates a personal learning experience and gives you all the benefit of hands-on training with the flexibility of doing it around your schedule 24/7.

7. ADA Compliant & JAWS Compatible Platform

uCertify course and labs are ADA (Americans with Disability Act) compliant. It is now more accessible to students with features such as:

- Change the font, size, and color of the content of the course
- Text-to-speech, reads the text into spoken words
- Interactive videos, how-tos videos come with transcripts and voice-over
- Interactive transcripts, each word is clickable. Students can clip a specific part of the video by clicking on a word or a portion of the text.

JAWS (Job Access with Speech) is a computer screen reader program for Microsoft Windows that reads the screen either with a text-to-speech output or by a Refreshable Braille display. Student can easily navigate uCertify course using JAWS shortcut keys.

8. State of the Art Educator Tools

uCertify knows the importance of instructors and provide tools to help them do their job effectively. Instructors are able to clone and customize course. Do ability grouping. Create sections. Design grade scale and grade formula. Create and schedule assessments. Educators can also move a student from self-paced to mentor-guided to instructor-led mode in three clicks.

9. Award Winning Learning Platform (LMS)

uCertify has developed an award winning, highly interactive yet simple to use platform. The SIIA CODiE Awards is the only peer-reviewed program to showcase business and education technology's finest products and services. Since 1986, thousands of products, services and solutions have been recognized for achieving excellence. uCertify has won CODiE awards consecutively for last 7 years:

- **2014**
    1. Best Postsecondary Learning Solution

- **2015**
    1. Best Education Solution

2. Best Virtual Learning Solution
3. Best Student Assessment Solution
4. Best Postsecondary Learning Solution
5. Best Career and Workforce Readiness Solution
6. Best Instructional Solution in Other Curriculum Areas
7. Best Corporate Learning/Workforce Development Solution

- **2016**
    1. Best Virtual Learning Solution
    2. Best Education Cloud-based Solution
    3. Best College and Career Readiness Solution
    4. Best Corporate / Workforce Learning Solution
    5. Best Postsecondary Learning Content Solution
    6. Best Postsecondary LMS or Learning Platform
    7. Best Learning Relationship Management Solution

- **2017**
    1. Best Overall Education Solution
    2. Best Student Assessment Solution
    3. Best Corporate/Workforce Learning Solution
    4. Best Higher Education LMS or Learning Platform

- **2018**
    1. Best Higher Education LMS or Learning Platform
    2. Best Instructional Solution in Other Curriculum Areas
    3. Best Learning Relationship Management Solution

- **2019**
    1. Best Virtual Learning Solution
    2. Best Content Authoring Development or Curation Solution
    3. Best Higher Education Learning Management Solution (LMS)

- **2020**

1. Best College and Career Readiness Solution
2. Best Cross-Curricular Solution
3. Best Virtual Learning Solution

10. Chapter & Lessons

uCertify brings these textbooks to life. It is full of interactive activities that keeps the learner engaged. uCertify brings all available learning resources for a topic in one place so that the learner can efficiently learn without going to multiple places. Challenge questions are also embedded in the chapters so learners can attempt those while they are learning about that particular topic. This helps them grasp the concepts better because they can go over it again right away which improves learning.

Learners can do Flashcards, Exercises, Quizzes and Labs related to each chapter. At the end of every lesson, uCertify courses guide the learners on the path they should follow.

Syllabus

Chapter 1: Information and Network Security Concepts

- Cybersecurity, Information Security, and Network Security
- The OSI Security Architecture
- Security Attacks
- Security Services
- Security Mechanisms
- Cryptography
- Network Security

- Trust and Trustworthiness
- Standards

Chapter 2: Introduction to Number Theory

- Divisibility and The Division Algorithm
- The Euclidean Algorithm
- Modular Arithmetic
- Prime Numbers4
- Fermat’s and Euler’s Theorems
- Testing for Primality
- The Chinese Remainder Theorem
- Discrete Logarithms
- Appendix 2A: The Meaning of Mod

Chapter 3: Classical Encryption Techniques

- Symmetric Cipher Model
- Substitution Techniques
- Transposition Techniques

Chapter 4: Block Ciphers and the Data Encryption Standard

- Traditional Block Cipher Structure
- The Data Encryption Standard
- A DES Example
- The Strength of DES
- Block Cipher Design Principles

