uCertify

# Course Outline

## Cryptography and Network Security: Techniques and Tools


24 May 2025

1. Exercises, Quizzes, Flashcards & Glossary

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

   Syllabus

   Chapter 1: Preface

   Chapter 2: An Overview of Network and Information Security

   Chapter 3: Introduction to Cryptography

   Chapter 4: Block Ciphers and Attacks

   Chapter 5: Number Theory Fundamentals

   Chapter 6: Algebraic Structures

   Chapter 7: Stream Ciphers and Cipher Modes

   Chapter 8: Secure Hash Functions

   Chapter 9: Message Authentication using MAC

   Chapter 10: Authentication and Message Integrity Using Digital Signatures

   Chapter 11: Advanced Encryption Standard

   Chapter 12: Pseudo-Random Numbers

   Chapter 13: Public Key Algorithms and RSA

   Chapter 14: Other Public Key Algorithms

   Chapter 15: Key Management and Exchange

   Chapter 16: User Authentication Using Kerberos

   Chapter 17: User Authentication Using Public Key Certificates

   Chapter 18: Email Security: PGP and SMIME

   Chapter 19: Transport Layer Security (TLS) and SSL

   Chapter 20: IP Security (IPsec)

Chapter 21: Wireless Security

Videos and How To

## 1. 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.


## 2. 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.


## 3. 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.

## 4.  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.

## 5.  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.

## 6.  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

## 7. 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: Preface

### Chapter 2: An Overview of Network and Information Security

- Introduction
- Why security is complex
- Security goals
- Different views on security
- Information security
- The relevance of security measures in the modern era

- Threats to information
- The security architecture
- The network security model
- Security service requirements
- Prerequisites to the application of security service
- Recapitulation
- Exercises

## Chapter 3: Introduction to Cryptography

- Introduction
- Difference between classic and modern ciphers
- Kerckhoffs’s principle
- Ingredients to a symmetric cipher
- Cryptography
- The Conventional Security Model
- Substitution and transposition
- Monoalphabetic substitution cipher
- Playfair cipher
- Hill cipher

- Vigenere cipher
- Vernam cipher and Onetime pads
- Transposition cipher
- Substitution cipher and S-box
- Transposition cipher and P-box
- Rotor Machines
- Recapitulation
- Exercises

## Chapter 4: Block Ciphers and Attacks

- Introduction
- Cryptographic systems
- Symmetric key algorithms
- Block ciphers
- Attacks
- Points to remember
- Excercises

## Chapter 5: Number Theory Fundamentals

- Divisibility
- Prime numbers
- Greatest common divisor
- Congruences
- Fermat’s little theorem and Euler’s theorem
- Generating large primes: primality tests
- Modular exponentiation (Exponentiation modular arithmetic)
- Discrete logarithms
- Additional reading
- Recommended reading/references
- Recapitulation
- Exercises

## Chapter 6: Algebraic Structures

- Algebraic structure
- Groups
- Algebraic systems with two binary operations
- Algebraic operations on polynomials

- Galois Field GF(pn)
- Recapitulation
- Exercises

## Chapter 7: Stream Ciphers and Cipher Modes

- Introduction
- Cypher feedback mode
- Output Feedback Mode
- Counter Mode
- IEEE XTS-AES mode
- IEEE XTS encryption process
- Recapitulation
- Exercises

## Chapter 8: Secure Hash Functions

- Introduction
- A simple hash function
- Secure hash functions using block ciphers and CBC
- Why a unique hash value is possible

- Applying a hash function for authentication
- Characteristics of the cryptographic hash function
- Security requirements attacks and countermeasures
- Folding
- Why simple folding fails
- Secure Hash Algorithm (SHA)
- Processing of each round
- The round function Rf ()
- Avalanche effect with SHA-512
- SHA-3
- Iteration function Keccak-f
- Theta Step function
- Rho step function
- Pi step function
- Chi step function
- Iota step function
- Applications of Cryptographic Hash Functions
- Recapitulatin