Chapter 5: Finite Fields

- Groups
- Rings
- Fields
- Finite Fields of the Form GF(p)
- Polynomial Arithmetic
- Finite Fields of the Form GF (2n)

Chapter 6: Advanced Encryption Standard

- Finite Field Arithmetic
- AES Structure

- AES Transformation Functions
- AES Key Expansion
- An AES Example
- AES Implementation
- Appendix 6A: Polynomials with Coefficients in GF(28)

Chapter 7: Block Cipher Operation

- Multiple Encryption and Triple DES
- Electronic CodeBook
- Cipher Block Chaining Mode
- Cipher Feedback Mode
- Output Feedback Mode
- Counter Mode
- XTS-AES Mode for Block-Oriented Storage Devices
- Format-Preserving Encryption

Chapter 8: Random Bit Generation and Stream Ciphers

- Principles of Pseudorandom Number Generation
- Pseudorandom Number Generators

- Pseudorandom Number Generation Using a Block Cipher
- Stream Ciphers
- RC4
- Stream Ciphers Using Feedback Shift Registers
- True Random Number Generators

Chapter 9: Public-Key Cryptography and RSA

- Principles of Public-Key Cryptosystems
- The RSA Algorithm

Chapter 10: Other Public-Key Cryptosystems

- Diffie–Hellman Key Exchange
- Elgamal Cryptographic System
- Elliptic Curve Arithmetic
- Elliptic Curve Cryptography

Chapter 11: Cryptographic Hash Functions

- Applications of Cryptographic Hash Functions
- Two Simple Hash Functions

- Requirements and Security
- Secure Hash Algorithm (SHA)
- SHA-3

Chapter 12: Message Authentication Codes

- Message Authentication Requirements
- Message Authentication Functions
- Requirements for Message Authentication Codes
- Security of MACs
- MACs Based on Hash Functions: HMAC
- MACs Based on Block Ciphers: DAA and CMAC
- Authenticated Encryption: CCM and GCM
- Key Wrapping
- Pseudorandom Number Generation Using Hash Functions and MACs

Chapter 13: Digital Signatures

- Digital Signatures
- Elgamal Digital Signature Scheme

- Schnorr Digital Signature Scheme
- Nist Digital Signature Algorithm
- Elliptic Curve Digital Signature Algorithm
- RSA-PSS Digital Signature Algorithm

Chapter 14: Lightweight Cryptography and Post-Quantum Cryptography

- Lightweight Cryptography Concepts
- Lightweight Cryptographic Algorithms
- Post-Quantum Cryptography Concepts
- Post-Quantum Cryptographic Algorithms

Chapter 15: Cryptographic Key Management and Distribution

- Symmetric Key Distribution Using Symmetric Encryption
- Symmetric Key Distribution Using Asymmetric Encryption
- Distribution of Public Keys
- X.509 Certificates
- Public-Key Infrastructure

Chapter 16: User Authentication

- Remote User-Authentication Principles
- Remote User-Authentication Using Symmetric Encryption
- Kerberos
- Remote User-Authentication Using Asymmetric Encryption
- Federated Identity Management

Chapter 17: Transport-Level Security

- Web Security Considerations
- Transport Layer Security
- HTTPS
- Secure Shell (SSH)

Chapter 18: Wireless Network Security

- Wireless Security
- Mobile Device Security
- IEEE 802.11 Wireless LAN Overview
- IEEE 802.11i Wireless LAN Security

Chapter 19: Electronic Mail Security

- Internet Mail Architecture
- Email Formats
- Email Threats and Comprehensive Email Security
- S/MIME
- DNSSEC
- DNS-Based Authentication of Named Entities
- Sender Policy Framework
- Domainkeys Identified Mail
- Domain-Based Message Authentication, Reporting, and Conformance

Chapter 20: IP Security

- IP Security Overview
- IP Security Policy
- Encapsulating Security Payload
- Combining Security Associations
- Internet Key Exchange

Chapter 21: Network Endpoint Security

- Firewalls

- Intrusion Detection Systems
- Malicious Software
- Distributed Denial of Service Attacks