- Exercises

## Chapter 9: Message Authentication using MAC

- Introduction
- Integrity check
- Other security needs for a message
- Meet in the middle attack
- Factors deciding the security of MAC
- Order of encryption and authentication
- HMAC
- Conventional message digest vs. HMAC
- Authenticated Encryption with Associated Data (AEAD)
- Counter with Cipher Block Chaining Message Authentication Code (CCM)
- GCM-GMAC (Galois Counter Mode-Galois Counter Message Authentication Code)
- Key wrapping (KW)
- Recapitulation
- Exercises

## Chapter 10: Authentication and Message Integrity Using Digital Signatures

- Introduction
- What is a digital signature
- Attacks on DS
- Why a digital signature
- Different DS schemes
- Improving the process of digital signature
- Recapitulation
- Exercises

## Chapter 11: Advanced Encryption Standard

- Introduction
- AES characteristics
- Prerequisites to AES
- AES architecture
- AES processing
- Substitute byte matrix generation
- Key expansion process
- Inverse operations
- Implementation and motivation

- Recapitulation
- Exercises

## Chapter 12: Pseudo-Random Numbers

- Introduction
- PRN, TRN, and PRF
- PRN for solving security problems
- Pseudo random number generators (PRNGs)
- Using a cipher-based PRNG
- Real-world PRNGs
- True Random Numbers (TRNs)
- Other methods
- Recapitulation
- Exercises

## Chapter 13: Public Key Algorithms and RSA

- Introduction
- The need for public-key systems
- How it works

- The prerequisites to understand RSA
- RSA and processing in RSA
- Improving efficiency
- Cryptanalysis and attacks on RSA
- Countermeasures
- Difference: symmetric and asymmetric encryption
- Recapitulation
- Exercises

## Chapter 14: Other Public Key Algorithms

- Introduction
- Introduction to Elliptic Curves
- Elliptic curve cryptography
- Recapitulation
- Exercises

## Chapter 15: Key Management and Exchange

- Introduction
- Key management

- Need for key management
- Encryption location
- The public key distribution
- Randomness and unpredictability of keys
- Symmetric key exchange for authentication
- Public key exchange using certificates
- Recapitulation
- Exercises

## Chapter 16: User Authentication Using Kerberos

- Introduction
- The authentication process in Kerberos
- Kerberos protocol overview
- The challenges and solutions in building a protocol
- Multiple Kerberos realms
- Kerberos version V protocol
- Kerberos limitations
- Recapitulation

- Exercises

## Chapter 17: User Authentication Using Public Key Certificates

- Introduction
- Using public-key cryptography for authentication
- X.509 certificate structure
- Authentication procedures
- Extensions in version 3
- Public key infrastructure
- Certificate Management Protocol
- XML key management protocol
- Recapitulation
- Exercises

## Chapter 18: Email Security: PGP and SMIME

- Introduction
- PGP (Pretty good privacy)
- PGP goals
- The reasons behind the success

- PGP services
- SMIME functionality
- Recapitulation
- Exercises

## Chapter 19: Transport Layer Security (TLS) and SSL

- Introduction
- Need for securing web transactions
- Different ways to secure web traffic
- TLS and SSL
- Connections and sessions
- TLS record protocol
- TLS handshake protocol
- Cryptographic computations
- Recapitulation
- Exercises

## Chapter 20: IP Security (IPsec)

- Introduction

- Need
- IPsec functionality
- Using IPsec
- IPsec functioning
- IPsec benefits
- IPsec components
- Why IKE
- IPsec services
- IPsec transport and tunnel modes
- Deploying the security policy
- Traffic processing
- Encapsulating Security Payload (ESP)
- ESP header design
- Encryption and ICV calculation
- Combining SAs
- Recapitulation
- Exercises

## Chapter 21: Wireless Security

- Introduction
- A brief about 802.11
- Why wireless devices need higher security
- Introduction 802.11i
- Security services in Wi-Fi (802.11i)
- 802.11i phases of operation
- Discovery
- Authentication phase
- Key management
- Secure data transfer
- WPA3
- Wireless security for mobile phones
- Recapitulation
- Exercises