Chapter 22: Cloud Security

- Cloud Computing
- Cloud Security Concepts
- Cloud Security Risks and Countermeasures
- Cloud Security as a Service
- An Open-Source Cloud Security Module

Chapter 23: Internet of Things (IoT) Security

- The Internet of Things
- IoT Security Concepts and Objectives
- An Open-Source IoT Security Module

Chapter 24: Appendix A: Basic Concepts from Linear Algebra

- A.1 Operations on Vectors and Matrices
- A.2 Linear Algebra Operations Over Zn

Chapter 25: Appendix B: Measures of Secrecy and Security

- B.1 Conditional Probability
- B.2 Perfect Secrecy
- B.3 Information and Entropy
- B.4 Entropy and Secrecy
- B.5 Min-Entropy

Chapter 26: Appendix C: Data Encryption Standard

Chapter 27: Appendix D: Simplified AES

- D.1 Overview
- D.2 S-AES Encryption and Decryption
- D.3 Key Expansion
- D.4 The S-box
- D.5 S-AES Structure

Chapter 28: Appendix E: Mathematical Basis of the Birthday Attack

- E.1 Related Problem

- E.2 The Birthday Paradox
- E.3 Useful Inequality
- E.4 The General Case of Duplications
- E.5 Overlap Between Two Sets

11. Practice Test

Here's what you get

60	2	60
PRE-ASSESSMENTS QUESTIONS	FULL LENGTH TESTS	POST-ASSESSMENTS QUESTIONS

Features

Each question comes with detailed remediation explaining not only why an answer option is correct but also why it is incorrect.

Unlimited Practice

Each test can be taken unlimited number of times until the learner feels they are prepared. Learner can review the test and read detailed remediation. Detailed test history is also available.

Each test set comes with learn, test and review modes. In learn mode, learners will attempt a question and will get immediate feedback and complete remediation as they move on to the next question. In test mode, learners can take a timed test simulating the actual exam conditions. In review mode,

learners can read through one item at a time without attempting it.

12.  Virtual Lab

The benefits of live-labs are:

- Exam based practical tasks
- Real equipment, absolutely no simulations
- Access to the latest industry technologies
- Available anytime, anywhere on any device
- Break and Reset functionality
- No hardware costs

Lab Tasks

Information and Network Security Concepts

- Obtaining Information about an IP Version
- Getting Information about the DNS
- Getting Information about the UDP Ports
- Getting Information about the Current Connection Statistics of UDP
- Getting the UDP Settings
- Getting Information about the TCP Ports
- Getting Information about the Current Connection Statistics of TCP
- Getting the TCP Settings
- Obtaining Information about the Net Firewall Profile
- Obtaining IP Route Information from the IP Routing Table

Classical Encryption Techniques

- Using OWASP ZAP

- Performing Symmetric Encryption

Advanced Encryption Standard

- Encrypting a File or Folder
- Configuring File and Share Permissions
- Using BitLocker in Windows 10
- Configuring MDT
- Creating a New Partition and Configuring BitLocker
- Implementing AES Encryption

Public-Key Cryptography and RSA

- Using OpenSSL to Create a Public/Private Key Pair
- Using the RSA Asymmetric Algorithm

Cryptographic Hash Functions

- Installing Windows Server Backup and Performing Backup of a Folder
- Creating a Backup Schedule
- Creating a Backup Once
- Configuring RAID
- Configuring RAID 5
- Installing the Failover Cluster Feature
- Using the Dependency Viewer

Cryptographic Key Management and Distribution

- Using Steganography
- Enabling a Keylogger in a Target Machine

IP Security

- Adding Revision to the Revision History
- Viewing and Downloading the Policy Templates
- Opening the Policy Template and Setting the Company Name
- Reviewing and Modifying the Policy Items

Here's what you get

33	32	44
VIRTUAL LAB		

13. Post-Assessment

After completion of the uCertify course Post-Assessments are given to students and often used in conjunction with a Pre-Assessment to measure their achievement and the effectiveness of the exam.

GET IN TOUCH:

3187 Independence Drive
Livermore, CA 94551,
United States

+1-415-763-6300

support@ucertify.com

www.ucertify.com